

Organizations, Governance, and Management in the Manufacturing Industry

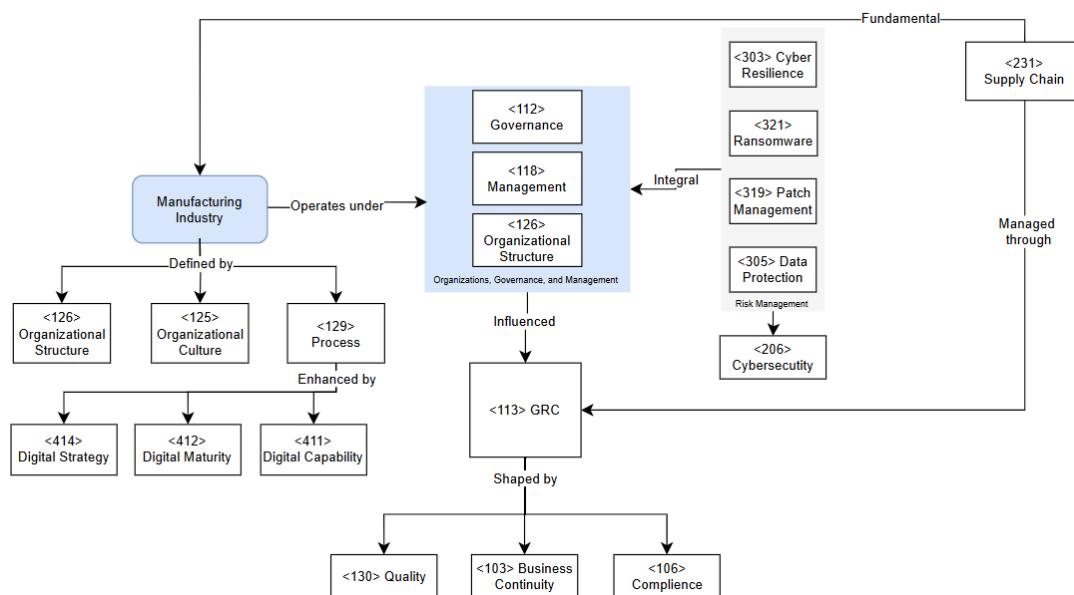
Manufacturing is defined as the process of transforming raw materials into finished goods through labour, machinery, and processing techniques. It is a key economic sector, characterised by high precision, capital intensity, and complex global supply chains.

The manufacturing industry operates within complex organizational structures that combine technical systems with social dynamics. As a capital-intensive sector, it requires clear governance models to ensure alignment between strategic goals, operational efficiency, and regulatory compliance. Organizations in this industry typically span multiple sites, involve diverse stakeholders, and rely on structured coordination between engineering, production, and IT teams.

Governance in manufacturing focuses on setting direction, ensuring accountability, and managing risk across the value chain. This includes compliance with international standards as well as frameworks for cybersecurity and industrial control systems. Boards and senior executives play a critical role in defining governance policies that balance performance with resilience and long-term value.

Effective management in manufacturing involves translating governance priorities into operational routines through structured management systems. Techniques such as Lean, Six Sigma, and Just-In-Time support continuous improvement, while Enterprise Resource Planning (ERP) and Manufacturing Execution Systems (MES) help coordinate activities across departments and geographies. A clear distribution of roles and responsibilities is essential for maintaining efficiency and responding to disruptions.

Ultimately, successful manufacturing organizations integrate governance, management, and operations into a cohesive system that supports innovation, ensures compliance, and adapts to evolving market and regulatory demands.



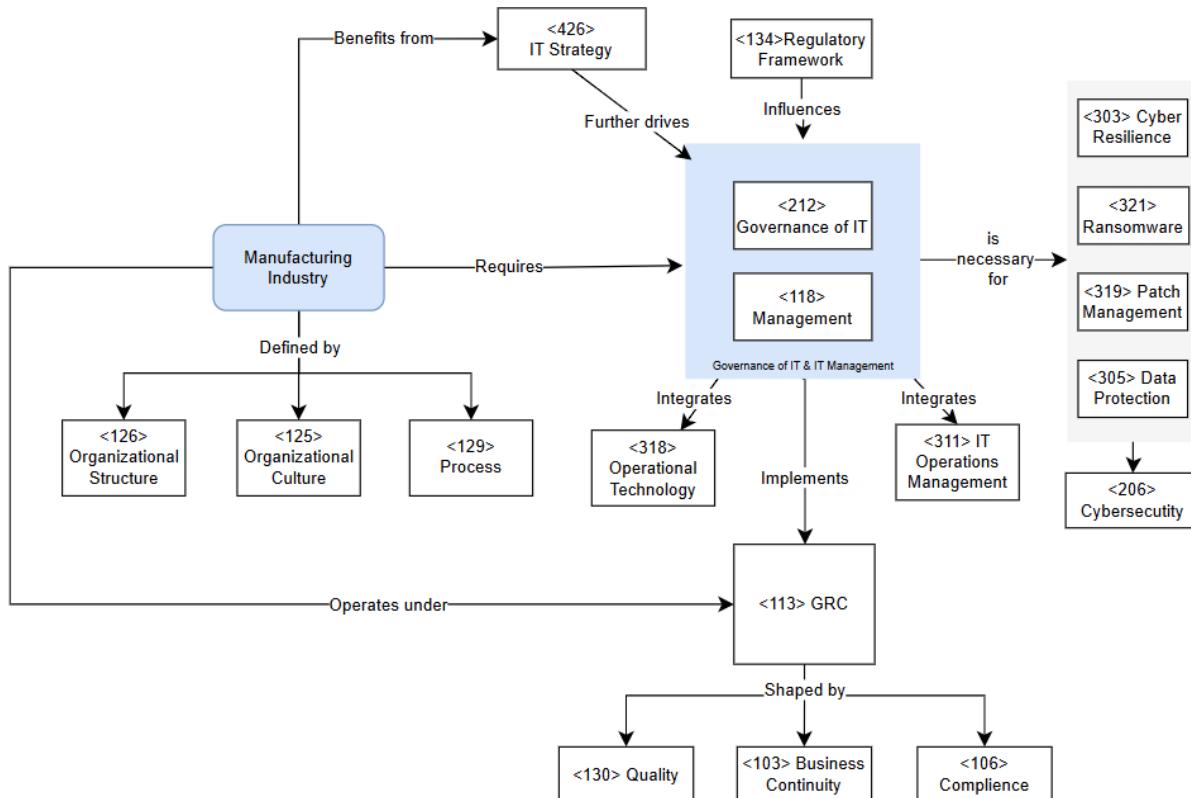
Governance of IT and IT Management in the Manufacturing Industry

In today's digital landscape, the manufacturing industry relies on strong IT management to boost efficiency, ensure cybersecurity, and stay competitive. As a capital-intensive sector with complex supply chains, it depends on integrated physical and digital systems. IT plays a strategic role in enabling smart manufacturing, predictive maintenance, and real-time decisions.

The Manufacturing Industry transforms raw materials into finished goods using labour, machinery, and various processes. It supports sectors like infrastructure, energy, and healthcare, ranging from small workshops to global automated networks. To meet demands for efficiency, quality, and compliance, manufacturers use systems like ERP and MES to manage operations and align with production goals.

Moreover, IT management in manufacturing must address Governance, Risk, and Compliance (GRC) requirements, particularly those related to cybersecurity. As Operational Technology (OT) becomes increasingly connected to IT networks, the risk of cyberattacks on industrial control systems rises. Risk management strategies must also consider equipment failure, supply chain disruptions, and data breaches, all of which can have significant operational and reputational consequences.

In this context, IT management drives digital transformation and resilience through strategic planning, integrated governance, and ongoing improvement. It plays a central role in helping manufacturers adapt to market shifts, regulations, and sustainability challenges.



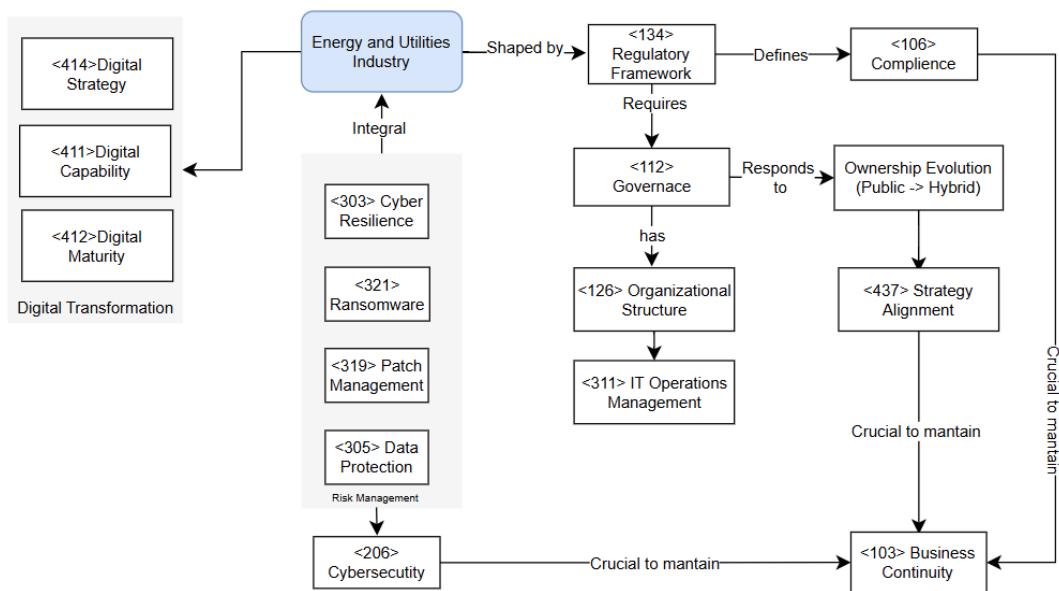
Organizations, Governance, and Management in the Energy and Utilities Industry

Governance in the Energy and Utilities Industry is defined by the necessity to cope with long-term infrastructure, public service provision, and complex regulatory environments. Historically dominated by public monopolies due to their natural monopoly characteristics, the sector has transitioned towards liberalised and hybrid forms, where security of supply, affordability, sustainability, and innovation need to be weighed by governance structures.

Boards and executive management must align strategic decisions with national climate and energy goals in the face of operational, market, regulatory, and geopolitical risks. Regulatory frameworks, such as the EU's Clean Energy Package, the Renewable Energy Directive, and NIS2 cybersecurity regulations, drive governance with far-reaching compliance demands on emissions, safety, pricing, and infrastructure resilience.

Digitalisation has also transformed governance by introducing smart grids, SCADA networks, and energy trading platforms, all of which require robust IT governance and cybersecurity controls. Subdomains such as electricity, gas, water, and retail services present distinctive governance challenges, from grid stability and cross-border gas dependence to consumer protection and decentralised energy participation.

With the sector responding to climate imperatives, decentralisation, and technological disruption, effective governance increasingly depends on strategic foresight, digital resilience, and strong regulatory synchronisation at both national and international levels.



Governance of IT and IT Management in the Energy and Utilities Industry

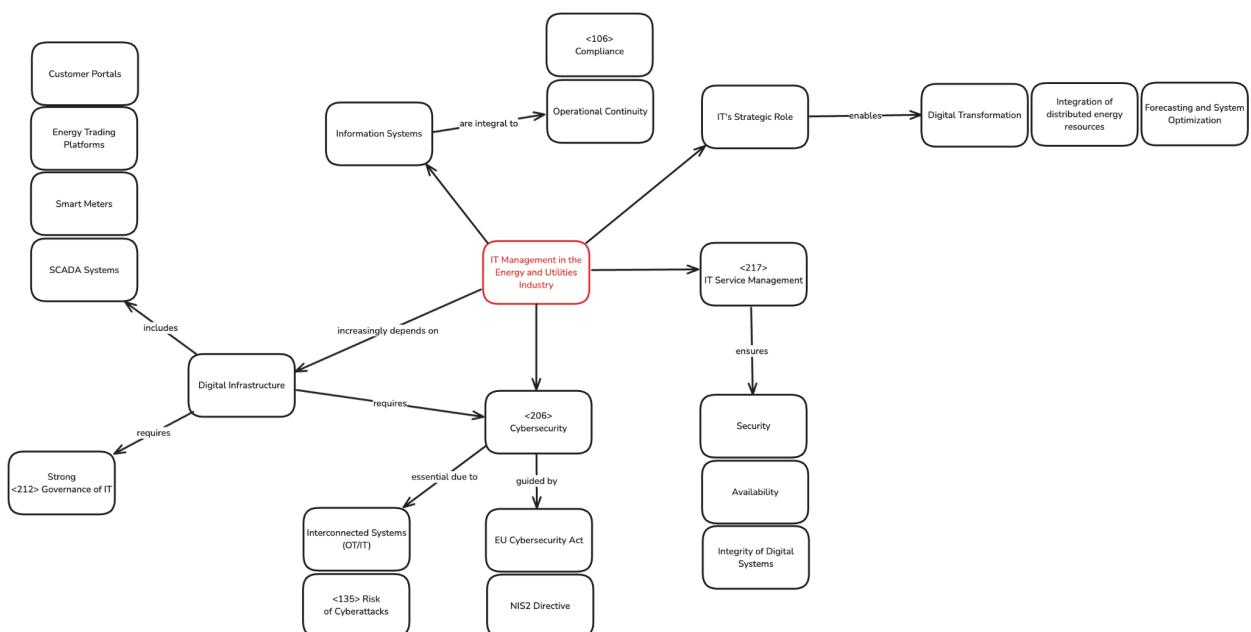
IT management in the energy, industry, and utilities sector has become a central pillar of operational and strategic performance, especially as digitalisation accelerates across the value chain. Traditionally reliant on analogue control systems, the sector now depends on integrated digital infrastructures such as SCADA systems, smart meters, energy trading platforms, and customer portals.

These technologies support real-time monitoring, predictive maintenance, demand forecasting, and consumer engagement. Effective IT management must ensure the security, availability, and integrity of these systems, as they underpin critical services and national infrastructure.

The convergence of operational technology (OT) and information technology (IT) presents new challenges, requiring coordinated oversight to manage cyber risks, data flows, and system interoperability. Regulatory mandates such as the EU's NIS2 Directive and Cybersecurity Act enforce strict requirements for cybersecurity governance, incident response, and risk assessment.

Additionally, IT plays a key role in enabling strategic transitions, such as the integration of distributed energy resources, the optimisation of grid performance, and the decarbonisation of heating and transport. Boards and IT leadership must collaborate to embed IT governance within corporate structures, ensuring that digital investments align with broader goals in sustainability, resilience, and compliance.

As the sector becomes increasingly reliant on data-driven processes and AI-enhanced decision-making, strong IT management is no longer a support function—it is a strategic enabler of transformation and system stability.



Organizations, Governance, and Management in the Retail and Digital Commerce Industry

This industry represents the final link connecting producers to consumers through physical stores, digital marketplaces, and omnichannel platforms. It's characterized by customer-centric focus, real-time market responsiveness, and hybrid physical-digital operations spanning fashion, electronics, groceries, and services, often within ecosystems retailers don't control.

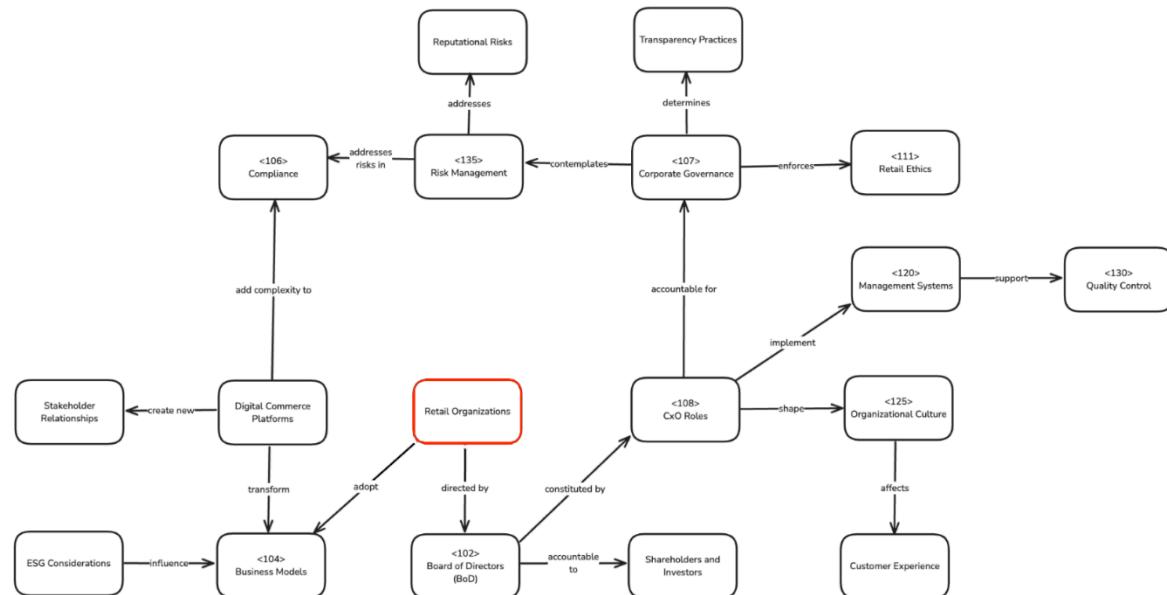
Retail and digital commerce governance frameworks must balance operational agility with risk management across physical and digital environments. Accountability extends beyond shareholders to customers, suppliers, and platform partners, creating multi-layered governance challenges.

Data governance is critical as customer information becomes a strategic asset. Governance structures must address GDPR compliance and ethical data usage, especially for personalization. This is complicated by retailers operating within uncontrolled ecosystems (marketplaces, app stores), creating dependencies where authority and accountability may be misaligned.

Evolving regulations, including the EU's Digital Services Act and Digital Markets Act, require transparent governance for content moderation and algorithmic decision-making. Global operations must accommodate jurisdictional variations in consumer protection while maintaining organizational cohesion.

Governance maturity varies significantly. Traditional retailers maintain hierarchical models focused on centralized control, while digital-native retailers employ distributed frameworks emphasizing speed and adaptation. This tension appears in digital transformation, where legacy governance structures may impede e-commerce agility.

Effective retail governance must address the sector's defining characteristics: customer-centricity, rapid market evolution, and physical-digital convergence, requiring both formal structures and cultural alignment.



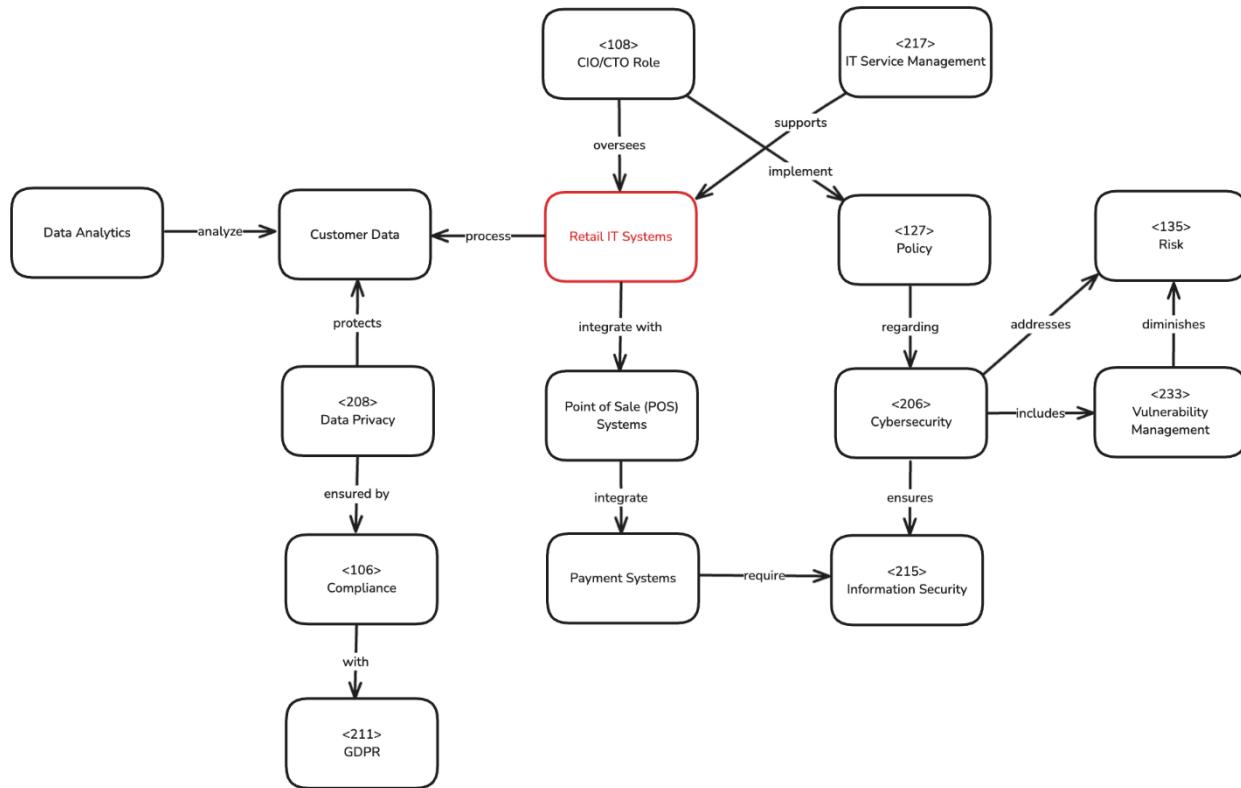
Governance of IT and IT Management in the Retail and Digital Commerce Industry

IT management in retail and digital commerce must seamlessly integrate physical and digital shopping experiences while supporting operations across omnichannel environments. Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Point of Sale (POS), and digital marketing platforms form the core IT infrastructure, requiring IT departments to balance standardization with flexibility, particularly when operating within ecosystems they don't fully control.

Data management presents significant complexity as customer information flows across touchpoints. IT management must implement robust governance frameworks ensuring GDPR compliance while enabling personalization and analytics capabilities that drive competitive advantage. The security landscape is equally challenging, with payment systems, customer data, and interconnected supply chains creating multiple vulnerability points that must be secured without compromising user experience.

IT management maturity varies substantially across the sector. Digital-native retailers typically employ DevOps practices, cloud-native architectures, and API-first approaches, while traditional retailers often struggle with legacy systems that impede innovation, evident in the uneven adoption of AI-driven merchandising, predictive analytics, and IoT-enabled inventory management.

Effective retail IT management requires strategic alignment of technology investments with business objectives while maintaining agility to respond to market changes and evolving consumer behaviors, necessitating close collaboration between IT leadership and business units.



Theme 2: Manufacturing Industry VS. Energy and Utilities Industry

From the perspective of Theme 1: Governance of IT and IT Management, the manufacturing and energy & utilities industries both require structured governance models due to their capital intensity and dependence on operational stability. They operate complex systems that integrate technical and human factors, demanding clear roles, accountability, and risk management.

In the energy and utilities sector, governance is shaped by strong regulatory obligations, public service responsibilities, and long-term infrastructure planning. Strategic decisions must align with national goals, and IT governance must ensure system resilience, security, and compliance across interconnected networks.

In contrast, the manufacturing industry focuses more on operational efficiency, supply chain coordination, and adaptability. IT governance in this sector supports process optimisation, innovation, and responsiveness to market dynamics.

While both industries face challenges in managing the convergence of IT and operational technologies, energy governance is driven by regulatory stability and service continuity, whereas manufacturing prioritises agility, performance, and continuous improvement

Theme 1: Manufacturing Industry VS. Energy and Utilities Industry

The manufacturing and energy, and utilities industries have distinct organizational and governance models shaped by their structure and public role. Manufacturing is defined as the transformation of raw materials into finished goods. It operates through private organizations that range from small factories to global production networks. Governance in manufacturing focuses on efficiency, quality, and coordination across supply chains. Decision-making is influenced by market conditions, trade policies, and the need for flexible production.

In contrast, the energy and utilities sector includes electricity, gas, water, and related services. It evolved from public monopolies and often remains under strong regulatory supervision. Organizations in this sector may be public, private, or mixed. Governance addresses long-term infrastructure planning, service continuity, and policy alignment. Boards must weigh national goals for energy, climate, and security of supply.

While both industries integrate technical systems with management practices, manufacturing emphasizes performance and cost control, whereas energy prioritizes stability and public accountability. In both cases, IT and engineering teams must coordinate to maintain operational reliability and regulatory compliance.

Theme 1: Energy and Utilities VS. Retail and Digital Commerce

Governance in the Energy and Utilities sector is traditionally strong, shaped by its role as critical infrastructure. It has a culture of regulation, public accountability, and formal structures like state ownership or tightly regulated entities. Leadership balances energy goals, environmental duties, and service continuity, guided by national policies and global factors. Its capital intensity drives a focus on long-term investment, risk management, and alignment with sustainability targets.

By contrast, governance in Retail and Digital Commerce is more decentralised and market-driven. The sector is highly competitive and fast-moving, leading to governance models that emphasise agility, innovation, and customer responsiveness. Retail boards often focus on brand reputation, ethical sourcing, marketing practices, and global supply chain accountability. There is typically less state involvement, and governance mechanisms vary widely depending on the scale and international presence of the firm. Retail governance also increasingly addresses societal concerns such as inclusivity, environmental claims, and consumer protection, often in response to shifting public expectations and reputational risks rather than formal regulation.

In summary, Energy and Utilities governance is structured, compliance-oriented, and policy-driven, reflecting its public service mandate and infrastructure reliance. Retail and Digital Commerce, while evolving rapidly, adopt more flexible and consumer-centric governance approaches, shaped by brand management, commercial pressures, and platform dynamics.

Theme 2: Energy and Utilities VS. Retail and Digital Commerce

Aspect	Energy and Utilities	Retail and Digital Commerce
Primary IT Focus	SCADA, smart grids, OT/IT convergence	ERP, CRM, POS, digital platforms
Risk Tolerance	Zero-failure tolerance	Business continuity focused
Regulatory Framework	NIS2, Cybersecurity Act, sector-specific safety	GDPR, Digital Services Act, consumer protection
Governance Maturity	High formalization, structured processes	Variable (digital-native vs traditional retailers)
Change Management	Long-term, methodical planning cycles	Rapid adaptation, agile methodologies
Strategic Priorities	Infrastructure resilience, decarbonization	Customer experience, market responsiveness
Compliance Approach	Mandatory reporting, formal oversight	Data protection, algorithmic transparency

P1 Report - Group 124

David Coelho, 113369
Francesco Pelizzari, 99217
Pedro Frigolet, 102419

1. Manufacturing: Smart Factory

The **Smart Factory** is an advanced manufacturing environment leveraging digital technologies, including Industry 4.0, AI <401>, and IT/OT convergence <318>, to optimize production and enhance operational efficiency <113>.

Theme: Governance in Smart Factory

Textual Analysis:

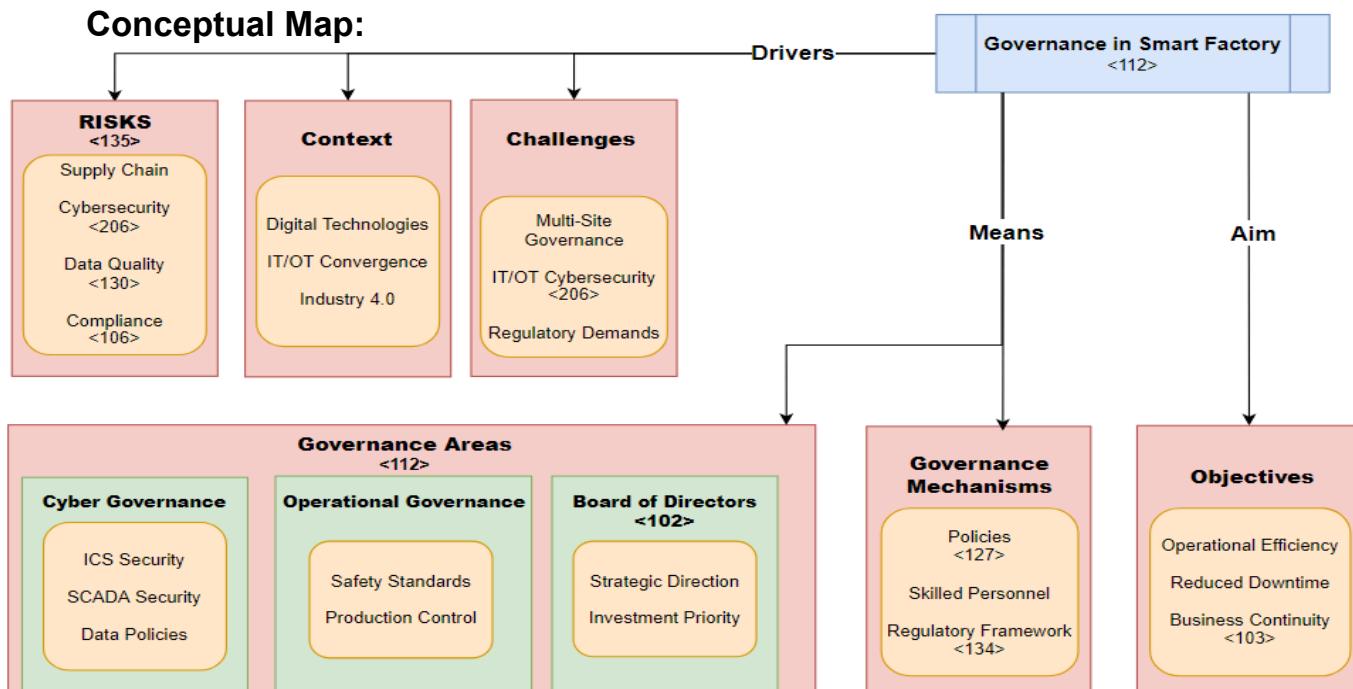
Governance within modern industrial sectors is increasingly complex due to digital technologies. This analysis focuses on Governance <112> within **Smart Factory** environments, where IT and Operational Technology (OT) convergence demand robust frameworks. **Industry 4.0**'s cyber-physical systems and real-time data necessitate integrated, proactive **Governance** <112>. Key challenges include managing Governance <112> across multi-site manufacturing, ensuring **robust Cybersecurity** <206> within interconnected IT/OT systems, and meeting diverse regulatory demands.

Strong **Cyber Governance** is crucial, including effective ICS/SCADA security and comprehensive data **Policies** <127> to protect sensitive production data and intellectual property. **Regulatory Frameworks** <134> (like ISO/IEC 38500, IEC 62443, and NIS2) provide essential guidance for **Risk mitigation** <135> and **Compliance** <106>.

Operational Governance within Smart Factories focuses on safety and efficient production control. **Board of Directors** <102> is vital, providing strategic direction and prioritizing **Cybersecurity** <206> and **Governance** <112> investments. Effective **Governance** <112> bridges plant-floor operations and leadership, enabling **Risk-informed** smart technology investments and addressing **Supply Chain**, **Cybersecurity** <206>, **Quality** <130>, and **Risks** <135> related to **Compliance** <106>.

Overcoming limitations like legacy systems requires structured **Governance** <112> **Policies** <127> and **Risk** <135> assessments for digital trust and **Business Continuity** <103>.

Conceptual Map:



P1 Report - Group 124

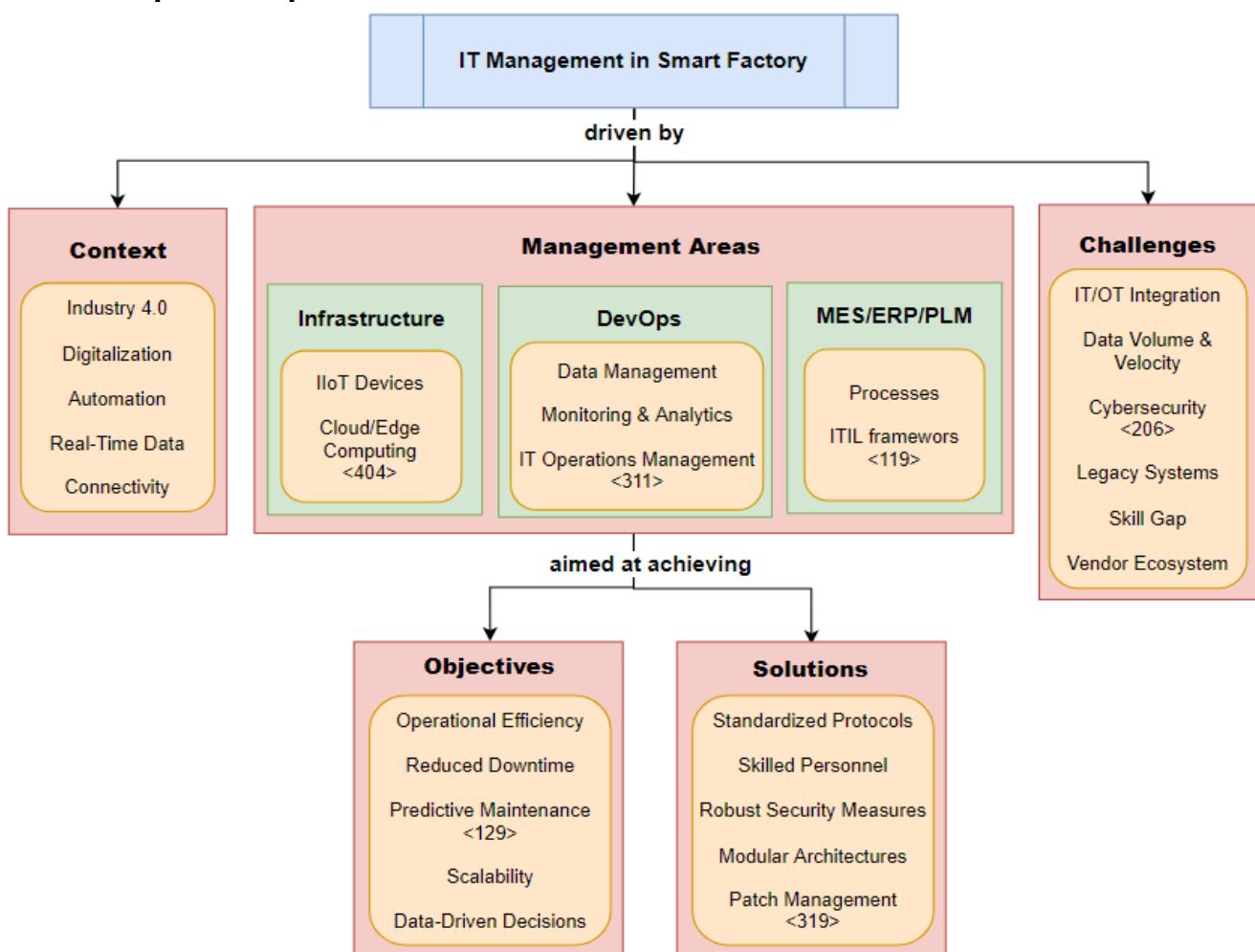
Theme: IT Management in Smart Factory

Textual Analysis:

Effective **IT Management** <311> in **Smart Factories**, focusing on **Predictive Maintenance** systems, requires orchestrating various technologies including **Cloud Computing** <404>, **AI** (Artificial Intelligence) <401>-driven analytics, and legacy automation into a resilient digital ecosystem. Core to this is the **convergence of IT and OT** (Operational Technology) <318>, integrating manufacturing systems and platforms with industrial devices for real-time equipment health monitoring. **ITIL frameworks** <119> help structure **IT Operations Management** <311> (service availability, incident response <310>), while **Patch Management** <319> is essential for system integrity and maintenance reliability. **Predictive Maintenance** <129>, enabled by **AI** <401>, shifts **IT Operations Management** <311> towards proactive strategies, **minimizing downtime and optimizing maintenance**.

However, Smart Factories face challenges including complex **vendor ecosystems**, potential **Cybersecurity** <206> gaps, legacy infrastructure issues, and the need to ensure data accuracy for reliable predictions. Strategically, **IT Management** <311> **must align** with **Business Goals** <104>, driving **Innovation** <113> and supporting **KPIs** (Key Performance Indicators) <116> such as incident response time, maintenance cost reduction, prediction accuracy, and **Security** <206>.

Conceptual Map:



P1 Report - Group 124

2. Energy and Utilities

The **Energy and Utilities** sector is a capital-intensive, tightly regulated backbone that invests for decades, balances the security-cost-carbon equation <102>, and safeguards SCADA and smart-grid systems <115> to keep essential services running.

Theme: Governance in Energy and Utilities

Textual Analysis:

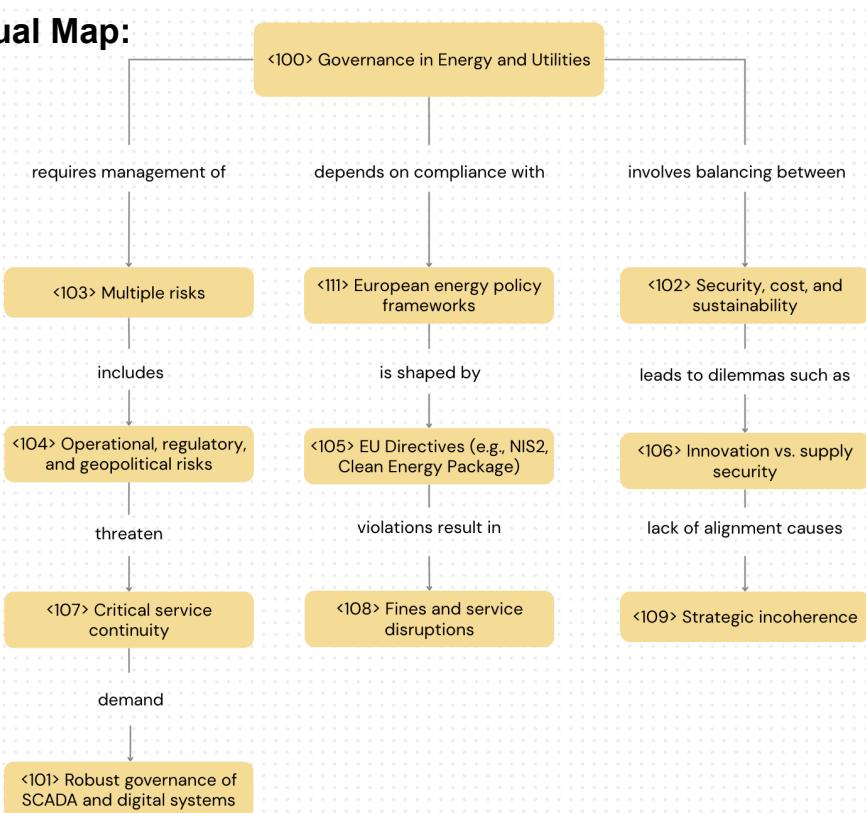
The **Energy and Utilities** sector underpins public health, economic stability and national security by supplying electricity, gas, water and an expanding mix of renewables with storage. Once dominated by state-run monopolies, it now spans public and private operators, reshaped by market liberalisation, climate goals and digitalisation.

Governance in this sector must navigate long investment cycles, critical infrastructure dependencies, and a multi-layered regulatory environment. Executive leadership is tasked with managing trade-offs between **security, cost, and sustainability** while addressing a <135> **multiple risks** portfolio that includes **operational, regulatory, and geopolitical risks**.

European energy policy frameworks — including <105> **EU Directives (e.g., NIS2, Clean Energy Package)** — significantly shape sector **governance** <100> by introducing mandatory cybersecurity requirements, decarbonisation targets, and consumer-empowerment mechanisms. Leaders must balance <106> **innovation vs. supply security** to guarantee **critical service continuity** and avoid <108> **fines and service disruptions**, preventing <109> **strategic incoherence**.

Robust governance of SCADA and digital systems underpins these objectives, ensuring cybersecurity controls are integral to operations. Energy companies must also align strategy with evolving regulation, public scrutiny, and innovation agendas, making **governance** both highly strategic and operationally grounded.

Conceptual Map:



P1 Report - Group 124

Theme: IT Management in Energy and Utilities

Textual Analysis:

The sector is undergoing a significant digital shift, where IT is a strategic enabler of **<113> operational resilience, efficiency, and digital transformation**. **IT management** is complicated by **IT/OT convergence and legacy systems** across infrastructures such as power grids, gas pipelines, and water networks.

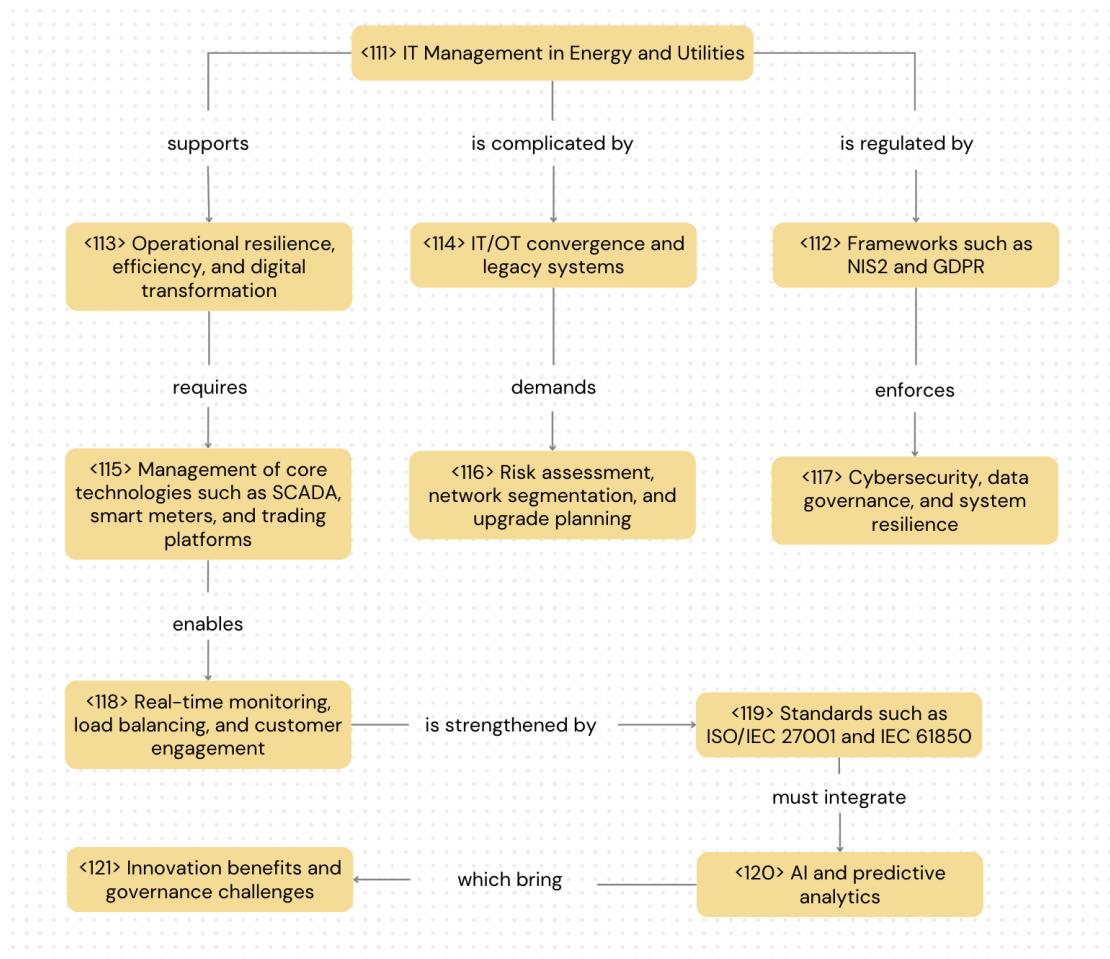
Core technologies include SCADA, smart meters, energy-trading platforms, and digital customer interfaces. Effective **<115> management of core technologies such as SCADA, smart meters, and trading platforms** requires **<135> risk assessment, network segmentation, and upgrade planning**, plus strong **<206> cybersecurity, data governance, and system resilience**. Regulatory pressure is heightened by **<112> frameworks such as NIS2 and GDPR**.

These systems enable **<118> real-time monitoring, load balancing, and customer engagement**. International **<119> standards such as ISO/IEC 27001 and IEC 61850** strengthen governance and compliance.

Digital innovation — notably **<120> AI and predictive analytics** — supports demand forecasting, grid optimisation, and predictive maintenance.

Yet these benefits bring **<121> innovation benefits and governance challenges** that must be addressed to balance modernisation with risk, safeguard service continuity, and advance sustainability, decentralisation, and customer-centricity.

Conceptual Map:



P1 Report - Group 124

4. Transport and Logistics

The **Transport and Logistics** sector is a global sector that has been around for a long time, encompassing the movement of goods and commodities, and it leverages modern technologies to better operational efficiency <113>.

Theme: Governance in Transport and Logistics

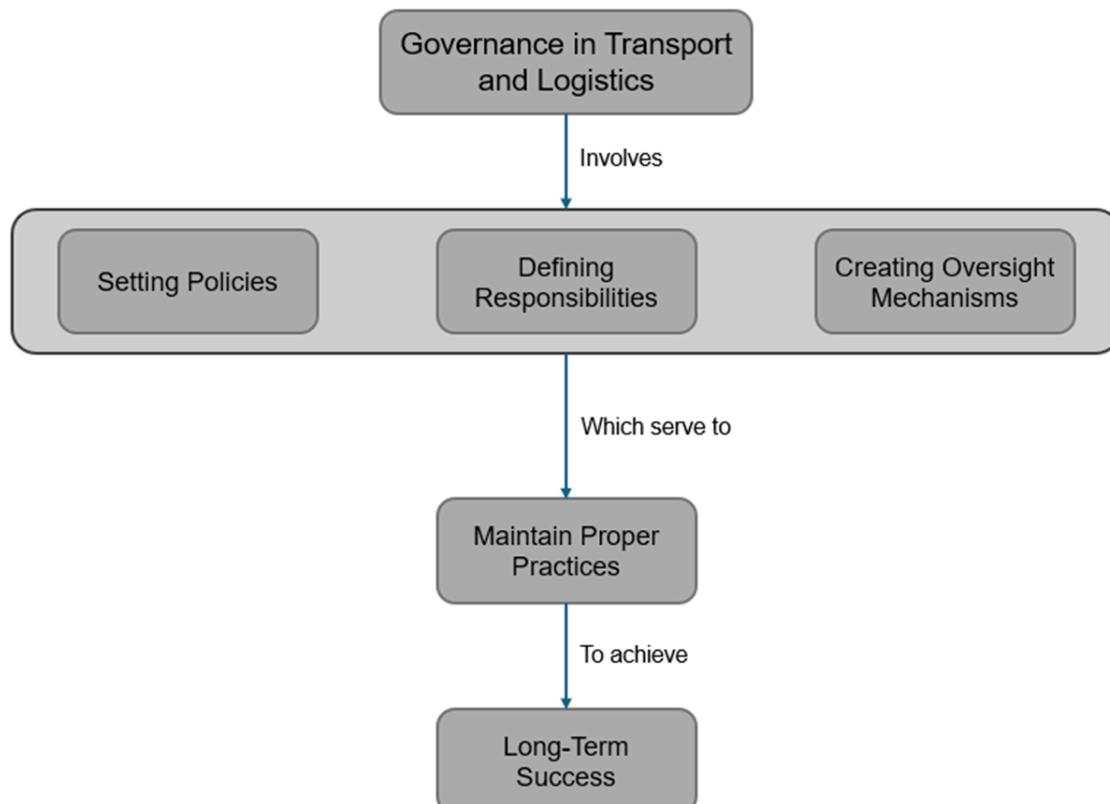
Textual Analysis:

Governance <112> plays a major role in transport and logistics, as it ensures that operations are carried out responsibly, efficiently, and in line with internal **company goals** <122> while **complying** <106> with all external **regulatory frameworks** <134>. It involves setting clear **policies** <127>, defining responsibilities, and creating oversight mechanisms that guide decision making at every level of the supply chain.

Effective **governance** <112> ensures that all activities such as procurement, fleet management, and warehousing are conducted in accordance with legal requirements, ethical standards, and environmental considerations. It also plays a central role in **risk** <135> **management**, helping organizations anticipate and respond to challenges such as regulatory changes, market disruptions, and labor issues.

In such a complex and globally connected industry, good **governance** <112> also supports coordination between various stakeholders, from carriers and warehouse managers to government agencies and customers. Clear structures help define responsibilities, prevent conflicts, and promote transparency across this interconnected network. It ensures that practices are consistent, ethical, and transparent, which is essential for maintaining trust and achieving long-term success in a highly competitive market.

Conceptual Map:



P1 Report - Group 124

Theme: IT Management in Transport and Logistics

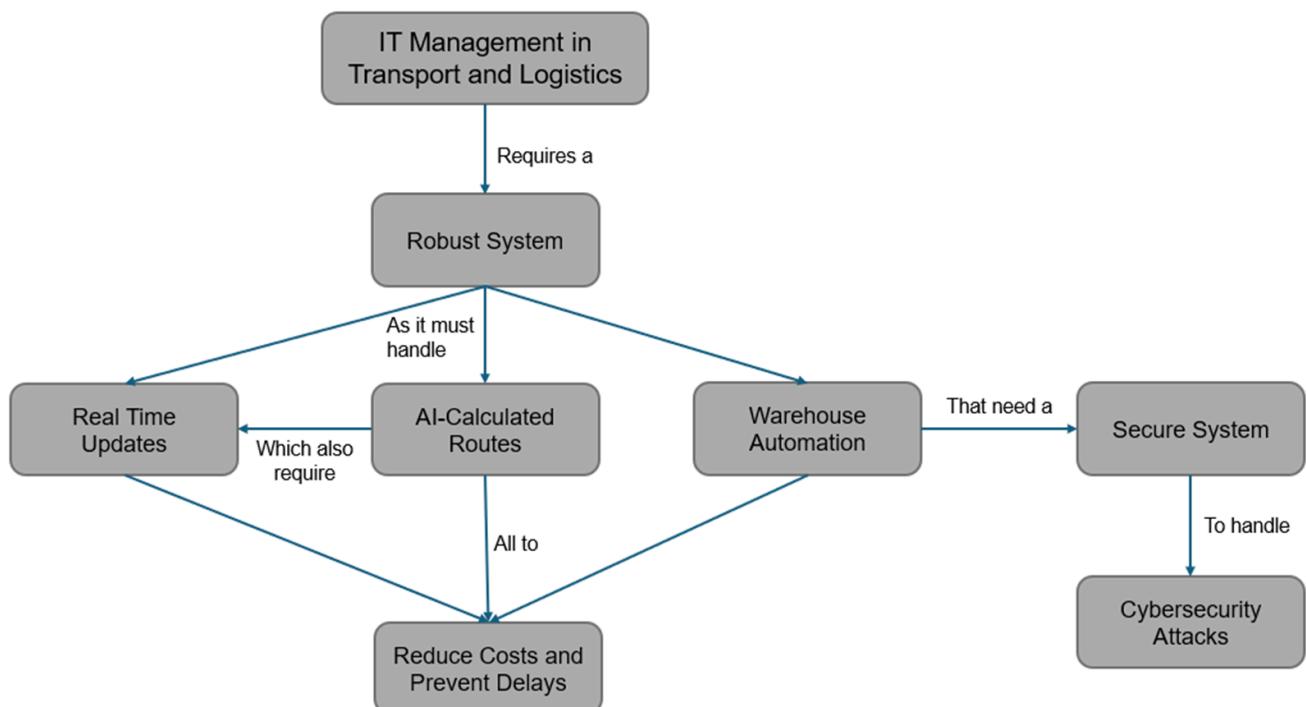
Textual Analysis:

IT Management <311> plays an important but often overlooked role in the transport and logistics sector, as the transport of goods and commodities requires that a number of digital systems operate smoothly and effectively. A fundamental system is real time tracking, upon which other important functionalities depend, as knowing where a package is at all times is essential and thus necessitates a robust system.

Effective **IT management <311>** is also necessary as most shipping depends on **AI <401>** calculated routes in order to minimize time taken and costs, thus multiple important values such as weather, traffic, fuel costs, and myriad others, need to be factored in, then the route communicated to whoever is doing the delivery. Moreover, the dynamic nature of logistics requires real time updates, as unexpected events can cause delays or increase costs, which businesses aim to minimize as much as possible.

Warehouses in particular also must be well managed as nowadays they are almost entirely automated, relying on barcode scanners and RFID tags to manage inventory. Thus a secure system is highly necessary as a **cybersecurity <206>** attack could compromise **private information <305>** such as addresses and packages contents, which would be disastrous to a company's reputation.

Conceptual Map:



P1 Report - Group 124

Comparisons

Governance: Manufacturing vs. Energy and Utilities

Governance <112> in **Manufacturing** (Smart Factory) and **Energy and Utilities**, while both critical, diverge significantly in their primary drivers and risk <135> landscapes.

Smart Factory governance prioritizes efficiency, quality, and the protection of intellectual property within highly integrated IT/OT environments. Its focus is on managing multi-site operations, ensuring robust Cybersecurity <206> for production data, and adhering to industry-specific quality and safety standards (ISO 9001). The Board of Directors <102> often emphasizes investments in digital transformation and automation to maintain competitive advantage and reduce downtime.

Conversely, governance in **Energy and Utilities** is fundamentally shaped by its role as a critical infrastructure sector, demanding unwavering operational continuity <103> and public safety. This necessitates adherence to rigid Regulatory Frameworks <134> like GDPR <211>, which impose mandatory cybersecurity requirements and long investment cycles. Risk management <135> extends to geopolitical factors and systemic outages, making the balancing of security, cost, and sustainability a constant challenge.

While both sectors manage IT/OT convergence, **Energy and Utilities** face higher public and governmental scrutiny, driving a more conservative, compliance-driven approach to Governance <112> compared to the innovation-focused agility of **Smart Manufacturing**.

Governance: Transport and Logistics vs. Energy and Utilities

Governance <112> as it pertains to **Transport and Logistics** is somewhat similar from how it is for **Energy and Utilities**, both demand a constant compliance with a number of ethical and legal requirements alongside similar risk management <135>, as both depend on operational, regulatory, geopolitical and environmental risks, since wars, natural disasters and other large scale events can cause major upsets to shipping lanes and energy costs.

However, there are differences, as governance in **Energy and Utilities** is much more focused on ensuring constant operational continuity <103>, while in **Transport and Logistics** continuity is important but nowhere near so, as while shipping blockades do happen and cause prices to spike, it's nowhere near as drastic as an energy crisis which can cause widespread blackouts, resulting in major problems.

There is also the matter of centralization, as **Energy and Utilities** is relatively centralized, there's places to manage, mostly just power generation and transport infrastructure, while **Transport and Logistics** has to deal with multiple different places such as ports, docks, warehouses, all under different companies which must function together harmoniously in order to properly do their job.

Finally, **Energy and Utilities** is often very closely linked to the governments and the overall public sector, thus having to deal with governmental oversight and regulations <134>, while **Transport and Logistics** is almost always completely privatized with few if any governmental links.

P1 Report - Group 124

IT Management: Manufacturing vs. Transport and Logistics

IT Management <311> in **Manufacturing** (Smart Factory) and **Transport and Logistics** both leverage advanced technologies but with distinct operational objectives.

In **Smart Manufacturing**, IT Management <311> is deeply intertwined with Operational Technology (OT) <318> to optimize production processes. Key functions include deploying IoT for real-time equipment monitoring, utilizing AI <401> and predictive analytics for maintenance, and managing complex digital twins. The aim is to enhance operational efficiency, minimize downtime, and enable data-driven decisions on the factory floor, often navigating challenges like legacy systems and technical debt <325>.

In **Transport and Logistics**, IT Management <311> primarily focuses on enabling the seamless, cost-effective, and secure movement of goods and information across vast networks. This involves robust real-time tracking systems, AI-calculated routes <401> that account for dynamic variables (weather, traffic), and highly automated warehouses relying on digital inventory management. Cybersecurity <206> is paramount to protect sensitive private information <305> (addresses, package contents) and prevent disruptions to the supply chain <231>.

While both sectors rely on automation, Manufacturing's IT management is geared towards internal production optimization, whereas Transport and Logistics' IT management is driven by external network coordination and dynamic logistical challenges.

IT Management: Energy and Utilities vs. Manufacturing

IT Management <311> within the **Energy and Utilities** and **Manufacturing (Smart Factory)** sectors share critical elements but diverge significantly regarding their strategic goals and operational cycles, resulting in distinct priorities within technological Governance <112>.

Both sectors heavily depend on OT/IT integration <318>, particularly with SCADA systems <115> and AI-driven analytical platforms <401>, crucial for Predictive Maintenance <129> and Operational Efficiency <113>. Cybersecurity <206> and the modernization of Legacy Infrastructure <114> present common challenges, requiring continuous and structured approaches in both industries.

However, there are notable differences. In the **Energy and Utilities** sector, investments follow longer cycles and stricter Regulations <134> (such as NIS2 <105> and GDPR <211>), driven by the critical nature of their services and an imperative need for Operational Continuity <103>.

Conversely, in **Smart Manufacturing**, flexibility and rapid Innovation <113> are essential, fostering continuous investment in technologies like Digital Twins <113> and Predictive Analytics <129>, aimed at immediate Downtime Reduction <129> and Operational Optimization <113>.

These distinctions significantly influence IT Management <311> strategies. The **Energy** sector emphasizes robust, conservative investments focused on maximum Operational Security <117> and Reliability <103>. **Manufacturing**, on the other hand, adopts a more aggressive and Innovative <113> approach, aligning IT <311> closely with immediate Business Goals <104> and rapid Technological Evolution <113>.

Security and Management of Information Systems
Project Delivery 1
2025

Group 125

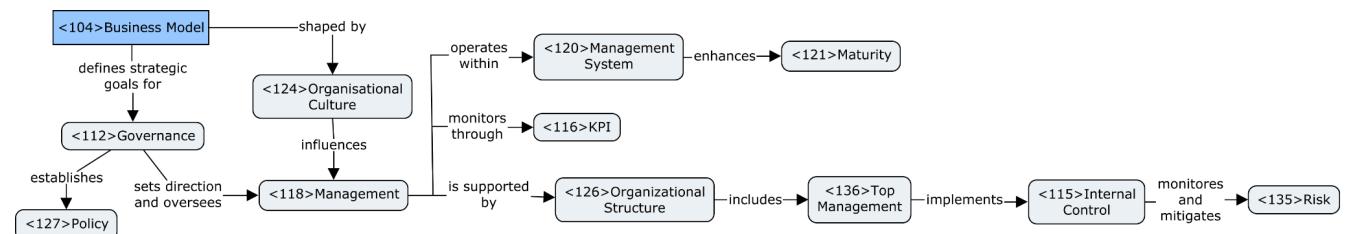
- Eduardo Afonso Correia Guerra (102681)
- Luís Miguel Gaspar Merca (113171)
- João Francisco António Freire de Andrade (78832)
- Oleksandr Peretyatko (113173)

Industry: Manufacturing

Theme: Organizations, Governance, and Management

Niche: Automotive Parts Production in Portugal

Conceptual map:



Textual analysis:

Automotive parts manufacturing plays a key role in Portugal's industrial economy, with companies like **Simoldes**, **Bosch**, and **ZF** producing components for global automotive brands. These firms operate within structured governance systems (<112> Governance), where <136> Top Management and <102> BoD define strategy and ensure accountability.

<118> Management transforms this strategy into operational plans, deploying <120> Management Systems such as **ISO 9001** and **IATF 16949**, common in the automotive sector. These systems formalize <127> Policies and drive <121> Maturity by enabling consistent, auditable processes.

<126> Organizational Structure supports process efficiency, while <116> KPIs—like defect rates and lead times—monitor performance. <115> Internal Control mechanisms help manage <135> Risk, especially in supply chains and regulatory compliance. The governance layer reinforces this with oversight and <101> Audits to validate <106> Compliance with safety and quality standards.

In Portugal, automotive parts manufacturers must also respond to industrial policy set by the government and EU funding programs for digitalization and sustainability (e.g., Portugal 2030). These external pressures further shape their <104> Business Model, pushing firms toward lean, smart, and sustainable production.

Sources:

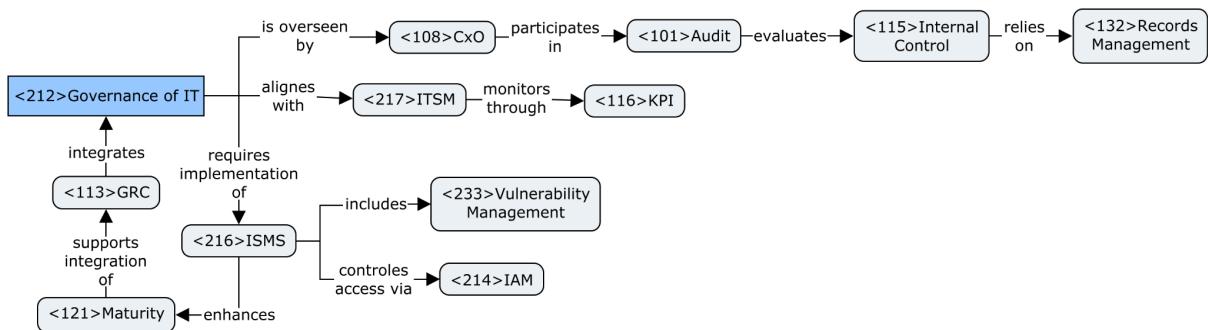
- Simoldes Tools. (2022, December 6). Home - SIMOLDES GROUP. Simoldes. <https://www.simoldes.com/en/>
- Home. (n.d.). Bosch Em Portugal. <https://www.bosch.pt/>
- Homepage ZF Friedrichshafen AG - ZF. (n.d.). <https://www.zf.com/>
- International Automotive Task Force. (n.d.). <https://www.iatfglobaloversight.org/>
- Portugal 2030. (2025, May 12). Homepage - Portugal 2030.<https://portugal2030.pt/>
- ISO - ISO 9000 family — Quality management. (2021, September 1). ISO.<https://www.iso.org/iso-9001-quality-management.html>

Industry: Manufacturing

Theme: Governance of IT and IT Management

Niche: Automotive Parts Production in Portugal

Conceptual Map:



Textual analysis:

Automotive parts production increasingly depends on digital infrastructure, making <212> Governance of IT essential to align IT capabilities with business objectives. Portuguese manufacturers like **Bosch Car Multimedia** and **Simoldes Plásticos** use integrated ERP and MES platforms to manage operations, quality, and supply chains, under the supervision of <108> CxO roles like CIOs and CISOs.

<217> ITSM (IT Service Management), typically structured around ITIL frameworks, ensures that technology services meet operational demands and customer expectations. Performance is tracked using <116> KPIs such as system uptime, incident resolution times, and support ticket closure rates.

Information security is governed through <216> ISMS (e.g., ISO/IEC 27001), which enables proactive <233> Vulnerability Management and strict <214> IAM protocols—crucial in environments where proprietary designs and production data must be safeguarded. These systems support <121> Maturity, moving organizations toward integrated, data-driven decision-making.

<113> GRC frameworks (Governance, Risk, and Compliance) help unify IT risk controls and compliance with standards like GDPR and IATF 16949. Regular <101> Audits and <115> Internal Control mechanisms (e.g., logs, role segregation, data retention protocols) validate controls, supported by systematic <132> Records Management.

By embedding IT governance in strategic and operational layers, Portuguese automotive manufacturers enhance resilience, enable real-time visibility, and ensure regulatory and cyber readiness—all critical as the industry shifts toward electrification and smart manufacturing.

Sources:

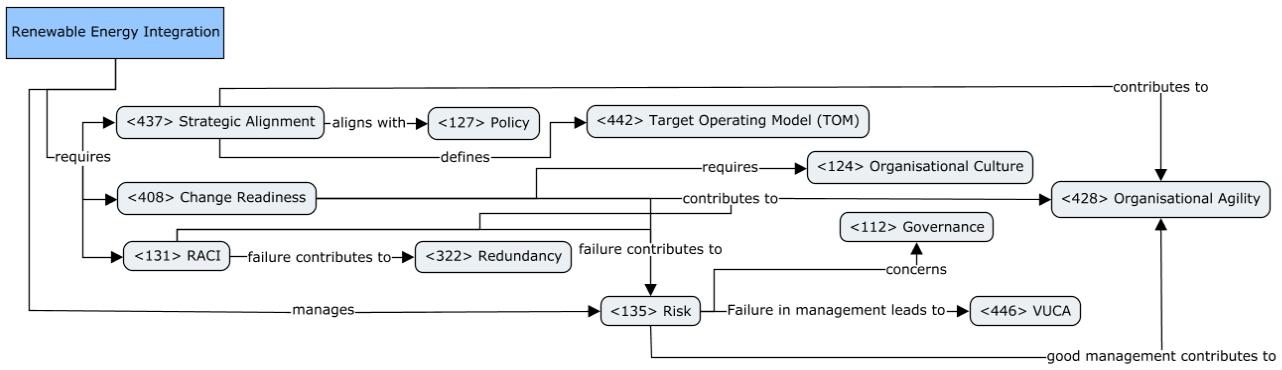
- Home. (n.d.). Bosch Em Portugal. <https://www.bosch.pt/>
- Simoldes Tools. (2022, December 6). Home - SIMOLDES GROUP. Simoldes. <https://www.simoldes.com/en/>
- ISO/IEC 27001:2022. (n.d.). ISO. <https://www.iso.org/isoiec-27001-information-security.html>
- International Automotive Task Force. (n.d.). <https://www.iatfglobaloversight.org/>

Industry: Energy and Utilities

Theme: Organizations, Governance, and Management

Niche: Renewable Energy Integration

Conceptual Map:



Textual analysis:

Portugal has become a leader in energy transition, with over 70% of its electricity from renewables in 2024. Projects like **Alqueva's floating solar farm** and **Alto Minho's wind park** highlight this. Yet, this rapid expansion demands a rethinking of how organizations operate — not only utilities like **EDP** or **REN**, but also government agencies and regulators.

Central to this shift is the need for stronger **<427> Strategic Alignment** — ensuring **<103> Business goals** and **<442> Target Operating Models** move together. Delays in permitting and grid access, despite ambitious climate goals, show misalignment between **<127> Policy** and execution.

Another key challenge is the lack of **<131> RACI** (Role Mapping), which clarifies who is Responsible, Accountable, Consulted, and Informed. In Portugal, overlapping roles between national and regional authorities — especially in licensing and grid connection — cause **<322> Redundancy** and delays.

<408> Change Readiness is also vital: it means having trained teams, flexible processes, and an **<124> Organisational Culture** that supports innovation. Public actors and grid operators still struggle, as seen during the April 2025 Iberian blackout, which exposed institutional rigidity.

Finally, **<135> Risk Management** practices often fail to address renewable-related volatility (**<446> VUCA**). Without integrated **<112> Governance** — including dependency mapping and compliance monitoring — organizations face rising operational and reputational risks.

To move forward, Portugal's energy sector must improve transparency, define clear RACI structures, and embed **<438> Strategic Planning** that fosters coordination and **<428> Organisational Agility** among all stakeholders.

Sources:

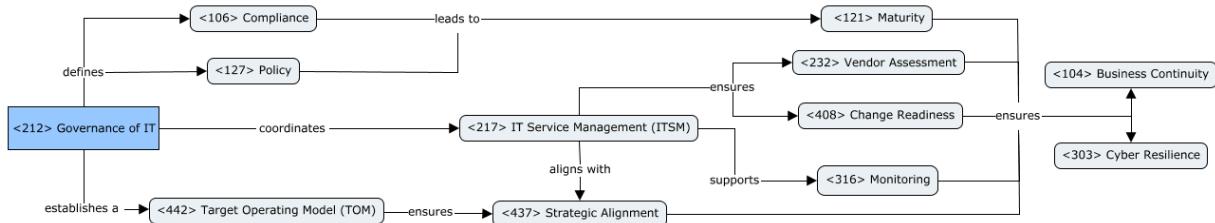
- Europe's savvy new clean energy champion. (2024, August 16). *Reuters*.
<https://www.reuters.com/business/energy/europe-s-savvy-new-clean-energy-champion-maguire-2024-08-16/>
- Jacobo, J. T. (2023, March 23). Portugal needs to step up on permitting issues and grid connection challenges. *PV Tech*.
<https://www.pv-tech.org/portugal-needs-to-step-up-on-permitting-issues-and-grid-connection-challenges/>
- Horton, H. (2025, April 29). What caused the blackout in Spain and Portugal and did renewable energy play a part? *The Guardian*.
<https://www.theguardian.com/environment/2025/apr/29/what-caused-the-blackout-in-spain-and-portugal-and-did-renewable-energy-play-a-part>

Industry: Energy and Utilities

Theme: Governance of IT and IT Management

Niche: Renewable Energy Integration

Conceptual Map:



Textual analysis:

The integration of renewables in Portugal demands reliable, secure, and well-governed IT systems. As the grid decentralises and becomes more volatile, IT must support real-time **<316> Monitoring**, automated responses, and predictive control.

Companies like **EDP** lead this shift, using **<401> AI** to forecast consumption and optimize storage. Projects like **InovGrid** in Évora show how smart grids enhance efficiency. Yet, challenges remain.

One major gap is the lack of a clear **<442> Target Operating Model (TOM)** — a blueprint aligning IT operations with business goals. Without it, data coordination suffers, and system-wide performance weakens.

Effective **<212> Governance of IT** ensures that technology investments deliver value, manage **<106> Compliance**, and support informed decisions. Weak governance can lead to poor data, security risks, and integration failures.

Portugal's grid still lacks full visibility and control of distributed assets, exposing limited Operational **<121> Maturity**. Improvements include automated failover, AI diagnostics, and consistent service delivery.

<232> Vendor Assessment is critical, as many platforms are outsourced. The 2025 blackout revealed fragilities in externally managed systems and the need for stronger contracts and contingency planning.

Finally, **<408> Change Readiness** is key. Adopting AI and cloud tools requires not just technology, but cultural and procedural capacity. Structured change processes reduce disruption and improve alignment.

Portugal's digital energy future relies on mature IT Management, strong Governance, and a clear TOM to ensure **<303> Cyber Resilience**, **<104> Business Continuity**, and public trust.

Sources:

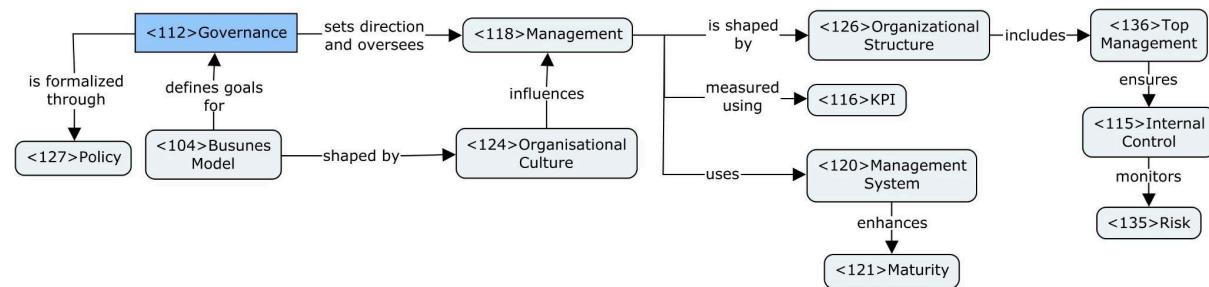
- Storyteller, A. (2023, September 19). Transforming the Future of Utilities: AI Advancements in Energias de Portugal (EDP) Cash Platform. <https://www.cash-platform.com/transforming-the-future-of-utilities-ai-advancements-in-energias-de-portugal-edp/>
- Wikipedia contributors. (2025, April 7). *Smart grid*. Wikipedia. https://en.wikipedia.org/wiki/Smart_grid
- Carter, P. (2025, April 29). Portugal's blackout recovery: a catalyst for renewable grid resilience and investment opportunities. *Ainvest*. <https://wwwainvestcomnewsportugal-blackout-recovery-catalyst-renewable-grid-resilience-investment-opportunities-2504>

Industry: Hospitality and Leisure

Theme: Organizations, Governance, and Management

Niche: Portuguese Hotel Chains

Conceptual Map:



Textual Analysis:

Hotels in Portugal—especially in regions like Lisbon, Porto, and the Algarve—operate within a highly competitive and seasonal market. Key players like **Pestana Group**, **Vila Galé**, and **Minor Hotels** balance service excellence with cost control under formal governance structures.

Top-level decision-making lies with **<136> Top Management**, which defines the **<104> Business Model** (e.g., luxury vs. budget accommodation, direct bookings vs. OTA reliance). They implement **<127> Policies** that support quality, safety, and guest satisfaction across properties, often guided by international standards like **ISO 9001** or **Green Key** for sustainability.

<118> Management is tasked with executing strategy via defined **<126> Organizational Structures**, from hotel managers to department heads. A **<120> Management System** is used to track performance—supported by **<116> KPIs** such as occupancy rate, RevPAR (Revenue per Available Room), and guest satisfaction scores.

<115> Internal Control mechanisms are vital, ensuring compliance with health, safety, and financial standards. These controls help manage **<135> Risk**, including reputational damage, staff shortages, or regulatory fines.

Success also hinges on **<124> Organisational Culture**—particularly in hospitality, where service excellence and responsiveness are cultural norms. Staff training, recognition programs, and leadership behavior all reinforce a culture that supports guest-centered values and long-term brand reputation.

Firms with higher **<121> Maturity** adopt continuous improvement practices and integrate governance into daily decision-making, enabling better crisis response and innovation (e.g., adapting to post-COVID travel shifts).

Sources:

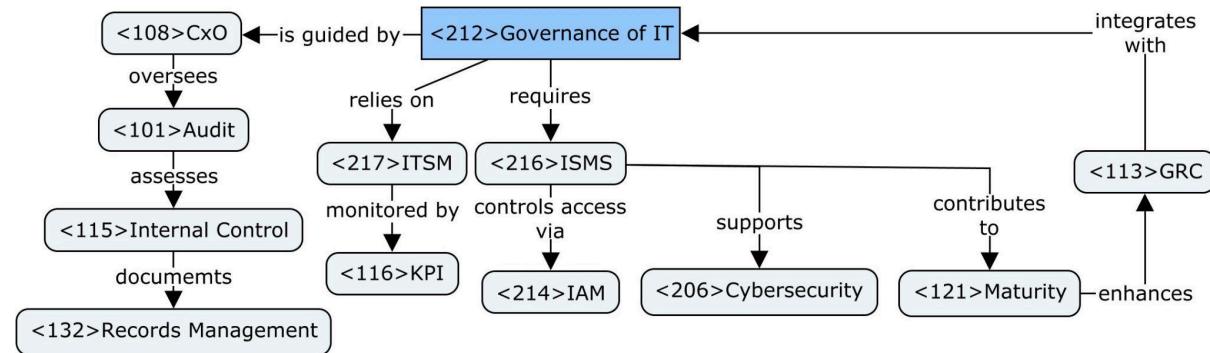
- Green Key. (2025, May 2). Green Key. <https://www.greenkey.global/>
- ISO - ISO 9000 family — Quality management. (2021, September 1). ISO. <https://www.iso.org/iso-9001-quality-management.html>

Industry: Hospitality and Leisure

Theme: Governance of IT and IT Management

Niche: Portuguese Hotel Chains

Conceptual Map:



Textual Analysis:

Hotels in Portugal increasingly rely on technology to support guest services, manage reservations, ensure data protection, and streamline operations. Effective **<212> Governance of IT** is critical for aligning these systems with business priorities while managing risks.

In major hotel groups like **Pestana** or **Vila Galé**, **<108> CxO** roles such as the CIO or IT Director are responsible for ensuring that IT investments support the hotel's goals. These roles implement **<217> ITSM** (e.g., ITIL practices), enabling the management of service requests, outages, and asset tracking, supported by **<116> KPIs** like system availability or ticket resolution time.

Hotels also use **<216> ISMS** frameworks (often based on ISO/IEC 27001) to structure their cybersecurity strategy. This includes **<214> IAM** to manage access to booking platforms, financial systems, and guest data. The growing importance of **<206> Cybersecurity** is evident with rising threats like phishing or ransomware targeting hotel chains worldwide.

<113> GRC frameworks help integrate compliance, risk management, and IT governance, especially relevant with **<132> Records Management** requirements under **<211> GDPR**. **<115> Internal Controls** ensure that procedures for financial transactions, data handling, and employee access are monitored and **<101> Audited** regularly.

As hotels adopt cloud-based PMS (Property Management Systems) and IoT (smart room controls), they must evolve their IT governance **<121> maturity**, not only to stay compliant but to remain competitive in digital guest experience delivery.

Sources:

- GDPR for Hotels: Here's What You Should Know (2025). (2024, December 2). Hoteltechreport. <https://hoteltechreport.com/news/data-protection-act>
- ISO/IEC 27001:2022. (n.d.). ISO. <https://www.iso.org/isoiec-27001-information-security.html>

Comparisons: Manufacturing with Hospitality and Leisure

Theme: Organizations, Governance, and Management

	Manufacturing (Simoldes, Bosch, and ZF)	Hospitality and Leisure (Pestana Group, Vila Galé, and Minor Hotels)
Organization	Centralized, functionally segmented, engineering-heavy	Decentralized, guest-oriented, flexible
Governance	Formal, <106> compliance -driven, quality-centric	Hybrid (formal and local autonomy), service-aligned
Management	Efficiency-focused, <116> KPI-driven, rigid protocols	Experience-focused, employee-driven, adaptive management

Comparisons: Manufacturing with Hospitality and Leisure

Theme: Governance of IT and IT Management

	Manufacturing (Bosch, Simoldes)	Hospitality & Leisure (Pestana, Vila Galé)
IT Governance Structure	Centralized, formal (COBIT, ISO/IEC 38500) with OT integration	Decentralized, focused on privacy and guest data
Risk & Compliance	Industrial risk, product traceability, and <106> compliance frameworks	<211> GDPR, guest data ethics, service availability
IT Management Style	Process-heavy, automation-driven, ISO-based	Agile, service-oriented
Data Governance Focus	Product and supply chain integrity	Customer data quality and protection
Strategic Role of IT	Core to operations and product innovation	Supportive of experience, branding, and marketing

Comparisons: Renewable Energy Integration with Hospitality industry

Theme: Organizations, Governance, and Management

	Renewable Energy Integration	Hospitality (Pestana Group, Vila Galé, and Minor Hotels)
Organization	Project/tech/infrastructure-driven entities	Decentralized, guest-oriented, flexible
Governance	Environmental compliance, grid standards, ESG	Hybrid (formal and local autonomy), service-aligned
Management	Technical, long-term strategic and operational	Experience-focused, employee-driven, adaptive management

The hospitality industry and the renewable energy integration sector differ significantly in their organizational structures, governance priorities, and management approaches. Hospitality is service-oriented, focused on customer experience, with hierarchical or owner-driven organizations and governance centered around health, safety, and labor compliance. In contrast, renewable energy integration involves complex, project-based or matrix organizations, with governance heavily influenced by environmental regulations and energy policies. Management in hospitality emphasizes operational efficiency and guest satisfaction, while in renewable energy, it is more technical and innovation-driven, focusing on system reliability, regulatory compliance, and long-term sustainability.

Comparisons: Renewable Energy Integration with Hospitality industry

Theme: Governance of IT and IT Management

	Renewable Energy Integration	Hospitality & Leisure (Pestana, Vila Galé)
IT Governance Structure	Structured and formalized, with clear alignment to regulatory and operational frameworks. IT governance is typically embedded in enterprise risk management and coordinated across engineering, operations, and compliance units.	Often decentralized or lightly structured in small/medium businesses; in large chains, governance frameworks like ITIL or COBIT may be adopted to ensure standardization across properties and regions.
Risk & Compliance	Faces high regulatory scrutiny. Risk management includes both IT and OT cybersecurity, with compliance requirements such as NERC-CIP, ISO/IEC 27001, and national energy regulations. Risks are tied to critical infrastructure reliability and national security.	Focuses on cybersecurity (e.g., protecting guest data and payment systems), GDPR compliance, and operational uptime. Compliance is mostly driven by customer trust and business continuity.
IT Management Style	Engineering-driven, proactive, and highly integrated with operations. IT management emphasizes high availability, predictive maintenance, and real-time system monitoring.	Customer-oriented and service-driven. IT management is often reactive and budget-conscious, with many services outsourced or centralized in corporate hubs.
Data Governance Focus	Data governance is critical for system monitoring, forecasting, regulatory reporting, and performance optimization. Strong controls exist over sensor data, SCADA logs, and usage analytics.	Focused on customer data privacy, loyalty program data, and booking system accuracy. Data governance is evolving, with growing interest in analytics for personalization and revenue optimization.
Strategic Role of IT	IT is a strategic backbone for the entire ecosystem, enabling smart grids, distributed energy resource management, and sustainable infrastructure. IT is deeply tied to the core mission and national energy goals.	IT supports competitive advantage mainly through digital guest experiences, marketing, and operational efficiency. It's a business enabler but not always seen as strategic.

Manufacturing - Theme 1

Niche: Aerospace and Defense Manufacturing

The manufacturing industry plays a critical role in the global economy, transforming raw materials into products that support every other sector, from healthcare to transportation to national defense. Given this immense outreach, we'll focus on a specific sub sector - Aerospace and Defense (A&D) manufacturing.

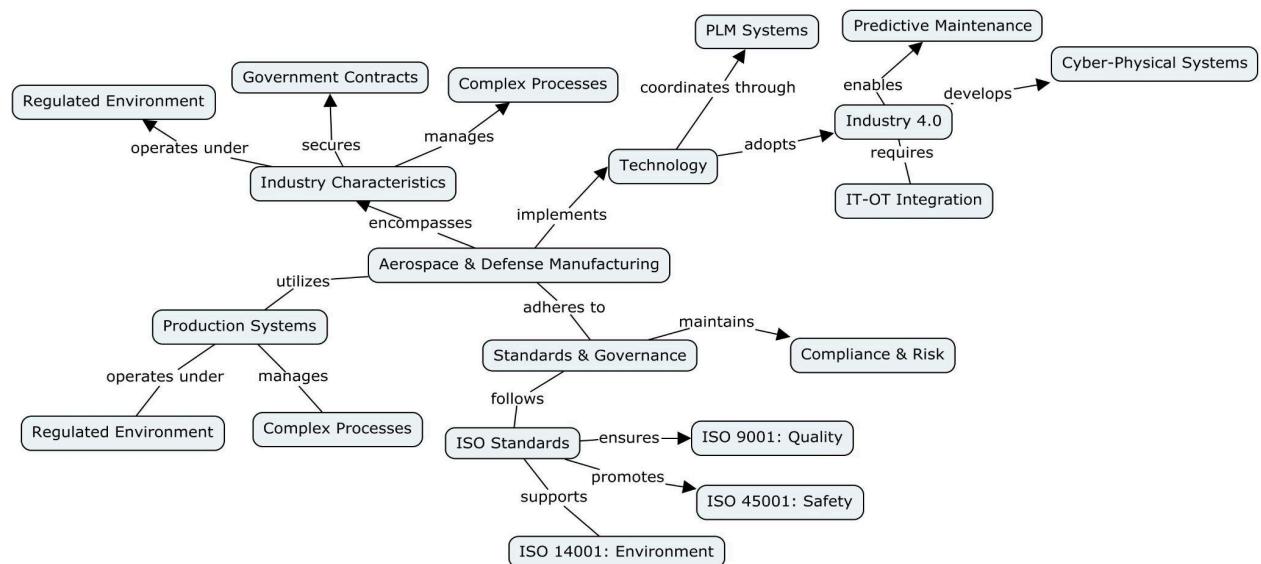
A&D is a highly specialized, high-stakes branch of manufacturing that includes companies that design, produce, and maintain aircraft, spacecraft, military systems and components. It encompasses both public and private sector entities that operate in highly regulated environments, often under government contracts, export control laws, and national security constraints.

This sector faces a dual challenge: delivering innovation (i.e, next generation aircraft, autonomous defense systems) while adhering to strict oversight from clients, regulators and international bodies. Operating in these highly regulated environments, these firms manage complex, long-cycle industrial processes using tools like Product Lifecycle Management and Supervisory Control and Data Acquisition systems, in a bid to stay organised and ensure traceability, compliance and coordination across all phases of production.

With the rise of Industry 4.0 technologies such as automation, predictive maintenance, and cyber-physical systems, the risk and overhead associated has grown tremendously, so firms must integrate these new technologies (IT) with Operational Technologies (OT) as securely as possible, and this demands mature governance and compliance frameworks.

Many of these firms manage risk using standards like ISO 9001, ISO 31000, ISO 14001, and ISO 45001 - these are all sets of rules and guidelines designed to promote consistent quality, structured risk assessment, environmental responsibility, and workplace safety. By following these standards, firms can ensure compliance, reduce operational disruptions, and build trust with regulators and clients.

Ultimately, A&D firms succeed not by avoiding risk, but by governing it strategically. Through structured oversight, integrated systems, and adherence to international standards, they balance innovation with resilience in one of the world's most demanding manufacturing sectors.



Manufacturing - Theme 2

With theme 1 we've seen the organizational structures and some risk management systems that provide a strong foundation for the Aerospace and Defense sector, and as A&D firms embrace Industry 4.0 technologies and shift toward data-driven operations, the governance of Information Technology (IT) becomes a central concern. From protecting sensitive data and managing cyber threats to ensuring alignment between digital infrastructure and defense objectives, A&D organizations face a new layer of risk and responsibility.

The main concern for these institutions is cybersecurity, particularly as firms handle classified data, proprietary designs, and critical infrastructure components. Attacks targeting this sector (through espionage or ransomware) can cause not just financial damage but also geopolitical consequences and to mitigate this, many organizations are adopting a Zero Trust model: an architecture that assumes no device or user can be trusted by default, even inside the network. This approach involves tightly controlled Identity and Access Management to prevent unauthorized access to sensitive systems.

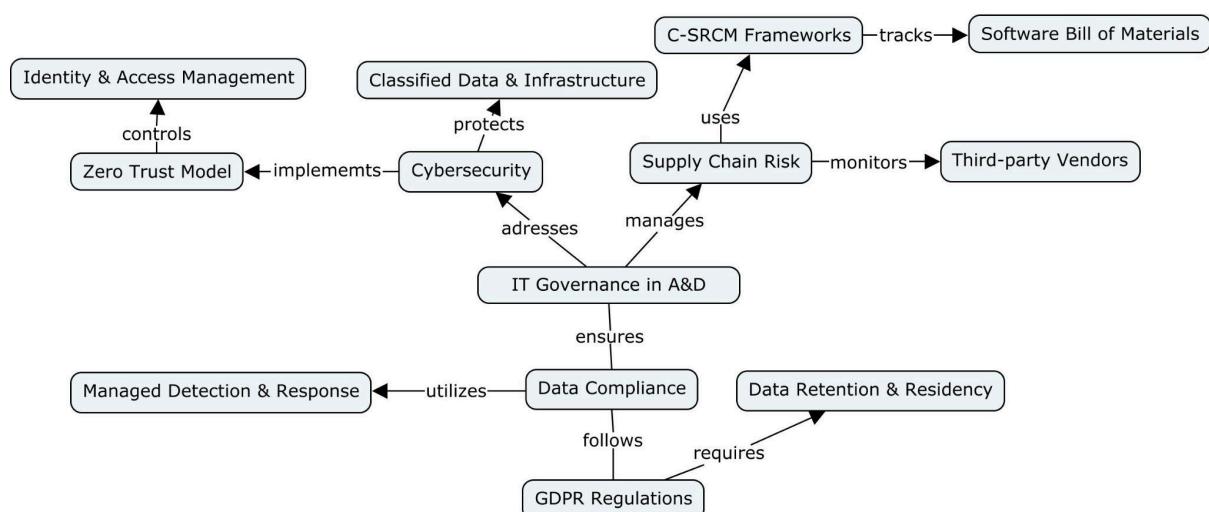
As A&D firms increasingly rely on remote workforces and global suppliers, the supply chain is another major vulnerability. C-SRCM frameworks (Cybersecurity Supply Chain Risk Management) helps companies address this issue by guiding vetting and monitoring processes for third-party vendors, particularly those involved in the development of digital systems. Knowing and understanding exactly what these third party digital systems run is vital, which is why tools like the Software Bill of Materials (SBOM), a detailed list of software components, are gaining prominence.

But even with the most advanced tools and rigorous processes, prevention from these intrusions isn't always assured, so companies must also be prepared to respond to them. This is where Managed Detection and Response (MDR) solutions come in. MDR providers offer 24/7 threat monitoring, detection, and incident response support, which is especially useful in a sector where response speed can be critical.

Data management is another key governance priority. Aerospace companies handle large volumes of personal identifiable information, which need to be properly protected.

Regulations such as the General Data Protection Regulation (GDPR) require clear policies for data retention, data residency, and consent mechanisms. Failing to comply can result in legal penalties or even loss of contract eligibility.

Overall, the successful governance of IT in the A&D world depends not just on tools and policies, but on embedding these practices into the organization's broader strategy.



Energy and Utilities - Theme 1

Niche: Water and Wastewater Services

Water and wastewater services face unique <107>**governance** challenges stemming from their hybrid nature between essential public service and infrastructure asset management. Unlike private utilities, water services often operate under municipal ownership with fragmented governance structures involving city councils, regional authorities, and environmental agencies. This creates complex accountability chains where <107>**Corporate Governance** principles must accommodate both democratic oversight and technical expertise requirements.

The sector's <126>**Organizational Structure** typically reflects low <121>**Maturity levels**, with many utilities operating through informal networks rather than formalized

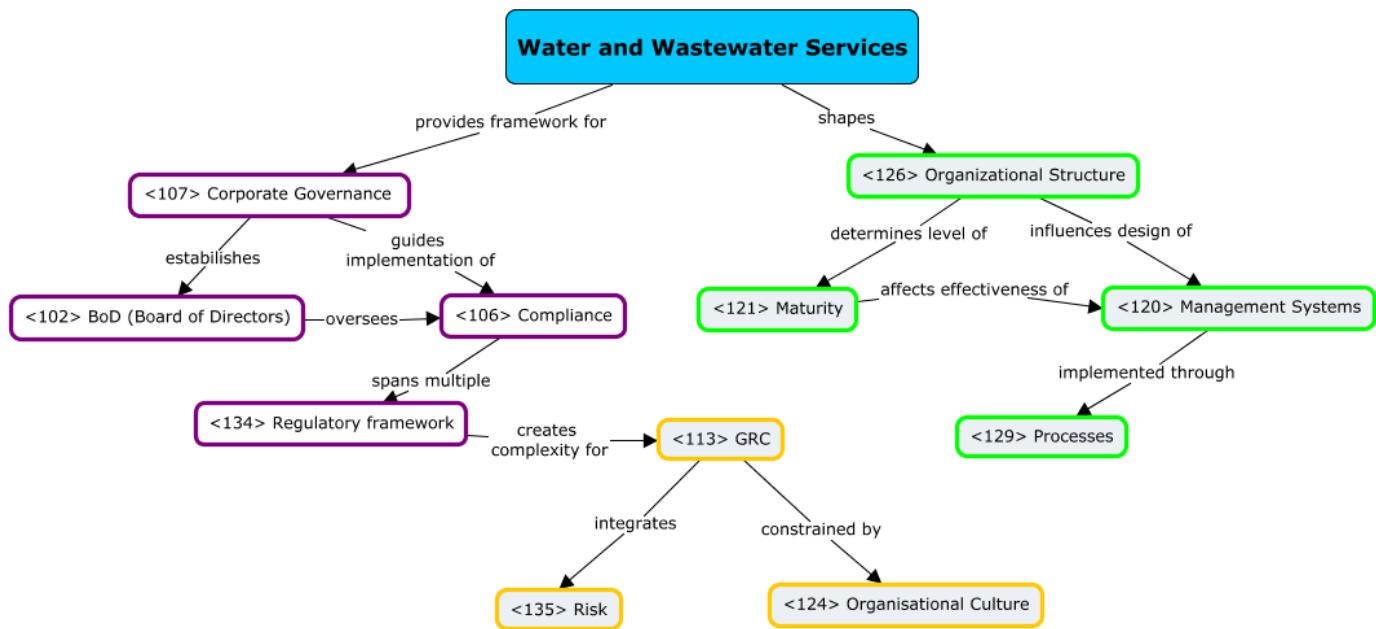
<120>**Management Systems**. Decision-making often relies on individual expertise rather than systematic <129>**Processes**, creating vulnerabilities when key personnel leave. The <102>**Board of Directors** frequently lacks technical competence in water treatment and distribution, while operational managers struggle to translate complex infrastructure needs into strategic language that boards can understand.

<106>**Compliance** requirements span multiple domains — environmental protection, public health, drinking water quality, and increasingly, climate adaptation. This creates a challenging <113>**GRC** environment where water utilities must satisfy diverse

<134>**Regulatory Frameworks** while maintaining affordability for essential services. The tension between long-term infrastructure investment needs and short political cycles further complicates strategic planning.

<135>**Risk** management becomes particularly complex as water infrastructure faces aging assets, climate change impacts, and emerging contaminants. Traditional

<119>**Management Frameworks** often prove inadequate for addressing interconnected risks spanning decades. The sector's conservative <124>**Organizational Culture** can resist innovation, yet regulatory pressures demand continuous improvement in treatment technologies and service delivery methods.



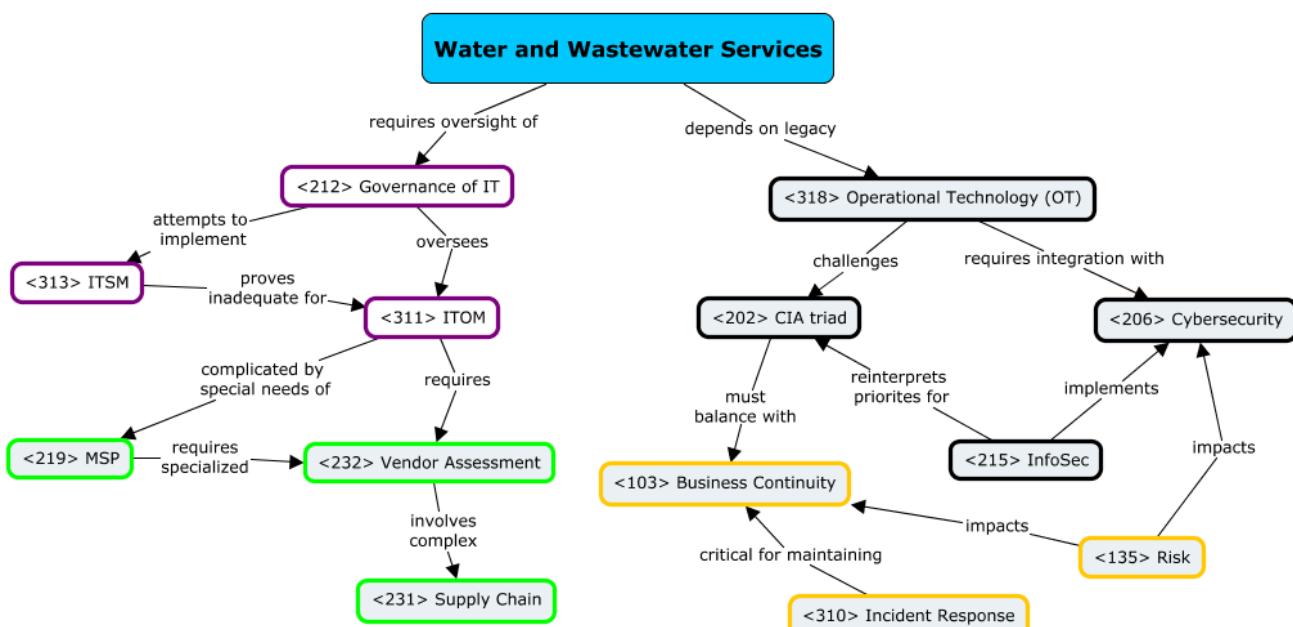
Energy and Utilities - Theme 2

Water and wastewater utilities face distinctive **<212>IT governance** challenges due to their **<318>Operational Technology** heritage and critical infrastructure status. **Governance of IT** in this sector must balance operational continuity with modernization pressures, as legacy **Operational Technology** systems controlling pumps, treatment processes, and distribution networks require careful integration with modern Information Security practices. The sector's IT landscape typically splits between operational control systems and administrative functions, creating governance complexities. **SCADA** systems managing water treatment cannot afford downtime, yet they often lack adequate **<206>Cybersecurity** protections due to historical air-gapping assumptions. **<313>IT Service Management** frameworks designed for business applications prove inadequate for industrial control systems where real-time performance and safety take precedence over standard **<323>Service Level Agreements**.

<135>Risk profiles in water utilities encompass both traditional IT risks and unique operational hazards. Cyberattacks on water systems can directly threaten public health, making **<103>Business Continuity** planning more complex than typical enterprise environments. The **<202>CIA Triad** requires reinterpretation, as availability often outweighs confidentiality concerns, yet integrity of treatment control data becomes life-critical.

Water utilities struggle with **<311>IT Operations Management** due to resource constraints and specialized skill requirements. Many rely on **<219>Managed Service Providers** for standard IT functions while maintaining internal expertise for operational systems. This hybrid approach complicates **<232>Vendor Assessment** processes and **<231>Supply Chain** security, as providers must understand both IT and water industry requirements.

<310>Incident Response procedures must account for cascading effects between IT failures and water service delivery. A compromised billing system affects customer relations, but compromised treatment controls threaten public safety. This dual-impact scenario requires integrated response strategies that traditional **IT governance** frameworks rarely address effectively.



Banking and Financial Services -

Theme 1

Niche: Credit Card Services

In the broader banking and financial services ecosystem, where capital allocation, risk management, and customer-centric innovation drive economic growth, Credit Card Services serve as a cornerstone, spanning from end-to-end transaction processing, fraud prevention, real-time fraud detection and end user relationship management.

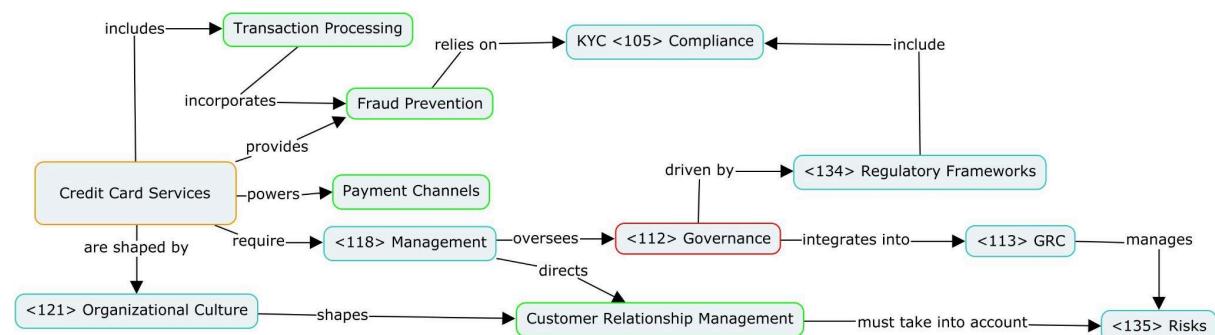
These types of services power traditional channels, such as e-commerce, points of sale terminals, as well as emerging use cases like in-vehicle digital payments, unlocking new monetization opportunities.

The niche brings its own challenges in terms of <112> Governance which is strongly influenced by <134> Regulatory Frameworks, including the Digital Operational Resilience Act (DORA), anti-money laundering (AML), and Know Your Customer (KYC - <105> Compliance) regulations. Institutions maintain robust governance structures, including <101> Audit committees and dedicated <106> Compliance departments, to oversee <135> Risks, both operational and credit risks. <113> Governance, Risk, and Compliance frameworks integrate these responsibilities, ensuring a stable approach to managing regulatory compliance, operational risks and strategic objectives, particularly in handling sensitive cardholder data.

<118> Management in Credit Card Services involves compliance monitoring and customer relationship management. The <121> Maturity of these practices is evident in the formalized structures, clear roles and continuous improvement mechanisms.

Operational activities, including card issuance, network tokenization (where standard, sensitive, credit card data is replaced with an unique and randomized token), transaction processing and fraud detection must leverage protocols such as 3D Secure (3DS) and its successor 3D Secure 2 (3DS2) to provide a seamless, secure and responsive experience that meets customer expectations and strict <106> Compliance requirements.

<121> Organizational culture also plays a fundamental role, shaping a standardization state of mind through shared values of risk awareness, ethics and a customer focused mentality, which is crucial for maintaining trust when handling transactions.



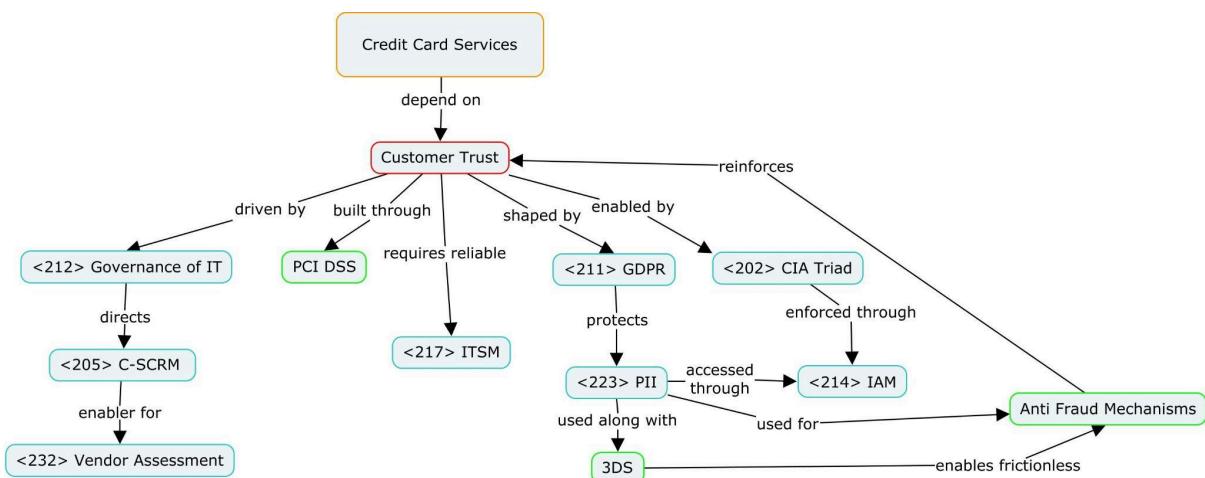
Banking and Financial Services - Theme 2

In the Credit Card Services niche, <212> Governance of IT establishes the vision that aligns technology with business goals, managing risks and ensuring compliance with regulations like Payment Card Industry Data Security Standard (PCI DSS) and <211> GDPR.

From a security standpoint, the integration of frameworks that enable the preservation of <202> confidentiality, integrity and availability is essential. This ideology is enforced when deploying mechanisms that rely on frictionless 3D Secure (3DS) as part of the authentication flow where <223> Personally Identifiable Information is transmitted, requiring careful integration with <214> Identity and Access Management to ensure secure access and to enable anti-fraud mechanisms.

This ideology around security and risk management has to extend through the <205> Cybersecurity Supply Chain Risk Management, especially when the integration relies on third-party vendors such as payment processors and fraud detection platforms. These third-party providers have to be governed by formal <232> Vendor Assessment procedures to evaluate their quality, potential risks and compliance.

The overall effectiveness of <212> Governance of IT in credit card services relies on the reliability and customer trust built through secure, compliant and user focused digital infrastructures. This is achieved by maintaining robust systems for authentication, fraud detection and service availability guided by <217> IT Service Management. Maintaining these philosophies support operational continuity and they also reinforce the importance of ethical and regulatory expectations that shape financial services.



Comparison 1 - GOVERNANCE

Manufacturing x Banking & Financial Services

Aerospace & Defense Manufacturing and Credit Card Services both operate in risky, high-stakes environments but show significantly different governance structures due to their industry needs. In A&D manufacturing, governance is shaped by long production cycles, public-private contracts, and multi-layered compliance frameworks such as ISO 9001 and 31000. Governance ensures traceability and resilience across complex, often globalized supply chains, highlighting risk governance as a key goal. Control structures here are deeply embedded in technical oversight, with tools like Product Lifecycle Management and SCADA systems being governance facilitators.

On the other hand, Credit Card Services in financial institutions operate under real-time pressure, where governance is shaped by regulatory responsiveness and customer trust. Frameworks such as DORA, AML, and KYC determine a governance model based on specific rules, with dedicated Audit Committees and Compliance Departments. The sector's maturity is visible through formalized GRC structures, continuous improvement mechanisms, and the use of protocols like 3DS2 for fraud prevention, highlighting how governance is included into the customer experience pipeline itself.

A&D's governance emphasizes strategic risk balancing, whereas Credit Card Services prioritize operational resilience and regulatory fidelity. With A&D's governance leaning on long-term oversight and technical traceability, and CCS' governance thriving on organizational agility and cultural alignment with ethical and risk-aware values, these distinctions end up illustrating how governance frameworks adapt to each industry's complexity, speed, and stakeholder pressures.

Manufacturing x Energy and Utilities

As mentioned before, Aerospace & Defense (A&D) Manufacturing relies on mature governance structures centered around technical oversight, agreement with international standards, and managing long production cycles in highly secure environments. Its governance is designed to ensure traceability, risk containment, and contractual integrity, especially in cross-border, defense-linked contexts.

The Energy and Utilities sector, while similarly high-stakes, presents a broader governance landscape. It must balance critical infrastructure management with public service obligations, evolving environmental policies, and growing digital complexity. Governance here is not only about operational stability but also about aligning with climate goals, market liberalization, and cybersecurity mandates like the NIS2 directive. Boards handle complex trade-offs between sustainability, affordability, and reliability, often in publicly accountable or hybrid ownership settings.

Both sectors depend heavily on systems like SCADA and face rising cyber risks, but while A&D governance is internally focused and pushing innovation, energy governance is policy-facing and shaped by geopolitical and consumer dynamics. It also requires quick and flexible adaptation in different areas, from renewables to water services.

In sum, A&D's governance emphasizes precision and resilience within controlled industrial ecosystems, whereas the Energy sector must govern for public trust, strategic flexibility, and cross-sector interdependence. Essentially, an industry's mission and its stakeholders interests are what drive the design and boundaries of its governance.

Comparison 2 - IT MANAGEMENT

Manufacturing x Banking & Financial Services

Effective IT Management in both **Manufacturing (A&D)** and **Banking (Credit Card Services)** hinges on balancing innovation with risk mitigation. Both sectors prioritize **<212> Governance of IT**, though their approaches diverge. In A&D, national security concerns demand strict **<234> Zero Trust models** and tightly enforced **<214> IAM**, while banking institutions deploy similar IAM controls to safeguard **<223> PII** under the **<202> CIA triad** and **<211> GDPR**.

Data governance plays a vital role across both industries. Manufacturing emphasizes **<209> Data Residency** and **<210> Data Retention** for compliance and contractual obligations, whereas banking integrates **<227> PIMS** and **<221> Opt-in mechanisms** to maintain customer trust. **<228> Privacy-by-design** is embedded into both sectors' digital infrastructure strategies to proactively mitigate privacy risks.

Third-party risks are another shared concern. Both industries leverage **<205> C-SCRM** and apply formal **<232> Vendor Assessment** procedures, though manufacturers additionally rely on **<230> SBOMs** to map out software components critical in embedded systems. To detect and respond to threats, both sectors increasingly deploy **<218> MDR** solutions, reflecting the growing importance of continuous monitoring. The sectors also differ in service orientation, banks lean on **<217> ITSM** and sometimes **<219> MSPs** to ensure always-on customer service, while manufacturers integrate IT with OT systems to secure production environments.

Ultimately, while one sector protects financial stability and user data, and the other defends intellectual property and physical infrastructure, both share a reliance on strategic, regulation-aware IT Management grounded in resilience, compliance, and evolving threat landscapes.

Manufacturing x Energy and Utilities

Both **Manufacturing (A&D)** and **Energy & Utilities** sectors face rising complexity in IT Management, driven by critical infrastructure demands and digital transformation. Cyber threats are a shared concern, but while A&D emphasizes **<234> Zero Trust** and **<214> IAM** to protect classified data and designs, water utilities contend with legacy **<318> Operational Technology** and air-gapped **<206> Cybersecurity gaps** that weren't built for today's threat landscape.

Both sectors rely on **<205> C-SCRM** and **<232> Vendor Assessment**, though A&D additionally uses **<230> SBOMs** to track third-party software, while utilities demand providers understand both IT and physical infrastructure. **<218> MDR** tools are gaining traction across both, supporting fast **<310> Incident Response** especially where downtime risks physical harm. A&D firms process sensitive **<223> PII**, requiring **<211> GDPR** compliance and strong **<210> Data Retention** policies, while utilities must protect customer and billing data under evolving privacy standards. Both benefit from **<228> Privacy-by-design** and clear **<203> Consent Mechanisms**.

However, IT priorities diverge, utilities prioritize availability under the **<202> CIA triad**, where a single failure impacts public health, while A&D may balance integrity and confidentiality more. Manufacturing leans on **<212> Governance of IT** to align systems with defense strategies, whereas utilities struggle to fit **<217> ITSM** into safety-critical OT systems, often turning to **<219> MSPs** for routine IT tasks.

Ultimately, both sectors require tailored IT Management strategies, where resilience, compliance, and context-specific risks shape every digital decision.

Group 127:
João Pires (99090) Rui Costa (99120)
Stefan Knutsen(99123) Chonghe Cui(108077)

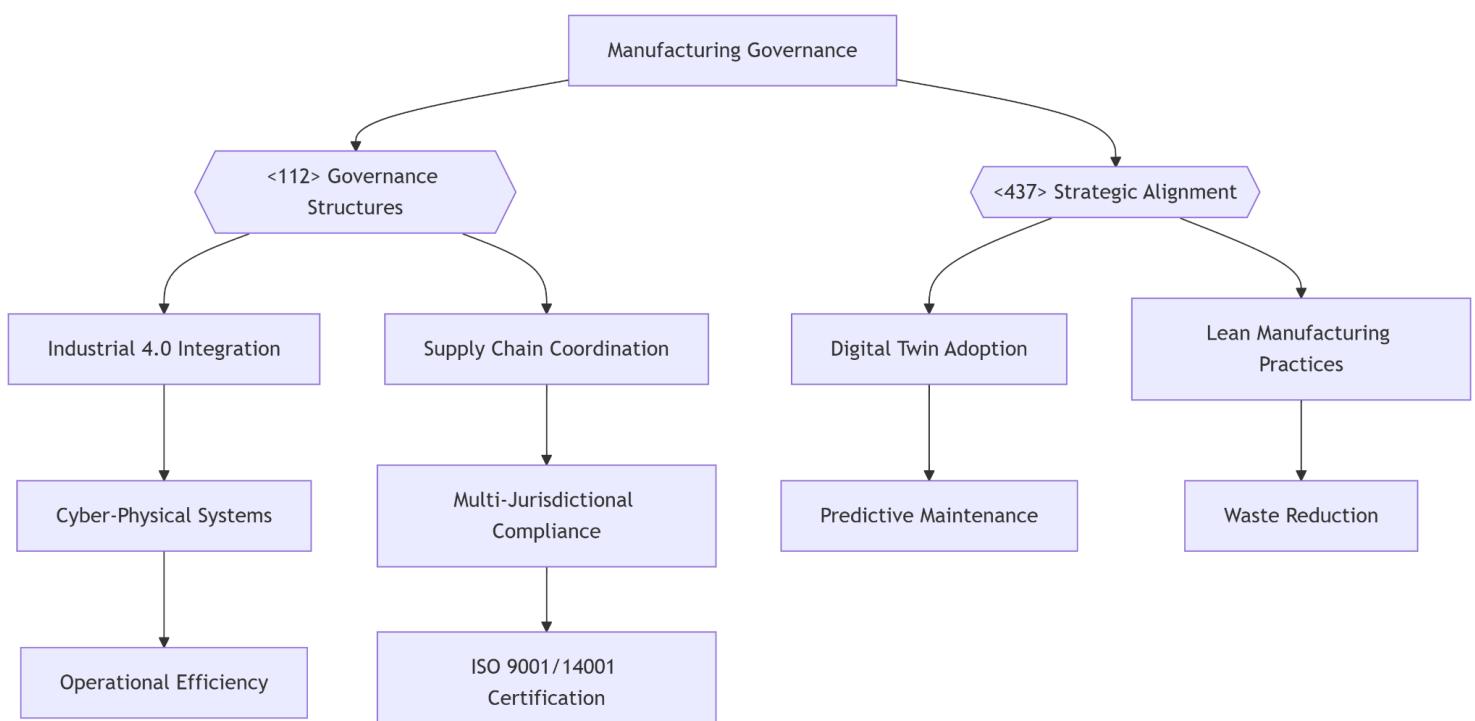
1 - Manufacturing: Governance

The **Manufacturing** industry covers a broad spectrum of activities that transform raw materials into finished goods, including sectors like automotive, aerospace, electronics, and pharmaceuticals. As production processes become increasingly digitised through Industry 4.0 technologies, the sector faces growing complexity in operations, supply chains, and technology integration.

The Manufacturing sector's **Governance** is shaped by the integration of Industry 4.0 technologies, which demand alignment between **Corporate Strategy** and **Operational Agility**. Large enterprises adopt formal governance frameworks, with **Boards of Directors** overseeing compliance with standards like ISO 9001 (quality) and ISO 14001 (environmental), while smaller manufacturers rely on lean methodologies to optimize workflows.

Strategic Alignment is critical in balancing capital-intensive investments (e.g., smart factories) with sustainability goals. For example, digital twins enable predictive maintenance, reducing downtime and **Operational Risk**. Governance also extends to supply chains, where multi-jurisdictional compliance ensures adherence to labor, safety, and environmental regulations across global networks.

Key challenges include reconciling legacy systems with automation and addressing workforce upskilling gaps. Stakeholders such as suppliers, regulators, and technology vendors play pivotal roles in shaping **Governance Maturity**, particularly in high-risk subdomains like pharmaceuticals (process manufacturing) and aerospace (discrete manufacturing).



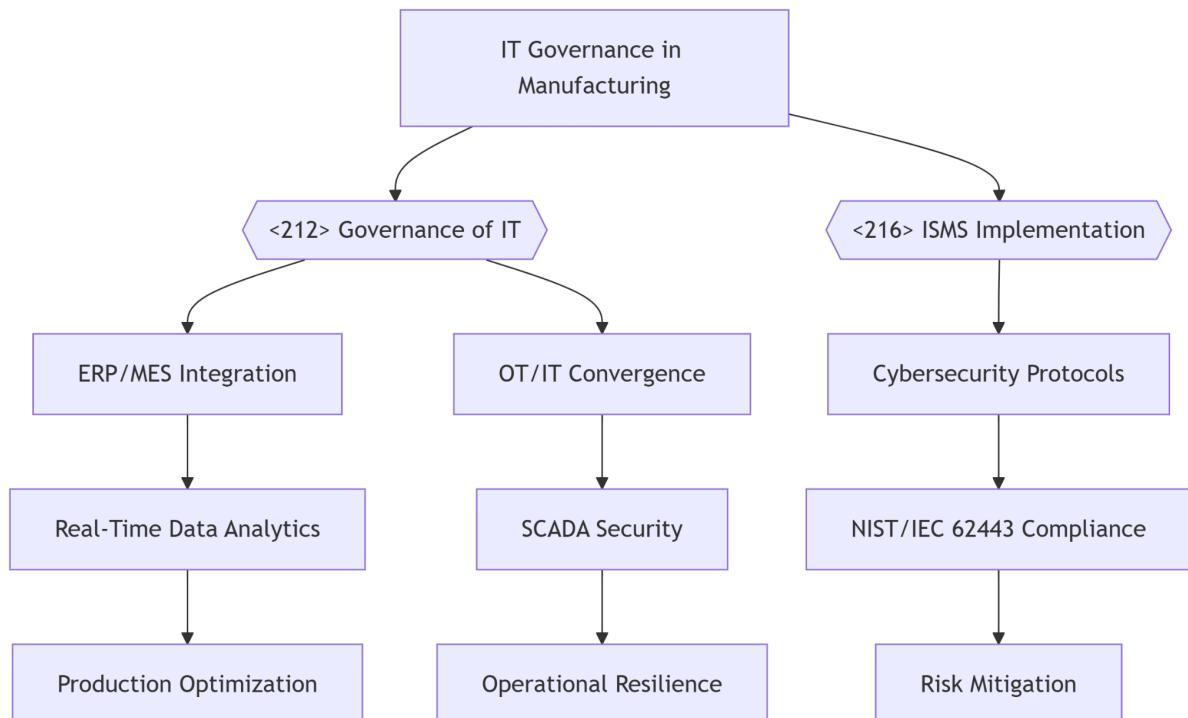
1 - Manufacturing: IT Management

IT Governance (<212>) in **Manufacturing** prioritizes the secure integration of **Enterprise Resource Planning (ERP)** and **Manufacturing Execution Systems (MES)** to enable real-time production monitoring. Industrial IoT and cyber-physical systems (<1.4>) blur the line between **Operational Technology (OT)** and **IT**, necessitating frameworks like NIST SP 800-82 to secure SCADA systems and prevent cyberattacks.

Large manufacturers deploy **Information Security Management Systems (ISMS) (<216>)** to safeguard intellectual property and production data, aligning with standards such as IEC 62443. Smaller firms, however, often lack internal IT expertise, relying on **Managed Service Providers (<219>)** for cloud infrastructure and patch management (<319>).

Key IT management challenges include:

- **Data Governance:** IoT-generated data (e.g., machine telemetry) requires ownership clarity and GDPR (<211>) compliance.
- **Interoperability:** Legacy machinery struggles to interface with modern analytics platforms, creating technical debt (<325>).
- **Connectivity Gaps:** Rural facilities face bandwidth limitations, hindering cloud adoption (<404>) and real-time decision-making.
- Public initiatives like Germany's Plattform Industrie 4.0 exemplify **Strategic Alignment (<437>)** between policy and digital infrastructure investment, fostering sector-wide **IT Maturity (<121>)**.



2 - Energy and Utilities: Governance

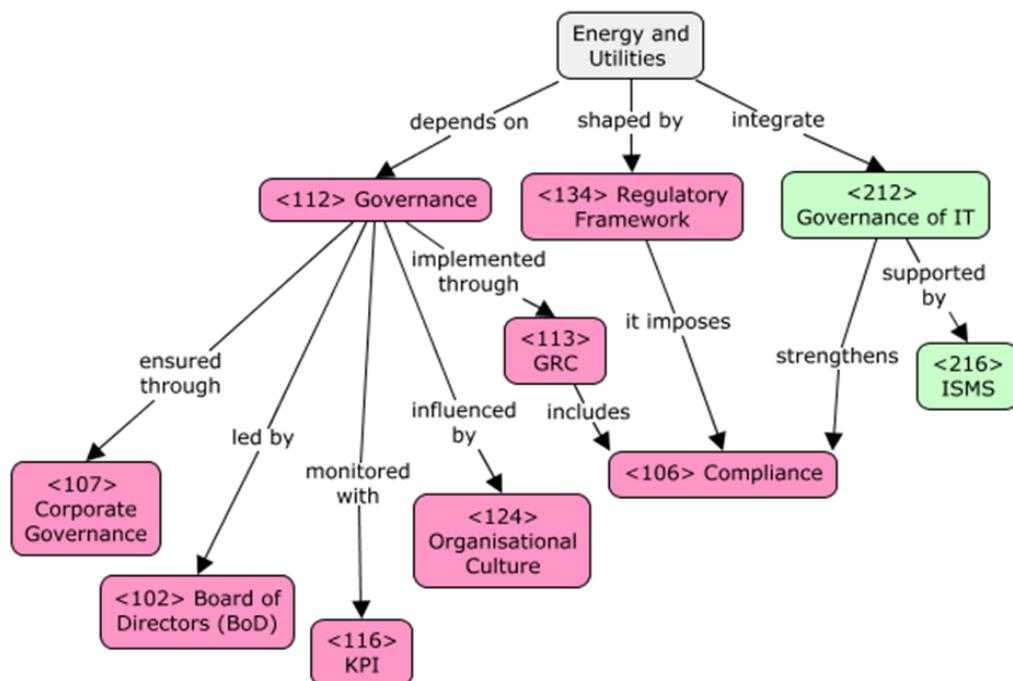
The **Energy and Utilities** industry, responsible for the production, distribution, and commercialization of electricity, gas, water, and related infrastructure services, faces complex **Governance** challenges due to its critical importance to public health, the economy, and national security. With market liberalization and the energy transition, new business models have emerged, requiring more robust **Corporate Governance** structures. The **Board of Directors (BoD)** and Top Management are responsible for ensuring alignment between the organizational mission, ethical values, sustainability, innovation, and supply security, relying on **KPIs** to monitor performance.

The **GRG (Governance, Risk and Compliance)** approach is essential to manage operational risks (such as technical failures and cyberattacks), market risks (volatility and supply chains), regulatory risks (changes in climate policies and public procurement), and geopolitical risks (dependence on imports and critical resources). Compliance extends to areas such as health and safety, environment, data protection (e.g., GDPR), and ESG reporting.

The sector operates under a demanding **regulatory framework**, notably EU directives such as the Clean Energy Package, the Renewable Energy Directive, and NIS2, as well as technical standards from ISO and IEC, which are fundamental for certification and the adoption of Management System Standards (MSS).

Digitalization brings a strong dependence on systems such as SCADA, smart grids, trading platforms, and asset management, requiring effective information and technology governance (**Governance of IT**). Security is reinforced through systems like **ISMS**, IAM, incident response, patch management, and practices based on the CIA triad, ensuring business continuity and cyber-resilience.

Finally, an **organizational culture** oriented toward **compliance**, ethics, and innovation is essential to responsibly integrate new technologies, promoting digital maturity and the strategic use of solutions such as AI governance and BPM. Thus, effective governance is crucial to ensuring a sustainable, resilient energy sector aligned with the public interest.



2 - Energy and Utilities: IT Management

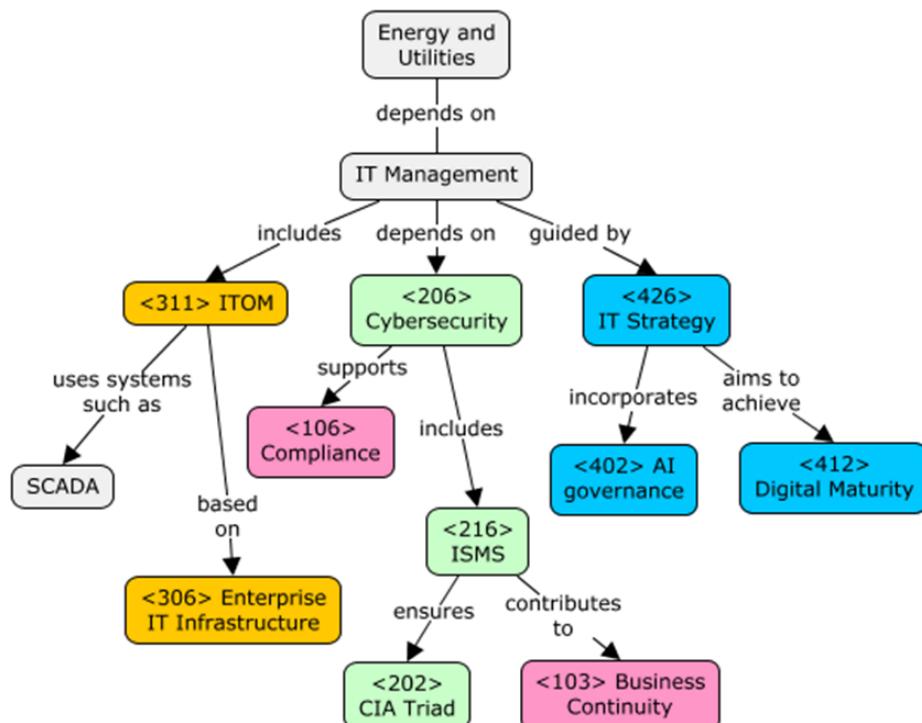
The **Energy and Utilities** industry is increasingly reliant on digital technologies to ensure efficiency, security, and continuity of its essential services. The growing digitalization of the sector demands a solid **IT Management** approach that ensures alignment between technological infrastructure and the strategic objectives of organizations. Systems such as **SCADA**, smart grids, energy trading platforms, customer portals, and asset management software have become critical to operations, requiring rigorous **IT Operations Management (ITOM)**, monitoring, and preventive maintenance practices.

The sector faces high **cybersecurity** risks and is classified as critical infrastructure under the NIS2 Directive and the EU Cybersecurity Act. Therefore, IT management must include a robust **Information Security Management System (ISMS)**, with access control (IAM), vulnerability management, patch management, and incident response capabilities. These elements ensure the protection of critical information and systems based on the **CIA triad** principles (Confidentiality, Integrity, and Availability).

The complexity of infrastructures and the need for operational resilience require practices such as redundancy, failover, and IT Service Continuity Management (ITSCM), ensuring **business continuity** even in the face of technical failures or cyberattacks. The management of Operational Technology (OT), often legacy-based, should be integrated with **Enterprise IT Infrastructure**, promoting the convergence of information technology and operational technology.

With the energy transition and the focus on sustainability, there is a growing use of AI for consumption forecasting, network optimization, and resource management. This requires **AI governance**, analytical capabilities, and well-defined digital capability strategies. The sector's **digital maturity** also involves the adoption of Business Process Management (BPM), Enterprise Architecture (EA), and frameworks such as the Cloud Adoption Framework (CAF), which are essential for managing hybrid and cloud environments securely and efficiently.

Finally, **IT Strategy** must be integrated into the overall organizational strategy, ensuring that technology investments contribute to digital transformation, innovation, and sustainability without compromising security, **compliance**, or service continuity. Effective IT management is therefore fundamental to the resilient and intelligent future of the energy sector.



7 - Agriculture and Farming: Governance

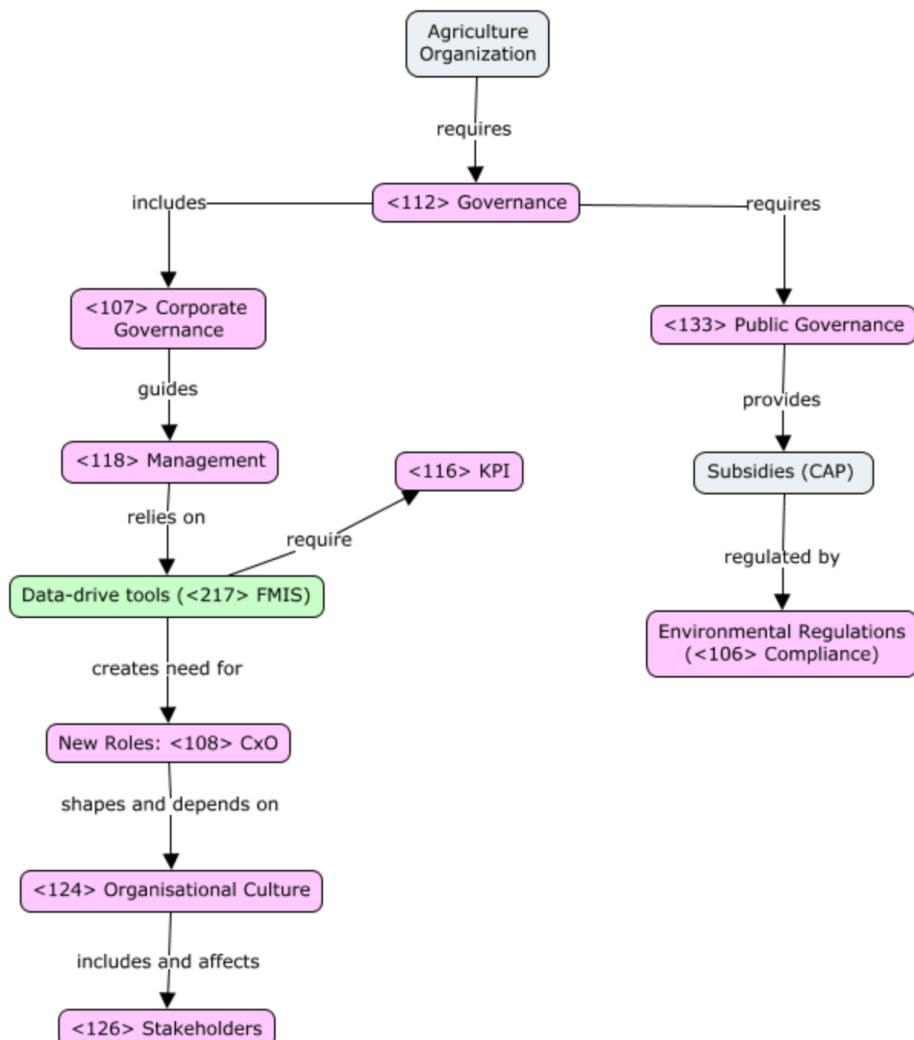
The **Agriculture and Farming sector** includes a diverse range of activities, from smallholder farms to large-scale **agribusinesses**. It is increasingly shaped by digital technologies such as **precision farming, IoT sensors, and satellite imagery**, which are transforming how food is produced, managed, and distributed across both local and global contexts.

Precision agriculture has redefined how farming organizations structure their **Management and Governance Systems**. Traditionally characterized by decentralized, family-run farms, the sector now includes highly structured agribusiness entities that manage thousands of hectares using real-time data. **Governance** in this space must adapt to diverse operational scales—supporting both **small-holders and corporations**.

Public Governance plays a critical role via subsidy schemes like the EU's **CAP**, which incentivize **digital transformation** and sustainable practices. Governance models within cooperatives often prioritize democratic decision-making, yet require compliance with complex environmental and traceability regulations.

Management practices have shifted from intuition-based decisions to data-supported strategies. **Farm Management Information Systems (FMIS)** are used to coordinate irrigation, fertilization, and harvesting, requiring new managerial roles with both agronomic and digital expertise. Organizations must balance operational efficiency with **Regulatory Compliance**, ethical land use, and environmental stewardship, all while navigating a fragmented but increasingly digitized sector.

Stakeholder roles are also evolving. Farmers are no longer only cultivators—they are data consumers and decision-makers. **Governments** set frameworks and offer digital incentives. Technology providers become strategic partners, and consumers demand **traceability, sustainability, and ethical production**. All these actors contribute to a multi-layered governance environment that must reconcile **economic, technological, and environmental priorities**.



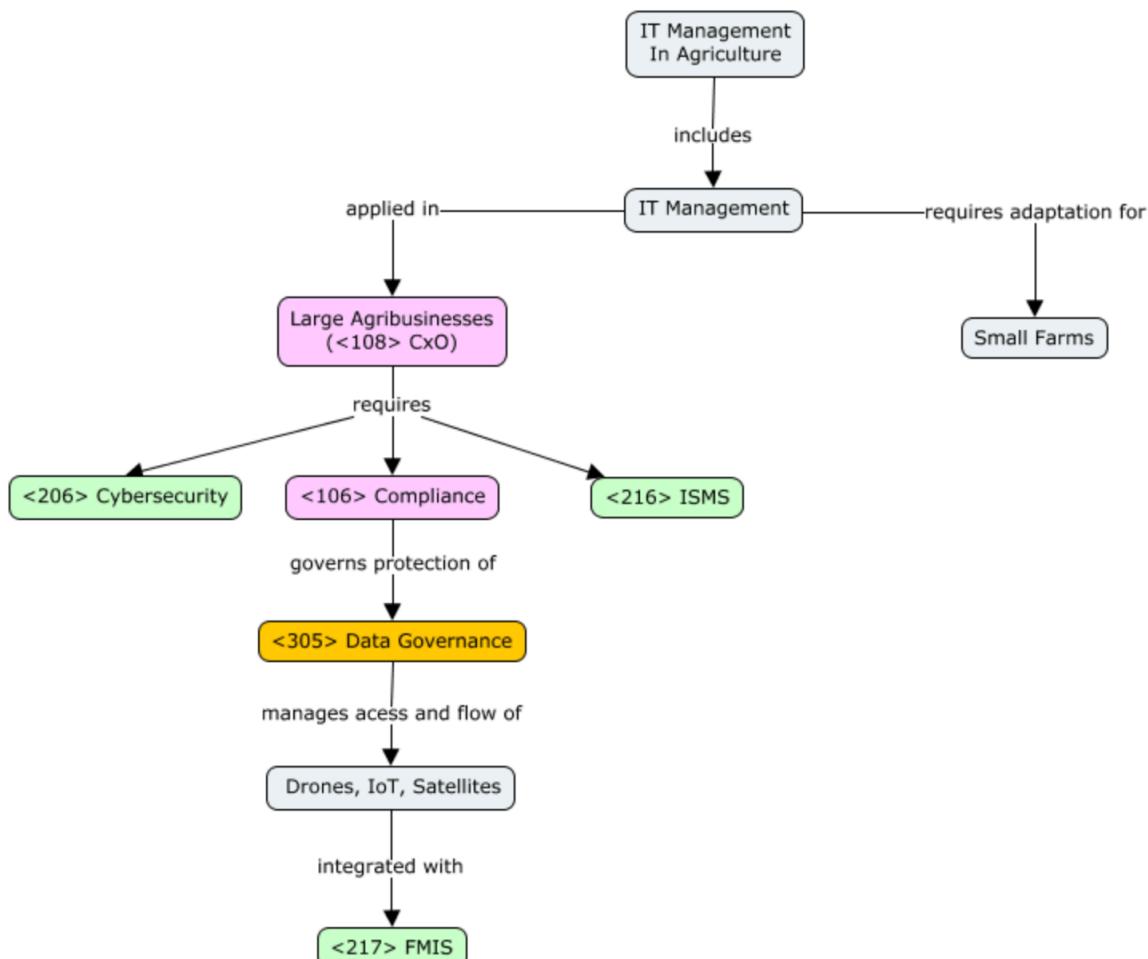
7 - Agriculture and Farming: IT Management

The **Governance of IT** in precision agriculture varies significantly depending on the **organizational scale** and the level of infrastructure maturity. Large **agribusinesses** tend to adopt formalized IT governance frameworks, featuring defined roles such as **CTOs**, dedicated in-house data teams, and established **cybersecurity** protocols. In contrast, smaller farms often lack the resources for internal IT departments and rely instead on cooperative-led support or third-party consultants, resulting in more fragmented **governance structures**.

A central issue across both large and small operations is **data governance**. Technologies used in precision agriculture—such as **drones, IoT sensors, and satellite imagery**—generate large volumes of sensitive data concerning soil conditions, crop performance, yield estimates, and geospatial variables. Managing this data requires careful evaluation of software vendors, particularly regarding **data ownership, portability, compliance** with food safety regulations, and protection against cyber threats. These concerns underscore the need for robust governance models that can adapt to various operational contexts.

Closely linked to governance is the domain of **IT management**, which involves the day-to-day operation of systems, ensuring they are secure, up-to-date, and interoperable. Tools like **FMIS** must connect seamlessly with **machinery, environmental sensors**, and databases. This demands **IT expertise** that is often lacking in rural or resource-constrained areas, creating a gap between digital potential and actual implementation.

Adding to this complexity is the persistent challenge of **connectivity**. Many rural areas suffer from **inadequate internet infrastructure**, which severely limits access to **cloud-based** services and real-time data processing. In this context, public investment in digital infrastructure and targeted policies becomes critical to enable the broad adoption of **IT systems**. Moreover, low levels of **digital literacy** among farmers highlight the importance of **training programs** and technical support, which are essential to ensure effective and sustainable use of agricultural technologies.



Governance: Energy and Utilities VS Agriculture and Farming

Governance in the agriculture and farming sector differs fundamentally from that of the energy and utilities industry in its structural formality, regulatory drivers, and technological integration. While both sectors are undergoing digital transformation and operate under growing public scrutiny, the energy industry embodies a highly institutionalised governance model centred around risk management, regulatory compliance, and infrastructure resilience. In contrast, agriculture presents a more fragmented landscape, combining traditional, often informal governance practices with emerging digital oversight, shaped significantly by public incentives and cooperative values.

Governance in the energy sector is characterised by a **top-down, compliance-driven model**, where Boards of Directors and executive leadership operate within tightly defined legal and regulatory frameworks, reinforced by binding standards like ISO/IEC 27001 and directives such as NIS2. Decision-making is formalised, performance is tracked through KPIs, and risks — whether operational, financial, or geopolitical — are proactively modelled and managed through integrated GRC structures. In contrast, governance in agriculture is more **bottom-up and structurally fragmented**. Smallholders often follow informal norms or cooperative rules, while larger agribusinesses may adopt more formal governance, but typically without the regulatory intensity seen in energy. Rather than driving digital change, governance in agriculture often trails behind it. Tools like FMIS are adopted for operational needs even when oversight mechanisms for data, compliance, or environmental accountability are still developing. Whereas energy governance leads with compliance and anticipates risk, agricultural governance tends to emerge more adaptively, shaped by decentralised actors and public incentives rather than central enforcement.

Another key difference lies in the **role of regulation as a driver**. In energy, regulation shapes governance architecture directly: compliance is not only enforced but fundamental to market access and reputation. In agriculture, regulation is more often incentivised than mandated, with tools like the EU's CAP providing funding contingent on compliance with sustainability goals. This creates a governance model that is less about institutional enforcement and more about **negotiated alignment between public goals and private practices**.

Overall, the energy sector's governance is purpose-built to manage risk, deliver reliability, and assure societal trust. Agriculture's governance, by comparison, must constantly navigate heterogeneity, balancing democratic values, environmental demands, and digital potential with less formal structure and weaker enforcement levers. Where energy is governed through obligation, agriculture is governed, more often, through adaptation.

IT Management: Energy and Utilities VS Agriculture and Farming

The agriculture and energy sectors differ sharply in their approach to IT management, primarily due to their structural complexity, regulatory obligations, and levels of digital maturity. In energy, IT management is not just a support function, it is an operational backbone. In agriculture, however, IT management is still emerging as a strategic concern, especially outside large-scale agribusinesses.

A core distinction lies in **infrastructure centrality**. In energy, digital systems such as SCADA and smart grids are mission-critical and fully integrated into organisational workflows. Their failure can halt national services. Consequently, IT management is comprehensive, proactive, and risk-oriented. By contrast, agriculture's digital systems (like FMIS, sensors, satellite feeds) are often implemented gradually and vary greatly across farm sizes. Here, IT management tends to be reactive and uneven, shaped by connectivity gaps and limited internal capacity.

The two industries also diverge in **cybersecurity posture**. In energy, security is embedded into IT management from the ground up, reflecting the sector's critical infrastructure status. This includes full deployment of IAM, patch management, and incident response protocols. In agriculture, cybersecurity is often a secondary concern, despite rising threats related to drone data, GPS spoofing, or crop analytics. Protection mechanisms are fragmented or absent, especially among resource-constrained actors.

Even where both sectors embrace **data-driven optimisation**, their execution differs. Energy uses predictive analytics and AI within mature IT architectures to optimise network performance and energy consumption. These initiatives are supported by enterprise-wide data strategies and governance frameworks. Agriculture, on the other hand, shows a wider implementation gap. While precision tools generate massive datasets, many farming operations struggle to integrate or govern them effectively, constrained by digital literacy, vendor lock-in, and the absence of interoperable systems.

In short, energy exemplifies **high IT governance maturity**, with IT management **tightly coupled to risk, resilience, and innovation**. Agriculture reveals a **fragmented, transitional landscape** where IT management is **uneven, dependent on scale, and support ecosystems**. This contrast highlights the urgent need for public investment and professionalisation in agricultural IT to close the gap between potential and practice.

Governance: Agriculture and Farming VS Manufacturing

Governance in agriculture and manufacturing diverges sharply in its structure, drivers, and approach to technological integration. While both sectors are undergoing digital transformation, manufacturing tends to approach governance as a strategic enabler, whereas agriculture often treats governance as a reactive or adaptive layer shaped by external incentives.

One of the most notable contrasts lies in the **origin of governance pressure**. In manufacturing, governance is largely **internally driven**—tied to competitiveness, productivity, and risk management. Boards oversee alignment with corporate strategy, standards like ISO 9001, and performance through measurable KPIs. In agriculture, governance is **externally shaped**, particularly by public subsidies like the EU's CAP, which encourage sustainability and digitalisation but offer more fragmented enforcement. Agricultural governance is, therefore, more dependent on policy frameworks and less tightly coupled to strategic execution.

Formality and standardisation also differ significantly. Manufacturing relies on well-established frameworks and certification regimes, making compliance a structured and auditable process across global supply chains. Agriculture, in contrast, features high variability: large agribusinesses may adopt formal systems, but smallholders and cooperatives often operate under informal or community-based rules. This creates a governance patchwork where maturity levels vary widely, even within the same country or region.

Finally, both sectors face **multi-stakeholder complexity**, but respond differently. Manufacturing builds governance around supply chain control and regulatory harmonisation across jurisdictions. Agriculture must balance a more diverse and less structured set of actors—farmers, cooperatives, policymakers, consumers—with evolving expectations around traceability, sustainability, and ethics. The result is a sector where governance must flexibly mediate between formal regulation and traditional, often informal, operating norms—something far less common in the more centralised governance environment of manufacturing.

In short, while manufacturing governance is **centralised, standardised, and strategy-driven**, agriculture's governance remains more **decentralised, adaptive, and externally influenced**, reflecting each sector's distinct structural realities and institutional pressures.

IT Management: Agriculture and Farming VS Manufacturing

IT management in agriculture and manufacturing reveals contrasting levels of structure, integration, and sectoral coordination. While both industries are embracing digital transformation, manufacturing exhibits a more mature, standardised, and centrally managed approach, whereas agriculture remains fragmented, often reactive, and heavily dependent on external support.

One of the most evident differences is **how IT is embedded in core operations**. In manufacturing, IT is inseparable from production. Systems like ERP and MES are integrated into daily workflows, and data from IoT devices feeds directly into performance optimisation and predictive maintenance. IT management in this context is tightly coupled with strategic goals and operational efficiency. Agriculture, by contrast, often treats IT as an add-on or support function. While tools like FMIS (Financial Management Information Systems) offer significant value, they are frequently deployed without comprehensive integration into organisational processes, especially among small to mid-sized farms.

Resource allocation and expertise also diverge significantly. Manufacturing firms, particularly larger ones, typically maintain in-house IT teams, follow formal security frameworks like Information Security Management Systems, and invest in long-term infrastructure. Even smaller manufacturers often compensate through Managed Service Providers. In agriculture, IT management capacity is highly uneven. Large agribusinesses may mirror industrial practice, but the majority of farms lack internal IT staff and rely instead on cooperatives or vendors, leading to inconsistent oversight, slower adoption, and minimal customisation.

Another key difference is the **handling of interoperability and legacy systems**. Manufacturing often faces technical debt as older machinery clashes with modern analytics platforms, but this issue is actively managed through digital retrofitting and standardised integration efforts. Agriculture faces a similar challenge with heterogeneous equipment and sensor systems, yet often lacks the institutional or technical capacity to address it at scale, resulting in isolated systems and underused data.

Finally, **sector-wide coordination and infrastructure investment** show a clear gap. Manufacturing benefits from national strategies and industry platforms that align policy, funding, and technological development. In contrast, agriculture depends more on scattered public incentives and policy-driven initiatives like CAP, which promote digitisation but do not systematically build IT management capacity. This leaves agriculture more exposed to uneven implementation, vendor dependency, and infrastructural bottlenecks, especially around connectivity in rural areas.

In sum, IT management in manufacturing is **proactive, standardised, and aligned with business strategy**, while in agriculture, it remains **reactive, fragmented, and reliant on external structures**, making the gap not just technical, but organisational and systemic.

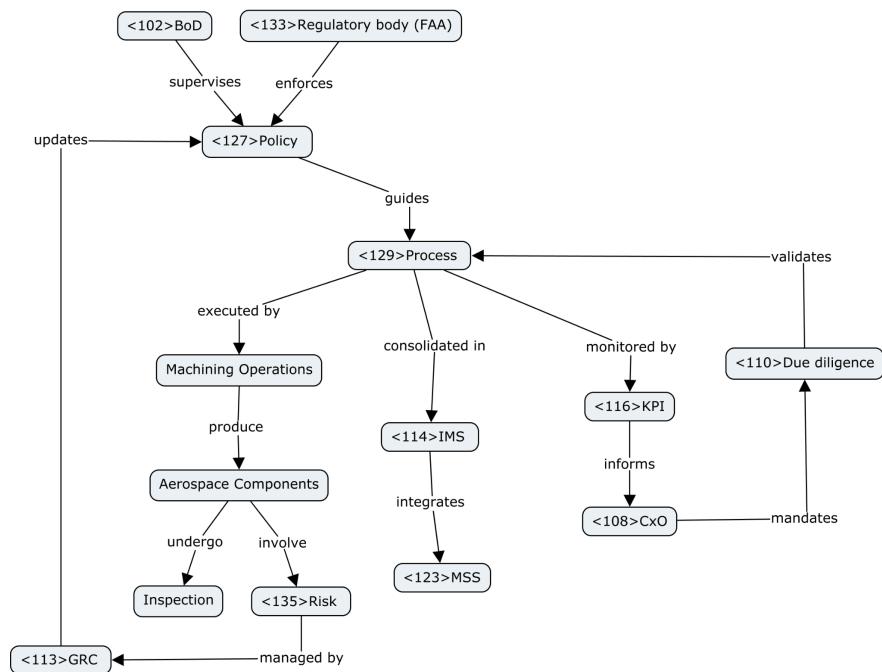
Industry 1: Manufacturing in aerospace industry + Theme 1

Aerospace components manufacturing focuses on the precision design, fabrication, and assembly of critical parts—such as turbine blades, control actuators, and avionics housings—used in aircraft and spacecraft. This niche operates under stringent regulations (e.g., FAA, EASA), demands ultra-tight tolerances, and relies on complex, globally dispersed supply chains. Manufacturers must ensure full traceability of every material batch and process step, maintain rigorous quality controls, and integrate advanced digital systems to validate performance and safety throughout each component's lifecycle.

In the aerospace components manufacturing niche, the governance framework must make sure every part meets strict safety, quality, and regulatory rules. <102>BoD sets up <127>Policy that follow <133>Regulatory body requirements like those from the FAA and EASA. These policies become standard <129>Process steps, from inspecting raw materials to final heat treatments, with roles and responsibilities laid out using <131>RACI. Because getting parts certified is expensive and mandatory, any slip in following these steps raises <135>Risk, a failed certification halts production, forces costly rework, and creates delays that damage both revenue and reputation.

To keep these processes consistent, an <114>IMS integrates several <123>MSS such as ISO 9001 and AS9100. Performance is tracked with <116>KPI—for example, non-conformity rates and cycle times—enabling the <108>CxO to decide where to invest in new machines or training. Overall <121>Maturity is evaluated through <101>Audit, which also confirms that <110>Due diligence when selecting suppliers meets stringent aerospace criteria.

Finally, <113>GRC unifies <135>Risk management and <106>Compliance controls into one system, covering design reviews, in-process inspections, and document approvals. A <124>Organisational Culture based on <111>Ethical Values ensures that quality and safety are never compromised for higher profits. Audit findings data then drive updates to policies and processes, creating a continuous cycle of improvement.



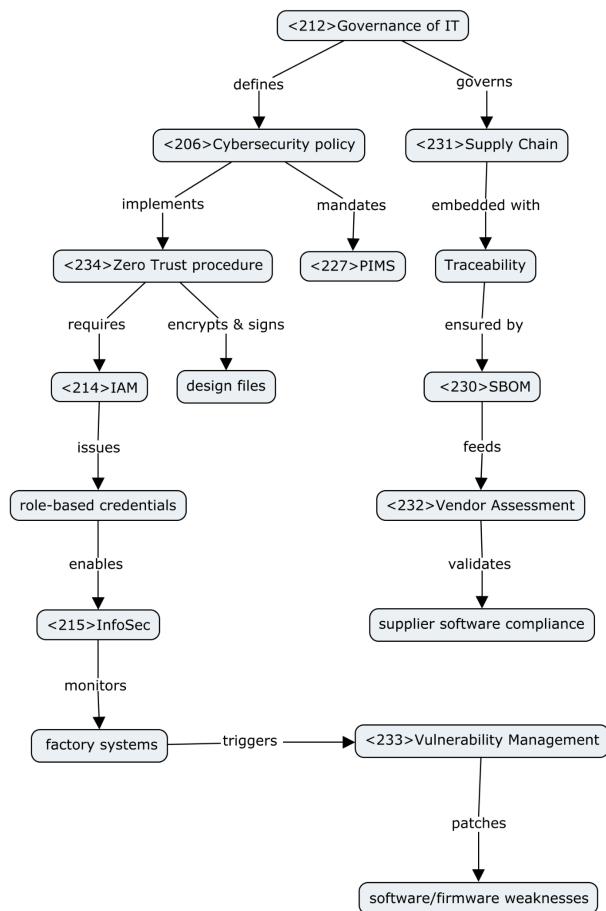
Industry 1: Manufacturing + Theme 2

In the aerospace components niche—where every precision part, from turbine blades to control actuators, must be tracked from raw material to final certification—a clear <212>Governance of IT framework sets the rules for how design software, digital testing environments, and shop-floor control systems are managed.

At its core is a custom <206>Cybersecurity program that protects sensitive design drawings and simulation data by encrypting files whenever they move or sit in storage, and by requiring each file to be digitally signed before it can be used in production planning. Access to these systems follows a <234>Zero Trust approach: every connection—from an engineer opening a part file to a technician running machine-control software—must prove its identity before any data is shared.

<214>IAM issues temporary, role-based credentials so only authorized staff and approved partners can view or change designs. A dedicated <215>InfoSec team constantly watches both office networks and the factory floor for unusual activity, while <233>Vulnerability Management ensures that any discovered software or firmware weakness—whether in design workstations or machine controllers—is fixed without delay.

To guarantee full traceability, each component carries a cryptographically signed tag linked to a live parts register, <230>SBOM. Automated <232>Vendor Assessment checks confirm that suppliers' firmware and software match the approved versions. Finally, all project data and test records are stored under a <227>PIMS to meet <211>GDPR and export-control requirements.



Industry 3: Retail and Digital Commerce + Theme 1

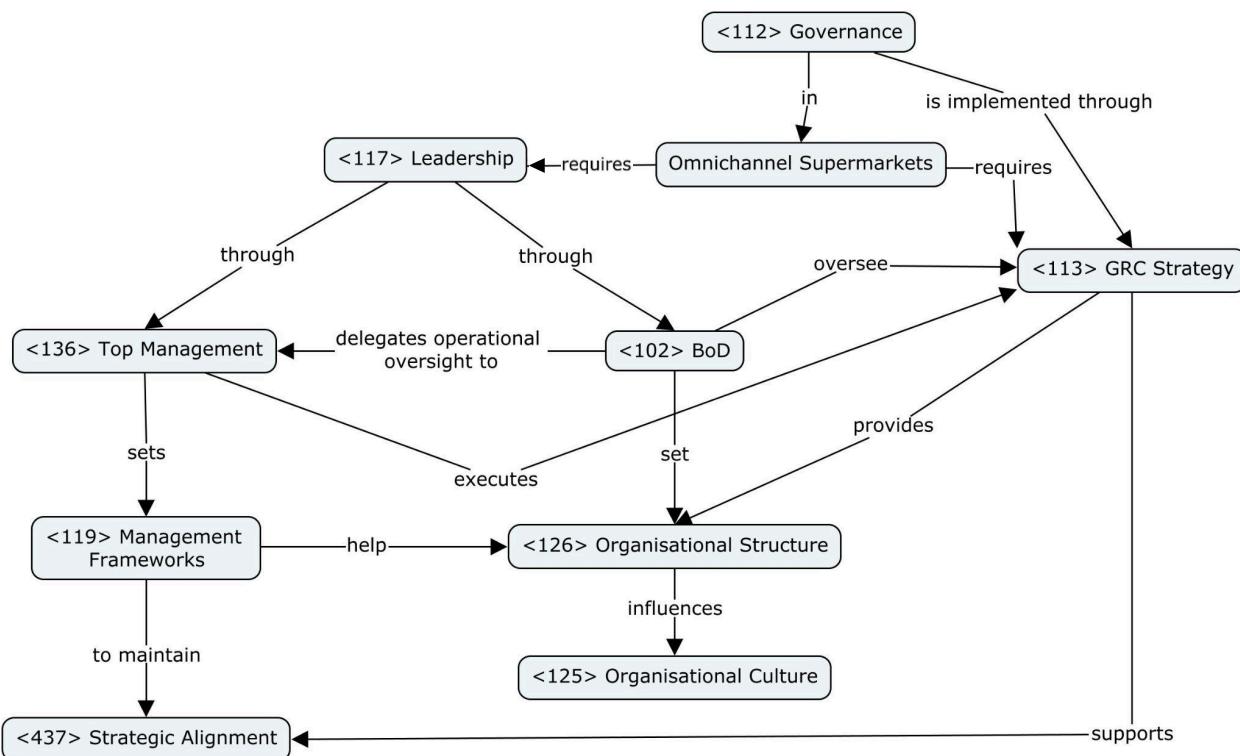
Retail connects producers to consumers through diverse formats—from stores to digital platforms—across sectors like groceries, electronics, and fashion. Omnichannel supermarkets merge physical and digital retail, allowing seamless transitions between in-store shopping, mobile apps, and delivery. This model integrates logistics, marketing, payment, and customer service systems.

These organisations adopt layered structures to manage retail and IT operations. Strategic decisions are led by <136> Top Management and the <102> BoD, with digital leadership roles such as <108> CIO and CDO. <117> Strong Leadership is essential to balance rapid responsiveness with long-term capability building, especially when integrating legacy systems. Disjointed <126> Organizational Structure can create operational silos that hinder real-time inventory updates and marketing campaigns.

The <125> Organisational Culture in omnichannel retail is defined by customer centricity, experimentation, and responsiveness. Agile decision-making and <119> Management Frameworks like Lean or Balanced Scorecard help coordinate cross-functional teams and support <437> Strategic Alignment.

Cultural misalignment between online and store teams can lead to inconsistency and internal friction. For example, store teams may resist process digitisation if not involved in <117> Leadership decision-making.

Managing <113> GRC becomes complex across jurisdictions, aligning internal controls with complex compliance environments, especially when global platforms interface with local labour laws, tax frameworks, or advertising standards. Retailers face increasing pressure to meet <211> GDPR and DSA requirements, particularly on data transparency and <203> Consent Mechanisms.



Industry 3: Retail and Digital Commerce + Theme 2

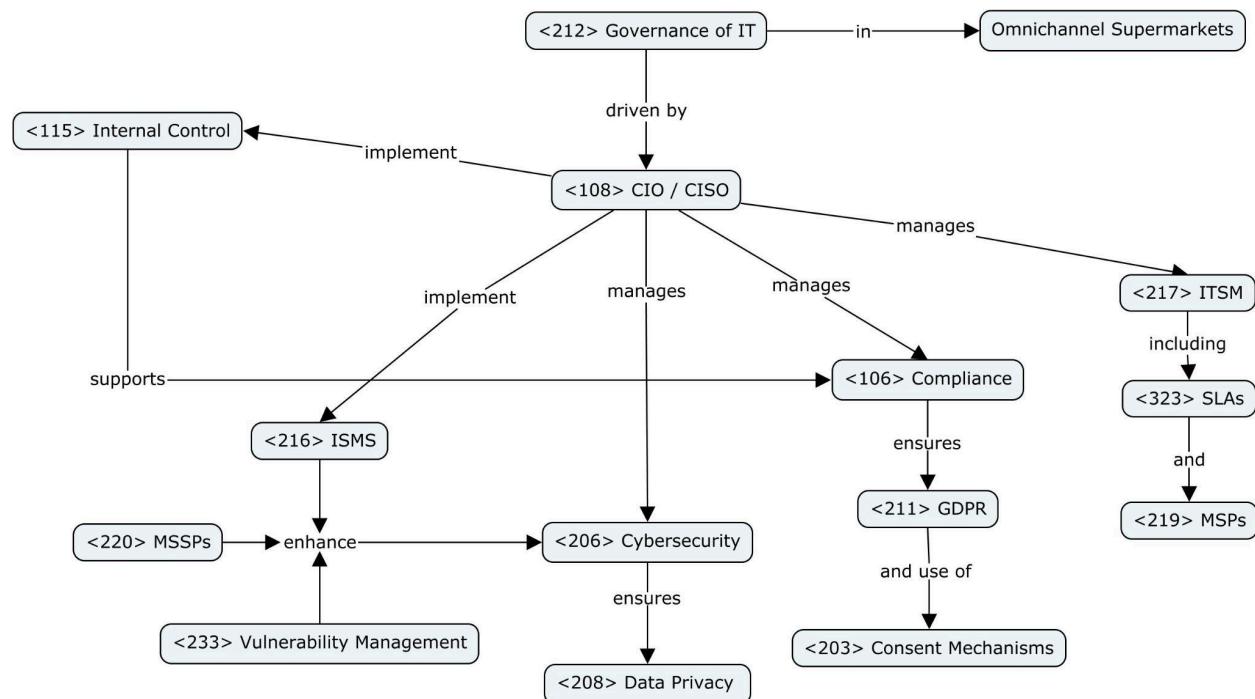
IT governance in the Omnichannel supermarket niche is critical to managing a digitally dependent ecosystem. Core systems include Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and electronic Point of Sale (ePOS) platforms. These must be integrated to support a seamless customer experience.

<212> Governance of IT is directed by <119> Strategic Frameworks, and executed by IT leadership—typically <108> CIOs and CISOs. Clear <127> Policies, <128> Procedures, and <115> Internal Controls help ensure information flows are secure, available, and compliant.

Supermarkets handle high volumes of sensitive <223> PII and financial data, increasing exposure to <206> Cybersecurity threats. Payment systems, user data, and behavioural analytics pipelines are all subject to <211> GDPR, <208> Data Privacy norms, and national security standards.

Supermarkets often deploy <216> ISMS, backed by <101> Audits and continuous <233> Vulnerability Management. Inadequate <227> PIMS implementation can compromise <228> Privacy-by-Design and <203> Consent Mechanisms obligations, which must be embedded in digital systems.

Commonly used IT Management Practices include the use of <323> SLAs with cloud providers, adoption of <217> ITSM principles to ensure uptime, and outsourcing certain operations to <219> MSP or <220> MSSP.

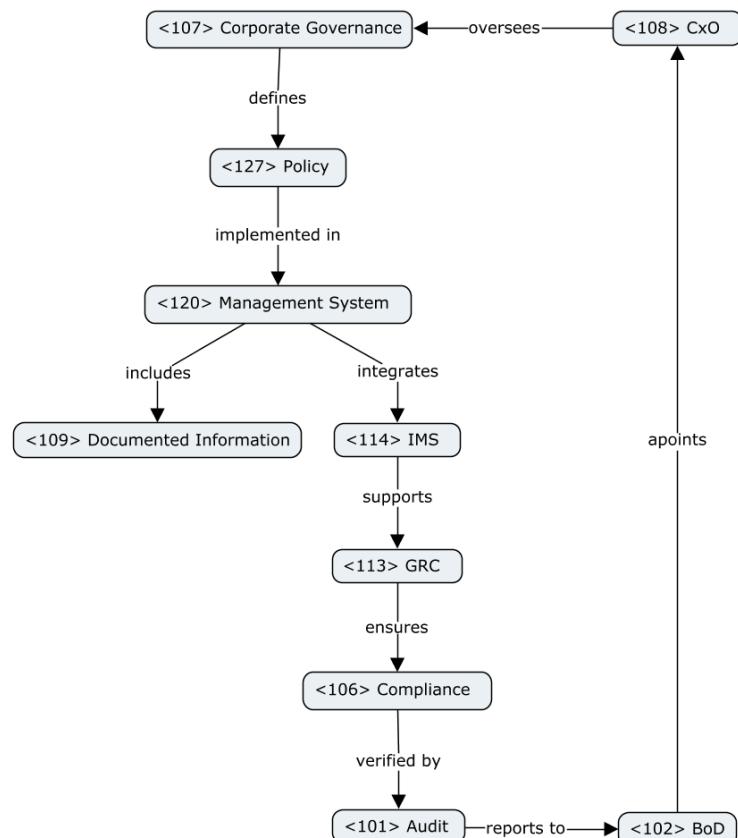


Industry 4: Transport and Logistics + Theme 1

The support and logistics industry enables the movement, storage, and distribution of goods and services across supply chains. In this industry, we focus on the last-mile urban delivery niche—the final stretch of a product's journey from a local fulfillment center to the consumer's doorstep. This sub-sector is critical for modern e-commerce, particularly in densely populated cities where speed, reliability, and cost-efficiency are essential. It combines physical infrastructure (e.g., vehicles, fulfillment hubs, smart lockers) with digital tools (e.g., route optimization software, delivery tracking, customer communication platforms). The sector is shaped by data-driven decision-making, regulatory frameworks—including <106>compliance and <208>data privacy—and real-time coordination among multiple <225>stakeholders.

<112>Governance in last-mile urban delivery must establish clear <117>leadership and accountability structures to manage the complexity of high-volume, time-sensitive shipments. At the top, the <102>Board of Directors and <108>CxO executives set strategic objectives—such as delivery-time and emission targets—and codify them into formal <127>policies. These policies are implemented through a <120>management system that incorporates <109>documented information, <128>procedures, and an <114>IMS to track performance, <106>compliance, and customer data.

Within this <114>IMS, a unified <113>GRC framework aligns <112>governance, <135>risk management, and <106>compliance activities, ensuring adherence to labor laws, traffic regulations, and <208>data privacy standards. <106>Compliance is regularly verified by internal and external <101>audits, which report findings to the <102>Board, ensuring top-down accountability. This method creates the transparency and control needed to deliver thousands of packages reliably in complex urban environments.

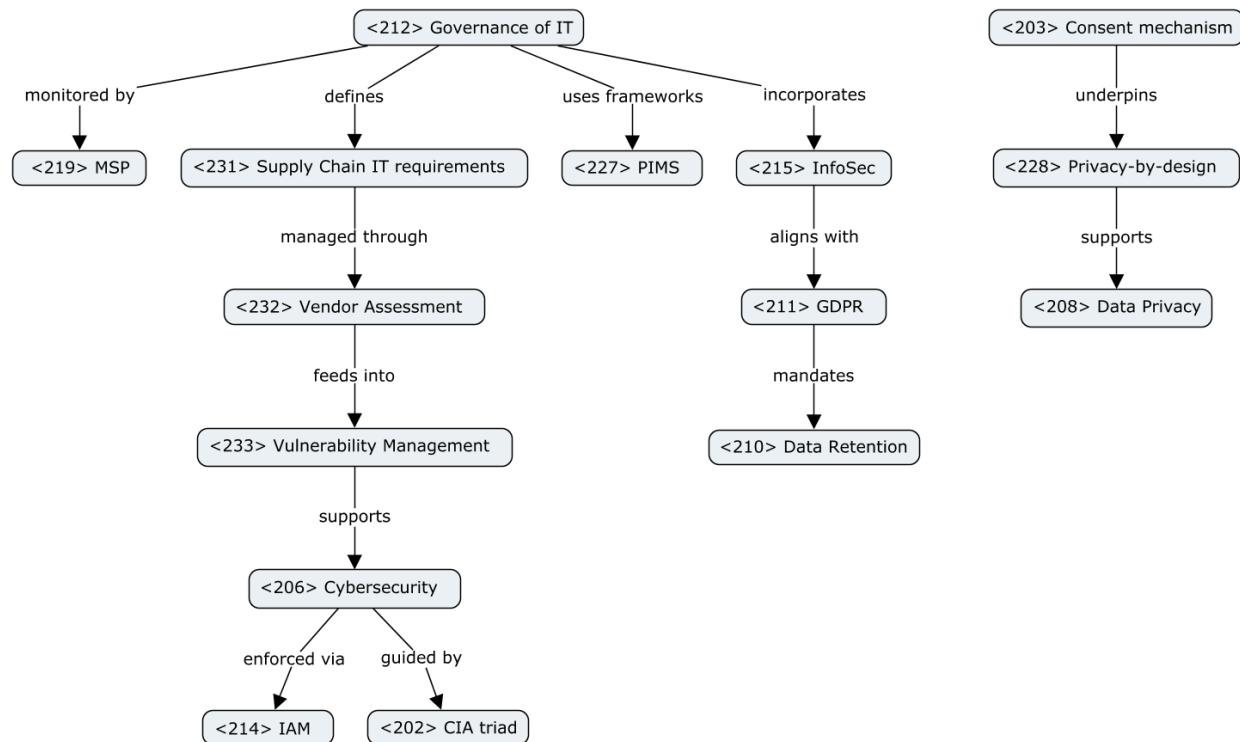


Industry 4: Transport and Logistics + Theme 2

In last-mile urban delivery, effective **<212>governance of IT** ensures that digital platforms—route optimization apps, customer portals, and warehouse systems—meet strict **<231>supply-chain IT requirements**. These requirements demand thorough **<232>vendor assessments** of logistics and software partners, followed by continuous **<233>vulnerability management** to identify and remediate security gaps. Strong **<206>cybersecurity programs**, guided by the **<202>CIA triad** and enforced with **<214>IAM**, protect sensitive delivery and customer data.

However, these IT systems face ongoing challenges such as integrating with legacy infrastructure, maintaining real-time data integrity, and defending against cyber threats. Governance of IT includes **<215>information security policies aligned with <211>GDPR**, reinforcing **<203>consent mechanisms** and adopting **<228>privacy-by-design principles**. These govern **<208>data privacy practices**—such as opt-in for location tracking—and **<210>data retention policies** for delivery records. To coordinate all these elements, organizations implement **<227>PIMS** for structured control and accountability, while **<220>MSSPs** provide 24/7 monitoring and incident response.

This layered approach helps organizations overcome complexity and risk, ensuring resilient, scalable, and trustworthy last-mile delivery operations.



Industry 1 + Industry 4 + Theme 1

In urban delivery, the <102>Board of Directors and <108>CxOs set targets for on-time performance and emissions, formalizing them into <127>policies that are implemented through a unified <120>management system. An <114>IMS tracks delivery metrics and customer data, while an integrated <113>GRC framework aligns <112>governance, <135>risk management, and <106>compliance with traffic laws, labour standards, and privacy rules. Routine <101>audits validate those procedures—from route planning to package hand-offs—adhere to policy, with findings reported back to the board to close the accountability loop.

By contrast, aerospace manufacturing translates <127>policies—driven by FAA/EASA regulations—into precise <129>process steps, with roles defined via <131>RACI to guarantee every inspection or heat treatment is performed correctly. Its <114>IMS integrates multiple <123>management standards (e.g., ISO 9001, AS9100) and tracks <116>KPIs like defect rates. <101>Audits and <110>due diligence on suppliers enforces rigorous certification requirements, while a strong <124>organizational culture rooted in <111>ethical values ensure quality and safety take precedence. Both sectors follow the policy-management system-GRC-audit-board structure, yet logistics prioritizes speed and customer responsiveness, whereas aerospace demands extreme precision, certification, and safety.

Industry 1 + Industry 4 + Theme 2

Both last-mile delivery and aerospace components manufacturing rely on a rigorous <212>Governance of IT framework to secure critical systems and data, tailored to their operational needs. In urban delivery, governance embeds <206>Cybersecurity into customer portals, routing apps, and warehouse systems, with every third-party carrier and software vendor undergoing automated <232>Vendor Assessment against security baselines. This supports continuous <233>Vulnerability Management—scanning for gaps in mobile apps or IoT-enabled lockers—and is enforced through a <214>IAM system that issues just-in-time credentials for drivers and dispatchers. Personal and location data collection follows <215>InfoSec policies aligned with <211>GDPR and <228>Privacy by Design, managed centrally through a <227>PIMS that tracks consent, retention, and audits.

In aerospace, the same <212>Governance of IT principles apply to design workstations, simulation environments, and shop-floor controllers, where the stakes are life-critical. <206>Cybersecurity encrypts and signs every CAD file and stress-test result, while a <234>Zero Trust architecture separates engineering from manufacturing networks. <214>IAM grants project-based, time-bound access, and a dedicated <215>InfoSec team monitors both IT and OT environments. Vulnerabilities—from firmware to CNC controllers—are triaged via <233>Vulnerability Management, with every part logged in an auditable <230>SBOM ledger. A <227>PIMS ensures all design data, logs, and supplier credentials comply with <211>GDPR and export-control rules. While delivery emphasizes agility and dynamic partnerships, and aerospace demands precision and traceability, both sectors build resilience through integrated IT governance, cybersecurity, and rigorous vendor oversight.

Industry 3 + Industry 4 + Theme 1

Both the retail and digital commerce, and transport and logistics sectors reveal complex organisational dynamics shaped by their structural and cultural configurations. In retail, a multilayered <126> Organizational Structure supports the integration of IT and in-store operations, but may hinder responsiveness. By contrast, delivery logistics rely on streamlined command chains and real-time coordination among <225> Stakeholders.

In <112> Governance, both sectors rely on the <102> BoD and <136> Top Management for strategic oversight—retail aligns with consumer demands through <437> Strategic Alignment and Omnichannel capabilities, while logistics targets operational efficiency and regulatory adherence.<108> CxO executives lead implementation, balancing legacy and digital systems in retail, and logistics executives translating <127> policies into delivery standards.

<117> Leadership plays a pivotal role in both industries. Retail fosters cross-functional teams and an <125> Organizational Culture of agility and experimentation, while logistics depends on clear leadership to manage high-volume and time-sensitive delivery networks.

Both use formal <120> Management Systems, logistics typically implements a unified <114> IMS, aligning <113> GRC components—<112> Governance, <135> Risk, and <106> Compliance. Retailers deal with jurisdictional variability, so they must meet <211> GDPR standards and use <203> Consent Mechanisms to maintain trust, transparency and compliance.

Industry 3 + Industry 4 + Theme 2

In both retail and digital commerce, and transport and logistics, effective <212> Governance of IT is essential to manage complex, technology-driven operations. Retail ecosystems rely on integrated platforms—ERP, CRM, and ePOS—while logistics operations depend on route optimization and warehouse systems aligned with <231> supply chain needs.

IT governance in both sectors is guided by <119> Strategic Frameworks and executed by <108> CxO roles, including CIOs and CISOs, through <127> Policies, <128> Procedures, and <115> Internal Controls. Retailers prioritize customer experience and <437> Strategic Alignment, while logistics focuses on data accuracy and system resilience.

Cyber risk is a shared concern. Supermarkets and logistics firms handle sensitive <223> PII and rely on <206> Cybersecurity controls such as the <202> CIA triad, <214> IAM, and <233> Vulnerability Management. Both sectors operate under <211> GDPR, enforcing <203> Consent Mechanisms and <228> Privacy-by-Design.

To ensure operational continuity and data protection, both sectors implement <216> ISMS and <227> PIMS, supported by <101> Audits. Retailers often use <217> ITSM practices and <323> SLAs with cloud vendors, while logistics firms engage <220> MSSPs for continuous monitoring and incident response.

INDUSTRIES PROJECT – Group 135

Industry 3: Retail and Digital Commerce (Omnichannel Grocery Retail)

Theme 1: Organizations, Governance & Management

Retail and Digital Commerce connects producers and consumers through formats such as physical stores, e-commerce platforms, and hybrid models. Traditionally local and fragmented, it has evolved into a global, platform-driven and data-intensive industry. Organizations vary from small shops to multinational chains, often relying on third-party platforms, vertical integration, and omnichannel strategies.

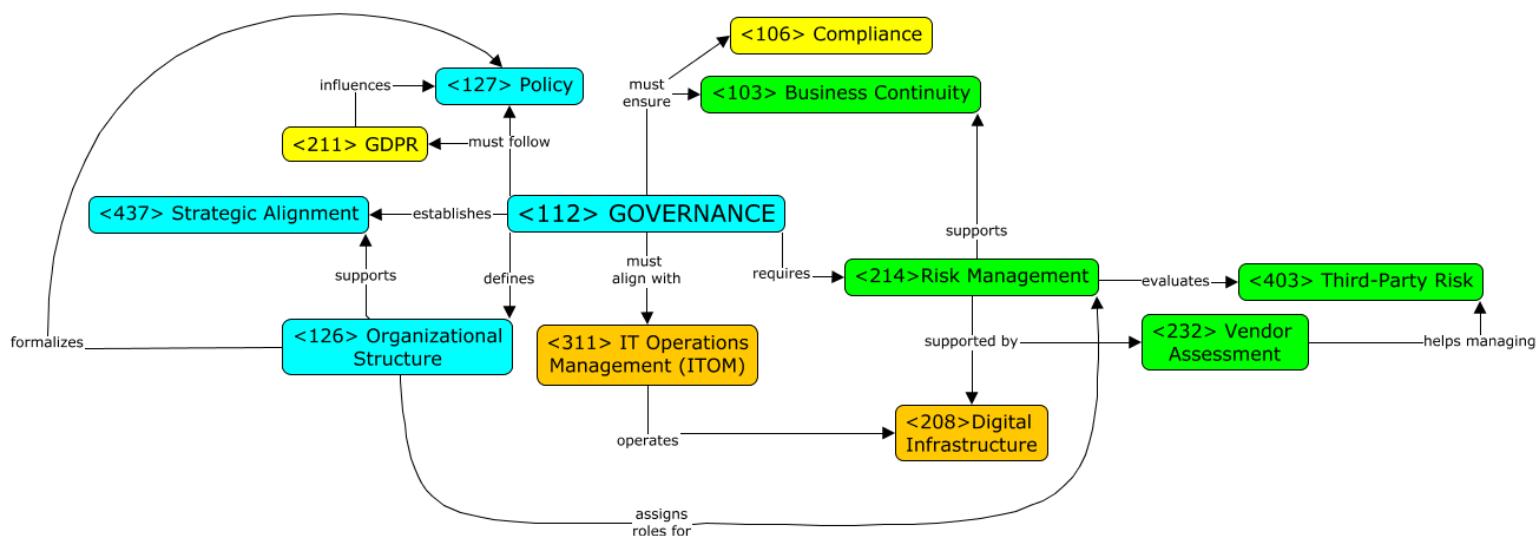
In the niche of **omnichannel grocery retail**, companies operate across physical supermarkets, mobile apps, websites, and delivery services, requiring governance structures that align strategic goals with ethical, operational, and regulatory demands.

Boards and executives oversee areas such as supply chain sourcing, digital marketing, loyalty programs, and logistics coordination, requiring strong **<437>Strategic Alignment** between business priorities and support systems. In an environment reliant on both in-house and outsourced services (e.g., last-mile delivery, cloud platforms), organizations face growing **<403>Third-Party Risk**, making adherence to **<127>Policy** and consistent **<232>Vendor Assessment** essential.

The sector is subject to complex regulatory regimes like the **<211>GDPR**, the Digital Services Act, and the Consumer Rights Directive, making **<214>Risk Management** and **<106>Compliance** critical governance concerns. Governance must also address responsible use of algorithms in pricing, ethical data practices in customer profiling, and the accuracy of environmental claims.

Internally, **<212>Governance of IT** and **<311>IT Operations Management** help ensure resilience and integration across ERP, ePOS, and CRM systems, supporting synchronized stock management, personalized promotions, and seamless customer experiences.

Overall, governance in this niche must balance operational flexibility with long-term accountability, ensuring **<103>Business Continuity**, consumer trust, and regulatory compliance in a highly competitive and data-driven market.



Theme 2: Governance of IT & IT Management

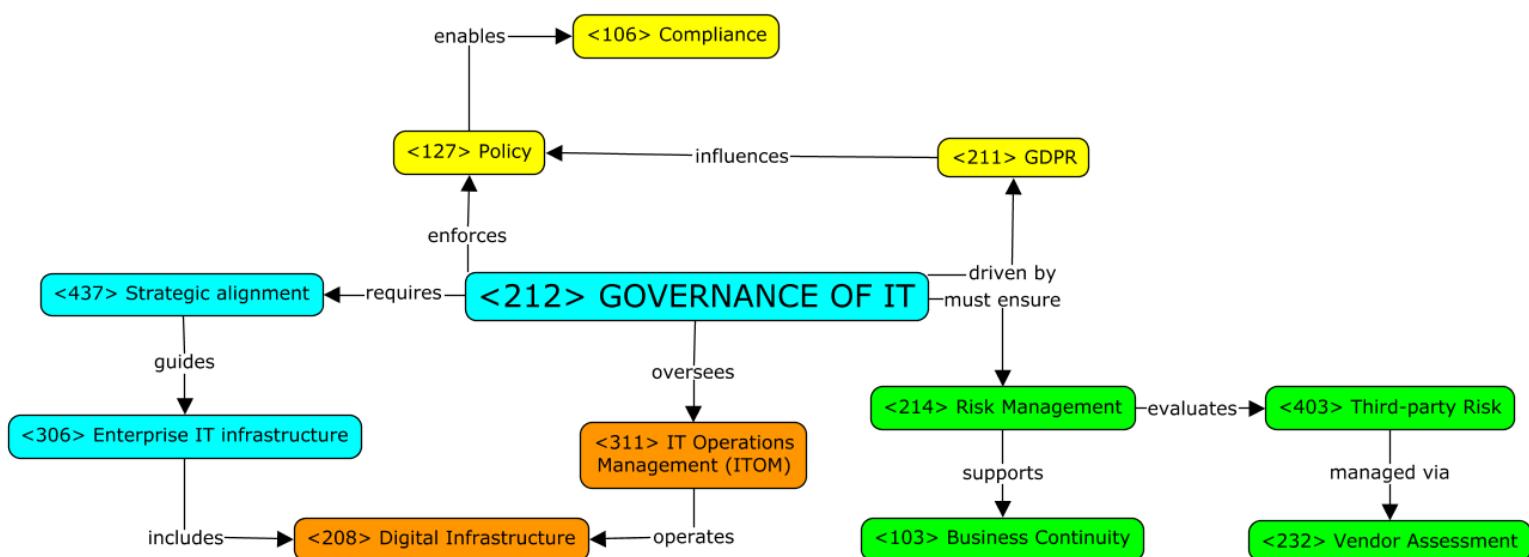
Retail and Digital Commerce is a dynamic, tech-driven industry where companies integrate physical stores with digital channels such as apps, websites, and marketplaces. This hybrid structure relies on complex IT ecosystems and cloud platforms—to enable seamless operations, personalized engagement, and agile logistics.

In the niche of **omnichannel grocery retail**, IT governance is essential to ensure smooth integration between physical supermarkets, mobile apps, delivery platforms, and loyalty systems. The complexity of these interconnected services requires strong **<437>Strategic Alignment** between business priorities and IT capabilities, particularly to coordinate real-time stock updates, digital coupons, and personalized promotions.

These retailers rely heavily on CRM, ERP, and ePOS systems, operated under **<311>IT Operations Management (ITOM)**, to deliver consistent and seamless customer experiences across all touchpoints. To prevent disruptions, **<212>Governance of IT** must ensure **<103>Business Continuity** and support **<214>Risk Management** across digital infrastructure and data flows.

With increasing dependence on third-party services such as payment processors, cloud platforms, and last-mile delivery providers, **<403>Third-Party Risk** becomes a key concern. This necessitates rigorous **<232>Vendor Assessment** and adherence to internal **<127>Policy** frameworks. Legal requirements such as the **<211>GDPR** also impose strict rules on customer data handling, directly influencing IT governance decisions.

Effective Governance of IT in this niche involves aligning IT services with operational processes, managing information security, and ensuring systems are scalable, reliable, and compliant. In this context, **<106>Compliance** and resilient digital infrastructure are critical to maintaining customer trust, operational agility, and regulatory adherence in a data-intensive retail environment.



Industry 1: Manufacturing (Micro-factories)

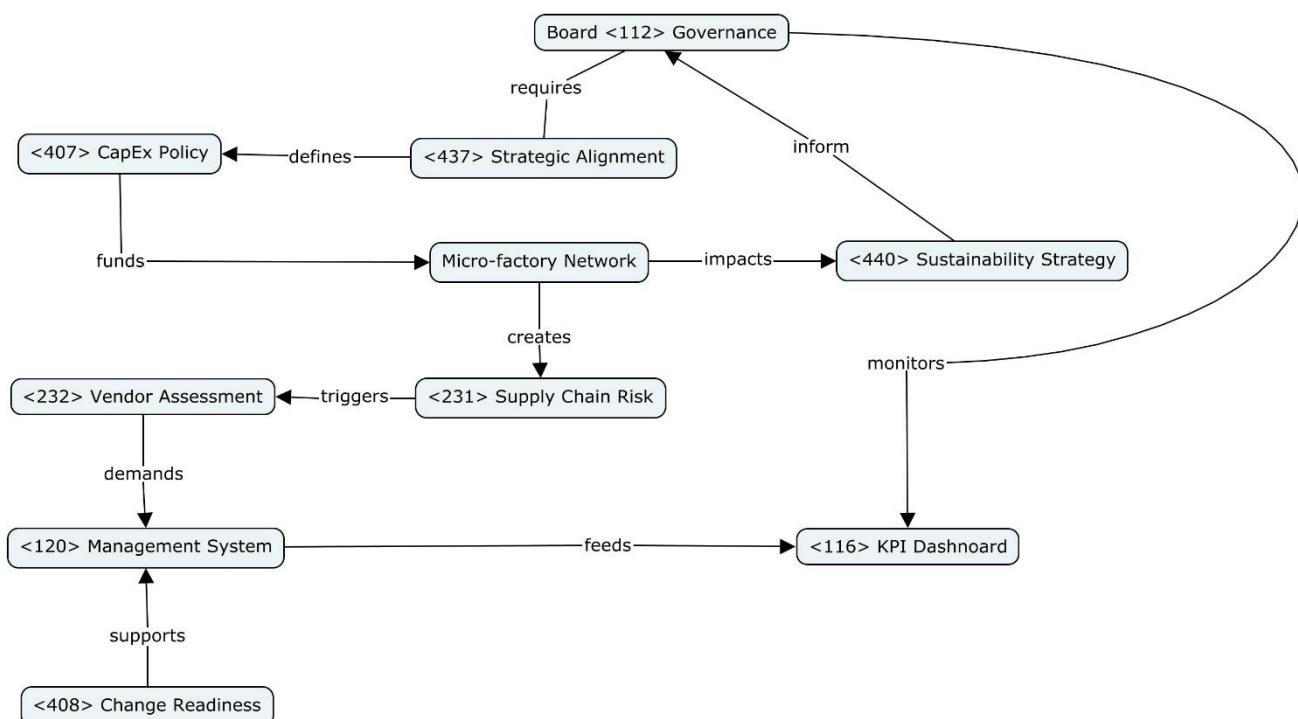
Theme 1: Organizations, Governance & Management

The manufacturing industry spans centuries-old mass-production lines, regional contract assemblers and, increasingly, highly digitised “smart” plants. Its modern trajectory is defined by relentless cost pressure, shorter product life cycles and regulators who now scrutinise both carbon footprints and cyber resilience. **Within this landscape, a fast-growing niche has emerged: distributed micro-factory manufacturing.**

Micro-factories replace the giant plant with “right-sized” sites close to consumers. Boards trade fixed assets for leases, data feeds and robotics service contracts, shifting oversight from depreciation to recurring operational risk and supply-network agility. Because a site can be stood-up—or wound-down—in months, executives run **<437>Strategic Alignment** cycles quarterly, deciding where the next cell pops up or which one pivots to a new SKU.

The dispersed footprint multiplies **<231>Supply Chain** touch points: local raw-material brokers, last-mile logistics and energy micro-grids. Boards impose a common **<232>Vendor Assessment** playbook and contract templates with embedded **<323>SLAs** to curb cross-jurisdiction variability.

Regulatory exposure fragments as well. A plant printing medical devices in Spain must satisfy ISO 13485 and MDR, while its UK sibling moulding consumer wearables faces different HSE and product-safety audits. Governance committees therefore elevate fleet-wide **<305>Data Protection** and **<303>Cyber Resilience** dashboards so local compliance never drifts outside corporate risk tolerance. Finally, the ethics lens widens algorithm-driven scheduling (**<403>Algorithmic system**) can maximise yield yet hide opaque order-prioritisations. Boards now demand audit trails and human-review gates before any optimisation engine is rolled across the fleet.



(Micro-factories)

Theme 2: Governance of IT & IT Management

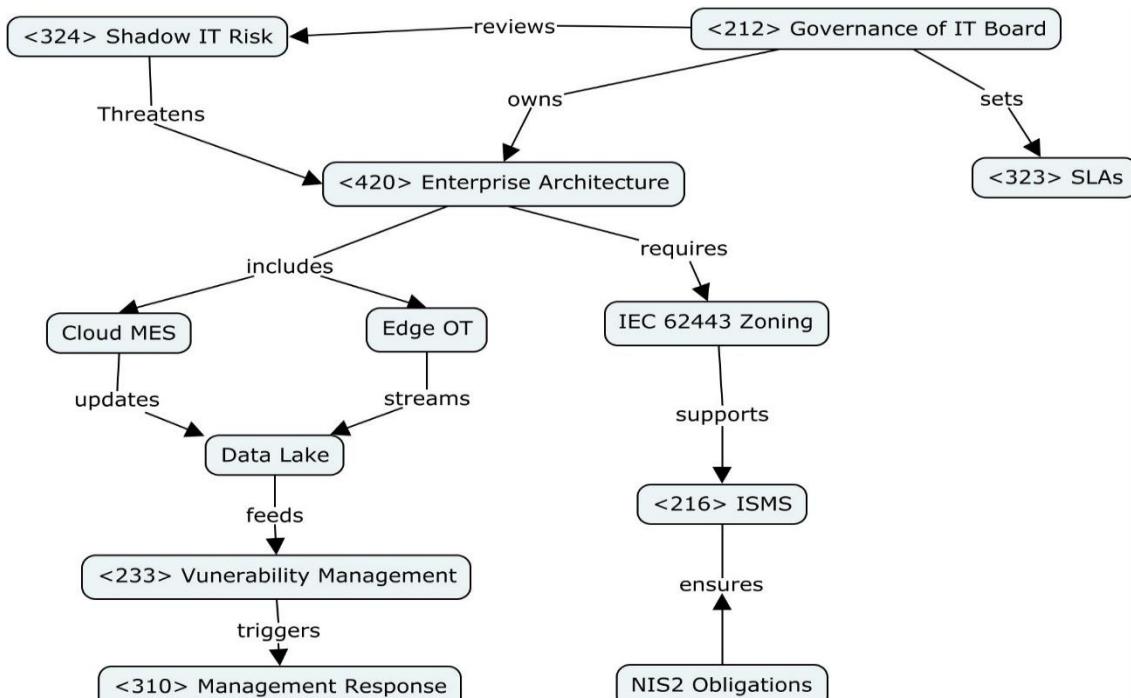
Across industrial production, the once-rigid line between Information Technology (IT) and Operational Technology (OT) has dissolved: cloud MES platforms orchestrate shop-floor robots, edge AI tunes yield in real time, and cybersecurity incidents travel from a PLC to the boardroom in minutes. **Within this broader movement of IT/OT convergence, our focus narrows to a specific configuration—micro-factory ecosystems.**

In a micro-factory, IT equals OT. Each cell runs cloud MES, floor robots, digital twins and edge AI. The CIO adopts a federated **<311>IT Operations Management** model: deterministic control loops on-prem, cloud MES (e.g., GE Proficy Smart Factory) synchronizing quality across sites.

Governance blends **IEC 62443** zone-conduit rules with enterprise policy. The CISO phases in **ISA/IEC 62443-3** controls to hard-segment robots, sensors and admin workstations, linking islands through a secure Industrial-Cyber overlay.

EU micro-factories fall under NIS2: incidents must be reported within 24 h and supply-chain cyber controls documented. Diverse vendors widen the attack surface, so governance enforces SBOMs every sprint and quarterly pen-tests, with **<323>SLA** penalties for any critical CVEs left unpatched.

Continuous improvement loops close via data lakes capturing process parameters and downtime, feeding a cross-site KAIZEN board. Leadership also tracks **<324>Shadow IT**: engineers love low-code edge apps, so a lightweight review board vets experiments before promotion to production.



Industry 2: Hospitality and Leisure

(Airbnb Listings for Vacation Stays)

Theme 1: Organizations, Governance & Management

The hospitality and leisure industry—spanning travel, lodging, and recreation—is being reshaped by platforms like Airbnb, which offer niche, experience-driven stays. This evolution raises key issues in governance and management, such as decentralized delivery, platform governance, and adaptive compliance.

Short-stay marketplaces integrate micro-hosts, apps, payments, and city rules. Boards must ensure **<437>Strategic Alignment** between growth and regulation, as seen when Spain forced Airbnb to remove 65,000 listings over licensing issues.

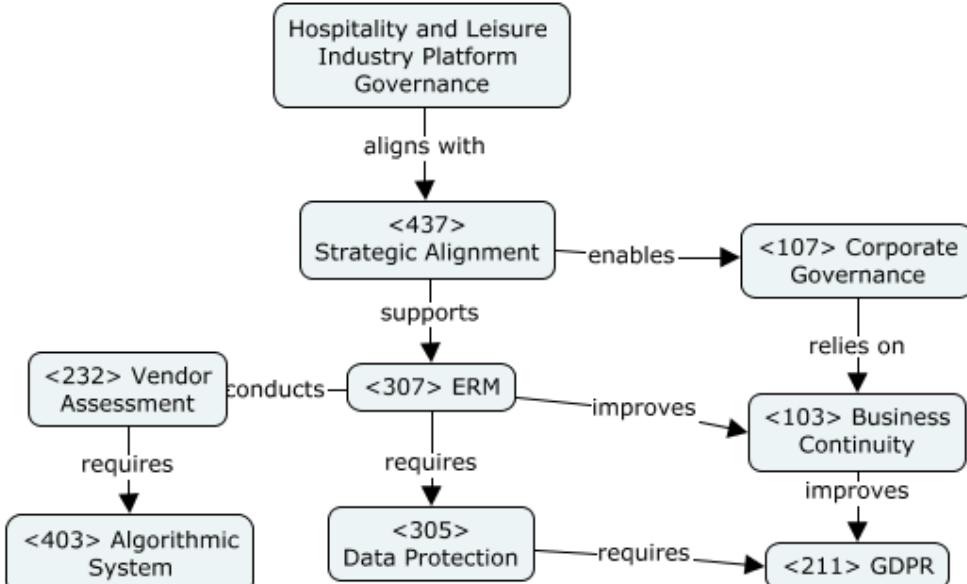
Bookings rely on third parties—cleaners, vendors, clouds—making risk management critical. Standard **<127>Policy** templates and **<232>Vendor Assessments** support **<307>ERM** dashboards that flag lapses like expired insurance or missing safety checks.

EU Regulation 2024/1028 mandates host ID verification and monthly reports; **<211>GDPR** still applies to guest data. All new features must pass a **<305>DPIA** before release.

Ethical concerns emerge from algorithmic pricing; boards add **<106>Compliance** reviews and AI-ethics audits with explainability and appeals.

Licence IDs and tax fields are now onboarding norms. City APIs pull compliance data directly—governance embedded in code. Yet resilience lags: **<103>Business Continuity** is a flagged risk, prompting investment in multi-cloud failover.

Platform trust and growth depend on strong **<437>Strategic Alignment**, thorough **<232>Vendor Assessment**, and ethical AI oversight.



Theme 2: Governance of IT & IT Management

The hospitality and leisure industry—focused on travel, lodging, and recreation—has been reshaped by platforms like Airbnb, especially through niche stays that offer personalized experiences. This transformation raises key themes in IT Governance & Management: data privacy, platform security, and decentralized IT-driven service delivery.

The short-stay marketplace acts as a cloud-native software supply chain. A permanent **<212>Governance of IT** Board ensures **<437>Strategic Alignment** between product cycles and expanding compliance. EU Regulation 2024/1028 mandates host ID checks and monthly reporting—turning data pipelines into regulatory infrastructure.

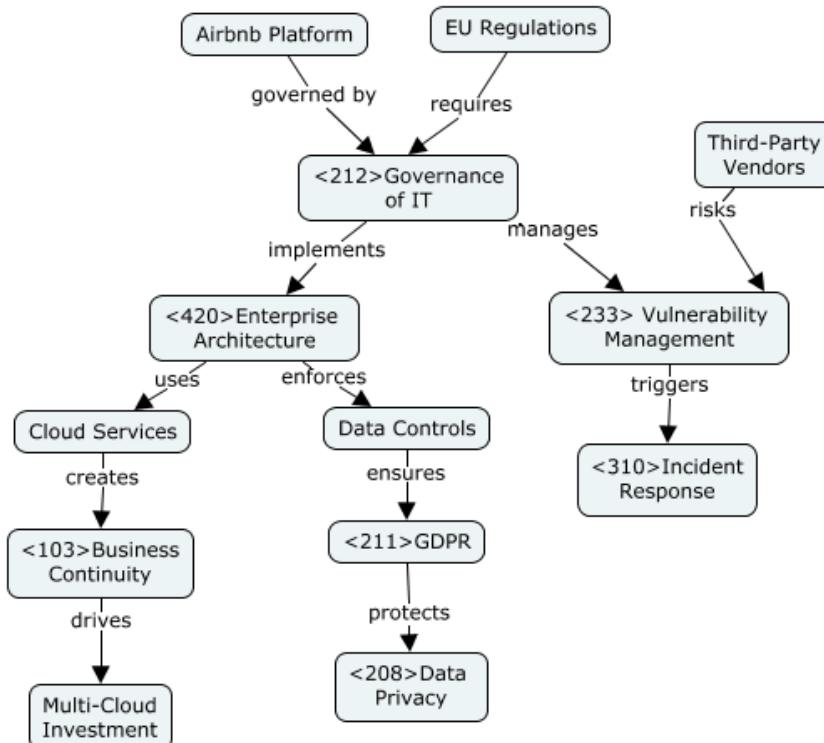
The board uses a federated **<420>Enterprise Architecture** with apps, microservices, and edge ML to block risky bookings. Release authority is enforced; unapproved scripts flag **<324>Shadow IT Risk**.

Controls sit within a unified **<216>ISMS** aligned with ISO 27001 and NIS2 rules. Sensitive data flows—like passport scans—must pass a **<305>DPIA**, fulfilling GDPR obligations.

Third-party risk is high due to reliance on clouds, vendors, and smart locks. Standard **<232>Vendor Assessments** collect SBOMs and uptime metrics, feeding **<233>Vulnerability Management** queues that escalate CVEs to a 24/7 **<310>Incident Response** team.

Still, resilience is fragile: the 2024 Form 10-K cites weak recovery plans, marking **<103>Business Continuity** as a key risk. This drives multi-cloud failover investment, aligning Opex with board risk tolerance.

By embedding architecture, algorithm oversight, and vendor rigor into its IT governance, the platform builds scalable trust alongside scalable operations.



Comparison relating Theme 1

Retail and Digital Commerce versus Manufacturing

Both industries demand agile **<112>Governance** but face divergent challenges. Omnichannel Retail depends on centralized **<136>Top Management** to synchronize both digital and physical operations via integrated **<120>Management Systems**, with **<116> KPIs** tracking real-time CX metrics. **<106>Compliance** and **<215>InfoSec** represent top governance priorities due to the high volume of consumer data and regulatory scrutiny.

In contrast, Micro-Factories prioritize **<428>Organizational Agility**, operating through semi-autonomous units that require governance frameworks capable of supporting rapid reconfiguration and deployment. In this context, **<317>Operational Risks** and **<231>Supply Chain** vulnerabilities become the dominant concerns.

Strategically, retail invests in seamless CX systems, while manufacturing focuses on modular, scalable production. Together, they demonstrate how governance must adapt to digital-era operational complexity.

Retail and Digital Commerce versus Leisure and Hospitality

In both industries, **Omnichannel Grocery Retail** and **Holiday Rental Platforms** (e.g., Airbnb-style services) operate in fast-paced, customer-centric markets—but they diverge significantly in **<112>Governance** priorities and **<126>Organizational Structure**.

Retailers prioritize **<437>Strategic Alignment** across digital and physical channels, enforcing strict **<106>Compliance** with **<211>GDPR** and food safety regulations through documented **<127>Policies**. In contrast, hospitality platforms emphasize **<428>Organizational Agility**, balancing global standards with local rental laws while managing **<317>Operational Risks** such as property damage via **<232>Vendor Assessments** of individual hosts.

From a management perspective, retail must synchronize **<311>IT Operations** across warehouses, apps, and physical stores, while safeguarding against **<215>InfoSec** breaches. For Airbnb-style platforms, the main challenges include maintaining **<303>Cyber Resilience** in booking infrastructure and addressing **<403>Algorithmic System** bias in dynamic pricing and search rankings.

Risk exposure also differs on these two models. Retail's centralized model must mitigate **<231>Supply Chain** disruptions, whereas the hospitality sector's distributed structure encounters **<135>Repudiation Risk** due to inconsistent guest experiences or host accountability.

In conclusion, both models show that digital transformation demands tailored governance. Retail thrives on centralized control and compliance, while hospitality relies on adaptive, trust-based systems. Each reflects a governance model shaped by its operational realities.

Comparison relating Theme 2

Retail and Digital Commerce versus Manufacturing

Both industries require robust **<212>Governance of IT** to align with **<437>Business Goals**, manage **<135>Risk**, and ensure operational resilience.

In omnichannel grocery retail, governance enables seamless integration between physical stores, mobile apps, e-commerce platforms, and delivery services. **<311>IT Operations Management** ensures synchronization across ERP, CRM, and ePOS systems, supporting consistent customer experiences. Key concerns include **<106>Compliance** with data protection regulations such as **<211>GDPR**, **<103>Business Continuity** to avoid operational disruption, and **<232>Vendor Assessment** to evaluate logistics and cloud service providers. Effective **<127>Policy** frameworks and **<437>Strategic Alignment** are essential to managing real-time inventory, digital loyalty systems, and personalized campaigns.

In contrast, manufacturing IT governance focuses on aligning **<318>Operational Technology** with IT, often using cloud-based MES and edge computing for local control. **<234>Zero Trust** models and **<230>SBOM** practices are applied to secure software components, while compliance with the NIS2 Directive requires rapid incident response. The role of the CISO is central in enforcing cybersecurity standards and controlling **<324>Shadow IT**, particularly across the **<231>Supply Chain** where integration risks are high.

Conclusion: While retail governance prioritizes customer experience and digital service continuity, manufacturing focuses on securing industrial systems and OT integration. Both adapt IT governance to sector-specific operational demands and regulatory frameworks.

Retail and Digital Commerce versus Leisure and Hospitality

Both industries require strong **<437>Strategic Alignment** between IT and business goals, but they face distinct governance priorities.

In Airbnb, **<212>Governance of IT** is embedded in the **<231>Supply Chain**, with the board aligning product development cycles to regulatory change. **<106>Compliance** is designed into architecture using **<305>Data Protection** gates and a federated **<420>Enterprise Architecture** to coordinate microservices and manage **<324>Shadow IT** risks. A unified **<216>ISMS** handles **<403>Third-Party Risk** from hyperscale clouds and IoT, enforced through **<232>Vendor Assessments** and **<233>Vulnerability Management** pipelines.

Retailers, by contrast, emphasize operational coordination across stores, apps, and e-commerce. Here, **<437>Strategic Alignment** ensures real-time inventory and consistent promotions, driven by **<311>IT Operations Management** via CRM and ePOS systems. **<403>Third-Party Risk** exists, but mostly in logistics. **<106>Compliance** focuses on **<211>GDPR** obligations tied to loyalty programs and consumer behavior.

Conclusion: Airbnb's governance is architecture- and compliance-led, while grocery retail priorities seamless operations and customer trust. Each adapts IT governance to its business model and regulatory environment.

INSTITUTO SUPERIOR TÉCNICO

SECURITY AND MANAGEMENT OF INFORMATION SYSTEMS

P1

Group 136

Federico Falcone - 112385
Max-Leon Matthies - 113343
João Vairinhos - 113183
Leonardo Schiavon - 113332

Academic Year 2024/2025

May 23, 2025

1 Industry I - Automotive Manufacturing

Automotive manufacturing is the process of designing, assembling, and producing motor vehicles through a complex integration of advanced machinery, robotics, skilled labor, and supply chain coordination.

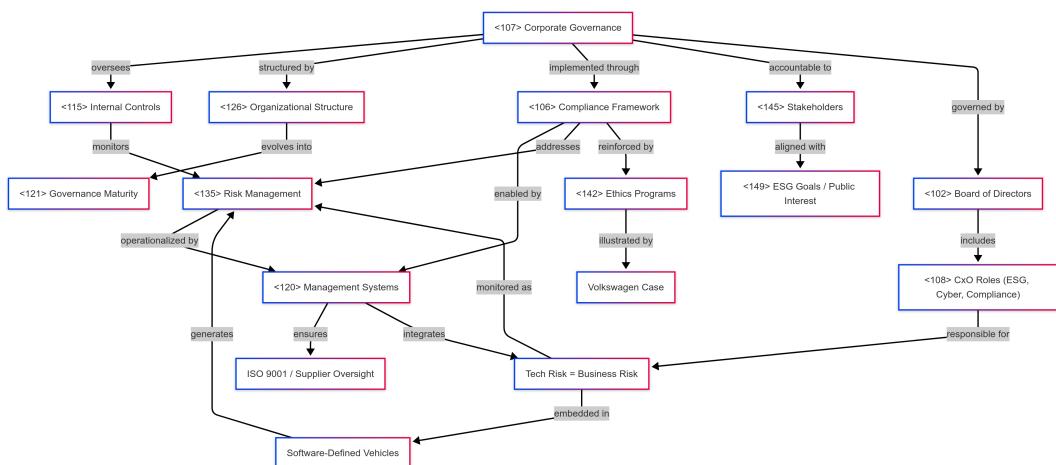
1.1 Governance

The automotive manufacturing industry operates through complex global supply chains under increasing regulatory pressure. Governance ensures strategic alignment, operational integrity, and stakeholder accountability.

Traditionally, automotive firms employed centralized, hierarchical governance models <107>enabling tight control over vertically integrated operations and quality systems like ISO 9001. Formal boards of directors <102>oversee these structures, supported by executive roles managing ESG, cybersecurity, and compliance <108>. Companies deploy comprehensive internal control systems <115>integrating risk management processes <135>and compliance policies <106>across procurement, product development, and supply chain operations. Governance maturity <121>has evolved toward flexible organizational structures <126>with platform-based teams and cross-functional governance bodies. Management systems <120>provide operational foundations for compliance and quality assurance, supporting structured auditing and supplier governance. Stakeholder governance <145>has gained prominence as regulators, investors, and workers increasingly influence corporate decisions, aligning governance with ESG objectives <149>.

The Volkswagen Dieselgate scandal exemplifies governance failures, catalyzing industry transformation through independent ethics programs and risk-based control mapping <142>.

Contemporary automotive governance must address technology risks, overseeing cyber-physical systems in software-defined vehicles and integrating IT with product oversight. This convergence positions governance as both control mechanism and strategic enabler of innovation and resilience.

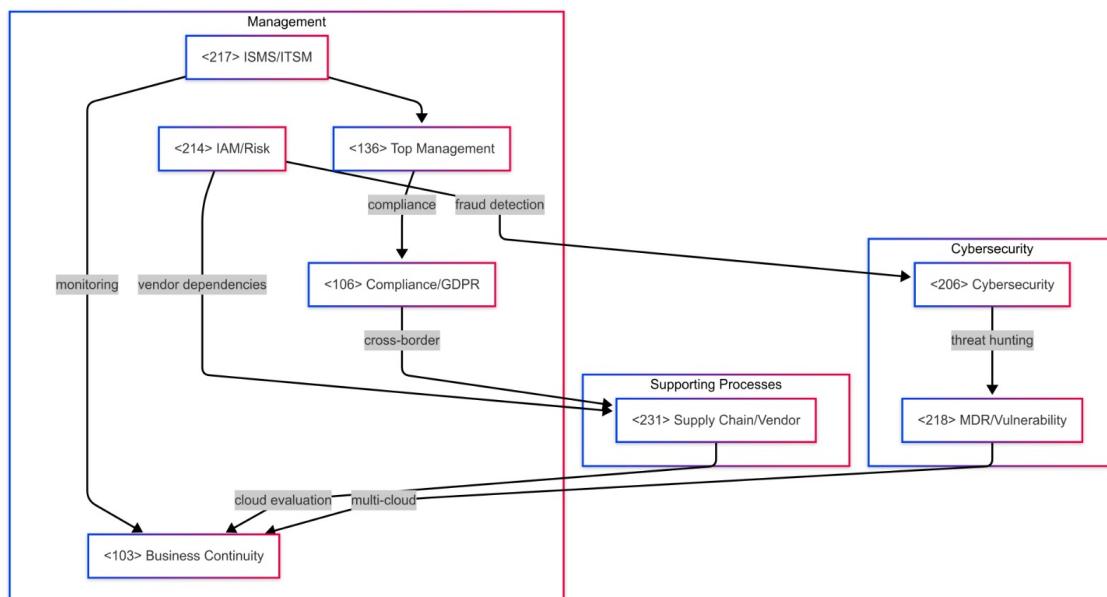


1.2 IT Management

utomotive manufacturers increasingly operate as technology-driven enterprises, where IT management plays a central role in ensuring operational resilience, efficiency, and innovation. Modern players like Tesla, Volkswagen, and Toyota rely on integrated digital infrastructure to power globally distributed supply chains and real-time production environments. Their IT environments are structured around enterprise resource planning (ERP) and manufacturing execution systems (MES), which form the digital backbone of factory operations. Volkswagen's SAP-based ERP achieves 99.9% uptime to maintain uninterrupted supply chain coordination.

Automation is at the core of operational efficiency. IT departments utilize infrastructure-as-code (IaC) and continuous integration/continuous deployment (CI/CD) pipelines to push updates rapidly without halting production. Tesla uses this approach to deliver over-the-air software updates, tightly coupling IT and product development. Change management is governed by formal approval workflows to ensure system stability. Service management follows ITIL-aligned practices, with service level agreements driving consistent performance. System failures are addressed within defined time windows to minimize downtime. AI-powered tools provide real-time anomaly detection and predictive analytics for proactive fault handling.

Security and business continuity are paramount. Companies adopt ISO/IEC 27001 standards, implementing automated patch management, identity and access control, and continuous monitoring. The 2021 ransomware attack on a Honda supplier underlined the need for resilient, failover-ready systems. Manufacturers design IT architecture to ensure essential services remain available through redundant systems. IT governance spans compliance, operational maturity, and business integration. Technology risks are treated as business risks, with IT managers working closely with engineering, quality assurance and compliance teams.

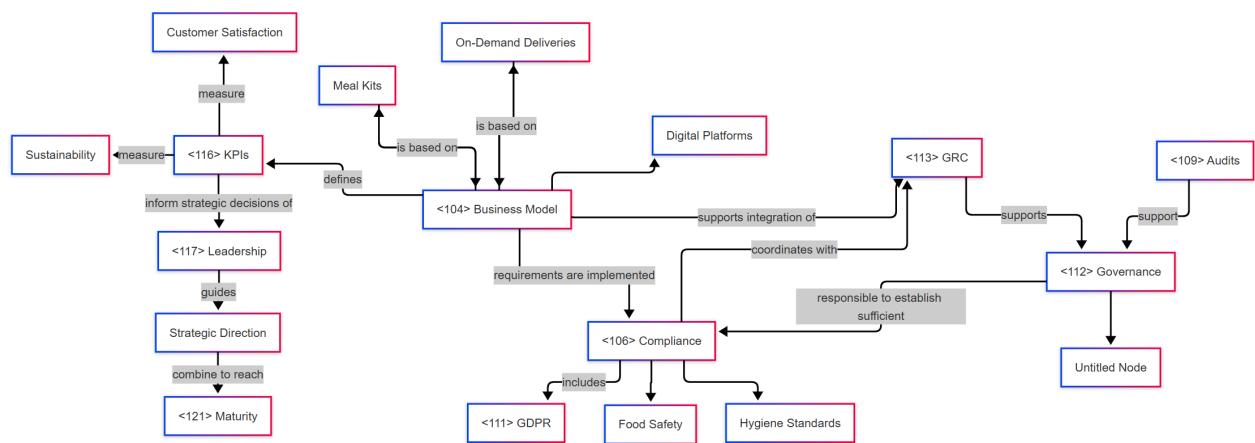


2 Industry II - Online Grocery Retail

Online grocery retail is a fast-growing niche within the broader retail industry that focuses on delivering fresh and packaged food directly to consumers. The online grocery market consists of retailers who rely on digital platforms to sell their goods. They use logistics networks to distribute their goods directly to consumers. Two well-known competitors in the market are Amazon Fresh and HelloFresh.

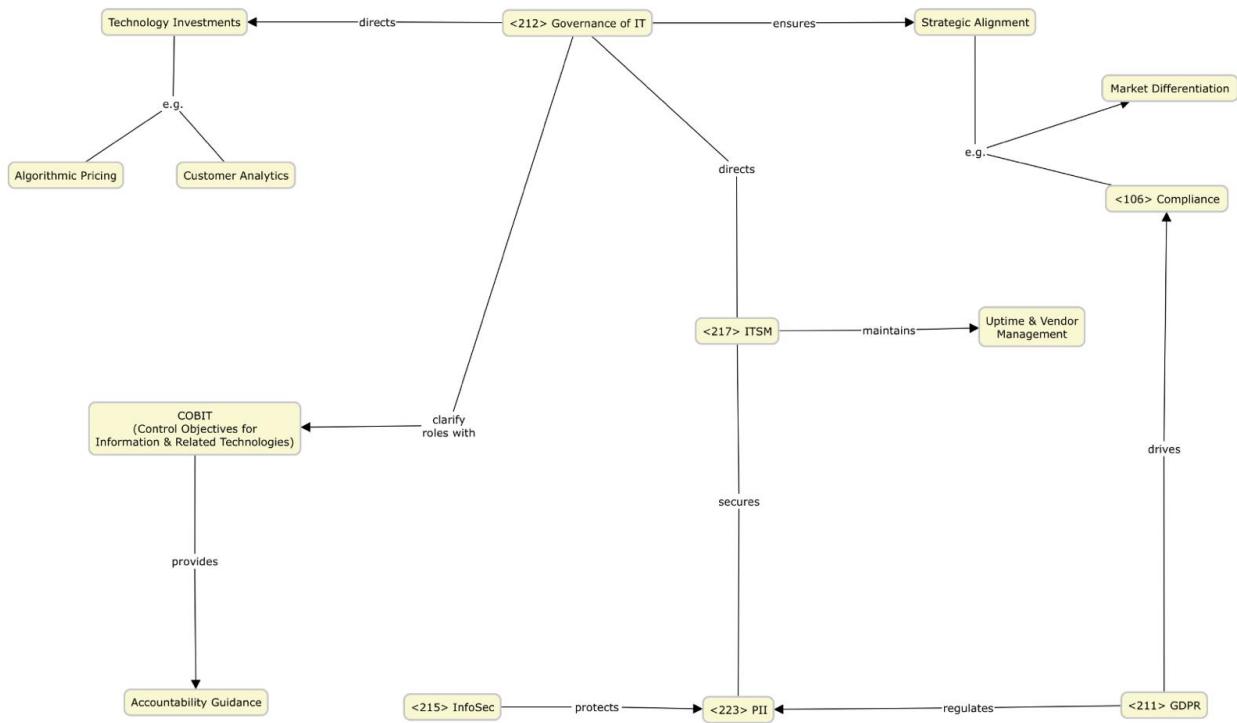
2.1 Governance

Their approaches to consumers differ strongly, HelloFresh sells meal kits with a focus on nutrition whereas Amazon specializes in on-demand grocery deliveries. However, both <104>business models emphasize scale, convenience, and data-driven personalization. <116>KPI metrics include delivery punctuality, customer satisfaction, food waste reduction and CO₂ footprint. Companies in this market typically adopt agile, tech-centric structures with cross-functional teams. Rapid product cycles demand dynamic coordination across tech, logistics, procurement, and customer service. Challenges for this type of business are operations efficiency, IT infrastructure and supply chain resilience. This requires integrated <113>GRG frameworks to manage delivery disruptions, <206>cybersecurity <135>risks, and regulatory <106>compliance. Strong <112>governance systems are essential to ensure that growing consumer expectations are met and increasingly complicated food safety as well as data privacy regulations are being followed. The <117>leadership is expected to be visionary yet ethical. Robust <115>internal control and <106>compliance is demanded to allow traceability in sourcing, hygiene standards and <211>GDPR <106>compliance. Through the implementation of internal and external <101>audits, <130>quality, cybersecurity, and regulatory <106>compliance are ensured. Most competitors in the online grocery retail business, like HelloFresh and Amazon Fresh, aim for strong growth by entering new markets. It is therefore particularly vital for them to acquire local delivery networks and to manage supplier relationships. Many online grocers, especially newer startups, still mature their formal process, balancing innovation with <112>governance.



2.2 IT Management

The online grocery sector relies heavily on robust IT systems to manage real-time inventory, logistics, and customer interfaces. Effective <212>Governance of IT is critical to align digital investments – such as algorithmic pricing, last mile delivery platforms, and customer data analytics – with strategic goals like market differentiation and regulatory <106>compliance (e.g. <211>GDPR, food safety). Yet many fast scaling players (e.g. Instacart) blur the lines between <112>governance and management, leading to reactive decision-making or tech overreach. Frameworks like COBIT can help clarify roles and accountability, ensuring that board-level oversight directs IT priorities that support resilience and ethical data use. Meanwhile, pIT Management practices rooted in ITIL are essential for maintaining uptime, managing vendors, and securing <223>PII in highly distributed environments. In a niche where digital trust and operational efficiency are both mission-critical, the interplay between <112>governance and management determines not only competitive edge but also long-term sustainability.



3 Industry III - Digital-Only Banks

The digital-only banking industry comprises financial institutions that operate exclusively through digital channels without traditional physical branch networks.

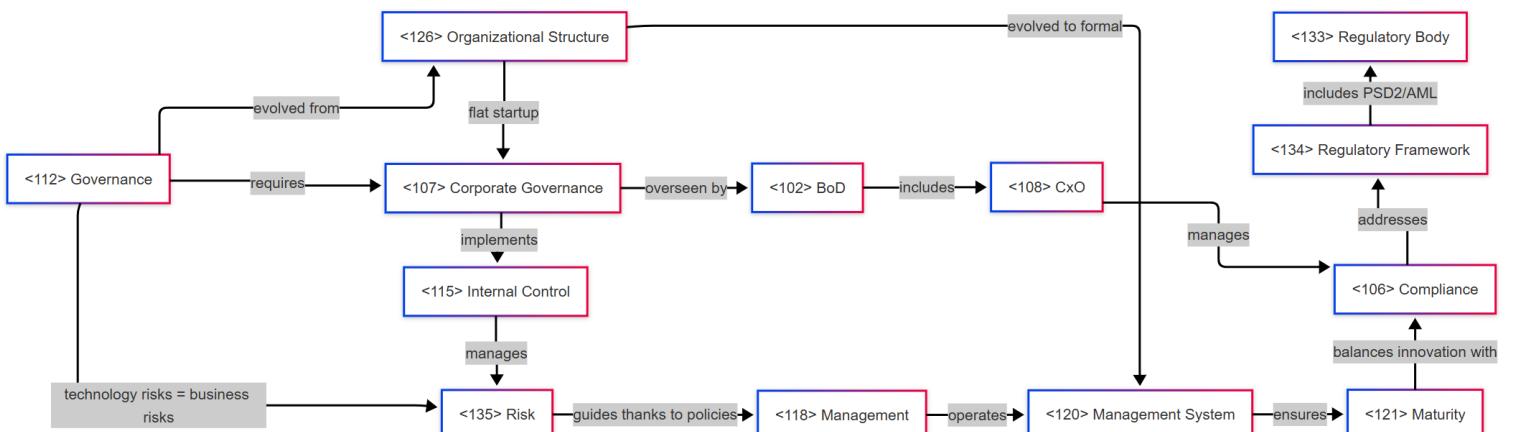
3.1 Governance

Digital-only banks like Revolut and N26 started as tech startups but quickly discovered they needed to master complex financial regulation while keeping their innovative advantage. Their initial organizational structure was flat and agile, teams moved fast and decisions were made quickly without traditional banking bureaucracy. However, as they scaled globally and attracted millions of customers, this informal approach hit regulatory walls.

Banking operates under strict regulatory frameworks like PSD2 and AML requirements. These challenger banks had to rapidly evolve from startup-style management to sophisticated corporate governance systems that could satisfy supervisory authorities like the FCA. The most significant governance failures came in anti-money laundering and transaction monitoring, fundamental compliance breakdowns that required complete changes of their internal control systems.

This led to major shifts in top management structure. Both banks now have specialized CxO roles for compliance, risk and cybersecurity. The informal oversight that worked with thousands of customers couldn't handle millions of transactions across dozens of countries. Today's Board of Directors must understand both traditional banking risks and technology-specific threats like third-party dependencies and cyber incidents.

The governance model evolved from reactive problem-solving to proactive risk management. These banks now operate formal management systems that handle audit requirements and cross-border operations while preserving innovation speed. The challenge is balancing control with innovation since too much kills creativity, too little invites regulatory action.



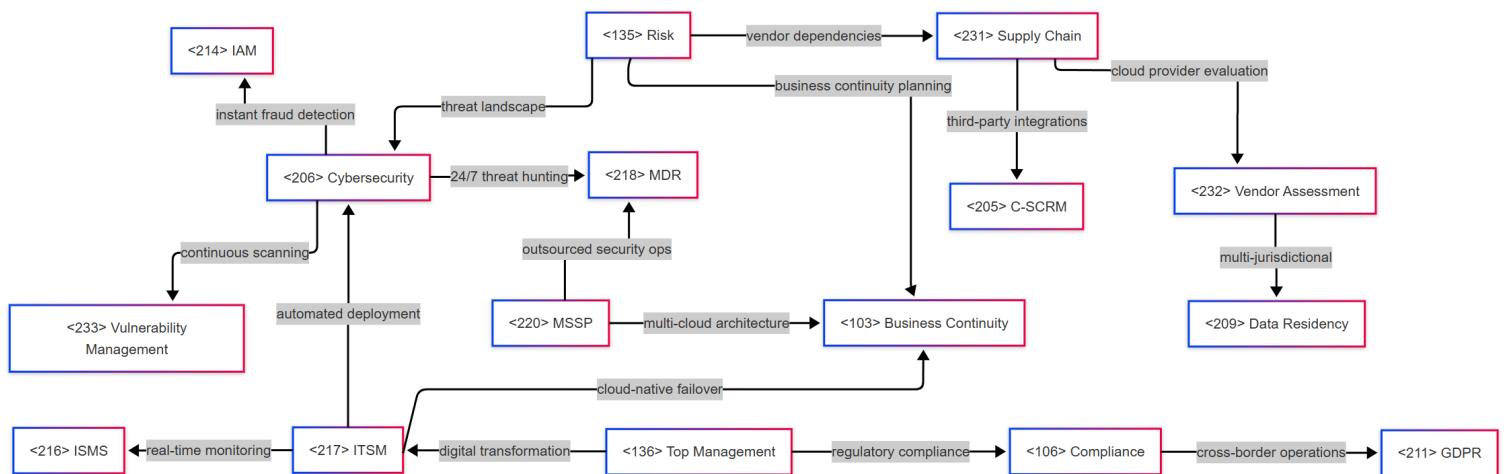
3.2 IT Management

These organizations exist purely as digital services, so their IT operations management differs fundamentally from traditional banks. Both built their enterprise IT infrastructure from scratch using cloud-native architectures for instant global scaling. When N26 expands to new countries, they're deploying software and not opening branches.

Their approach centers on automation and business continuity. Instead of manual processes, they use infrastructure-as-code and continuous deployment with multiple daily software updates rather than monthly maintenance windows. Every code change goes through automated testing, security scanning and compliance checks in order to ensure risk management.

Cybersecurity is the biggest among every aspect of IT service management through real-time monitoring and automated threat detection. These banks design for failure from day one. Revolut operates across multiple cloud providers ensuring failover capabilities (if one system fails, traffic automatically routes to backups without customer impact). Real-time fraud detection and risk analytics depend on processing enormous data volumes instantly.

IT governance must satisfy technical excellence and regulatory compliance through detailed audit trails, strict IAM controls and documented procedures. Their ITSM practices align with ISO/IEC 27001 but are adapted for rapid deployment. The most distinctive aspect is tight integration with business functions: product managers, engineers and compliance officers work in the same teams. This extends to vendor assessment and supply chain management, evaluating functionality alongside regulatory implications and data residency requirements. Both banks treat technology as platforms with reusable components, where technology risks are business risks managed through integrated monitoring and automated compliance reporting.



4 Comparisons

4.1 Online Grocery Retail Vs. Digital-Only Banks in IT Management

First thing came to our mind is that banks and online grocery companies approach IT management from fundamentally different risk perspectives. Digital banks treat IT failure as existential threat, because when Revolut's systems fail, customers cannot access their money, destroying trust immediately. This drives their "design for failure" philosophy with multi-cloud architectures and automatic failover systems. Online grocery companies indeed face operational risks, where system failures mean delayed deliveries or inventory problems, but customers can still buy food elsewhere. This difference explains why banks invest heavily in redundant systems while grocery companies often accept some instability as normal business cost.

Additionally, when banks want to enter new countries, they can copy their software everywhere easily. But each country has different banking rules they must follow. When grocery companies want to expand, they face the opposite problem. The rules about selling food online are usually similar between countries, but they need to build delivery trucks, find local suppliers, and set up warehouses in each new place. This creates a "paradox" situation: banks move technology fast but get stuck on legal rules, while grocery handles legal issues but gets stuck on physical operations. For IT teams, banks need systems that adapt quickly to changing laws, while grocery needs systems that work with different delivery companies and suppliers.

4.2 Online Grocery Retail Vs. Digital-Only Banks in Governance

Both digital banks and online grocery (let aside Amazon Fresh) started as fast-moving tech companies with flat teams and quick decisions. But we think they started differentiating especially when they hit different walls in scaling up. Digital banks like Revolut got shut down by regulators for breaking anti-money laundering rules. Grocery companies face food safety and privacy rules but rarely get shut down for violations.

This created opposite survival strategies. Banks had to hire compliance executives and build automated rule-checking into every software update. Grocery companies could keep their informal approach longer because mistakes just cost money, not business licenses.

While the regulatory environments differ in intensity the governance transformation follows a similar trajectory. Both sectors moved from reactive problem-solving to proactive risk management, aligning leadership structures with their risk profiles. Still, the reasons for these changes are not the same. Online grocery companies care more about smooth operations and what customers expect. Digital banks, on the other hand, must follow hard and detailed laws from financial authorities in many countries.

4.3 Automotive vs. Digital-Only Banks – Governance

Governance in automotive and digital banking started from opposite models but converged toward risk-oriented maturity. Automotive firms relied on centralized structures and quality standards, evolving gradually under industrial and reputational pressure. The Volkswagen case marked a shift toward ethics and compliance reforms.

Digital banks began with flat, agile teams, but regulatory breaches forced them to adopt formal governance, including board oversight and CxO roles for compliance. While automotive responds to safety and supply chain accountability, digital banks are shaped by tight legal frameworks and financial risk.

Despite different origins, both sectors evolved toward integrated governance, balancing innovation, compliance, and operational control.

4.4 Automotive Manufacturing vs. Digital-Only Banks in IT Management

Automotive manufacturers structure their IT around tightly controlled and optimized environments to keep assembly lines working at 99.9 percent uptime. Updates roll out in lean, batch-oriented windows, and every firmware push passes through CI/CD pipelines with ISO 26262 safety and ISO 9001 quality gates, plus formal CAB reviews and CAPA logs to prevent even the smallest defect from halting production. In contrast, digital-only banks live in the cloud: they spin up containerized services and serverless functions across multiple regions, using infrastructure-as-code and continuous deployment to push dozens of changes daily. Policy-as-code scanners enforce AML/KYC and PSD2 consent rules before any code hits production, so new features and security patches arrive in minutes rather than weeks.

When it comes to keeping systems running, manufacturers lean on AI-driven anomaly detection—monitoring vibration, temperature, and cycle-time data at the edge—and self-healing scripts that reroute workloads around failing nodes, with Six Sigma-informed digital-twin simulations driving incremental uptime gains. Banks, by comparison, deploy explainable-AI fraud engines and active-active database clusters with sub-second failover, backed by 24×7 Security Operations Centers that detect and remediate threats in real time. Their tight integration of ITSM with business and compliance teams means technology risks are treated as financial risks, ensuring uninterrupted access to funds and regulatory peace of mind.

Security and Management of Information Systems - P1



Group 137

Roy van den Munckhof - 115295
Renske Lijcklama à Nijeholt - 115554
Tobias Machiavello - 115393
Daan Ransdorp - 115376

Smart manufacturing/Industry 4.0 - theme 1

Introduction

Smart Manufacturing/ Industry 4.0 refers to the integration of advanced digital technologies into industrial production. It combines Internet of Things (IoT) and artificial intelligence to create highly automated, adaptive, and efficient manufacturing environments. Combining advanced IT systems and manufacturing requires maturity in management and governance for efficient operations and cybersecurity.

Relation to theme 1

Combining advanced software with manufacturing comes with great responsibility. When software-driven systems fail, the entire production environment can halt. To mitigate this <135> Risk, <121> Maturity in <112> Governance and <118> Management is needed. To achieve this smart industries should operate in a structured way, where all digital systems are embedded into robust <119> Management Frameworks that ensure consistency and rapid response to issues. <131> RACI frameworks help clarify roles and accountability across IT, engineering, and operations, which is critical when dealing with interconnected cyber-physical systems. At last, <134> Regulatory Frameworks will ensure <106> Compliance with operational standards and help to operate in a structured way across different departments.

To control and monitor the implementation of these different frameworks <102> BOD should actively use <101> Audits.

Key lessons and issues

Adopting Industry 4.0 is not purely technical. It requires the <124> Organizational Culture toward a more data-driven decision-making. Intuitive <117> Leadership styles should be changed to leadership styles more adaptive to data. It also requires internal <129> Processes to be checked and updated. A new system requires a new way of thinking and working. For these new processes and activities, it is important to have a <131> RACI framework as explained in the previous part. <121> Maturity through this and other <119> Management Frameworks is not only needed to ensure consistency but also to decrease vulnerability and increase cybersecurity, since the whole organisation is dependent on the software.

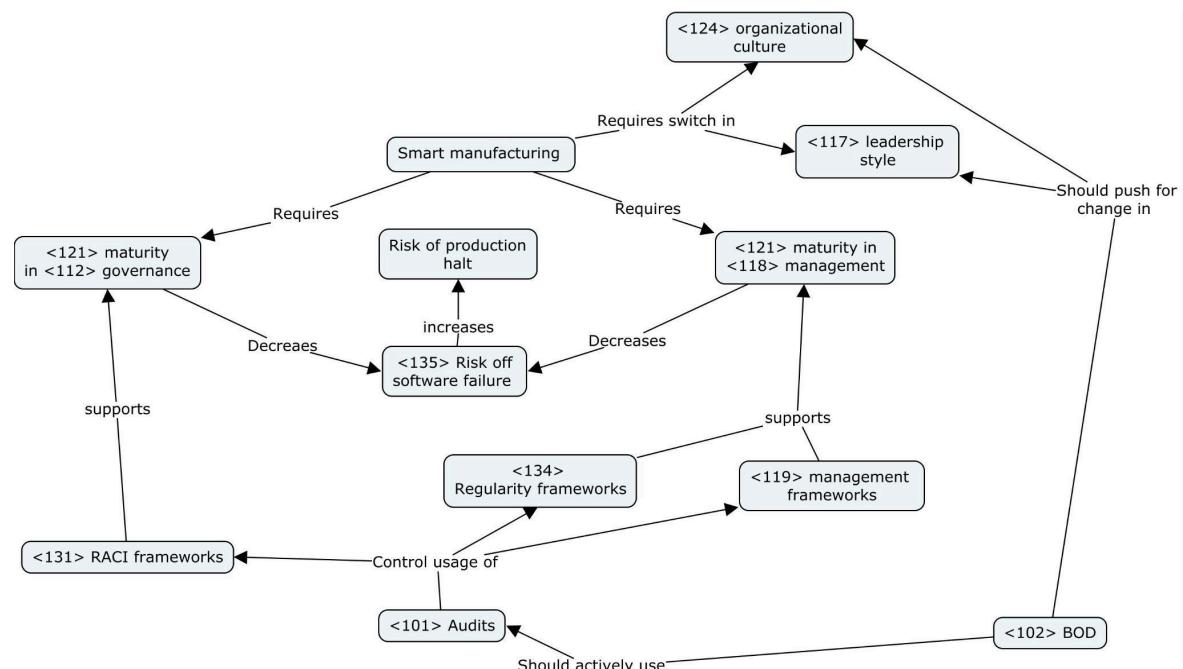


Figure 1: Concept map smart manufacturing, theme 1

Smart manufacturing/Industry 4.0 - theme 2

Introduction

Smart manufacturing tightly integrates digital and physical systems. It links the traditional manufacturing environment to sensors, robotics, AI, and cloud platforms. By combining these fields, new governance challenges in IT and IT management arise. Unlike earlier IT governance models, smart manufacturing requires alignment between IT and the operational technology that runs the machinery and processes.

Relation to theme 2

This new requirement poses extra challenges for <212> the Governance of IT and IT management. Issues like <205> Cybersecurity Supply Chain Risk Management and <216> Information Security Management System become central as IT disruptions also have operational and financial consequences. To manage the new systems, <219> Managed Service Providers may be employed. Governance of the full digital supply chain is crucial in this case to foster smooth collaboration and prevent disruptions. Lastly, the interconnectedness of the systems means <233> Vulnerability Management becomes critical, as the high interdependency between systems means the consequences of poor segmentation or patching can be severe. These complexities require proper governance of the alignment between IT systems and operational technology.

Key issues and lessons

The smart manufacturing industry teaches that <212> Governance of IT must go beyond IT departments and include industrial operations in its risk management. Digital systems that automate critical operational functions need a strong <216> Information Security Management System to ensure the protection of production data and ensure system availability. <205> Cybersecurity Supply Chain Risk Management is equally indispensable, as without full visibility of the complex interconnected systems and possible <219> Managed Service Providers, organizations are exposed to disruptions and cannot minimize their effects. Lastly, <233> Vulnerability Management is indispensable to ensure the segmentation and patching to ensure risks to the whole system are limited.

Smart manufacturing clearly shows the need for industry-specific <212> Governance of IT. In this industry, where IT systems and operational technology are so interconnected, governance of IT must make sure that risks are minimized by not only having proper <205> C-SCRM and <216> ISMS, but it must also manage the connection to operational technology.

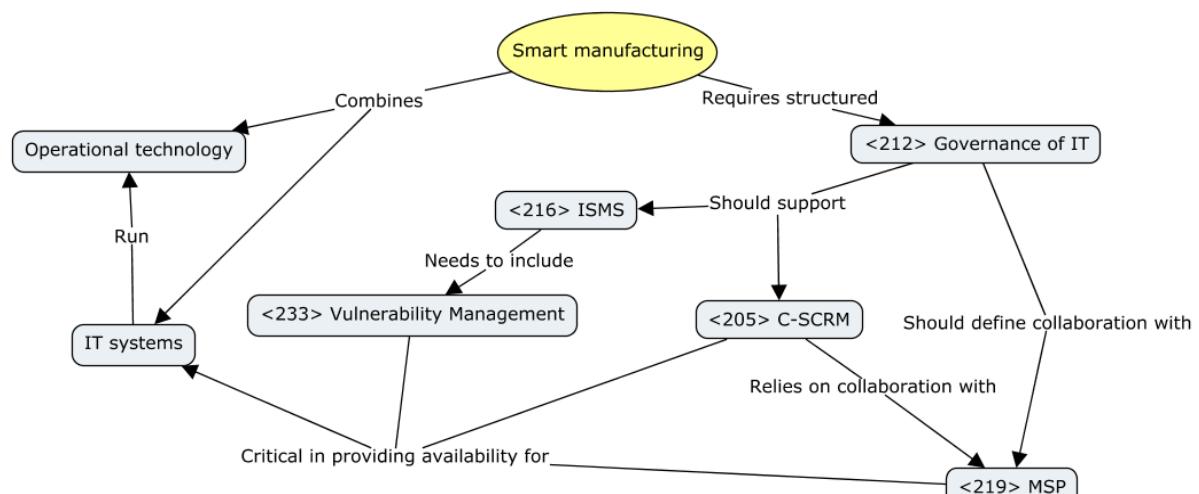


Figure 2: Concept map smart manufacturing, theme 2

Retail and Digital Commerce: Omnichannel retail - theme 1

Introduction

Omnichannel retailers are complex organisations that coordinate online and offline operations, inventory, logistics, marketing, and customer service. This subdomain of retail requires structured systems that integrate the different channels toward shared goals (e.g., customer satisfaction, brand consistency)

Relation to theme 1

Since omnichannel retail is a multi-channel process, it requires effective corporate governance. The <102> Board of Directors (BoD) and <108> CxOs must oversee diverse and dynamic domains - from vendor management and product sourcing to data protection and brand reputation. The <126> Organizational Culture must support cross-functional integration. There must be coherence across the different environments by having a well-defined <122> Mission and <127> Policy.

Key Issues and Lessons

Omnichannel retail <112> Governance and <118> Management involve creating a cohesive strategy that integrates all customer touchpoints. This is more complex than subdomains, in which the focus is solely on physical or online sales. The <135> Risks encompass a broader range of threats.

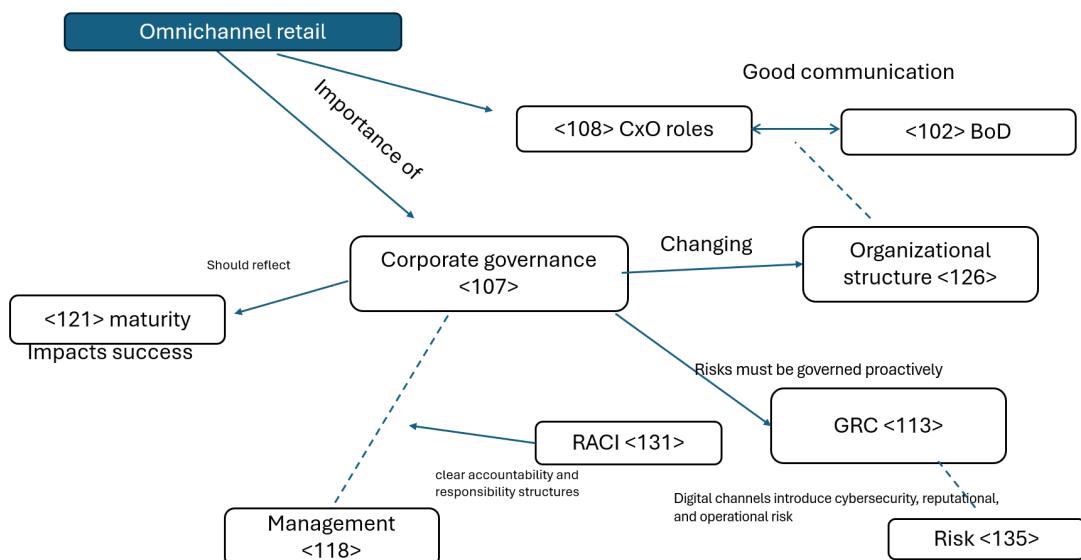


Figure 3: Concept map Retail and Digital Commerce, theme 1

Retail and Digital Commerce: Omnichannel retail - theme 2

Introduction

In Theme 2, we explore how governance structures must evolve when organisations undergo digital transformation. Omnichannel retail companies that began as brick-and-mortar only provide a particularly strong case for illustrating that governance of IT is not merely about managing technology, but about strategic decision-making.

Relation to theme 2

The shift from brick-and-mortar to omnichannel retail is not just a technological upgrade. This digital transformation reshapes the entire <112> Governance landscape with new structures. Companies that transition to omnichannel retail start with minimal <212> IT Governance, and their IT management is largely tactical but not strategic. However, the expansion into online channels (e-commerce, mobile apps, digital customer experience) requires <437> Strategic Alignment of IT with business goals, clear accountability, and decision-making structures. A shift in the <124> Organisational Culture is needed, and <108> CIOs and CTOs must participate in the <102> BoD, signaling that the organization treats IT governance as a strategic priority.

As customer data becomes central to omnichannel operations, implementing an <216> Information Security Management System (ISMS) is essential. And given the reliance on external platforms and service providers, <232> Vendor Assessment becomes a critical governance function. To ensure these third parties meet the standards for performance, clearly defined <323> Service Level Agreements (SLAs) must be established

All these changes reflect the main idea of theme 2: that leadership must recognize and position IT as a strategic enabler of value and transformation, rather than merely a support function.

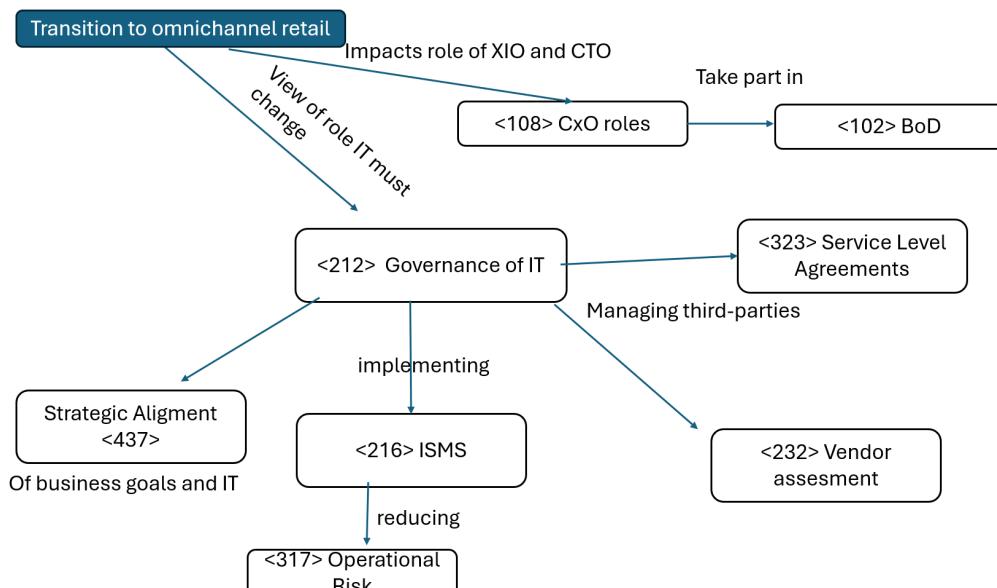


Figure 4: Concept map Retail and Digital Commerce, theme 2

Agriculture and Farming - theme 1

Introduction

Crop farming involves the production of grains, vegetables, and industrial crops. It is a foundational part of the agri-food sector, increasingly influenced by data-driven tools such as precision agriculture and Farm Management Information Systems (FMIS).

Relation to Theme 1

Crop farming spans diverse organisational models, including small family farms, cooperatives, and multinational agribusinesses. These actors differ in their <112> Governance capacity and <126> Organisational Structure. Many smallholders lack formal <120> Management Systems and operate with low <121> Maturity, relying on informal routines rather than documented processes. Larger actors may have clearer control structures, yet coordination between <118> Management and governance levels remains weak.

Key Issues and Lessons

Low <412> Digital Maturity in farming often reflects weak role and responsibility frameworks such as <131> RACI. This limits consistent execution of strategies for managing <135> Risk and ensuring <106> Compliance. The introduction of Farm Management Information Systems (FMIS) can support maturity growth, but only if aligned with local <112> Governance structures. To improve resilience and accountability, organisations must embed <113> GRC (Governance, Risk and Compliance) capabilities, adopt structured <119> Management Frameworks, and clarify decision rights across actors.

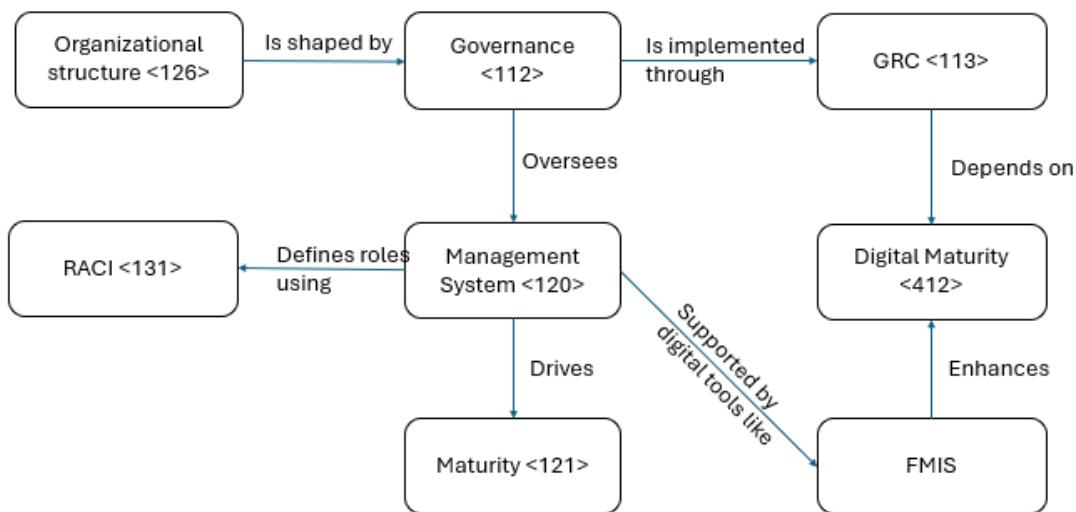


Figure 5: Concept map Agriculture and Farming, theme 1

Agriculture and Farming - theme 2

Introduction

Crop farming increasingly relies on digital infrastructure for core processes such as irrigation control, yield monitoring, and planning. Tools like Farm Management Information Systems improve precision and efficiency, but also introduce new dependencies. As digital systems become more embedded, farming operations become more exposed to IT disruptions. System failures can have serious consequences for food security.

Relation to Theme 2

Managing this digital dependency requires clear **Governance of IT** to define responsibilities for IT decision-making and system oversight. Crop farming uses both digital systems and physical equipment, so effective management of **Operational Technology** is also critical. Ensuring that digital tools support farm objectives falls under **Strategic Alignment**, which connects IT planning with operational outcomes.

Key Issues and Lessons

Many farms do not conduct **Business Impact Analysis (BIA)**, so they lack insight into which digital failures would critically disrupt operations. Without this, recovery plans and system prioritisation remain weak. Formal **IT Service Management (ITSM)** practices, such as incident handling, system monitoring, and support coordination, are often missing in smaller farms.

This increases **Operational Risk**, especially in farms with limited IT expertise. At the same time, exposure to external threats continues to grow. Strong **Cybersecurity** controls are needed to protect digital tools used in crop production. To ensure resilience, farms must integrate governance, risk awareness, and IT operations into a unified strategy.

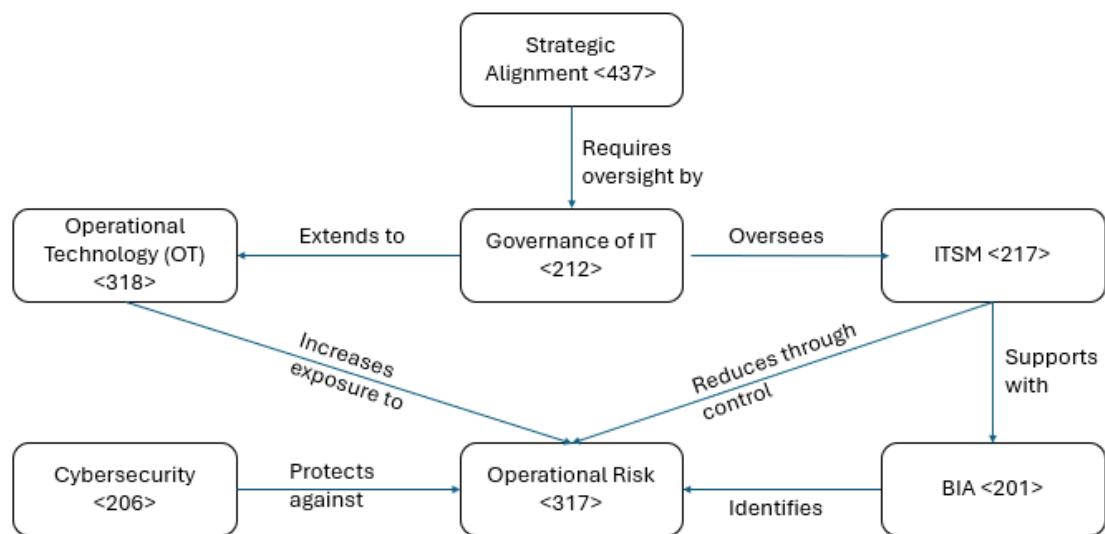


Figure 6: Concept map Agriculture and Farming, theme 2

Comparison of manufacturing and retail & digital commerce - theme 1

In both the smart manufacturing industry and the omnichannel retail industry, there is a need for maturity in management and governance, but the reasons for this differ. In the smart manufacturing industry, maturity in governance and management will decrease the risk of software failure. Within the omnichannel industry, this maturity is needed for cross-functional alignment of governance and management. This alignment is for subjects like the company's mission, policy, and brand consistency.

In both industries, there is a need for clear RACI frameworks. Within the smart manufacturing industry, this is needed due to the high interdependence of software and the production environment. RACI frameworks will avoid gaps in responsibility and ensure safe, coordinated actions. Within the omnichannel industry, role clarity ensures consistent execution across digital and physical platforms. Although the technology may be less complex than in manufacturing, the coordination demands are higher due to customer-facing variability.

The risks in the two industries are different. In smart manufacturing, risk is closely tied to operational continuity and cybersecurity. A single system failure can have big effects. The biggest risks are internal mistakes or failures within the organization. In the omnichannel industry, the biggest risks are more from outside the organization. Think about vendors failing the supply or customers with inconsistent behaviour.

Comparison of manufacturing and retail & digital commerce - theme 2

Manufacturing and retail are both undergoing major digital transformations, but their IT governance challenges differ due to sector-specific structures and risks. Smart manufacturing integrates IT and operational systems. Systems like IoT, robotics, and MES must be governed not just for performance, but for safety and uptime. This requires structured governance to align IT and industrial operations, especially as disruptions can halt production and incur significant losses. Governance in manufacturing must also address technical complexity, third-party risk, and lifecycle vulnerability management.

In contrast, retail and digital commerce, especially brick-and-mortar firms shifting to omnichannel models, face governance challenges centered on data, customer experience, and digital scalability. Initially, IT governance in these firms is often reactive. But as digital channels expand, strategic alignment becomes crucial. IT leaders must gain board-level influence, and governance must evolve to manage vendor relationships, customer data protection, and cross-channel integration. Omnichannel transformation makes clear that IT is a strategic enabler, not just a support role.

Smart manufacturing and omnichannel retail have similar needs from governance of IT, they need to keep the systems running. However, reasons differ as manufacturing emphasizes operational continuity as disruptions cause major losses, while retail focuses on the security of customer data, strategic agility, and digital service management, as customer privacy must be respected, and they aim to get competitive advantages over competitors. Both demonstrate that governance of IT must adapt to sector-specific pressures to effectively support transformation and mitigate risk.

Comparison of manufacturing and agriculture & farming - theme 1

Looking at the maturity within governance and management, there is a big difference between the agriculture and farming industry and the smart manufacturing industry. Within the agriculture industry, there are lots of different organizational models. There are small organizations that rely more on informal practices, and there are big organizations that have more maturity in governance and management. Within the smart manufacturing industry, the need for maturity in governance and management is way bigger because of the dependence on software and cyber-physical systems.

Looking at the role and responsibilities framework, agricultural operations often lack structured role definitions, especially in small or informal settings. The absence of RACI frameworks weakens accountability and limits the ability to manage risk consistently. Smart manufacturing environments depend on precise role mapping due to the interdependence of cyber-physical systems. RACI frameworks are critical to avoid blind spots and ensure coordinated actions across IT and production teams.

There is also a clear difference in organizational culture and change. Within smart manufacturing organizations, the shift towards new technologies requires big changes in the organizational culture. In agricultural organizations, the opposite thing happens. Cultural resistance to formalization and data use is common, particularly among traditional family farms.

Comparison of manufacturing and agriculture & farming - theme 2

Both manufacturing and agriculture are becoming more digital, but they differ a lot in how IT Governance. In smart manufacturing, technologies like IoT, AI, and cloud platforms are integrated with physical manufacturing. This demands strong management of the interface between IT and operational technology. Because automation is high and system failure can halt production, the Governance of IT should focus on defining structured ISMS, C-SCRM, and Vulnerability Management to reduce risk.

In agriculture, particularly crop farming, digital tools support irrigation, planning, and yield analysis. In some more advanced settings, the IT systems are being embedded in the operational systems. These advanced settings are thus similar to the smart manufacturing industry, and disruptions thus cause similar consequences, and the same need for defining structured ISMS, C-SCRM, and Vulnerability Management to reduce risk is present, critical. However, in less advanced settings, mostly smaller farms, there are fewer embedded systems and rely less on the systems. Here, governance of IT is less critical as the consequences of disruption are not as impactful. ITSM practices like incident response and system monitoring are rarely in place, and few smaller farms conduct Business Impact Analysis. This would need to be addressed if a farm wants to expand and become more efficient using IT systems.

While both industries are becoming more digitally integrated, their need for governance of IT varies based on technological maturity. Smart manufacturing needs robust, formal governance to manage the high interdependencies between IT and operational systems. In agriculture, the urgency for governance increases with digital advancement, but many smaller farms remain underprepared for IT-related expansion as they lack the procedures to prevent and resolve disruptions.

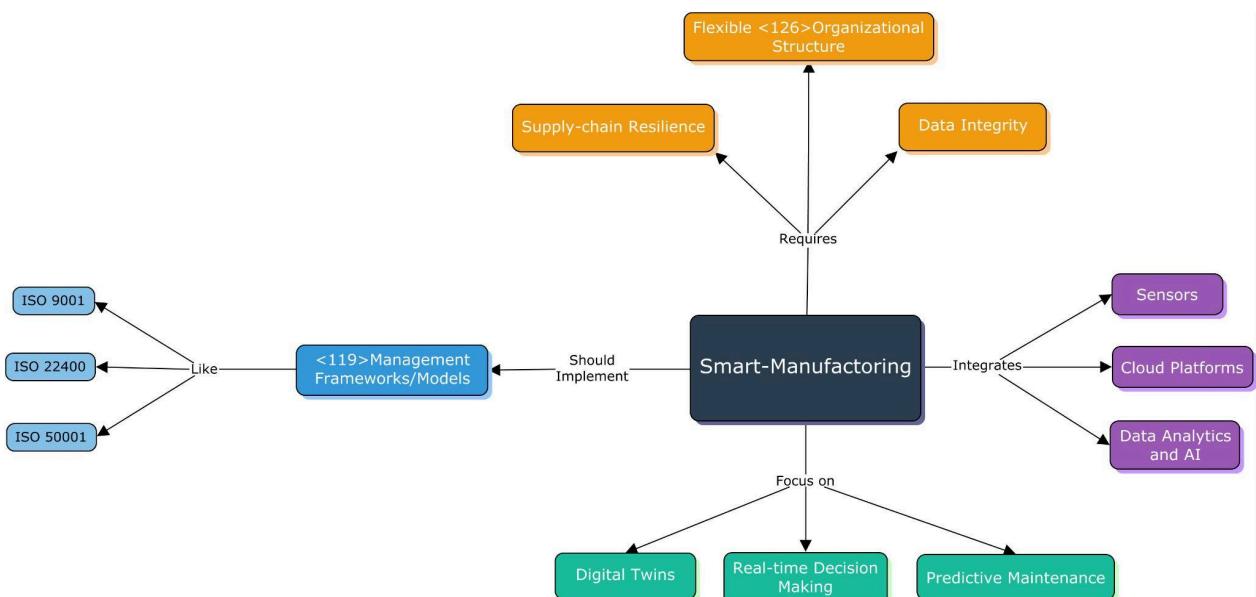
THEME 1

Manufacturing (Smart Manufacturing/Automation)

Manufacturing today is undergoing a profound shift as traditional production processes become deeply intertwined with digital technologies. In the **Smart Manufacturing** niche, factories leverage Industrial IoT, robotics, **digital twins**, and **advanced analytics** to transform raw materials into high-value products with unprecedented speed and precision. This convergence demands flexible **<126> Organizational Structure** to support both capital-intensive machinery and real-time data flows, and drives new **<104> Business Model** innovation where responsiveness and customisation replace one-size-fits-all mass production.

At the governance level, Smart Manufacturing elevates the role of **<112> Governance** bodies to oversee integrated IT/OT environments and embed **<113> GRC** (Governance, Risk and Compliance) across every layer of the enterprise. Boards and executive committees must extend their oversight beyond traditional safety and quality standards to include cybersecurity frameworks, ensuring that supply-chain resilience and data integrity are managed with equal rigor.

On the management side, Smart Manufacturing rests on robust **<120> Management System** standards and **<119> Management Frameworks** (such as ISO 9001 for quality, ISO 22400 for **<116> KPI** and ISO 50001 for more sustainable energy) that coordinate cross-functional workflows and continuous improvement cycles. Leaders monitor not only traditional **<116> KPIs** but also **predictive maintenance** metrics, energy efficiency, and digital maturity indicators advancing **<121> Maturity** and nurturing an **<124> Organisational Culture** where data-driven decision-making and operational agility go hand-in-hand.



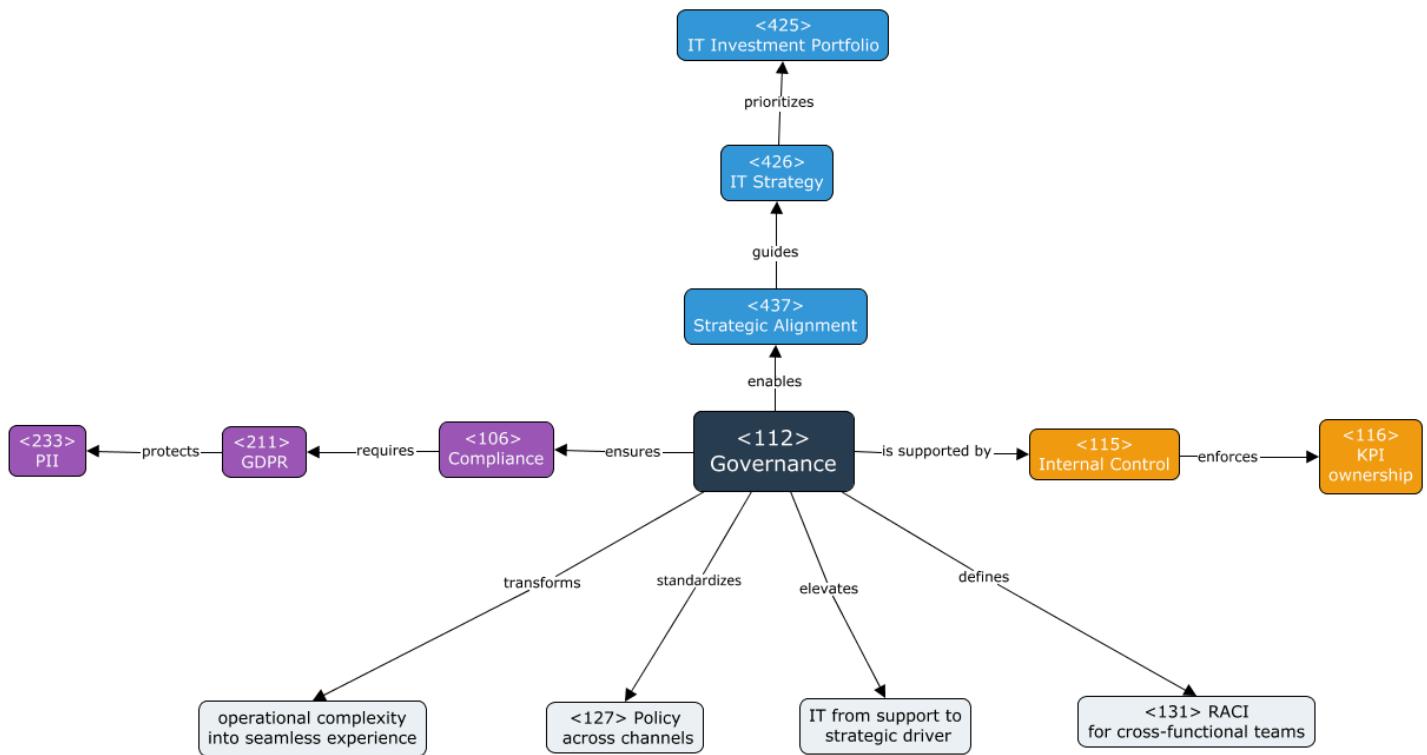
Retail (OmniChannel Retail)

In the ultra-dynamic retail landscape, omnichannel models have revolutionized the way firms interact with customers, blending physical, digital, and mobile touchpoints. This amplifies the importance of **<112> Governance**, which insulates decision-making frameworks, accountability, and risk management on each converged channel.

Clear **<131> RACI** structures and defined decision rights are essential to manage responsibilities across marketing, inventory, and customer support. **<115> Internal Controls** play a critical role in enforcing accountability for key **<116> KPIs**, such as delivery time and customer satisfaction, especially within cross-functional teams.

Compliance with legal and regulatory obligations, such as the **<211> GDPR**, falls into the domain of **<106> Compliance**, requiring robust data governance to protect **<223> PII** and uphold customer trust. Unified **<127> Policies** ensure consistent returns, promotions, and messaging across all platforms.

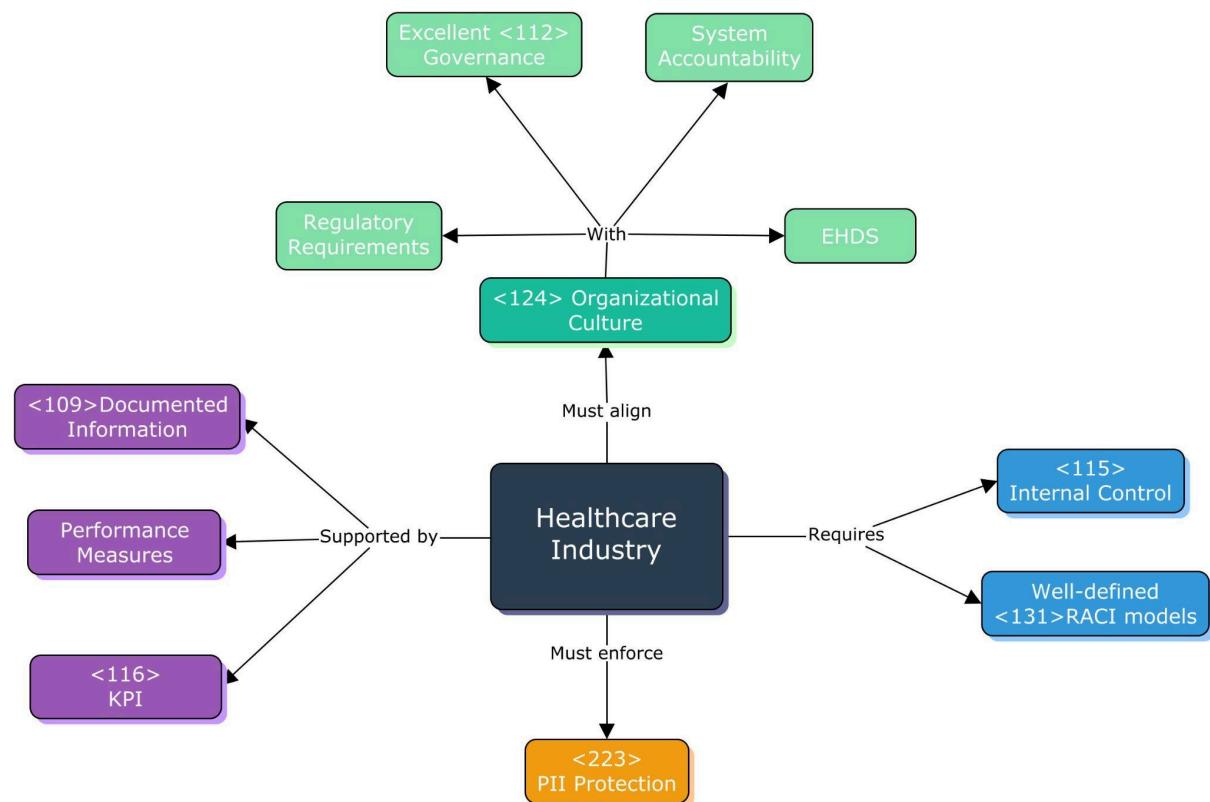
Strategically, **<437> Strategic Alignment** bridges IT governance and long-term business goals, influencing **<426> IT Strategy** and investment in tools like CRM and OMS. Ultimately, governance transforms operational complexity into sustainable, high-quality customer experiences, turning IT from a support function into a business enabler.



Healthcare (Hospital IT / EHR Systems)

The healthcare sector, and hospitals in particular, are highly regulated environments that require excellent **<112> Governance** to maintain ethical care, operational control and system accountability. Hospital information technology systems, or electronic health record (EHR) systems, infuse **<120> Management Systems** into clinical and administrative workflows to smooth the performance, continuity of care and strategic alignment. Within this structure, **<107> Corporate Governance** is facilitated through clearly defined **<126> Organizational Structure** and the presence of **<136> Top Management** and **<108> CxO** roles.

A robust **<115> Internal Control** and a well-defined **<131> RACI** models give responsibility and traceability between functions. Protection of **<223> PII** is critical and calls for strict **<106> Compliance** with **<211> GDPR** and future EU standards like the EHDS. Healthcare organisations depend on structural **<119> Management Frameworks** supported by **<109> Documented Information** and performance measures such as **<116> KPI** (Key Performance Indicator). The development of digital capabilities tracks the **<121> Maturity** of governance arrangements, which must align **<124> Organisational Culture** with regulatory requirements, ethical expectations, and public accountability.



THEME 1

Retail e IT Management (OmniChannel Retail)

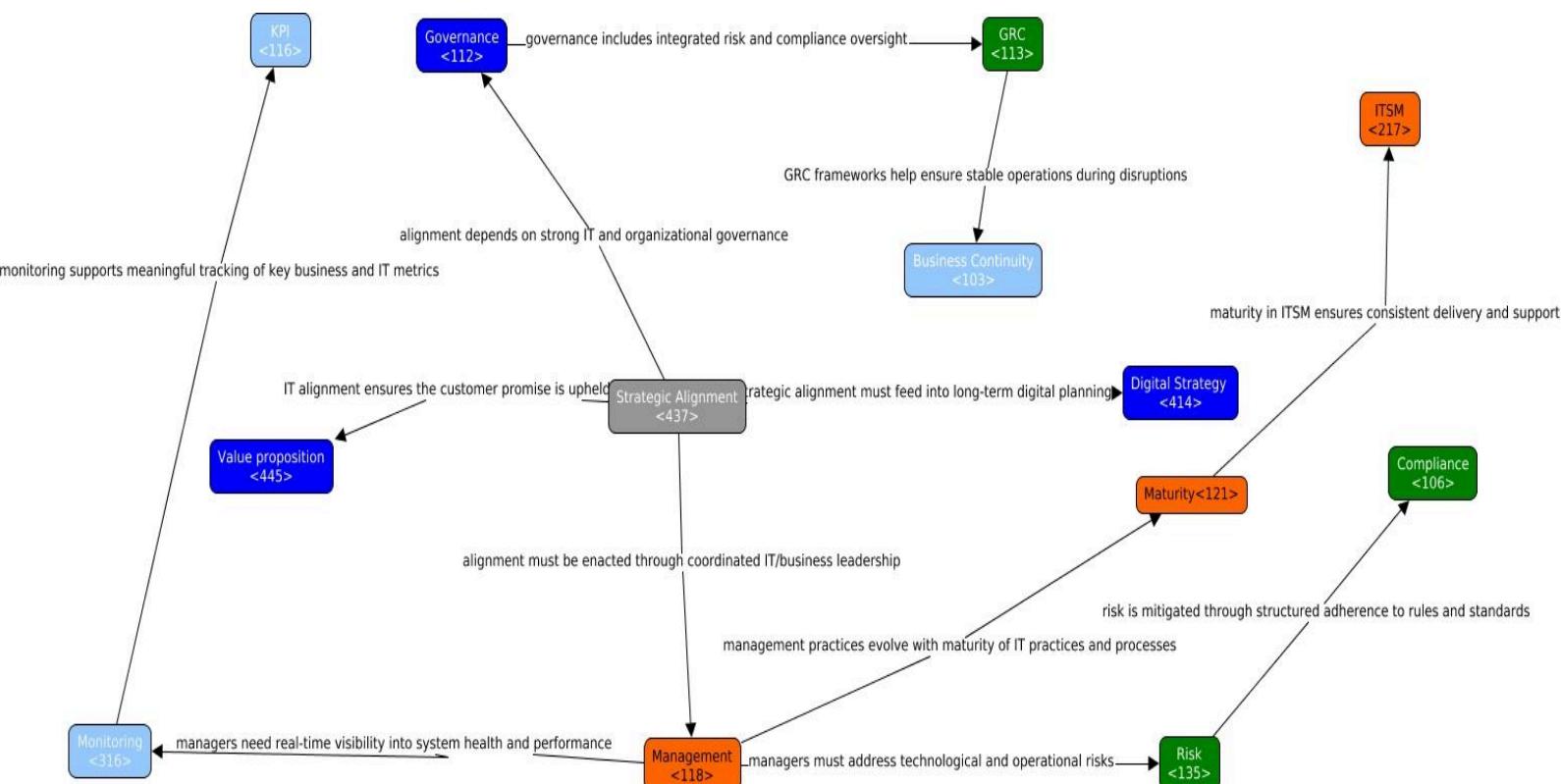
The retail industry consists of all companies that sell goods and services to consumers. There are many different retail sales and store types worldwide, including grocery, convenience, discounts, independents, department stores, DIY, electrical and speciality. This is one of the most dynamic and technological sectors in the global economy.

Retail businesses use complex systems and processes, from inventory and supply chain platforms to customer relationship management and digital marketing platforms. Managing this ecosystem not only requires some know-how, but it demands some concerns about **<215>** information security and the **<202>** CIA triad, mostly focused around the user information.

These principles become especially important in the case of omnichannel retail, where there are multiple different channels that need to be coordinated to ensure a seamless experience for the user, which is the most important part.

IT Management in the context of *Omnichannel Retail* requires great **<212>** governance of all the IT systems. This not only ensures that these systems follow the regulations imposed by a specific governing body (e.g. **<211>** GDPR) regarding user information, but maintains an efficient **<231>** supply chain between all the involved parts, to guarantee the best experience for the user.

The success of omnichannel retail relies on the implementation of multiple technologies and systems, such as Customer Relationship Management platforms, order management systems, and real-time inventory tools. This is even more relevant with new technologies like AI-powered shopping agents. IT Management must evolve to be able to tend the way computers think, which could be very different from the systems implemented now.



Healthcare and IT Management

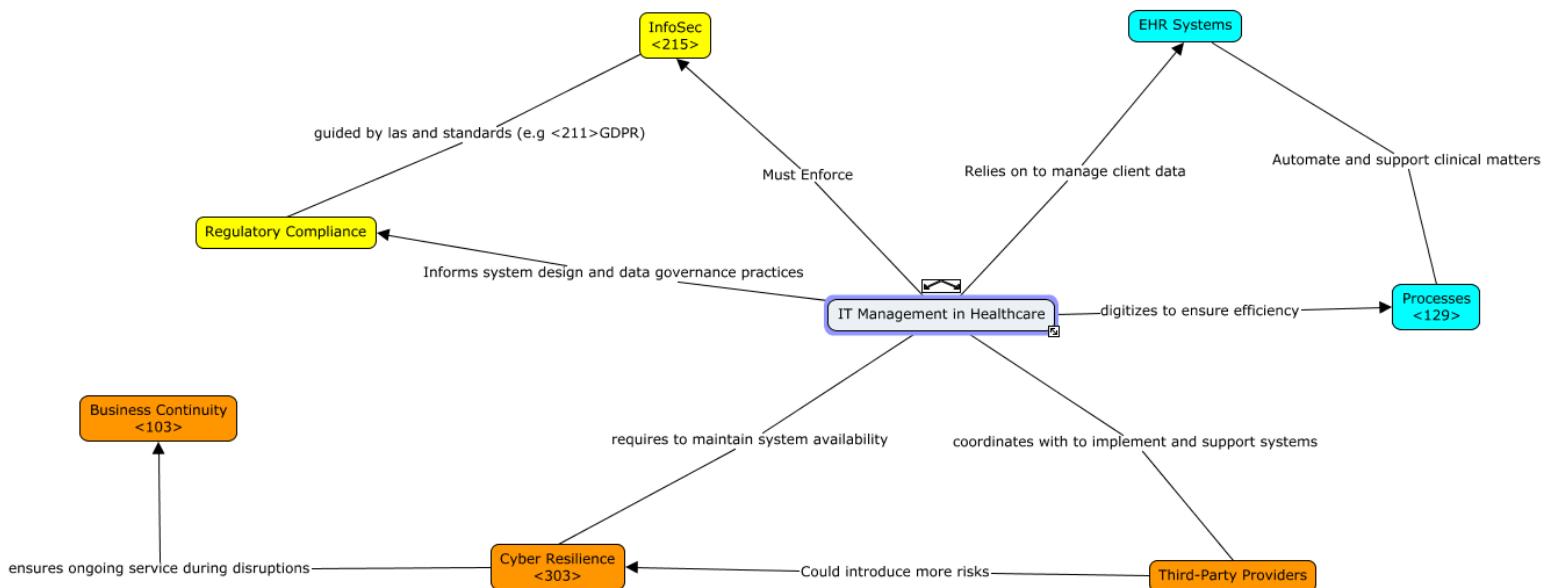
The healthcare industry is getting more reliant on IT to improve patient outcomes, make operations easier, and follow complex regulations. In this environment, IT Management is crucial in ensuring that systems not only function reliably but also comply with the <202> CIA triad, accessibility, and care quality. Almost all the steps involved with healthcare require IT to be efficient. IT management becomes very important to synchronize all the steps present in this big system.

This is especially evident in hospitals, where IT infrastructure must support a big range of <129> processes across clinical, administrative, and logistical fields. This is made even more important with Electronic Health Record (EHR) systems, which are basically centralized databases for managing patient information.

Effective IT Management ensures that EHR systems are coordinated with laboratory tools, medical imaging systems, and pharmacy platforms, ensuring that all these systems work together and maintain the same level of <206> cybersecurity throughout all of them.

The complexity of hospital settings can come with some difficulties, especially in managing all of its different components. These systems must be highly available and <303> cyber resilient, ensuring <103> business continuity. At the same time, they must follow rules to ensure that <215>information security and <208>privacy of its users is up to <211> GDPR standards . This is done through coordination between IT staff, clinical personnel, and third-party entities.

Finally, healthcare systems and especially EHR systems, must be very flexible. This is in fact true for most systems that work on a large scale, to ensure availability of the service. As these systems have a lot of moving parts, it is required to ensure that these parts do not depend on each other, and can handle errors in a subtle way.



Manufacturing and IT Management

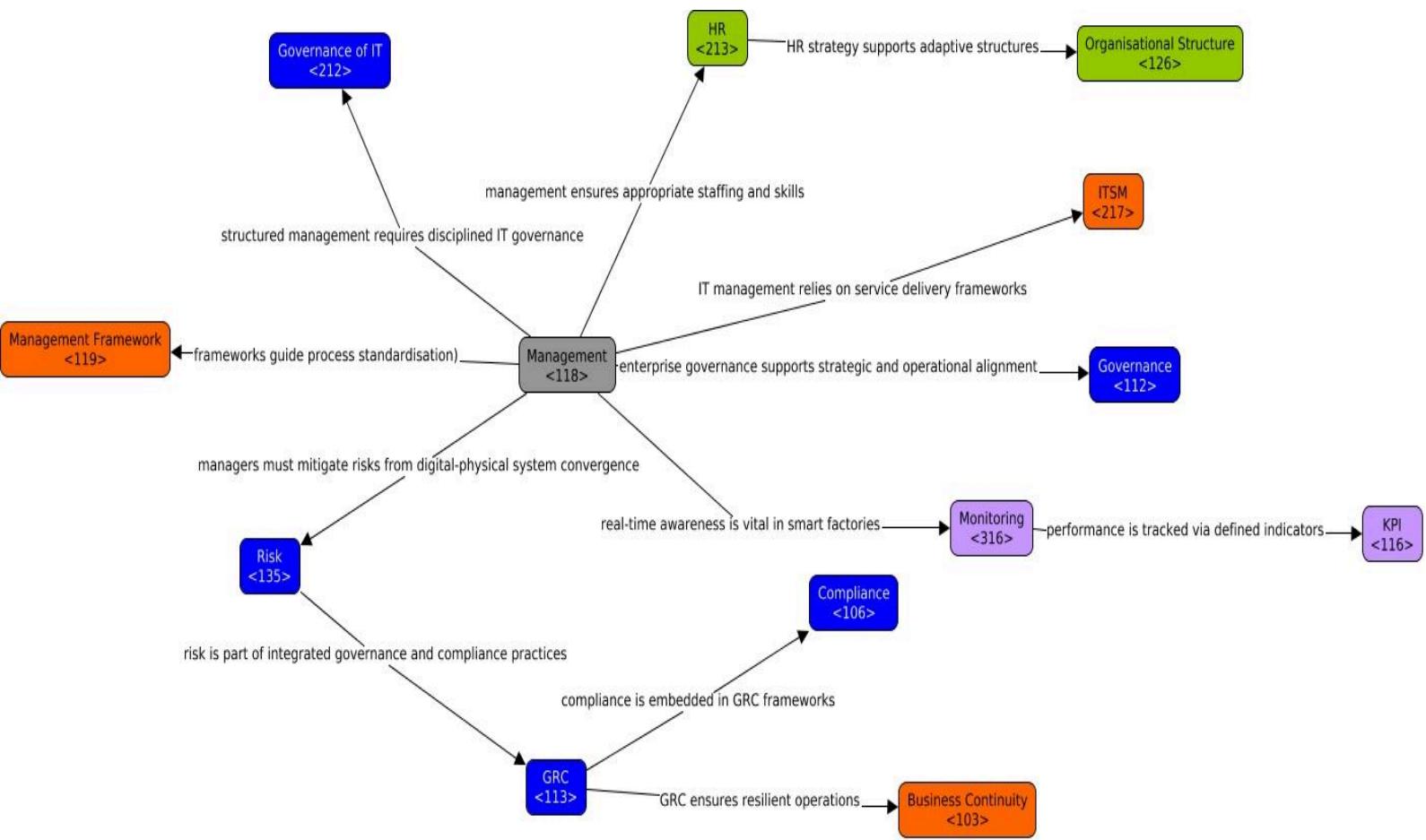
Smart Manufacturing integrates physical production with intelligent digital platforms like Industrial IoT, robotics, and predictive analytics. In this context, IT Management plays a pivotal role — not only in supporting the technology stack but in ensuring strategic alignment, resilience, and operational control across the factory floor.

Managing IT in Smart Manufacturing requires mature <118> Management structures and disciplined <212> Governance of IT to coordinate complex IT/OT environments. Clear <112> Governance and decision rights are essential, particularly during incidents requiring fast cross-domain response. The convergence of digital and industrial systems also increases <135> Risk, making <113> GRC and <106> Compliance critical to ensuring <103> Business Continuity in high-stakes environments.

Structured <217> ITSM practices and <119> Management Frameworks (like ISO 27001) help enforce reliable operations and change control across IT/OT systems. An adaptive <126> Organisational Structure and strategic <213> HR planning ensure the right talent is in place to manage complex digital infrastructure.

IT Management also depends on continuous <316> Monitoring and robust <116> KPI frameworks to maintain performance, safety, and quality. Real-time data enables predictive maintenance and operational agility, helping organisations advance <121> Maturity and position IT as a driver of continuous improvements to the production line.

IT Management also has a heavy focus on machine maintenance, as the technological integrations put into the manufacturing process could halt entire productions if they break. Choices made by management on what machines to invest in should take into account maintainability and replaceability of these machines.



THEME 1

Manufacturing vs Retail

Organizational Design & Governance Structures - Smart Manufacturing adopts hybrid or matrix models to balance heavy capital-equipment investments with agile, data-driven teams embodying a more flexible **<126>Organizational Structure** that supports cyber-physical integration. **<112>Governance** bodies extend oversight into both IT and OT domains, elevating **<113>GRC** from a compliance activity to a strategic imperative that spans cybersecurity, quality, and supply-chain resilience .

Standards, Controls & Compliance - OmniChannel Retail, by contrast, hinges on clear **<131>RACI** structures and robust **<115>Internal Controls** to allocate responsibilities across marketing, inventory, and support . Ensuring **<106>Compliance** with **<211>GDPR** and enforcing unified **<127>Policies** for returns, promotions, and data protection safeguard PII and uphold customer trust across all channels.

Strategic Alignment & Organisational Maturity - Both sectors hinge on strong **<437>Strategic Alignment** between IT investments and business objectives . Smart Manufacturing leverages digital-twin simulations and integrated ERP–MES–PLM systems to optimize end-to-end supply-chain resilience, while Retail channels investments into CRM and Order Management Systems that unify customer experiences. In each case, advancing organisational **<121>Maturity**, from ad hoc to optimised, depends on embedding governance and management practices into everyday operations, ensuring agility, resilience, and continuous improvement are not just goals but lived realities .

Manufacturing vs Healthcare

Both Healthcare IT and Smart Manufacturing require strong organizational and governance capabilities, but in ways specific to the sector. In manufacturing, industrial IoT and automation use require adaptive organizational structures and crisp management coordination for coordinating production with digital systems. Governance bodies prioritize operational effectiveness, quality management, and resiliency, usually through integrated risk and compliance practices such as **<113> GRC** and performance tracking through **<116> KPIs**.

Healthcare, particularly in hospitals, is centered on patient safety, compliance with rules, and moral responsibility. The implementation of Electronic Health Records (EHRs) increases the need for robust **<112> Governance** and data protection law compliance, such as **<211> GDPR**, mainly because of the sensitivity of **<223> PII**. Governance bodies in this case involve synchronizing clinical, technical, and administrative tasks within frameworks that offer continuity of service and legal compliance.

Although each industry depends on computerized systems and systematic **<119> Management Frameworks**, their cultures differ: manufacturing emphasizes adaptability and streamlining, while healthcare requires prudence, trust, and public accountability.

THEME 2

Retail vs Healthcare

Despite both industries operating in very different fields, both are getting much more dependent on IT systems to perform their operations on a larger scale.

In omnichannel retail, IT Management is centered on integrating diverse sales and communication channels (websites, apps, physical stores, and social platforms) into a seamless customer experience. This requires real-time data synchronization, agile system design, good coordination between IT strategy and business objectives.

Similarly, in hospital settings, IT Management is focused around the coordination of Electronic Health Record (EHR) systems with various clinical and operational tools. EHR platforms must ensure accurate, up-to-date patient data across departments, including labs, pharmacies, and imaging services. The focus here is not customer convenience, but clinical safety, reliability, and compliance with strict privacy and security standards.

Despite their similarities, the thing that makes them the most distinct is the regulations they are subjected to. Healthcare is “strangled” in regulations that not only have zero tolerance for error, but are very focused on <215> InfoSec.

On the other hand, retail can sometimes be the polar opposite of that. This field is focused on getting the most information possible from its users (and now even AI models) to cater to their preferences. There are still regulations around user information, but these are a bit more bendable than in the previous example.

Retail vs Manufacturing

While operating in different domains, both Omnichannel Retail and Smart Manufacturing rely heavily on IT Management to ensure operational efficiency and strategic value. In retail, IT Management focuses on integrating diverse customer touchpoints — apps, websites, and stores — to deliver a seamless experience. This requires agile <118> Management, real-time <316> Monitoring, and <437> Strategic Alignment with logistics and marketing, often measured by customer-centric <116> KPIs like conversion rates or engagement.

In Smart Manufacturing, IT is tightly integrated with physical systems like robotics and industrial IoT. IT Management here centers on <217> ITSM processes, <103> Business Continuity, and <135> Risk mitigation to ensure uptime and production quality. Unlike retail, which often embraces rapid change, manufacturing tends to adopt new tech more cautiously due to physical infrastructure constraints and stricter <113> GRC requirements.

The biggest difference lies in how data is used. Retail IT thrives on capturing user behavior to personalise experiences — navigating <106> Compliance rules creatively. Manufacturing, however, requires strict data integrity to enable automation and traceability. Ultimately, Retail IT is driven by customer engagement and innovation, while Manufacturing IT is anchored in system resilience and process control.

Governance & IT Management Across Industries

Security and Management of Information Systems



Authors:

- Vasco Félix (IST ID: 99131)
- Andre (IST ID: 99730)
- Tomás Taborda (IST ID: 103641)
- Diogo Cadete (IST ID: 102477)

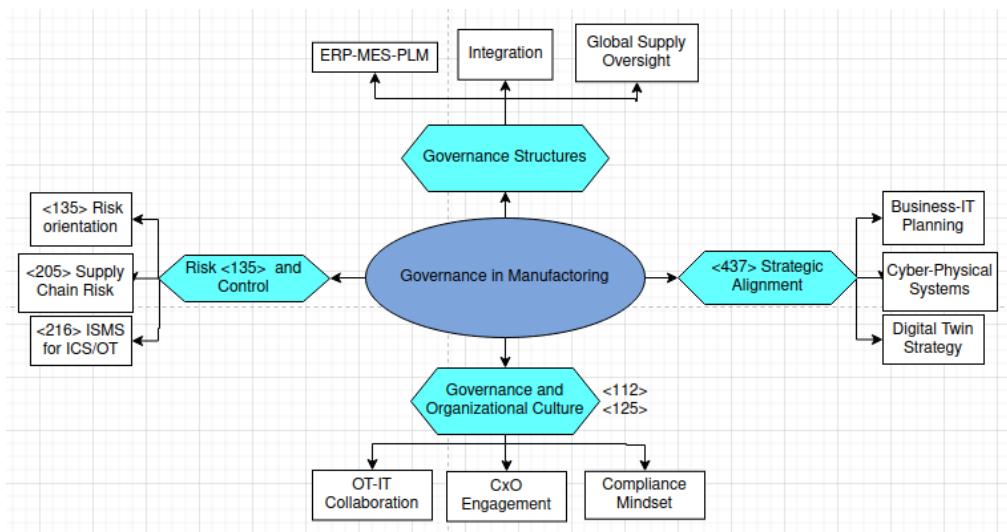
Industries:

- Manufacturing
- Transport and Logistics
- Hospitality and Leisure

Governance in Manufacturing

Governance in the manufacturing industry is inherently complex, as it must coordinate large-scale production systems, multi-tier global supply chains, and technology platforms while maintaining regulatory compliance and business continuity. Effective governance requires mature governance structures that enable integrated oversight across business, operations, and digital domains. These structures must align executive strategy with shop-floor execution, facilitating coordination between board-level decision-makers, <108> CxOs, and production engineers. In multinational manufacturing environments, governance also spans jurisdictional boundaries, necessitating mechanisms for legal conformity, performance accountability, and supplier control across regions. At the cultural level, <112> Governance and <124> Organisational Culture plays a pivotal role in shaping how governance structures operate in practice. Manufacturing organisations often face the challenge of bridging legacy operational mindsets with modern, data-driven approaches. Embedding a culture of compliance, continuous improvement, and cross-functional communication is essential to reduce silos between IT, OT, and management. This is particularly important in the context of Industry 4.0, where cyber-physical systems and predictive analytics are transforming traditional workflows and demanding closer alignment between digital and physical governance domains.

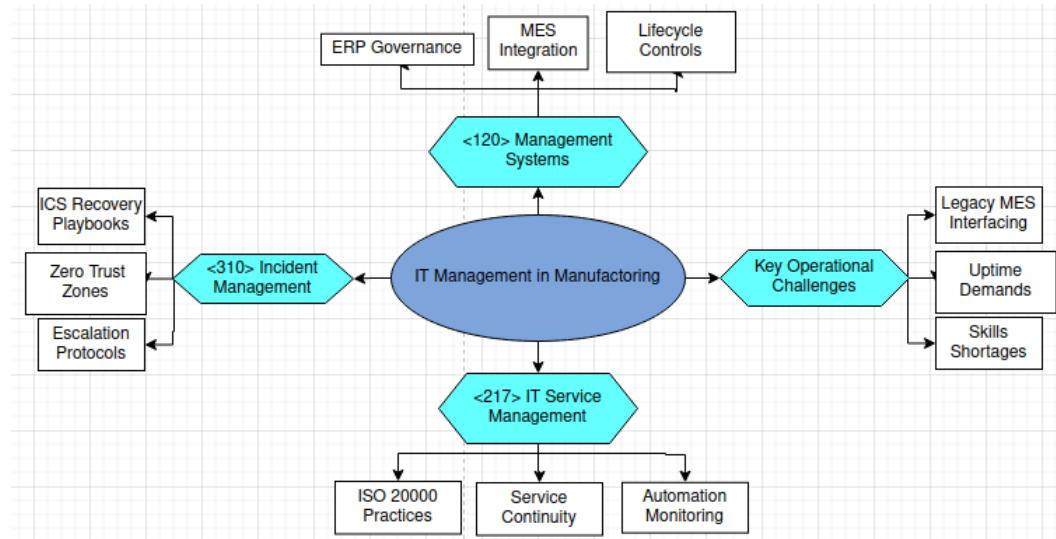
Strategic coherence is facilitated through <437> Strategic Alignment, which ensures that governance decisions reflect both long-term industrial objectives and emerging digital opportunities. Initiatives such as digital twin deployments, predictive maintenance platforms, and supply chain traceability require governance models that can balance innovation with operational resilience. Governance must also address systemic exposure to <135> Risk orientation, as manufacturing environments are susceptible to a wide range of disruptions—from equipment failures and cyberattacks to regulatory changes and geopolitical instability. These risks are magnified by <205> Supply Chain Risk, especially when dependencies on third-party suppliers lack proper evaluation and oversight. To address these risks, governance must embed robust control frameworks, including sector-specific <216> Information Security Management Systems (ISMS) that protect Industrial Control Systems (ICS) and ensure secure convergence between OT and IT. These systems not only guard against data breaches and sabotage but also uphold product quality, worker safety, and intellectual property integrity. Ultimately, strong governance in manufacturing enables organisations to remain competitive, compliant, and resilient in the face of ongoing industrial transformation.



IT management in Manufacturing

IT management in the manufacturing sector operates at the intersection of digital coordination and physical production, requiring a well-structured <120> Management System that governs system architecture, change control, and lifecycle planning. These management systems must support the orchestration of ERP, MES, and OT systems while maintaining compliance with industry-specific standards and facilitating real-time data exchange across production lines. Unlike purely digital sectors, manufacturing must ensure that IT decisions do not compromise mechanical reliability, physical safety, or regulatory obligations—placing increased weight on configuration management, patching discipline, and system documentation. A key component of effective IT management is a mature <217> IT Service Management (ITSM) function. In the manufacturing context, ITSM practices should be grounded in frameworks such as ISO 20000, tailored to support automation infrastructure, machine-to-machine communication, and asset-intensive environments. ITSM must guarantee service availability, performance monitoring, and structured change management in environments where even minor service disruptions can halt production and trigger cascading delays across the supply chain. Emphasis must also be placed on service continuity plans that account for both IT and OT downtime scenarios.

Equally important is the presence of an agile and well-documented <310> Incident Response process. Given the cyber-physical nature of manufacturing, incident management must address not just data breaches or malware infections, but also failures in programmable logic controllers (PLCs), industrial protocols (e.g., Modbus, OPC-UA), and SCADA systems. ICS-specific recovery playbooks, defined escalation paths, and incident communication protocols are essential for responding rapidly to threats while minimizing operational and financial damage. As OT environments are increasingly targeted by sophisticated threats such as ransomware and supply chain attacks, incident management cannot remain reactive—it must be predictive and rehearsed through frequent tabletop and technical simulations. Finally, IT management in manufacturing must grapple with persistent <317> Operational Risk arising from legacy equipment, aging infrastructure, and workforce skills gaps. Many facilities operate on outdated MES or SCADA systems that cannot be easily patched or replaced, requiring creative mitigation strategies and strict access control mechanisms. The shortage of personnel with cross-disciplinary skills in both industrial systems and cybersecurity exacerbates these risks. Successful IT management in manufacturing, therefore, hinges on the ability to align technology operations with strategic industrial objectives, maintain system integrity across diverse lifecycles, and build a culture of continuous learning, resilience, and operational excellence.



Governance in Transport and Logistics

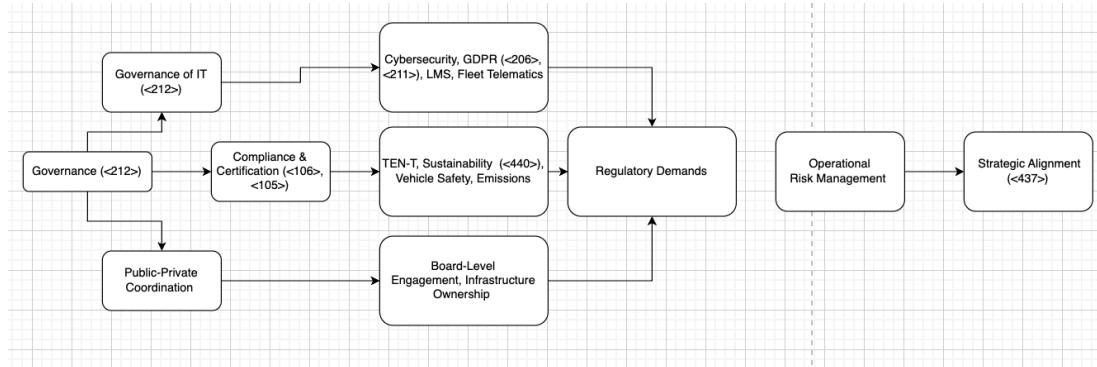
In the Transport and Logistics sector, **<112>** Governance is fundamentally shaped by its infrastructure-intensive nature and the sector's dependency on both physical networks and digital interoperability. Governance responsibilities extend beyond internal structures to include regulatory compliance, stakeholder coordination, and alignment with national and international strategies such as TEN-T and the **<440>** Sustainability Strategy .

Governance must account for the complexity of public-private coordination, where infrastructure is often publicly owned but operations are managed by private or mixed entities. This hybrid environment requires transparent decision-making, board-level engagement, and clear accountability models to ensure safety, service continuity, and user trust.

Strategically, governance frameworks oversee both **<106>** compliance with technical and environmental regulations, and **<105>** certification processes related to vehicle safety, emissions, and operational audits. This also includes ensuring integration between transport modes — a challenge addressed by principles of intermodality and data-sharing mandates such as the eFTI Regulation.

Digitalisation adds a layer of complexity: systems such as LMS (Logistics Management Systems) and Fleet Telematics must be governed with attention to **<206>** cybersecurity , data protection (e.g., **<211>** GDPR), and resilience. While these elements fall under **<212>** Governance of IT, they are increasingly embedded in broader governance agendas due to the strategic role technology plays in logistics coordination and safety management.

In sum, governance in this sector must balance regulatory demands, operational **<135>** risk management, and the need for innovation. Mature governance models integrate inter-organisational agreements, ensure strategic **<437>** alignment, and embed risk governance structures that adapt to geopolitical shifts, climate challenges, and evolving user expectations.



In this image, the tag comes after the concept*

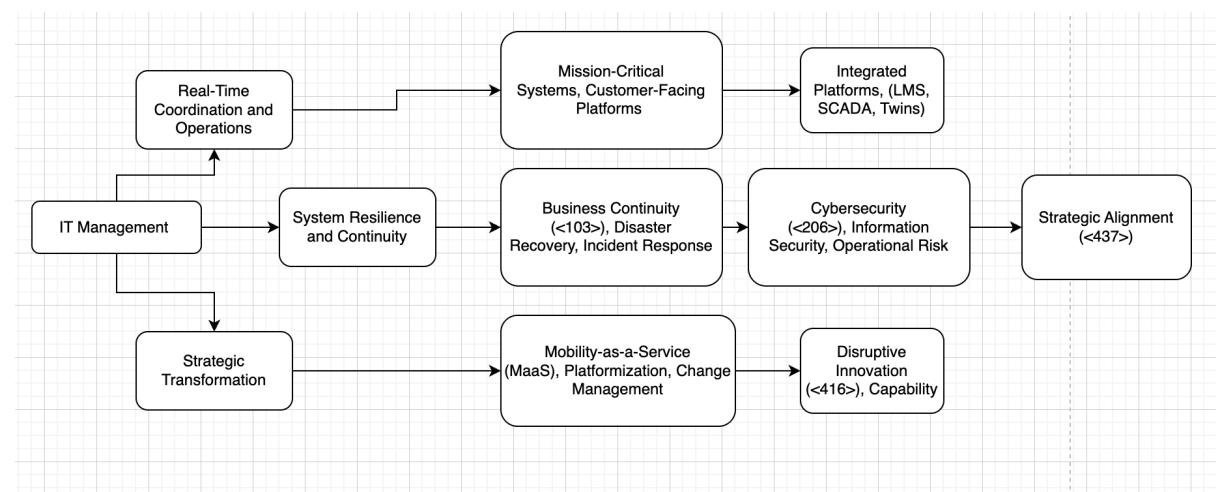
IT Management in Transport and Logistics

IT Management in the Transport and Logistics industry revolves around real-time coordination, system resilience, and the digital orchestration of complex, multimodal operations. Unlike in purely service-based sectors, transport IT spans both mission-critical systems (e.g., fleet telematics, routing algorithms) and customer-facing platforms (e.g., passenger information systems, ticketing apps) — all part of the broader Information Systems.

The challenge is to maintain high availability and performance under dynamic conditions — traffic, weather, geopolitical disruption — which necessitates robust incident response, disaster recovery, and Business <103> Continuity frameworks. <206> Cybersecurity is no longer peripheral but central to operational risk management, tied closely to Information Security.

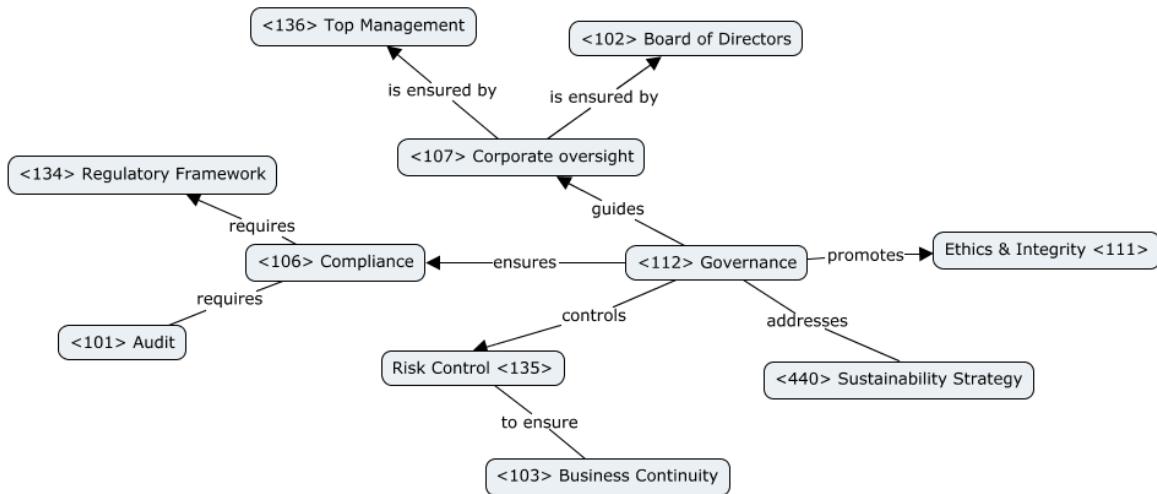
Systems like LMS, SCADA, and port/airport digital twins are increasingly integrated into enterprise-wide IT platforms, supporting infrastructure monitoring and workflow automation. Emerging trends such as AI, drones, and predictive maintenance reflect the growing role of <416> Disruptive Innovation and operational capability.

Strategically, the sector is shifting toward Mobility-as-a-Service (MaaS) — part of the broader Platformization trend — where data orchestration and API management become key. This requires Change Management capabilities to balance short-term operational control with long-term transformation aligned with European strategies like the Sustainable and Smart Mobility Strategy.



In this image, the tag comes after the concept*

Governance in Hospitality and Leisure



Effective governance in the hospitality and leisure sector ensures that companies meet not only financial objectives but also growing social and environmental expectations. As public facing businesses, hotels, resorts, entertainment venues and travel operators must maintain high standards of responsibility and transparency. The foundation for this lies in a well-established <112> Governance System, which provides the structure for guiding long term decisions, defining accountability and ensuring consistent organizational behavior.

At the highest level, <107> Corporate Governance is driven by the <102> Board of Directors and <136> Top Management, who are responsible for setting strategic direction and ensuring that operational standards are upheld. In this industry where service quality, customer satisfaction and safety are very important, leadership must achieve balance between commercial success and customer well-being.

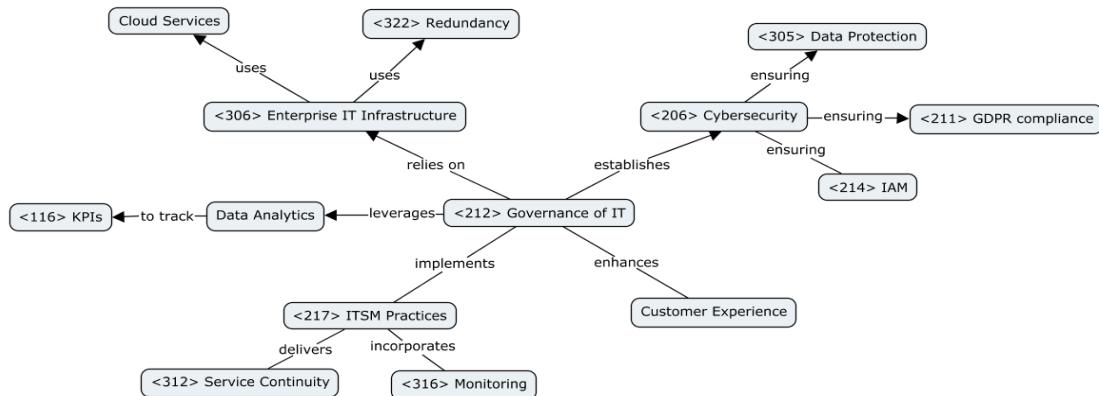
One critical domain within governance is <135> Risk Management. Hospitality businesses are especially exposed to risks.. Preparing for such disruptions means maintaining <103> Business Continuity, that is, ensuring that hotels, venues or theme parks remain operational with minimal interruption. This capability depends heavily on strong <115> Internal Controls and clearly defined documented procedures that staff can follow during emergencies.

Equally important is <106> Compliance with applicable laws and <134> Regulatory Frameworks, such as labor legislation, safety standards and consumer protection rules. Many organizations rely on independent <101> Audit processes, which provide impartial assessments and help ensure that governance practices meet required standards.

Modern governance in hospitality also incorporates a proactive <440> Sustainability Strategy. This involves aligning the organization's practices with environmental, social and governance principles whether through energy efficient operations, ethical sourcing of goods or community engagement.

To sum up, a robust governance framework built on the pillars of leadership, transparency, risk control and sustainability, enables hospitality and leisure organizations to adapt and thrive in a fast-changing world.

IT Management in Hospitality and Leisure



In the hospitality and leisure industry, effective IT Management is a strategic driver of customer satisfaction, operational efficiency and competitiveness. Guests today expect seamless digital experiences like booking a room online. Delivering these services reliably demands structured oversight through **<212> Governance of IT**.

It is crucial to have a robust **<306> Digital Infrastructure**. Hotels, resorts and entertainment venues increasingly rely on cloud based platforms to run reservations, payments, check-ins, etc. To avoid downtime and ensure reliability, such infrastructure is designed with built-in **<322> Redundancy** meaning backup systems are ready to take over if failures occur.

With the rise of online transactions and digital identities, cybersecurity has become a top concern. **<206> Cybersecurity** practices are essential. This includes complying with strict regulations such as **<211> GDPR**. Organizations also implement **<214> IAM** solutions to control who can access systems, ensuring that only authorized users can handle sensitive information.

To ensure operational excellence, many hospitality providers adopt **<217> ITSM** practices, which structure how IT services are designed and improved. This includes setting expectations through **<323> SLA's** and **<316> Monitoring** tools. In the event of disruption, continuity plans governed by **<312> ITSCM** ensure that essential services can be restored quickly, minimizing impact on the guest experience.

Technologies are powered by platforms that leverage data analytics. These tools help organizations monitor **<116> KPIs** enabling continuous improvement. Tailored experiences like personalized room preferences are supported by insights drawn from guest behavior.

Strategically, IT must not operate in isolation. It must be aligned with business strategy through a clear **<426> IT Strategy** and periodic assessments of **<412> Digital Maturity**. This ensures that investments in technology deliver value. Organizations that evaluate their digital maturity can better identify gaps and prioritize initiatives that enhance resilience and agility.

In conclusion, IT Management in the hospitality and leisure industry is not just about managing systems, it's about delivering secure, reliable and innovative services that meet evolving guest expectations.

Governance in Manufacturing vs Transport and Logistics

In Manufacturing, Governance is embedded within formalized Management Systems, often guided by MSS such as ISO 9001 or ISO 14001. These systems promote consistent IMS integration, ensuring that Policies align with organizational Mission and performance is measured through KPI. The governance model typically reflects a structured, hierarchical approach, where Leadership steers decision-making through predefined Management Frameworks and strict Internal Controls. This supports high levels of Maturity in handling GRC obligations.

In contrast, Transport and Logistics operates within a more fluid Governance environment. The industry must respond to dynamic external variables, including international regulation and intermodal coordination. Governance here depends on adaptable IMS and interoperable Processes, designed to manage variability in the Supply Chain. Leadership is exercised through networked collaboration, and Management Frameworks such as ITIL or COBIT are used to enhance responsiveness and digital integration. While standards matter, agility often overrides rigid Management System design.

In summary, while both sectors leverage Governance to ensure alignment with Mission and oversight of GRC, Manufacturing emphasizes control and standardization, whereas Transport requires flexibility and cross-boundary coordination, each reflecting a different path toward Maturity in governance.

Governance in Transport and Logistics vs Hospitality and Leisure

In Transport and Logistics, Governance focuses on managing complex Processes and ensuring operational reliability across the Supply Chain. Strong Leadership is required to align Policies with regulatory and infrastructure demands. Management Systems integrate real-time control and Internal Control, supporting GRC through standards-driven IMS and KPI monitoring. The sector's Maturity is shaped by cross-border coordination and public-private roles.

By contrast, Hospitality and Leisure emphasizes customer-centric Governance, balancing brand consistency with local responsiveness. Leadership manages decentralized operations guided by service-oriented Policies. IMS supports data, quality, and experience delivery. Here, GRC focuses on privacy, safety, and ethical service, with Management Systems fostering adaptability over standardization.

Both sectors rely on Governance to align their Mission with operational realities, one through structural control, the other through responsive flexibility.

IT Management in Manufacturing vs Hospitality and Leisure

In Manufacturing, IT Management is closely integrated with **<129>Processes** such as production control and supply coordination. **<114>IMS** supports systems like MES and PLM, aligned with **<123>MSS** (e.g. ISO 9001). **<117>Leadership** ensures alignment of **<127>Policies** and **<122>Mission** through structured **<120>Management Systems**. Cybersecurity and OT integration demand strong **<115>Internal Control** and adherence to **<113>GRC** frameworks, aiming at high **<121>Maturity** and efficiency-driven **<116>KPI** performance.

In Hospitality and Leisure, IT Management focuses on customer experience and operational flexibility. **<114>IMS** supports booking platforms, CRM, and loyalty systems. **<117>Leadership** adapts **<119>Management Frameworks** to diverse service contexts, maintaining brand standards and data protection. While less standardized than in Manufacturing, **<120>Management Systems** ensure responsive service delivery and regulatory **<113>GRC** compliance in areas like privacy and health safety.

Thus, Manufacturing uses IT to optimize structured, high-precision environments, while Hospitality leverages it for agility and guest-centered service, both aligning IT Management with their distinct **<122>Mission** and sector needs.

IT Management in Manufacturing vs Transport and Logistics

In Manufacturing, IT Management supports tightly integrated **<129>Processes** such as production planning, quality control, and automation. **<114>IMS** connects systems like MES and ERP, structured within formal **<120>Management Systems** and aligned to **<123>MSS** (e.g. ISO 9001 and IEC 62443). **<117>Leadership** uses predefined **<119>Management Frameworks** to maintain strict **<115>Internal Control**, driving performance through **<116>KPI** and ensuring **<113>GRC** in regulated environments. IT is embedded in **<129>Processes** with strong links to **<129>Operational Technology** and **<231>Supply Chain** systems, reinforcing high **<121>Maturity**.

In Transport and Logistics, IT Management emphasizes real-time coordination and adaptability. **<114>IMS** integrates platforms like TMS and LMS, ensuring visibility across the **<231>Supply Chain**. **<117>Leadership** applies flexible **<119>Management Frameworks**, focusing on service continuity and responsiveness. While **<120>Management Systems** are less rigid than in manufacturing, they still support essential **<113>GRC** practices, especially regarding data protection and compliance with transport regulations. Here, IT Management enables agility over control.

In summary, Manufacturing prioritizes stability and integration, while Transport values flexibility and visibility, each aligning IT Management with their operational and strategic **<122>Mission**.

Industries Project – Group 146

Industry 1 – Manufacturing

Theme 1

The manufacturing industry is rooted in structured, hierarchical organisations (1.1), shaped by capital intensity, long investment cycles, and operational complexity. Governance is structured through formal systems, embedded in <120> management systems and guided by <117> leadership accountability. These systems ensure consistency in quality, safety, and regulatory conformance—reinforcing a <106> compliance-driven culture that often leads to <105> certifications such as ISO 9001 and ISO 45001.

Manufacturing governance reflects an integrated <113> GRC posture, where regulatory obligations intersect with operational control and risk awareness. Risk exposure spans equipment failure, supply chain disruption, and cyber-physical threats from the convergence of IT and OT systems (e.g., SCADA, MES, PLM). Addressing these risks requires structured governance and proactive control frameworks.

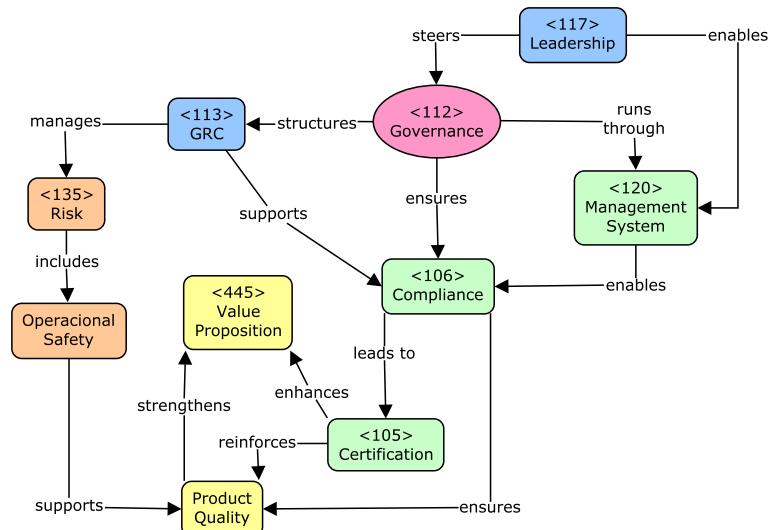
The sector aligns with layered control models—Three Lines of Defence (1.10)—assigning oversight across leadership, middle management, and operational units. Frameworks like <131> RACI help clarify responsibilities across functions. A strong <106> compliance culture, reinforced by <113> GRC structures, supports control, risk visibility, and certification practices.

Compliance and governance efforts are closely tied to product quality, enhancing the organisation's <445> value proposition by linking internal controls to competitive positioning and customer trust.

Management maturity (1.12) is reflected in continuous improvement approaches such as Lean and Six Sigma, promoting adaptability and performance in dynamic environments.

Ethics and sustainability (1.18) are gaining strategic weight. With rising ESG and regulatory expectations (e.g., NIS2, CSRD), <111> ethical governance and environmental responsibility are increasingly embedded under <117> leadership oversight.

The sector exemplifies governance maturity—anchored in structured systems, strong compliance, and risk-informed decisions—while facing the ongoing challenge of adapting digitally without compromising control, resilience, or ethical responsibility.



Industry 1 – Manufacturing

Theme 2

In manufacturing, **<212>** governance of IT is essential to aligning digital systems with business goals while managing operational risk. The convergence of IT and OT—through MES platforms, SCADA systems, and Industrial IoT—demands governance models that link technology to business direction, reinforce **<206>** cybersecurity, and ensure reliability. This reflects a governance approach focused on value delivery and managing digital complexity at scale.

Oversight is typically exercised by the **<102>** Board of Directors, supported by steering structures that translate strategy into system-level decisions. However, alignment is often challenged by fragmented ownership and legacy infrastructure. Effective governance requires clear decision rights, lifecycle control, and integration with enterprise planning.

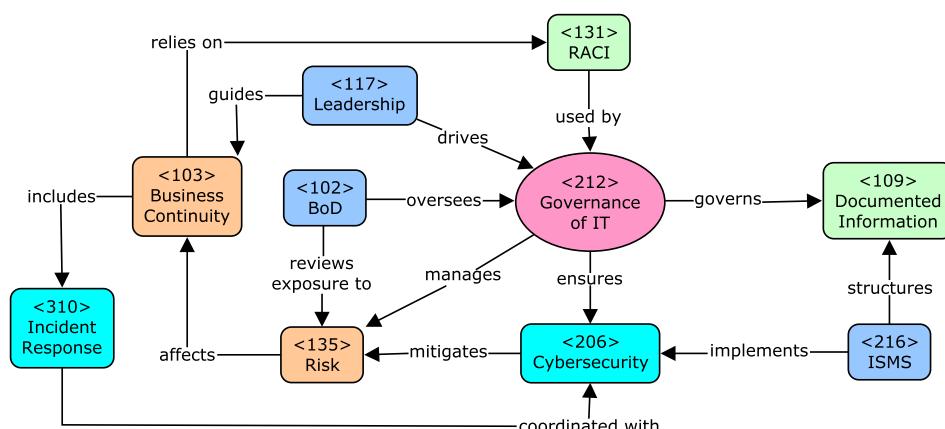
Cybersecurity is a growing priority due to the exposure of industrial systems to targeted threats. Strong **<206>** cybersecurity depends on risk-based policies implemented within an **<216>** ISMS and aligned with standards such as IEC 62443 or NIST CSF. An independent, capable CISO is critical to maintaining trust and operational resilience.

Information governance also plays a key role. With vast volumes of operational and product data, manufacturers must control access, retention, and quality. Effective **<109>** documented information and **<132>** records management practices support traceability and compliance with industry-specific requirements.

Resilience planning must span both IT and OT. Escalation delays or unclear roles can hinder recovery efforts. Integrated **<103>** business continuity and **<310>** incident response capabilities remain a common area for improvement across the sector.

Third-party technologies introduce additional risk. Digital supply chains and embedded systems require formalised responsibilities. Applying **<131>** RACI frameworks helps clarify accountability across vendors and internal functions.

Ultimately, IT governance in manufacturing must evolve to manage legacy complexity, enhance cyber resilience, and support digital transformation. This progress depends on committed leadership, mature systems, and coordinated execution across technical and organisational layers.



Organisational structures are typically hierarchical (1.1), divided among operators, authorities, and service platforms. Long-term planning and infrastructure management are central, especially in safety-critical or publicly funded networks.

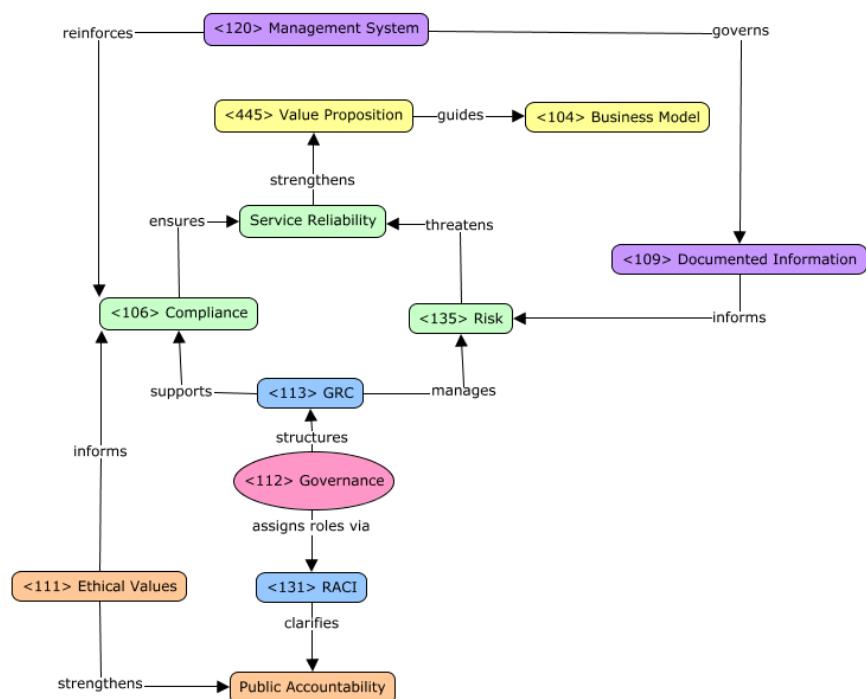
<112> Governance in this sector focuses on aligning technical, operational, and regulatory layers. <113> GRC frameworks support this integration by linking maintenance regimes, service standards, and regulatory compliance. These frameworks also help structure <135> risk, which spans operational incidents, delays, and growing exposure to cyber threats.

A strong <106> compliance culture is reinforced by audits and oversight mechanisms (1.21). This is further operationalised through formal <120> management systems—common in rail, maritime, and aviation—which establish consistent practices around safety, reporting, and service quality. These systems also govern <109> documented information, supporting traceability and informed risk control.

Responsibility is structured through <131> RACI frameworks, clarifying control ownership in complex public-private environments. This is especially important in contexts with layered oversight and high levels of public scrutiny. The sector’s governance is shaped not only by formal control, but also by rising ethical expectations. <111> Ethical values influence compliance priorities and reinforce <106> accountability, especially around sustainability and equitable service provision (1.18).

<135> Risk directly affects performance outcomes. Disruptions can compromise service continuity and punctuality, placing <445> value proposition at the heart of governance objectives. In this context, service reliability becomes both a performance target and a public expectation—linking governance to trust. As such, <445> value proposition also informs the design of the <104> business model, especially in organisations balancing commercial viability with public responsibility.

Altogether, the sector reflects a mature and adaptive governance model—anchored in regulation, performance, and ethical responsibility—where resilience and service delivery are deeply embedded in organisational control.



Industry 4 – Transport and Logistics

Theme 2

In the transport and logistics sector, <212> governance of IT plays a vital role in coordinating digital infrastructure with operational performance. As mobility services, logistics platforms, and infrastructure systems become increasingly connected, IT governance must ensure alignment across technical layers while maintaining resilience and service continuity.

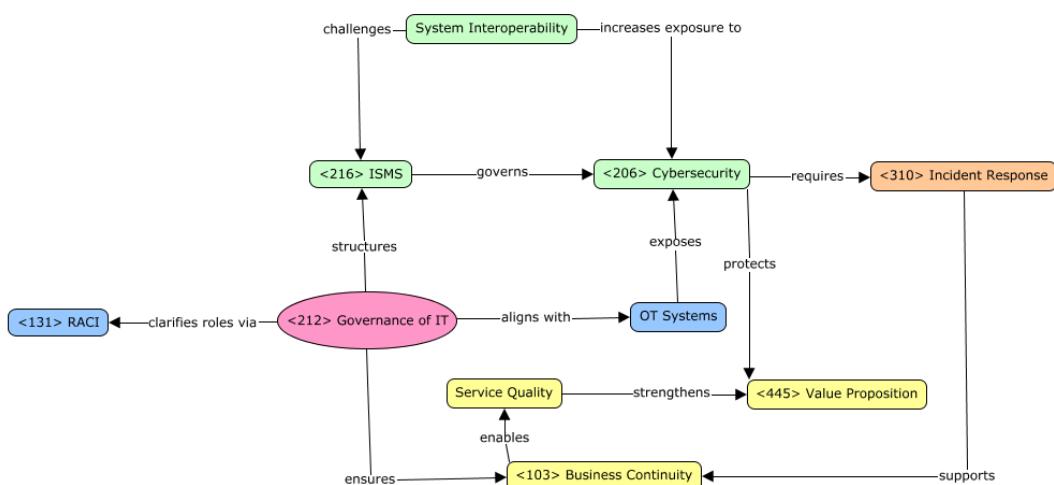
A structured <216> ISMS supports this coordination by embedding security and control practices into core processes. In this context, <206> cybersecurity is essential to safeguard critical systems, from SCADA networks and fleet management tools to ticketing platforms. The convergence of physical and digital infrastructure introduces complexity, especially in environments that depend on <131> RACI-defined roles to manage distributed teams and service providers.

System interoperability is a persistent challenge. Public transport and logistics operators often work across diverse technologies and vendors, requiring IT governance to resolve integration risks and protect against exposure introduced by <OT Systems>. These systems, while operationally indispensable, increase the threat surface and can trigger cascading disruptions.

To respond effectively, <310> incident response capabilities must be tightly aligned with real-time operational requirements. Escalation and containment protocols are often tested under pressure and must be integrated into <103> business continuity planning. These continuity plans do not only cover data and infrastructure recovery — they must also support uninterrupted physical service flows.

Ultimately, both IT protection and recovery mechanisms serve a strategic purpose. Reliable digital systems underpin <445> value proposition by maintaining public confidence, safety, and punctuality. In this sector, <Service Quality> is not just a KPI — it is a governance outcome shaped by digital performance.

This reflects how IT governance in transport and logistics balances system integration, risk control, and resilience — all in service of critical infrastructure and societal mobility.



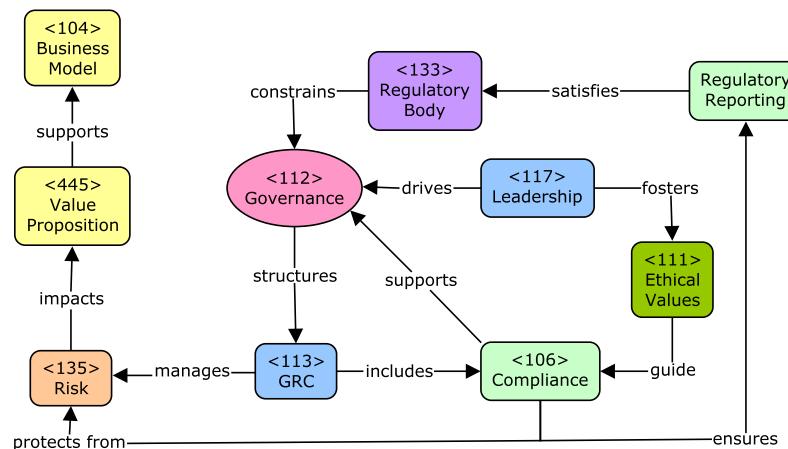
The banking and financial services sector operates in one of the most structured and regulated environments, marked by layered governance, intensive risk oversight, and multi-level accountability. Organisational models are formal and hierarchical (1.1), shaped by both internal policy frameworks and the influence of <440> external supervision. Institutions like the ECB and EBA shape governance by defining expectations for structure, oversight, and reporting (1.4, 1.21), which significantly constrain internal governance decisions.

<112> Governance in this sector is mature but must remain responsive to evolving supervisory demands. <117> Leadership plays a critical role in translating governance principles into institutional practice, promoting alignment across teams while fostering a culture built on transparency and accountability. The presence of <111> ethical values has become essential, not only as a response to past misconduct but as a foundation for ESG integration and long-term credibility.

Well-established <113> GRC structures support effective coordination between governance, control, and assurance functions. <135> Risk management is deeply embedded, covering a wide scope that includes not only financial exposures but also reputational risk—one of the most consequential threats to institutional trust. The <106> compliance function serves as a key operational safeguard, ensuring that obligations in areas such as AML, conduct, and ESG are addressed in both policy and practice. It also underpins <421> regulatory reporting, which is vital for satisfying supervisory scrutiny and maintaining regulatory alignment.

The organisation's <445> value proposition is closely tied to how well it embeds compliance and governance into day-to-day operations. These internal capabilities strengthen the institution's standing with customers and regulators alike. In turn, they help define the direction and viability of the <104> business model, influencing risk appetite, strategic priorities, and social responsibility.

Altogether, the sector demonstrates high governance maturity—anchored in structured oversight, ethical leadership, and supervisory integration. The challenge ahead lies in maintaining resilience and trust while continuing to adapt to shifting regulatory, technological, and societal expectations.



In the banking and financial services sector, <212> governance of IT plays a foundational role in sustaining trust, maintaining operational continuity, and meeting regulatory expectations.

Technology supports many of the sector's most sensitive and high-impact processes, placing IT governance at the core of institutional stability (2.2).

Oversight is shaped by <133> regulatory bodies such as the ECB and EBA, which set out formal expectations for resilience, transparency, and supervisory visibility (2.9, 2.28). To meet these, institutions align governance structures with compliance objectives, often through integrated IT-Compliance Alignment frameworks that coordinate responsibilities across technical and regulatory domains.

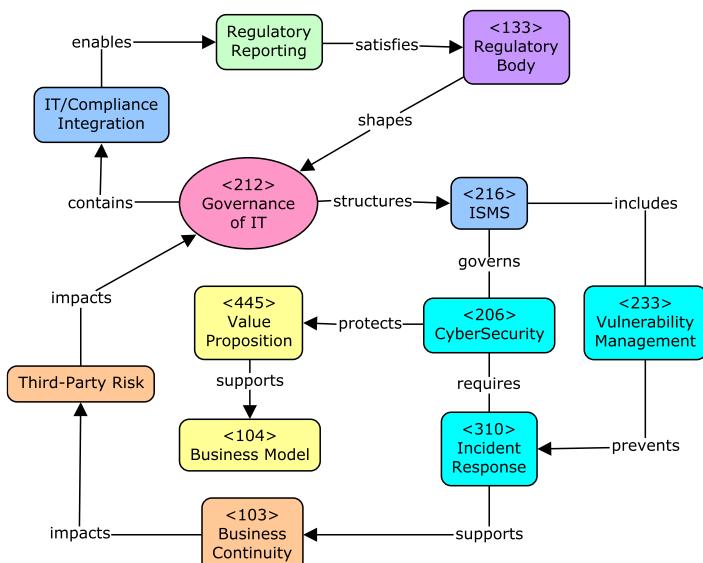
A structured <216> ISMS supports this architecture by embedding rules for access, threat monitoring, and accountability (2.19). Within this framework, <206> cybersecurity plays a critical role in protecting infrastructure and reputation. It is reinforced by <233> vulnerability management and guided by <310> incident response procedures that ensure threats are identified and contained effectively (2.17).

To support continuity, <103> business continuity planning includes digital recovery strategies and procedures for dealing with critical third-party dependencies. The growing importance of third-party risk, especially under DORA, highlights the need for extended governance beyond internal systems.

Responsibility and escalation paths are clarified through <131> RACI frameworks, which help maintain control across distributed teams and complex service environments (2.27). These structures also ensure consistency in regulatory reporting, a key indicator of control effectiveness and institutional accountability.

Ultimately, strong IT governance contributes directly to the institution's <445> value proposition. Reliability and resilience enhance stakeholder confidence and support the strategic direction of the <104> business model.

This reflects how the sector's approach to IT governance blends regulatory alignment with digital risk control, reinforcing a stable foundation for innovation and long-term trust.



Theme 1: Transport and Logistics vs. Banking and Financial Services

Both industries operate under complex governance models but differ substantially in drivers and structure. Transport and Logistics (T&L) governance is shaped by infrastructure lifecycles, public-private coordination and service continuity. Organisational structures tend to be layered across operators, authorities, and platforms, with oversight mechanisms reinforced by national and EU-level transport policies. Risk management in T&L includes operational disruptions, safety incidents, and growing cyber exposure, often managed through management systems and <131> RACI-based responsibility structures.

Banking and Financial Services (BFS), in contrast, operates in one of the most formally structured governance environments. Organisational control is influenced heavily by <440> external supervision from institutions like the ECB and EBA. Governance in BFS is deeply embedded within regulatory compliance frameworks, with strict reporting cycles, high board accountability, and well-established <113> GRC functions. <117> Leadership and <111> ethical values are central to internal culture and strategic integrity.

This reflects distinct governance cultures: one rooted in regulatory control, the other in technical coordination and public value.

Theme 2: Transport and Logistics vs. Banking and Financial Services

IT governance in Transport and Logistics (T&L) is challenged by system interoperability, vendor dependency, and cyber-physical integration across OT and digital platforms. It must address real-time systems. <212> Governance of IT ensures alignment between technical assets and performance outcomes such as <445> service quality, while <216> ISMS and <310> incident response frameworks aim to maintain continuity across distributed environments. RACI-based structures help manage complex accountability in public-private and multi-vendor contexts.

In Banking and Financial Services (BFS), <212> IT governance is highly formalised and deeply tied to regulatory expectations. The sector's reliance on high-frequency transactions, customer data, and third-party systems necessitates structured cybersecurity and digital risk governance, backed by <206> cybersecurity, <233> vulnerability management, and supervisory visibility. <216> ISMS and <103> business continuity are mandated and tightly audited.

While both sectors prioritise resilience and risk management, T&L focuses on integration and reliability, BFS on compliance and trust each reflecting the different stakes and digital exposure of their core operations.

Theme 1: Transport and Logistics vs. Manufacturing

Manufacturing and Transport and Logistics (T&L) share structured governance models, but diverge in how they apply them. Manufacturing governance centres on internal control, certification, and <106> compliance. It leverages integrated <120> management systems, supported by <117> leadership and continuous improvement practices. Risk is largely internal relating to production, quality, or supply chain issues and is addressed through proactive control structures within <113> GRC frameworks.

T&L, on the other hand, balances technical, regulatory, and operational governance across more fluid networks. Its governance systems must manage multi-modal infrastructure, layered public-private partnerships, and political accountability. While management systems also exist, governance here is shaped as much by external coordination and public expectations as by internal process control. <131> RACI frameworks and <111> ethical governance are especially visible in clarifying responsibilities in diverse stakeholder environments.

Concluding, manufacturing focuses on internal integration and quality, while T&L emphasizes coordination and service reliability. Both require strong oversight and compliance, but is based on production-centric, the other mobility-oriented.

Theme 2: Banking and Financial Services vs. Manufacturing

Both Manufacturing and Banking and Financial Services (BFS) face complex IT governance challenges, but their contexts diverge significantly. Manufacturing integrates <212> IT governance with operational technology (OT) systems like MES and SCADA. The goal is to maintain production continuity while enabling digital transformation, often under standards like IEC 62443 and <216> ISMS frameworks. Governance addresses cyber-physical convergence, legacy infrastructure, and embedded system risk, requiring oversight that spans both enterprise IT and plant-floor technology.

In contrast, BFS IT governance is shaped primarily by regulatory expectations. IT and cybersecurity governance are embedded in supervisory regimes, with emphasis on <103> business continuity, <206> cybersecurity, and <131> role clarity. IT Management in BFS supports both compliance and service reliability, while data sensitivity and systemic exposure place extra weight on resilience, reporting, and third-party risk.

Manufacturing's IT governance is integration-driven focused on aligning systems across the value chain while BFS emphasizes control, compliance, and auditability. In essence, both sectors use mature governance models but with different lenses: manufacturing to protect operations and evolve digitally, banking to protect trust, fulfil regulation, and uphold systemic stability.

Agriculture and Farming

Theme 1

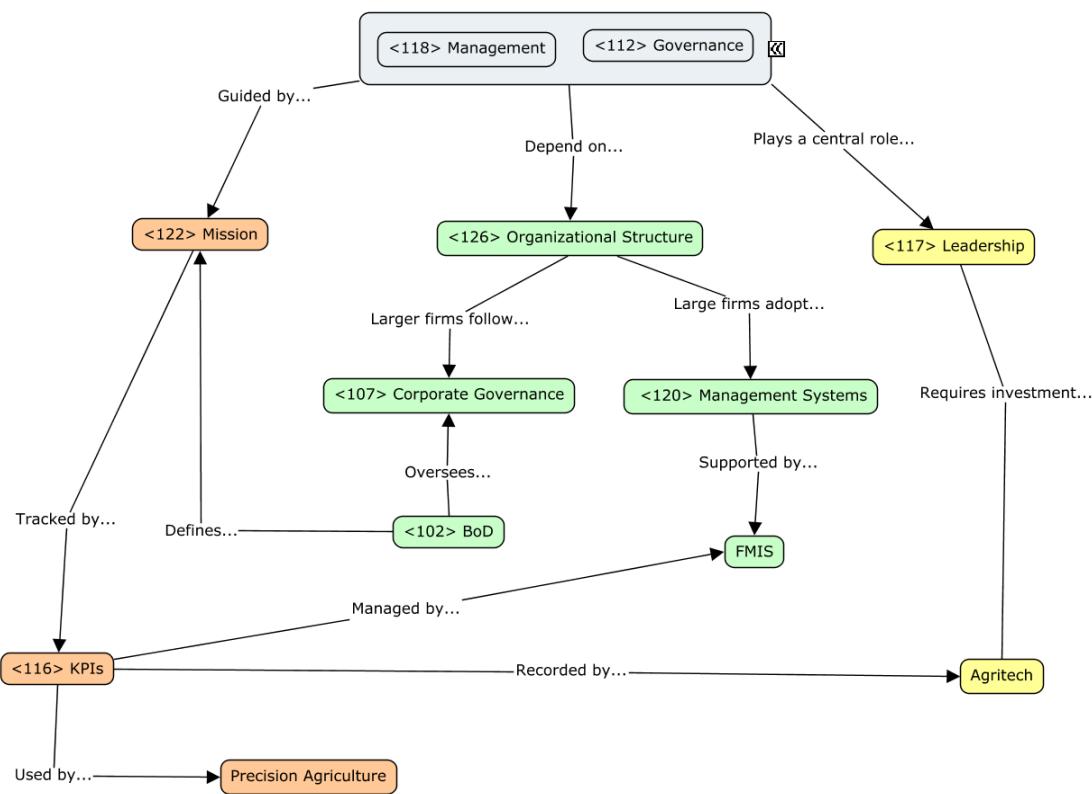
Crop farming is a segment of the agriculture and farming industry, encompassing the cultivation of grains, vegetables, fruits, and industrial crops for food, feed, fiber, or fuel. It's defined by the organized production of cultivated plants, supported by operational, technological, and governance systems aimed at optimizing yield, ensuring sustainability, and meeting regulatory and market demands.

The agriculture and farming industry and crop farming spans diverse <126> **organizational structures**—from smallholder farms to large agribusinesses and cooperatives. These forms influence how <112> **governance** and <118> **management** are carried out. Larger operations often adopt <107> **corporate governance** with oversight from a <102> **Board of Directors (BoD)**, while smaller farms may rely on informal leadership.

Larger firms increasingly use <120> **management systems** supported by **Farm Management Information Systems (FMIS)** to optimize key <129> **processes** such as planting, irrigation, and harvesting of crops. These tools also support <106> **compliance** with environmental and market regulations, which may be verified through <101> **audits** and third-party certifications.

Strategic direction is guided by a clear <122> **mission**, defined, approved and revised by the <102> **BoD**, reinforced through policies and tracked using <116> **key performance indicators (KPIs)** like yield or resource efficiency, recorded by **agritech** and managed by **FMIS**. **Precision agriculture** further enhances performance and sustainability through data-driven input optimization, especially in crop farming.

Strong <117> **leadership** helps address market risks and climate variability, while promoting an adaptive <125> **organizational culture**. Integrating **agritech** requires investment and openness to transformation but can have great impact in crop farming. However, **rural connectivity** challenges can hinder the adoption of such innovations, especially where digital infrastructure remains weak.



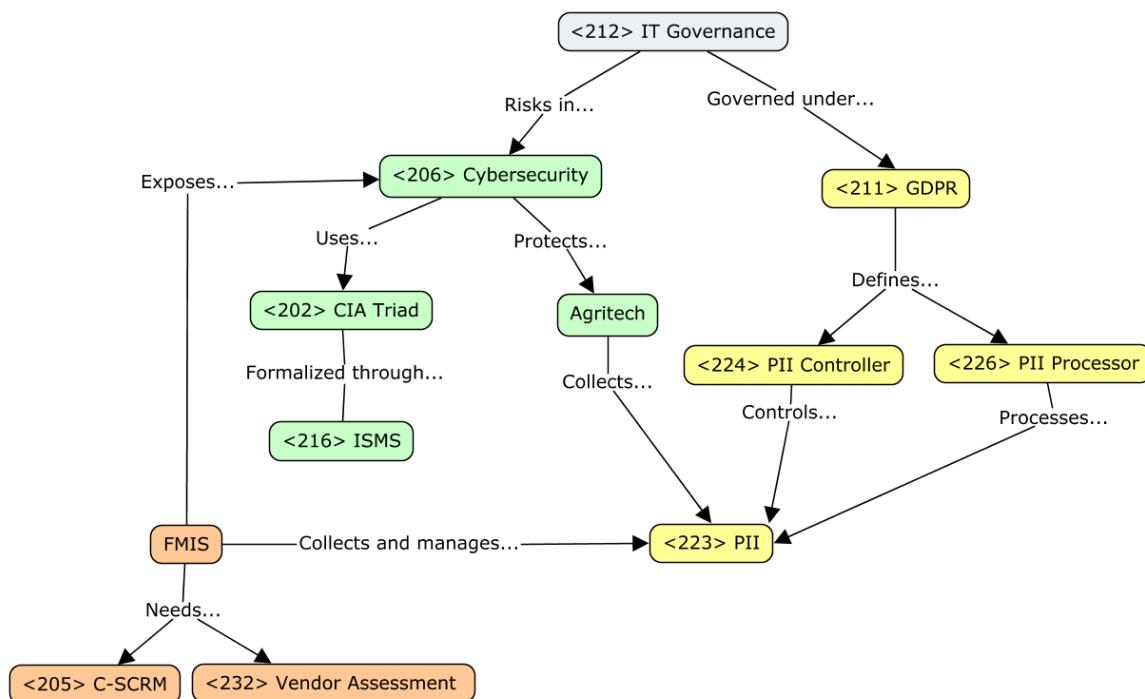
Theme 2

Larger crop farming enterprises increasingly adopt <212>**Governance of IT** frameworks to support goals such as export compliance, traceability, and sustainable production. In contrast, many smallholders lack these systems, making them more vulnerable to inefficiencies and <206>**cybersecurity** threats. The widespread use of **agritech** - such as soil sensors, drones, and smart irrigation - requires robust protection based on the <202>**CIA Triad**: ensuring the confidentiality, integrity, and availability of information. These protections are formalized through an <216>**Information Security Management System (ISMS)**.

Modern **Farm Management Information Systems (FMIS)** in crop farming collect and manage large volumes of sensitive data, including <223>**Personally Identifiable Information (PII)** such as farmer records and geolocation data. Under <211>**GDPR**, this data must be handled with strict safeguards: organizations must clearly define the roles of the <224>**PII Controller** and <226>**PII Processor** and apply data protection principles across all systems.

Digitized supply networks and **FMIS** platforms expose farms to external risks, particularly through third-party software and services. Managing these exposures requires strong <205>**Cybersecurity Supply Chain Risk Management (C-SCRM)** strategies and regular <232>**Vendor Assessments** to evaluate software providers and service partners.

As **agritech** solutions become more interconnected, crop farms must ensure their IT infrastructure meets resilience and compliance standards. Whether dealing with pest detection analytics or cloud-based crop monitoring, the integration of systems must prioritize cybersecurity and data governance.



Manufacturing

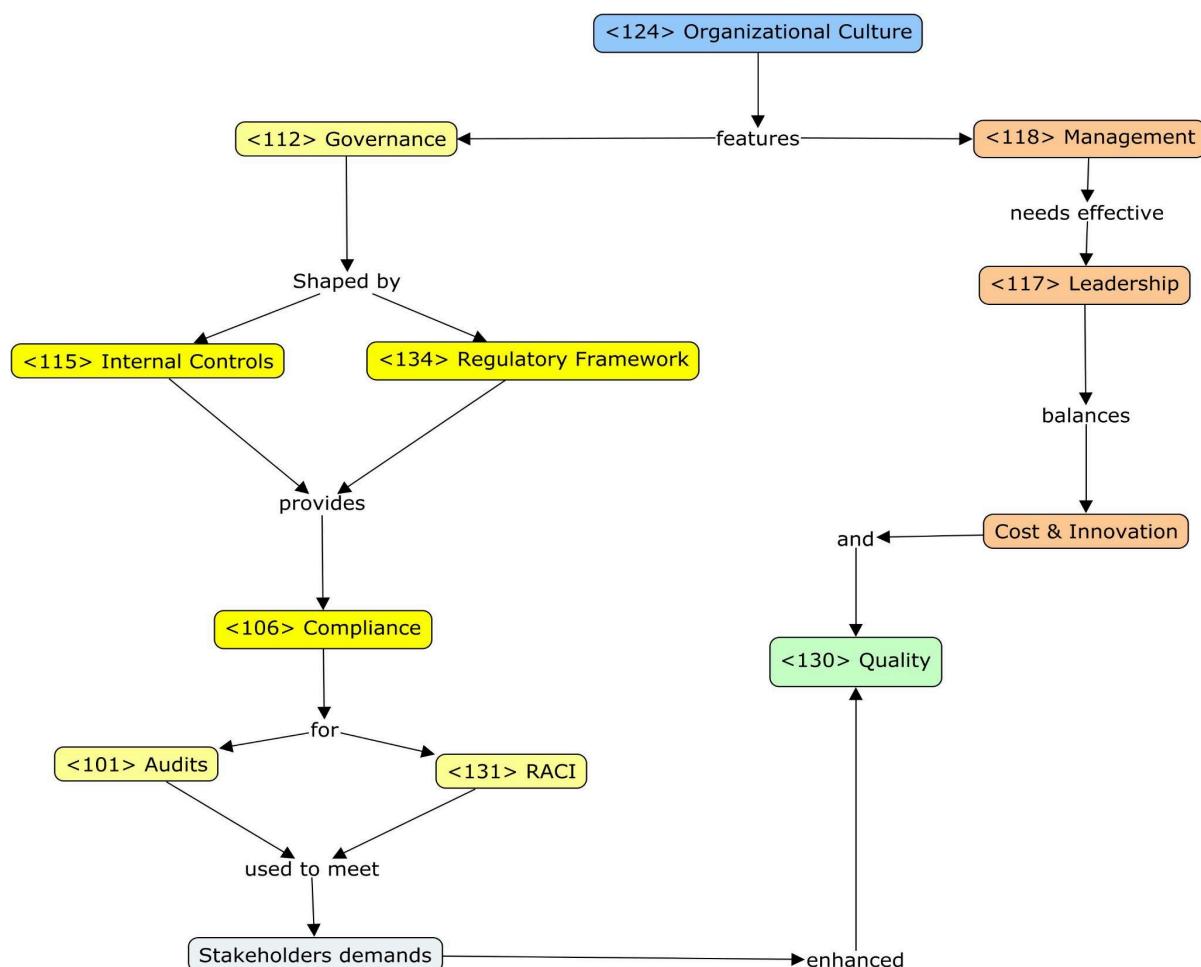
Theme 1

The electronics manufacturing industry features complex **<126> organizational structures**, strict **<112> governance** and advanced **<118> management** practices. It operates through global supply chains involving **original equipment manufacturers (OEMs)**, contract manufacturers, suppliers, and design firms. Modular production models have replaced some traditional **<129> processes**, enabling greater flexibility and scalability.

<107> Corporate governance is shaped by **<115> internal controls** and external **<134> regulatory framework**, focusing on intellectual property protection, environmental **<106> compliance** (e.g., RoHS, WEEE), and labour standards (e.g., ILO). Transparency, third-party **<101> audits**, and **<131> RACI** frameworks are increasingly used to meet stakeholder demands. Geopolitical factors also affect supply chain **<112> governance**, especially across diverse regulatory environments.

Effective **<120> management system** requires **<428> organizational agility**, tech acumen, and strategic foresight. **<117> Leadership** balances cost, innovation, and **<135> risks** —especially supply chain disruptions and rapid market shifts. **Lean manufacturing**, **Six Sigma**, and digital tools like **Industry 4.0** and **IoT** are widely used to enhance productivity and **<130> quality**. Additionally, **<213> human resource management** plays a key role, as firms compete for skilled labour in engineering, software development, and advanced manufacturing.

In summary, the industry demonstrates how **<113> governance, risk, and compliance (GRC)** frameworks enable innovation and regulatory alignment in a dynamic global context.



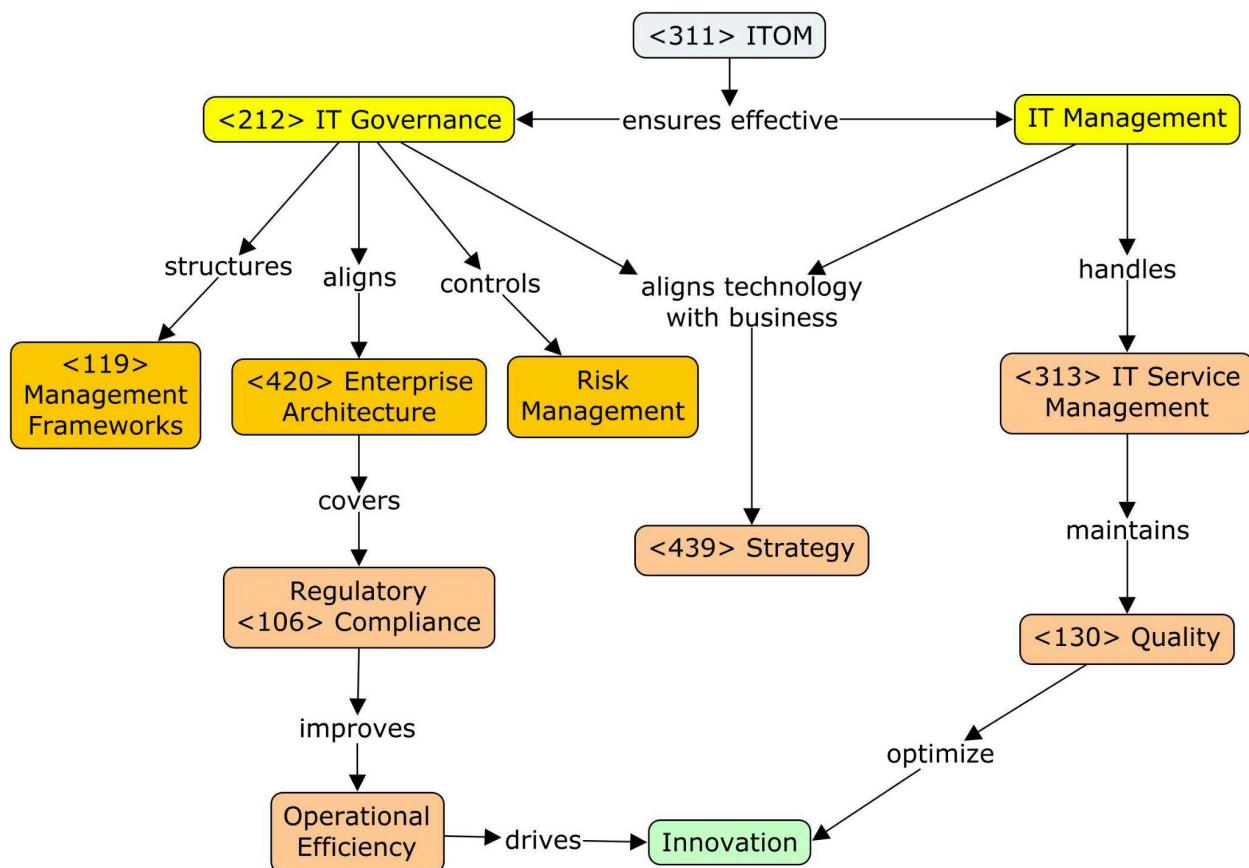
Theme 2

The electronics manufacturing industry relies heavily on robust **<311> IT Operations Management (ITOM)** to handle complex supply chains, maintain **<130> quality**, optimize production, and support global distribution. Effective **<112>Governance** and **<118> management** are critical for aligning technology with business **<439> strategy**, improving efficiency, and meeting **<134> regulatory frameworks**.

<212>Governance of IT in this sector involves **<119> management frameworks** and **<127> policies** that ensure IT investments align with **<125> organizational culture**. Key components include **<420> enterprise architecture** planning, IT **<135> risk management**, and performance **<316> monitoring** through **<116> KPIs** and balanced scorecards. Governance also covers regulatory **<106> compliance** with standards such as ISO/IEC, environmental regulations, cybersecurity mandates like NIST and **<211> GDPR** compliance.

With increased digitalisation in this industry, **<206>cybersecurity** has become an increasingly important concern. Access to proprietary designs by unauthorized actors, attacks on Industrial Control Systems (ICS) and loss of data are some of the dangers to the **<202>CIA Triad** in this industry. Proper **<205>C-SCRM** is, therefore, essential across an ever more globalized supply chain. A proper **<216>ISMS** to ensure data integrity and **<208>Data Privacy** is also a necessity.

IT management handles daily operations of **<306> enterprise IT infrastructure** and services. This includes oversight of ERP, MES, and PLM systems. Efficient **<313> IT Service Management (ITSM)** practices ensure high availability, data accuracy, and rapid incident response—vital for just-in-time, high-volume manufacturing.



Transportation and Logistics

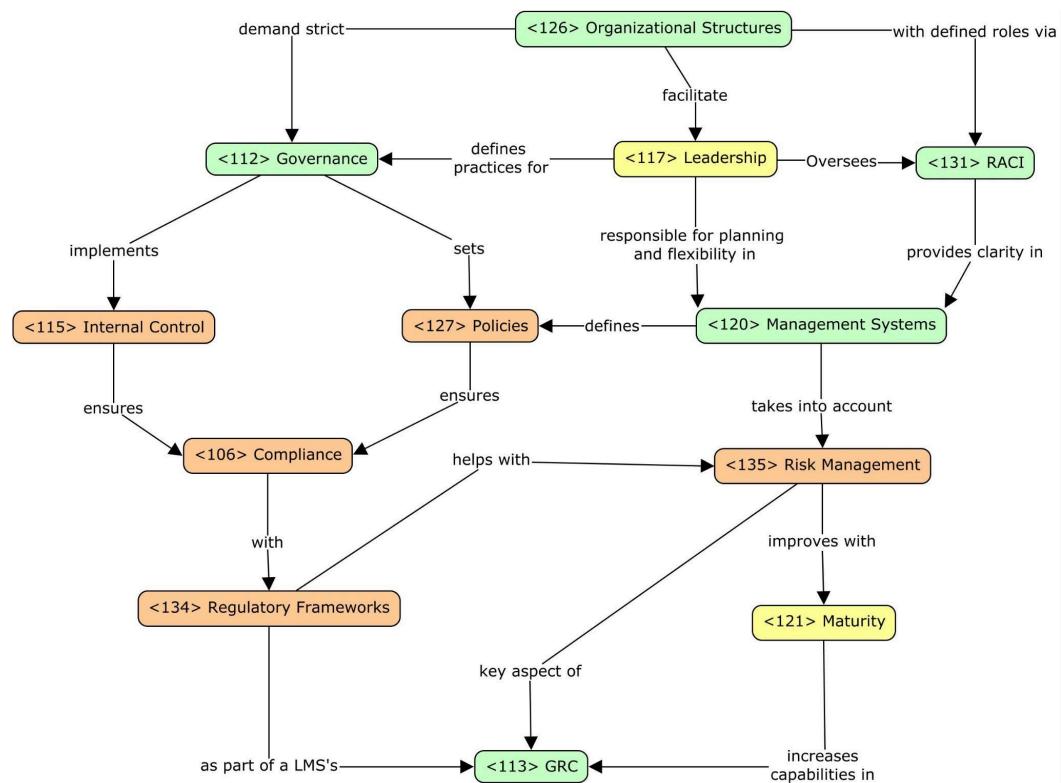
Theme 1

Logistics Management Systems (LMS) require strict **<112> Governance** within complex **<126> organizational structures**. The **<102> Board of Directors** oversees strategic decisions while **<131> RACI frameworks** define roles. High-level **<127> policies** and **<115> internal controls** govern data integrity and user access, ensuring compliance with **<134> regulatory frameworks**, including customs and trade requirements. Documented **<128> procedures** and third-party audits build stakeholder trust.

Integrated **<135> risk management** uses real-time dashboards to identify operational disruptions and cybersecurity threats, enabling quick corrective actions. Built-in **<106> compliance checks** enforce SLA performance and customs accuracy, while regular **<101> audits** drive continuous improvement. As organizations **<121> mature**, they shift from reactive fixes to predictive analytics using transaction histories and anomaly detection.

Effective **<120> management systems** balance strategic planning with operational flexibility. **<117> Leadership** aligns cost control, service **<130> quality**, and innovation through digital tools like IoT integration and cloud platforms. **<116> KPIs** guide process optimization. Strong vendor management ensures external providers follow defined **<127> policies**.

LMS governance and management unite through a **<113> GRC** framework, aligning board oversight with operational excellence, transforming the LMS into a strategic asset that strengthens resilience and competitive advantage.



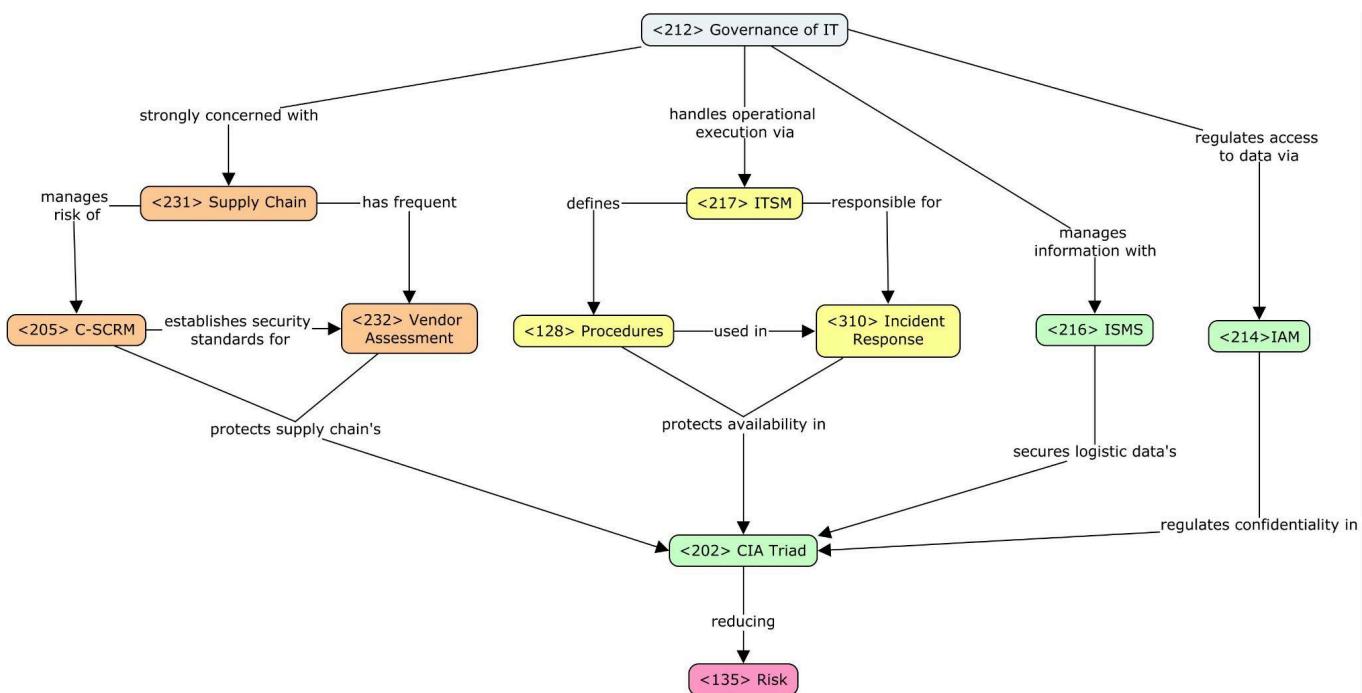
Theme 2

Effective Logistics Management Systems require robust **<212> Governance of IT** structures to guide their strategic function within **<231> Supply Chain** operations. **<117> Leadership** decides IT investments, determining deployment of specific LMS components like warehouse management and transport planning modules. The **<108> CIO** and IT steering committees maintain alignment with overarching business objectives, utilizing **<119> Management Frameworks** such as COBIT and ISO/IEC 38500 to establish governance principles and control mechanisms.

These frameworks define measurement of **<116> KPI** (project ROI and system uptime), while enforcing compliance with regulatory requirements like customs and trade mandates. The governance framework incorporates **<205> C-SCRM**, mandating that third-party **<232> vendors** and APIs meet established security standards before system integration.

Operational execution falls under **<217> IT Service Management** processes. Service-desk protocols, **<310> Incident Response**, and **<128> procedures** prevent software updates or configuration modifications from disrupting critical functions like order fulfillment and delivery tracking. **<216> ISMS** maintains logistics data's **<202> CIA triad** across all operations.

<214> Identity and Access Management policies regulate access to shipment records, establishing a clear separation of duties among operations, finance, and compliance personnel. **<116> KPIs** spanning order-fulfillment rates to API response times drive continuous improvement initiatives, with results feeding into governance reviews that recalibrate strategic priorities and organizational **<135> Risk** tolerance levels.



Comparisons

Theme 1 - Manufacturing / Agriculture and Farming

Electronics manufacturing is more formalized, having high **<112>Governance** and **<118>Management** **<121>maturity**. Uses formal structures, follows strict regulations to avoid **<135>risks** and is already heavily digitally integrated. Crop farming on the other hand, is still continually evolving, demonstrating drastic differences between smallholder farms and large agribusinesses. Noticeable in the **<112>Governance** and **<118>Management** **<121>maturity** that range from very low in rural agricultural towns, to very high in large scale companies that have formalized **<126>Organizational Structures**.

	Electronics manufacturing	Crop Farming
Governance and Structure	Formal corporate Governance	Diverse Structures, but more informal in general
Management Practices	Standardized management system frameworks	Increasing adoption of management system standards
Technology and Digital Tools	Advance digital integration	Emerging use of agritech
Regulations and Environment	Governed by strict compliance frameworks	Shaped by local regulations, and emphasis sustainability
Market and External Factors	Influenced by supply and demand in global markets	Driven by seasoned supply and demand and climate variability

Theme 2 - Manufacturing / Agriculture and Farming

Electronic manufacturing and Crop farming both make use of structured frameworks to help with their day-to-day operations coordinated by **<212>Governance of IT** structures. In Electronic manufacturing these structures are formalized, a sign of high **<121>Maturity** in IT operations, and are normally used for automation of processes and real-time analytics. Crop farming differs from manufacturing by having a high variability of **<121>Maturity** of IT management between small rural farms and big farming corporations, focusing on robotic automation of labor, predictive seasonal features and precision farming.

	Electronics Manufacturing	Crop Farming
IT Governance	Formalized governance	Varies widely, but often informal
IT Management	Highly mature	Uneven maturity; Growing with FMIS adoption in agribusinesses
Risk and Compliance	Subject to global IT regulations	Local regulations for IT apply
IT Providers	Large-Scale contracts with IT solution vendors	High reliance on local MSPs/MSSPs vendors

Theme 1 - Transportation and Logistics / Agriculture and Farming

Logistic Management systems have decidedly formalized <112>**Governance** that oversees a highly <121>**matured** <120>**management system** focused on precise <128>**procedures** that are bound by a strict <133>**regulating body**. Crop farming has a large variety of <112>**Governance** structures depending on the size of the local industry, these oversee the <118>**management** of the operation that may vary from highly <121>**mature** supported by <120>**management systems**, to very informal activities.

	Logistic Management Systems	Crop Farming
Governance and Structure	Complex structures, heavily formalized and with a focus on transparency and documentation	Diverse Structures, but more informal in general
Management Practices	Use of comprehensive management systems and RACI frameworks	Increasing adoption of management system standards
Technology and Digital Tools	Integration with IoT devices, focused on gathering analytics	Emerging use of agritech
Regulations and Environment	Subject to international technical and safety regulations	Shaped by local regulations, and emphasis sustainability

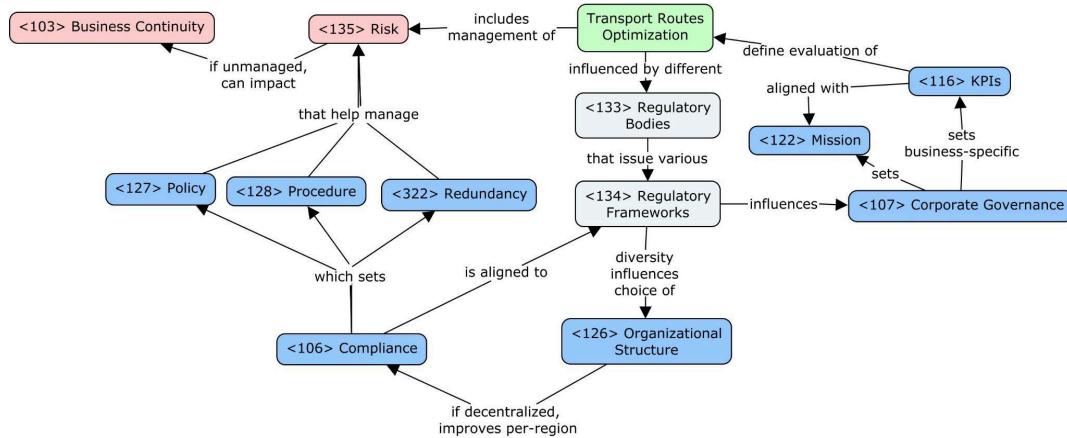
Theme 2 - Agriculture and Farming / Transportation and Logistics

Both Logistics Management Systems and Crop Farming have leveraged <119>**Management Frameworks** in order to guide their <212>**Governance of IT**. Where they differ is in how widespread these practices are. While the big players in LMS and Crop Farming may have similar levels of <121>**Maturity** in IT Management, small farmers adopt a more ad hoc approach to cyber <135>**Risk**, making them more susceptible to <206>**Cybersecurity** threats when compared to their LMS counterparts.

Both sectors depend on global <231>**Supply Chains**, with proper <205>**C-SCRM**, combined with regular <232>**Vendor Assessments** being essential to ensure <103>**Business Continuity**.

	Logistic Management Systems	Crop Farming
IT Governance	Formalized and guided by the use of management frameworks	Varies widely, but often informal and lacking frameworks in small farmers
IT Management	Focused on minimizing downtime, and on proper IAM; Highly mature	Uneven maturity; Growing with FMIS adoption in agribusinesses
Data Governance	Shaped heavily by GDPR and other similar frameworks, especially in the e-commerce sector	Farmer records and geolocation must be handled according to GDPR standards
Supply Chain Risk Management	Focus on vulnerabilities across telematics and cloud interfaces	Vendor assessments focused on software and service providers

Transports & Logistics - Transport Routes Optimization Organizations, Governance and Management



Multinational logistics corporations face complex governance [112](#) challenges as they operate across jurisdictions with divergent regulatory frameworks [134](#), such as the EU Mobility Package that governs rules such as the maximum driving time for workers. Unlike regional operators that typically need only to comply with the regulations of the country in which they operate, and therefore benefit from centralized governance and consistent compliance procedures [106](#), global firms must adapt their organizational structure [126](#) to decentralize decision-making processes in order to focus on maintaining compliance and efficiency through more specific Internal Controls [115](#).

Transport Routes Optimization also requires coordination among multiple stakeholders, such as shipping and rail operators and infrastructure providers. When all parties are aligned in terms of corporate governance [107](#) protocols and data-sharing standards, this collaboration enhances the coverage area for product delivery and also facilitates smoother transitions between transport modes, thus contributing to a more effective ecosystem.

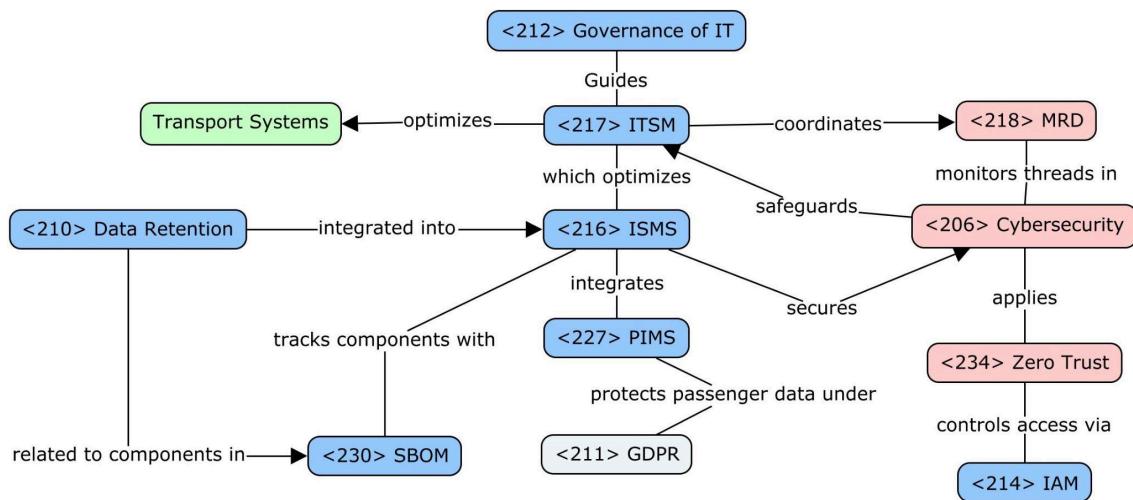
Another key distinction is the difference in the business models [104](#) of publicly-owned logistics organizations versus private-sector companies. Since public agencies are funded by the respective countries' governments, they are often tasked with serving underserved areas, and aiming to prioritize equal access and service continuity. On the other hand, privately-owned logistics firms tend to focus on procedures [128](#) that positively impact the delivery efficiency and profitability, and thus employ advanced KPIs [116](#) such as delivery times, costs per km, and load utilization to reduce transportation costs, while at the same time improving the delivery speed and quality [130](#) for higher profit margins.

Given that this industry is also part of the backbone of many other industries' operations, management of risk [135](#) is important to maintain Business Continuity [103](#) in the case of critical occurrences that can impact the entire supply chain. Therefore, logistics organizations must implement robust risk assessment frameworks, diversify transport modes and develop contingency plans to swiftly adapt to disruptions such as geopolitical conflicts, natural disasters, or system-wide IT failures.

Finally, governance in this space is increasingly influenced by global sustainability imperatives. Transport managers must now integrate carbon emission tracking, vehicle standard policies [127](#), and green logistics planning into their strategic frameworks, aligning organizational objectives with evolving regulatory and environmental values [111](#).

Transport & Logistics

Governance of IT and IT Management



Optimizing transport routes requires a secure and planned framework. <212>Governance of IT establishes the strategic direction for technology, ensuring <217>ITSM effectively manages the complex routing services, traffic and fleet telematics, and logistics platforms that support efficient operations.

ITSM also contributes to a better and robust <216>ISMS, which integrates <227>PIMS to handle sensitive personal data related to clients and logistics, ensuring compliance with <211>GDPR protection policies.

<206>Cybersecurity is reinforced by applying a <234>Zero Trust model across all interconnected transport systems, for example, including traffic management, booking platforms, and communication networks, thereby minimizing and isolating potential risks.

Access to all the different computer systems is carefully managed (<214> IAM) for everyone involved, like drivers and dispatchers. At the same time, a detailed list of all the software parts in the transport systems (<230> SBOM) helps find and fix any weaknesses that could come from the software supply chain (<205> C-SCRM).

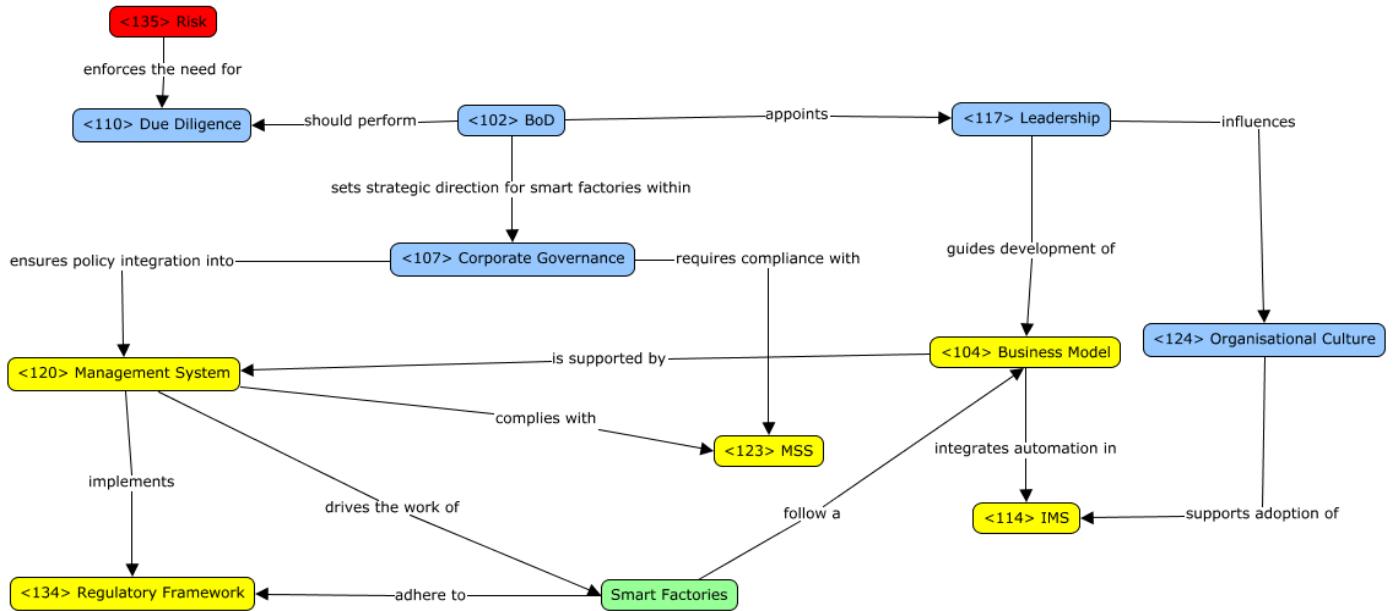
<218>MDR provides continuous threat monitoring across the digital infrastructure, proactively enhancing the overall <303>Cyber Resilience of transport route operations against evolving cyber threats.

<218>MDR also provides continuous threat monitoring, proactively supporting the <303>Cyber Resilience of transport route operations against evolving cyber threats. The use of redundant systems also plays a crucial role in reducing the potential <201> Business Impact Analysis by ensuring that service disruptions are minimized. This redundancy directly contributes to increased <103>Business Continuity, allowing transport operations to continue working even in failure scenarios.

Lastly, rules about keeping data <210>Data Retention make part of the security management system <216>ISMS and are also thought about when looking at the durability of software parts <230> SBOM. This makes sure the right records are kept for following rules and for understanding what happened if there's a problem.

Manufacturing - Smart Factories

Organizations, Governance and Management



Smart factories integrate cyber-physical systems into manufacturing, blending operational excellence with digital innovation. This transformation redefines <102> Board of Directors oversight, requiring strategic guidance across <113> GRC, <117> leadership, and <114> IMS adoption.

Governance in smart factories shifts from traditional top-down models to more agile, cross-functional structures. <131> RACI frameworks clarify roles between IT, OT, and engineering, supported by <109> documented information and digital workflows.

<135> Risk management and <106> compliance are elevated through formal controls like <101> audits and <110> due diligence, particularly for high-stakes systems and suppliers. <123> MSS certifications (e.g., ISO 9001, ISO 45001) reinforce product and worker safety.

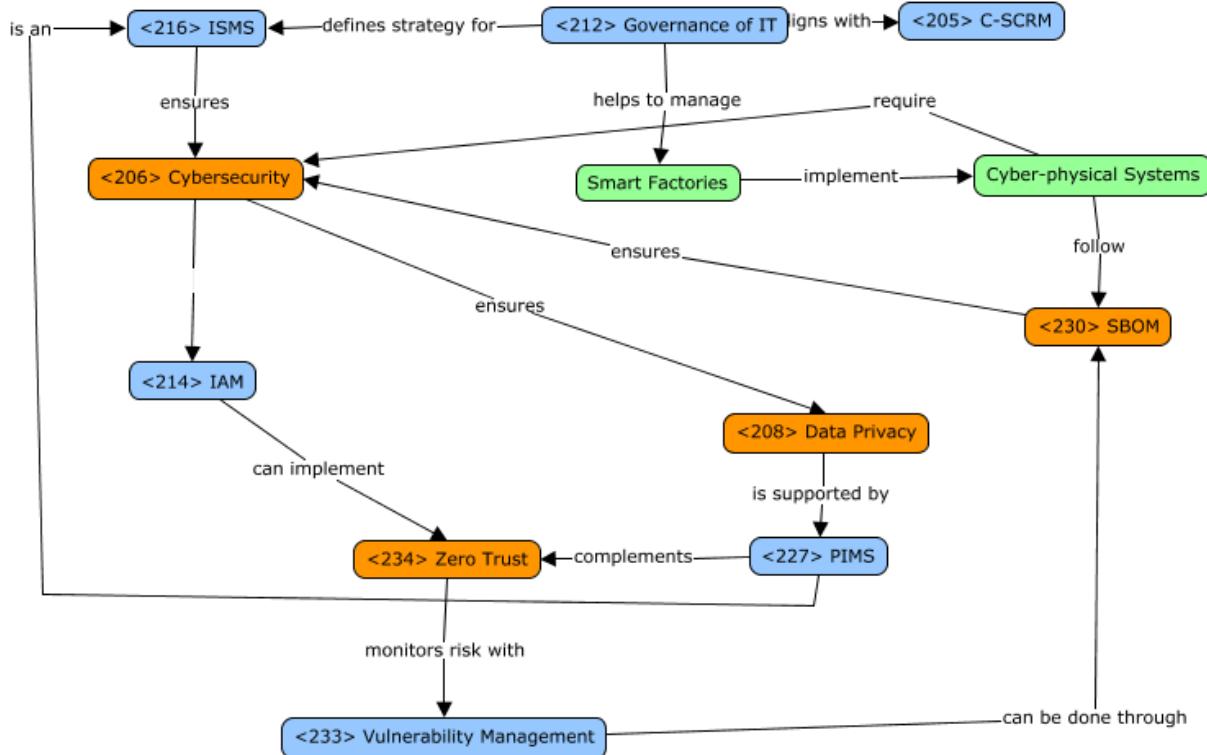
Strategically, <104> business models evolve to prioritize adaptability and digital efficiency. <120> Management systems align operational objectives with regulatory and sustainability goals, while <124> organizational culture must promote innovation, data literacy, and ethical AI use.

The <107> corporate governance model expands to oversee data protection, automation, and resilience. <121> Maturity models guide continuous improvement, ensuring systems are scalable and standards-compliant.

Ultimately, governance and management in smart factories must bridge people, processes, and technologies—ensuring trust, accountability, and performance in complex, data-driven environments.

Manufacturing - Smart Factories

Governance of IT and IT Management



In smart factories, <2> governance of IT is central to secure, efficient production. IT systems manage real-time operations—blurring lines with <205> operational technology (OT).

<216> ISMS and <206> cybersecurity controls are essential, often structured under <113> GRC frameworks. <234> Zero Trust and <215> InfoSec principles (e.g., the <202> CIA triad) protect both systems and data, especially in networked environments like MES and SCADA. <108> CxO roles (e.g., CIO, CISO) coordinate with operations to ensure <56> strategic alignment, while <214> IAM and <233> vulnerability management protect access and infrastructure.

Smart factories depend on external vendors, necessitating rigorous <232> vendor assessment and oversight of <226> PII processors. <208> Data privacy and <227> PIMS frameworks extend compliance even in industrial settings.

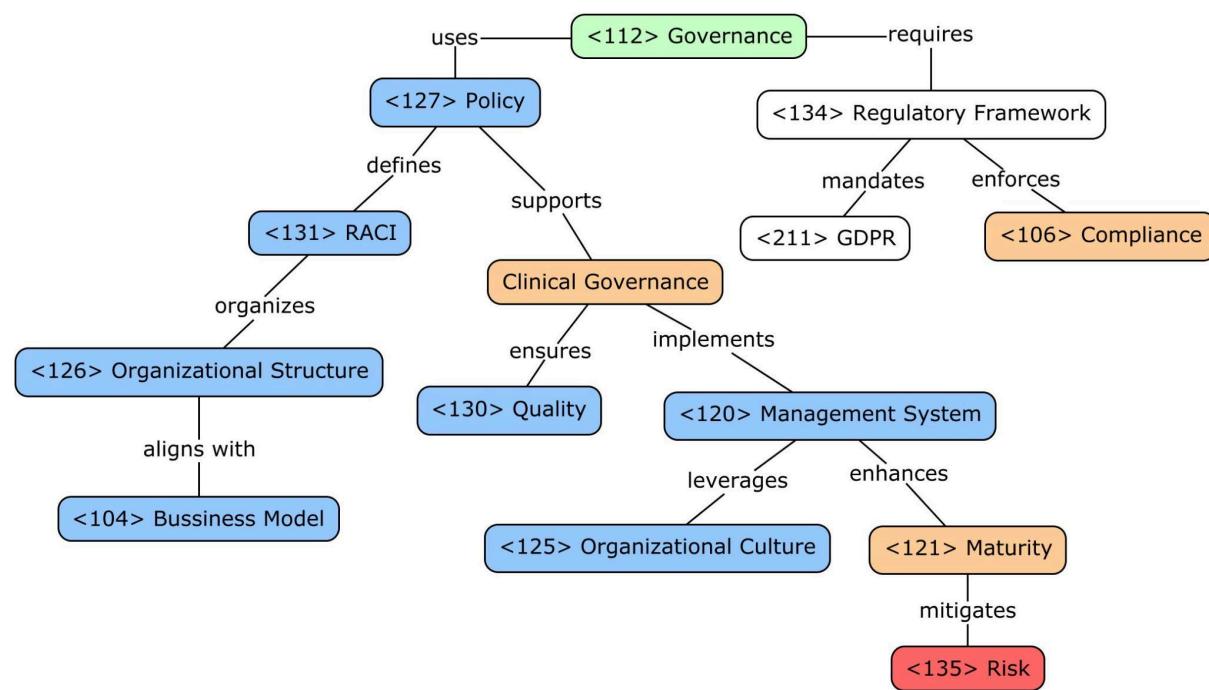
<204> Consultants and external partners, including <218> MDR and <220> MSSPs, support implementation of standards (e.g., ISO/IEC 27001, NIST CSF). Performance and integrity are monitored through <116> KPIs and reported using <119> management frameworks.

Ethical governance demands user transparency through <221> opt-in and <222> opt-out consent where applicable. All this is enabled by clear roles, traceable data, and proactive governance culture.

Governance of IT in smart factories is more than infrastructure—it is the backbone of resilient, data-driven, and ethical manufacturing.

Healthcare - Scheduling Scales

Organizations, Governance and Management



The governance <112> and management <118> of scheduling scales for healthcare professionals are critical to organizational effectiveness in the healthcare industry, ensuring alignment with patient rights and clinical governance principles. This process <129> is essential across all major healthcare business models <104>, Beveridge-style, Bismarck-style and Market-based systems, and involves structured frameworks to allocate doctors, nurses, and support staff.

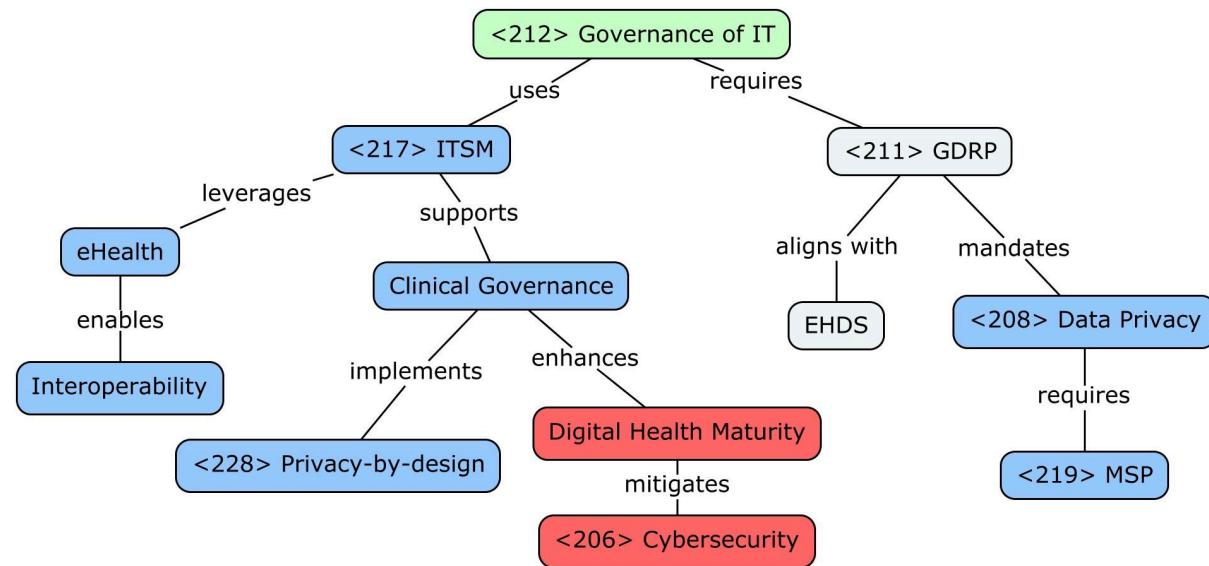
Governance <112> establishes policies <127> and RACI <131> frameworks to define responsibilities, in order to ensure accountability in both public sector systems, which prioritizes access to everyone fairly, and private sector entities, which emphasizes efficiency and profitability. Compliance <106> with regulations like GDPR <211> safeguards patient data used in scheduling, while management systems <120>, often organized around ISO frameworks, coordinate resources to maintain service quality <130>.

In urgent care scenarios, scheduling scales significantly impact responsiveness. Robust governance mitigates risks <135> like staff shortages or unexpected demand surges, which can compromise patient safety and basic rights. Clinical governance <112> ensures that urgent care prioritization aligns with ethical values and regulatory standards, particularly in public systems where transparency is fundamental to maintaining trust, preventing corruption or mismanagement, and complying with regulatory requirements that often mandate this kind of openness.

Maturity <121> in scheduling is reflected in automated, interoperable IT systems that enable rapid adjustments during crises. Organizational culture, rooted in patient-centered care, reinforces adherence to these protocols, enhancing resilience and upholding patient rights to timely interventions across diverse healthcare models.

Healthcare - Scheduling Scales

Governance of IT and IT Management



In the healthcare industry, the governance of IT **<212>** and IT management support the effective scheduling of scales for professionals, ensuring operational efficiency and patient safety across the three healthcare main systems implemented across the world.

Governance of IT **<212>** establishes accountability through defined decision rights, ensuring scheduling systems support clinical governance and patient rights to timely care. IT management leverages eHealth platforms, such as electronic health records (EHRs) integrated with Portugal's SPMS, to optimize staff allocation while adhering to GDPR **<211>** and privacy-by-design **<228>** principles for data privacy **<208>**.

The impact on urgencies is profound. Robust IT governance enables dynamic scheduling adjustments by prioritizing real-time data integration and cybersecurity **<206>**, through the CIA triad **<202>**, critical for managing patient surges or emergencies. Mature data governance ensures interoperability across public and private sectors, facilitating rapid staff redeployment during crises.

Vendor assessment **<232>** oversees third-party scheduling tools, aligning them with the European Health Data Space (EHDS) standards and applying MSP **<219>** principles to coordinate programme-level governance, mitigate risks, and ensure strategic fit within clinical and operational priorities.

Ethical governance ensures fairness in urgent care prioritization, mitigating risks like system outages that could delay critical interventions, thus enhancing system robustness and trust in healthcare delivery.

Transport & Logistics vs Manufacturing

Organizations, Governance and Management

Aspect	Smart Factories (Manufacturing)	Transport Routes Optimization (Transport & Logistics)
Focus	Cyber-physical systems, IoT, and AI enable automation and real-time control.	AI, GPS, and analytics optimize delivery paths and reduce delays.
<112> Governance	Structured <114> IMS supports integration of IT/OT; led by <108> CxO roles.	Governance driven by <136> Top Management , focusing on compliance and service continuity.
<135> Risk	Key risks: cyberattacks on <318> OT , downtime; managed through <103> Business Continuity .	Risks include disruption, regulatory issues; mitigated with <115> Internal Controls .
<106> Compliance	<101> Audited under standards like ISO 9001, IEC 62443; <105> certification [105] required.	Compliance with logistics and environmental rules; performance often verified through audits.
<104> Strategy	Emphasis on digital twins, predictive maintenance; aligned with <119> Management Frameworks .	Strategic goal: efficiency and sustainability; embedded in a broader <104> business model .
<116> KPIs	Tracks uptime, defect rates, energy use.	Measures delivery times, route efficiency, and CO ₂ emissions.
<126> Structure	Often vertically integrated; uses <131> RACI to clarify roles.	Distributed structure with third parties; requires coordinated data sharing.

Governance of IT and IT Management

IT governance and management differ across industries due to different operational needs, influencing system implementation, cyber-risk priorities, and data handling.

Firstly, we can notice differences in the usage of Identity and Access Management **<214>** systems. Logistics requires decentralized IAM to support remote access across warehouses, fleets, and frontline workers, along with robust ITSM **<217>** to handle high user ticket volumes, while manufacturing centralizes IAM to focus on office and factory IT systems.

Manufacturing often seeks consultancy firms for automation strategies for the factory floor, while Transport and Logistics focuses on getting outside insights for their information systems, such as cloud migration and securing remote access through MSSPs **<220>** to prevent cyber threats like man-in-the-middle attacks or DDoS takedowns.

The application of **<205>C-SCRM** varies significantly between the two sectors. Manufacturing focuses on protecting industrial production centers from cyber threats **<206>** to maintain physical integrity. In contrast, Logistics focuses on securing coordination networks and enabling alternative routes for optimization, thereby ensuring uninterrupted information flows against all types of risks.

Finally, we can notice a huge disparity in the quantity of **<223>PII** that is stored by each industry. Whereas the manufacturing industry only needs to take into account the data of its coworkers, the Transportation industry needs to safely handle a lot more information, whether it's because of commuters that pay for public transportation in a monthly basis, or about getting packages to their destinations - introducing possible concerns in Data Residency **<209>** in the case of international shipping.

Transport & Logistics vs Healthcare

Organizations, Governance and Management

Both of these industries are essential to the functioning of society, yet their different core missions need distinct approaches for effective levels of organization, governance, and management.

In terms of organizational structure <126>, Logistics industries tend to embrace decentralization, requiring coordination across multiple national and international entities (<133>) for operational efficiency; while healthcare providers generally operate within more hierarchical and centrally managed systems, with hospitals often serving as central hubs.

The leadership <117> in Transport & Logistics organizations primarily prioritizes commercial performance and service efficiency. Relationships between stakeholders are often formalized through contractual agreements such as SLAs <323>, and international trade laws, created by different regulatory bodies <133> play a critical role in administering global shipping operations. Thus, this industry tends to focus on key KPIs <116> such as delivery times and load utilization to control costs and maximize revenue.

The healthcare industry's mission <122>, however, is more driven by human well-being, and is therefore driven more on factors such as quality of care and patient safety. To achieve this, governance <112> often prioritizes ethical values <111> (accountability, transparency, etc.) over just efficiency and revenue, and establishes RACI <131> to better clarify roles of staff, since failures in care delivery can have life-threatening consequences and lead to severe legal disputes. KPIs usually factor in client satisfaction (such as waiting time in the ER) and treatment effectiveness (like mortality and readmission rates).

Governance of IT and IT Management

Transport & Logistics and Healthcare, while both critical and digitally nowadays dependent, have different operational priorities.

In Transport & Logistics, <212>Governance of IT primarily focuses on efficiency, cost optimization, and <231>Supply Chain, coordinating infrastructure and service reliability to ensure connectivity between networks. <206>Cybersecurity focuses on preventing operational disruptions, such as booking platforms and supply chain software, where cyber risk is significant. <303>Cyber Resilience aims for quick fix of logistics to minimize economic impact, with a <234>Zero Trust model included to protect networks. <217>ITSM and <311>IT Operations Management prioritize optimizing real time data and ensuring platform functionalities with the objective of respecting deadlines and reducing costs.

In Healthcare, <212>Governance of IT focuses mostly on patient safety, ethics and clinical results, prioritizing secure Electronic Health Record systems. <206>Cybersecurity is critical due to direct impacts on sensitive patient data, such as ransomware. <234>Zero Trust is fundamental for controlling access to highly sensitive health information and while <218>MDR provides continuous threat monitoring for both topics, consequences of failure are more severe in healthcare. <217>ITSM and <311>IT Operations Management prioritize the availability and accuracy of clinical systems, with patient well being over pure efficiency.

Regarding data, Transport handles passenger/e-commerce logistics data under privacy laws like <211>GDPR, focusing on transparency (e.g., eFTI Regulation). Healthcare manages highly sensitive patient data under GDPR's strict categories, demanding precise consent and long term record keeping (e.g., EHDS). Supply chain risk in Transport involves asset operations, while in Healthcare, it's critical for medical devices and pharmaceuticals, where software integrity impacts patient safety.

Security and Management of Information Systems

**Delivery 1
group 156**

1 - Manufacturing

1.1. Governance

1.1.1 Analysis

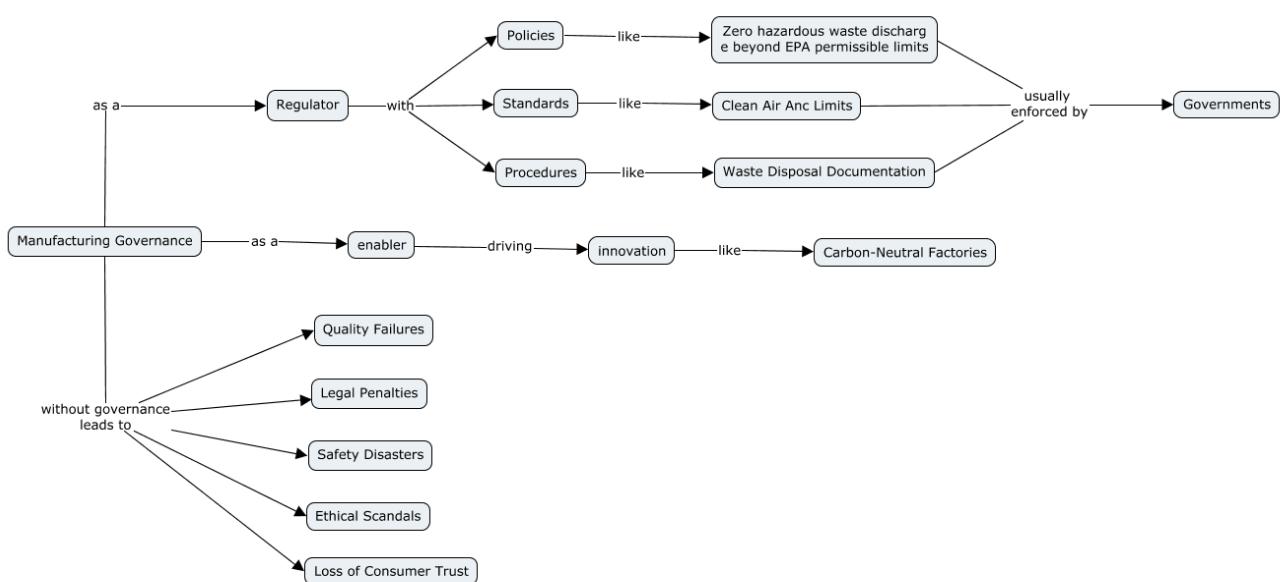
The manufacturing Industry is a cornerstone of economic development, but its growth and sustainability heavily depend on effective governance. It shapes how manufacturers operate, innovate, and contribute to society. Government regulations that enforce laws on manufacturing activities, such as environmental compliance, manufacturing facilities are required to comply with emission limits, and labour laws for occupational safety, can influence manufacturing in multiple ways. Tax breaks from governments can also stimulate manufacturing.

Internal governance determines a company's long-term success. Effective corporate governance is vital in the manufacturing industry, where non-compliance with regulatory requirements can lead to legal liabilities, reputational damage, and financial losses (Cornejo, 2024). These include economic and data transparency, ethical values, and compliance with legal obligations.

Governance acts as both a regulator (for example, penalties for pollution) and an enabler (drives innovation). A well-designed governance framework enables organisations to navigate complex regulatory requirements, manage risk, and optimise performance.

Without governance, the manufacturing sector faces severe repercussions. Environmental safeguards collapse, leading to unchecked pollution and disasters. Labor protections erode, resulting in unsafe working conditions and exploitation. Quality control falters, causing defective products that trigger massive recalls and loss of public trust. Regulatory violations invite billion-dollar fines, while corruption scandals dismantle corporate integrity. In the absence of governance, manufacturing risks becoming a liability rather than the engine of progress it is meant to be.

1.1.2 Conceptual Map



1.2 IT Management

1.1.1 Analysis

IT Management plays a crucial role in optimizing operations, improving efficiency, and driving innovation in the manufacturing industry. IT systems automate production lines, reducing human error, it allows to track raw materials and finished goods in real time, and also, it helps analyze production trends, defects, and demand forecasting. Other IT tools, such as AI and robots, allow the creation of “smart factories” with self-optimizing production.

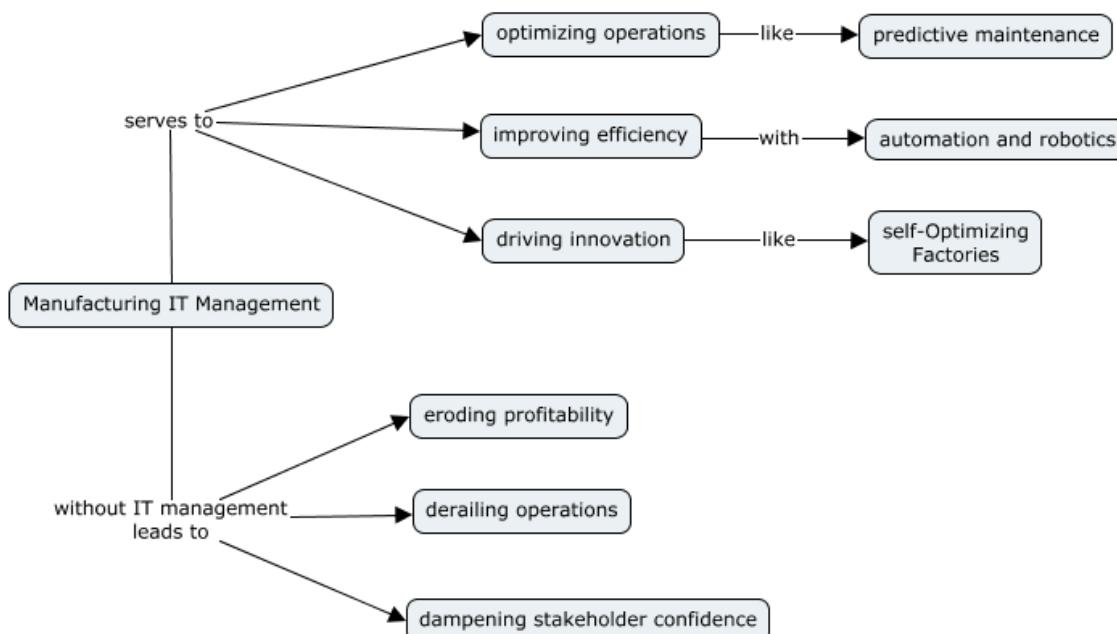
IT Management transforms manufacturing by enhancing automation, efficiency, security, and innovation. Through IoT, AI, cybersecurity, and cloud technologies, it enables smart factories with self-optimizing production, predictive maintenance, and sustainable operations. By integrating digital tools with workforce training and supply chain optimization, IT management serves as the backbone of modern Industry 4.0. (“Managing IT Systems in the Manufacturing Industry - Explitia,” 2024)

In manufacturing, poor IT management fragments production, exposes factories to cyberattacks, and erodes profitability. Unlike other industries, manufacturing relies on tightly integrated systems where a single IT failure can cascade into production stoppages, defective batches, supply chain chaos, and even safety hazards.(Baumann, 2025)

1.1.2 Conceptual Map

Predictive Maintenance - Predictive maintenance works by capturing and analyzing equipment data in real time to predict potential issues before they lead to equipment failure. (“What Is Predictive Maintenance? A Complete Overview | SAP,” 2022)

Self-optimizing Factories - Proactively identifying and addressing inefficiencies, bottlenecks, and vulnerabilities in factories (Procter, 2024)



2 - Hospitality and Leisure

2.1. Governance

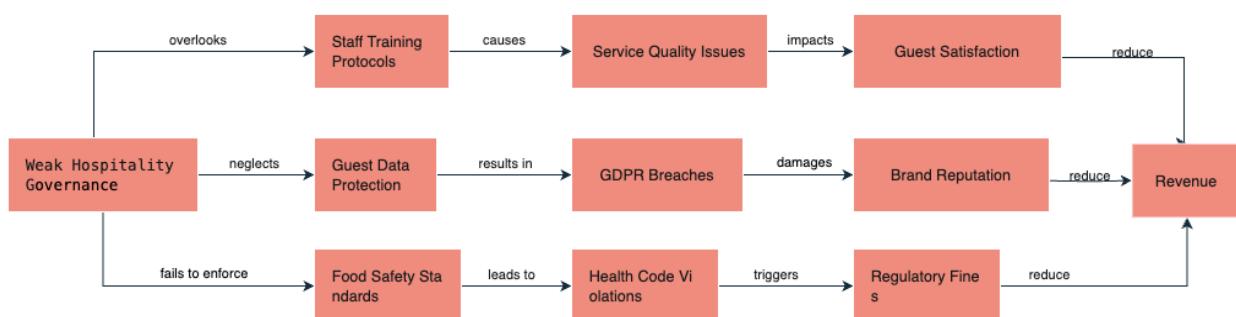
2.1.1 Analysis

The contemporary hospitality and leisure industry operates within an increasingly complex ecosystem where exceptional customer experiences must be delivered alongside rigorous compliance standards and technological innovation. This sector's governance framework has become a critical differentiator, requiring organisations to simultaneously address three fundamental pillars: regulatory compliance, digital reputation management, and technological transformation. At its regulatory core, hospitality governance must navigate an intricate web of standards, including HACCP protocols for food safety, ISO 22000 certification requirements, and the stringent data protection mandates of GDPR (EU GDPR, 2018). These compliance obligations extend beyond basic legal adherence, directly impacting operational workflows, staff training protocols, and technology infrastructure investments. The consequences of non-compliance have grown more severe, with potential fines reaching 4% of global turnover under GDPR and reputational damage that can take years to repair. The sector's technological transformation presents both its greatest opportunities and most significant vulnerabilities.

While Property Management Systems have revolutionised operational efficiency, they've also created new attack vectors for cyber threats. Modern governance frameworks must therefore balance innovation adoption with robust cybersecurity measures, particularly as properties increasingly rely on IoT devices, contactless technologies, and cloud-based solutions. This requires continuous investment in both technological infrastructure and human capital, training staff to recognise threats while implementing advanced security protocols.

Looking forward, the most successful hospitality operators will be those that develop adaptive governance models capable of evolving alongside regulatory changes, technological advancements, and shifting consumer expectations. This necessitates governance structures that are simultaneously rigorous in their standards yet flexible in their implementation - a challenging balance that will separate industry leaders from followers in the coming decade.

2.1.2 Conceptual Map



2.2 IT Management

2.2.1 Analysis

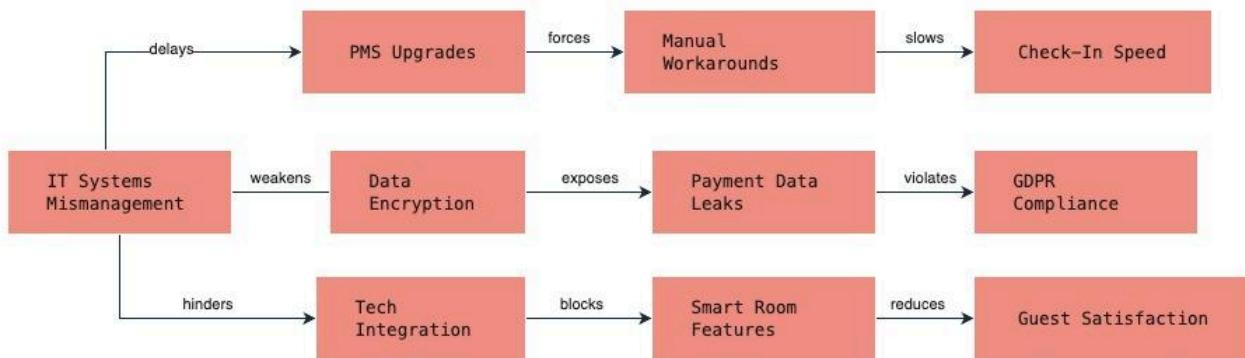
The hospitality industry's digital transformation has elevated IT management from operational support to a strategic imperative, creating both opportunities and vulnerabilities that demand careful governance.

Modern property management systems now serve as central nervous systems for hospitality operations, integrating reservations, housekeeping, and revenue management while processing sensitive guest data across multiple touchpoints. These technological advancements have introduced complex dependencies where system failures can cascade into immediate operational disruptions and lasting reputational damage. Hospitality IT ecosystems face unique security challenges as they balance open accessibility with data protection requirements.

The sector's widespread adoption of cloud-based solutions and IoT devices has expanded attack surfaces, particularly for payment systems and guest data storage. GDPR compliance adds another layer of complexity, requiring meticulous data mapping across booking platforms, loyalty programs, and service delivery systems. These security concerns exist alongside pressing innovation needs, as properties race to implement contactless technologies, AI-driven personalisation, and dynamic pricing engines that guests increasingly expect. The most successful operators are those developing IT governance frameworks that simultaneously enable innovation and mitigate risk. This requires continuous investment in both technological infrastructure and human capital, ensuring staff at all levels understand their role in maintaining system integrity.

Looking ahead, hospitality IT leaders must cultivate adaptive strategies that can evolve with emerging technologies while maintaining compliance with an ever-changing regulatory landscape. The organisations that master this balance will gain a significant competitive advantage in delivering seamless, secure guest experiences.

2.2.2 Conceptual Map



3 - Banking and Financial Services

3.1 Governance

3.1.1 Analysis

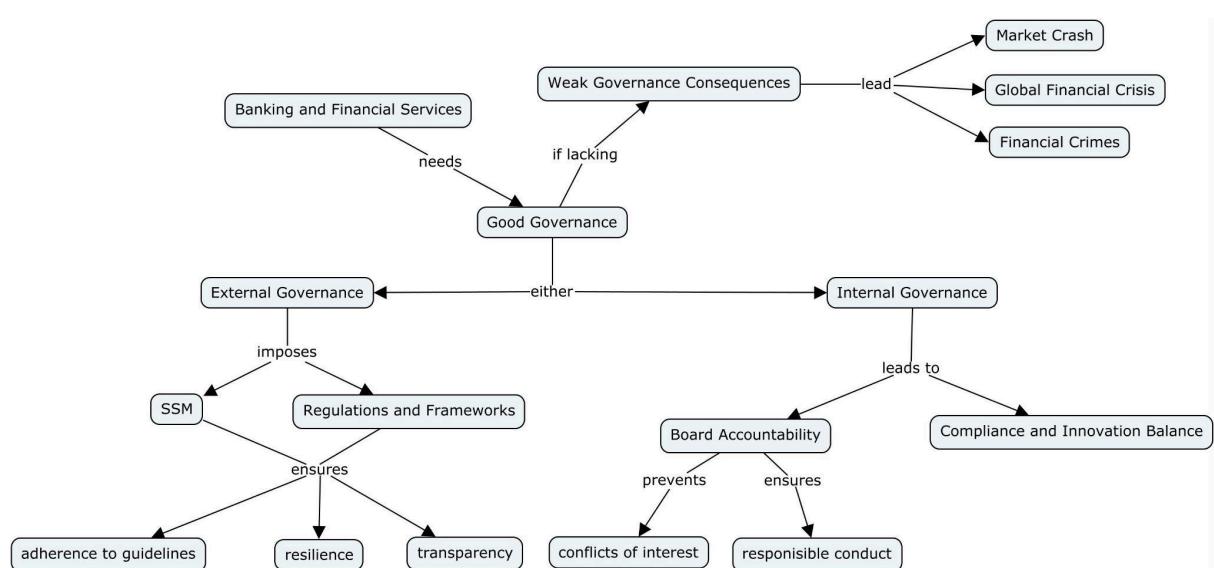
The banking and financial services industry acts as one of the most pivotal pillars of societal and economical development. Since encompasses all the economic activities and every sector of this industry is interconnected it is extremely important to have strong governance frameworks, be it external (for example regulatory measures from governments) or internal (directly from the corporations policies), to avoid vulnerabilities or failures to spread from institutions to the entire society.

For example the Single Supervisory Mechanism is a key component of Europe's banking oversight. It makes sure organizations adhere to strict requirements like the Basel III/IV, reducing the risk of financial crisis. It also imposes transparency with MiFID II and digital security guidelines with DORA.

On an organizational level institutions have an important task balancing compliance with these guidelines and innovation. For that strong governance ensures that the boards are accountable, preventing conflicts of interest or other problems that could jeopardize the normal operations. It can prevent operational hazards resulting from poor resilience, which can occur if the international guidelines are not followed. And it also plays an important role in ensuring transparency and protecting depositors and investors.

Without strong governance from regulatory agencies or the organizations themselves the sector could suffer catastrophic consequences - systemic bank failures, unchecked financial crimes (money laundering, fraud) and loss of public trust with financial intuitions that could lead to market crashes and global economic crises.

3.1.2 Concept Map



3.2 IT management

3.2.1 Analysis

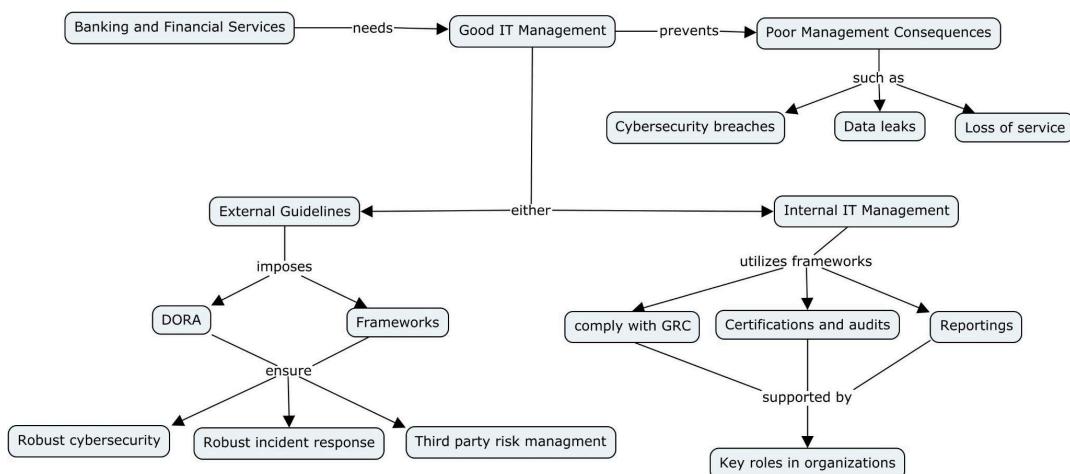
Banking and financial services institutions today operate in an environment of rapid digital transformation. Strong IT management is essential not only for innovation but also for managing risk and meeting growing regulatory demands resulting from the increase in reliance from third-party technologies. Failures in IT systems or cybersecurity can result in chain failures disrupting the entire market and for that IT governance and management should be one of the top priorities of the industry.

For that, regulatory frameworks like the Digital Operational Resilience Act (DORA) in the EU emphasize the need for robust cybersecurity, incident response, and third-party risk management. These frameworks emphasize the importance that international governing bodies give to digital resilience, understanding that without there is no financial stability in the current times.

Internally, institutions should align IT operations with the governance, risk and compliance functions (GRC). Key roles, such as the CIO, CRO and CISO ensure that IT systems are secure, compliant and resilient. They are the responsible for maintaining the critical infrastructures that can mitigate failures, cyberattacks and manage the risks associated with the use of external softwares and IT solutions. Mature IT management should also support certifications, audits and reportings to ensure organizational transparency and robustness.

Without effective IT management, the sector faces considerable risks: cybersecurity breaches, data leaks, loss of service availability. These vulnerabilities can lead to regulatory penalties and even systemic crises if not properly addressed. Therefore, aligning IT strategy with operational goals and regulatory expectations is not optional, it is vital for the health and integrity of the financial system.

3.2.2 Concept Map



4 - Manufacturing & Banking and Financial Services

4.1 Governance

Governance in manufacturing and banking and financial services shares the goal of ensuring operational resilience and regulatory compliance, but the drivers and risks have core differences. In manufacturing, governance focuses on quality (ISO 9001), safety (ISO 45001), environmental compliance (ISO 14001), and more recently, the integration of IT and Operational Technology (OT) under Industry 4.0. This convergence brings cyber-physical risks, governed by standards like IEC 62443 and directives such as NIS2, especially across complex global supply chains.

In contrast, governance in banking centers on financial stability, market integrity, and consumer protection. It is shaped by strict frameworks such as Basel III/IV (capital adequacy), AML/KYC, MiFID II, and DORA, embedding risk management deeply into IT, operations, and board oversight. Banks must govern not only for efficiency but also to prevent systemic risk, as failures can propagate across the global economy, unlike manufacturing failures, which are typically more localized.

Despite these differences, both sectors are converging around the need for robust digital governance to navigate complex regulatory landscapes, protect stakeholder interests, and enable secure innovation. Evidence from India shows that tailored credit allocation significantly boosted manufacturing output in regions with stronger local banking systems (Thamby & Tiwary, 2021).

4.2 IT Management

IT management plays a critical but context-dependent role in both manufacturing and banking and financial services, showing each sector's operations and risk profiles. In manufacturing, IT enables operational efficiency and Industry 4.0, integrating ERP, MES, and PLM with Operational Technology. Innovations such as Industrial IoT and AI for predictive maintenance tend to improve uptime, while simultaneously introducing cyber-physical risks. Failures affect output, supply chains, and safety, demanding robust and production-aligned governance.

Banking, on the other hand, centers IT on transaction integrity, data security, and regulatory compliance (DORA, Basel III). Core systems span digital channels, fraud detection, and core banking platforms, operating under strict oversight. IT failures can trigger legal, reputational, or systemic financial harm, making resilience and compliance top priorities.

Both sectors pursue IT driven innovation, but banking emphasizes security and systemic risk mitigation, while manufacturing focuses on efficiency and cyber-physical integration, reflecting their distinct governance demands.

5 - Banking and Financial Services & Hospitality and Leisure

5.1 Governance

The Banking and Financial Services sector in terms of governance is molded by systemic stability, financial integrity, consumer assets protection and public confidence. Financial institutions are subject to extensive regulatory oversight, setting strict expectations for operational integrity and risk control, with frameworks for capital adequacy, market transparency, digital resilience, anti-money laundering and customer due diligence. It is also enforced by external entities like the European Central Bank, requiring financial institutions to maintain board accountability, and comprehensive compliance programs.

In comparison, governance in Hospitality and Leisure is less centralized but equally essential, focusing on guest safety, legal compliance, and digital reputation. Operators must comply with standards for food safety, risk management, and data privacy. The challenges stem from its high customer interaction and decentralized operations, which increase exposure to reputational risks and legal penalties.

Despite the differences, both sectors share a growing dependence on governance frameworks that prioritize customer trust, ethical conduct, and agility. Both must adapt to emerging technologies and evolving consumer expectations while upholding compliance and operational excellence. Governance in these sectors are becoming more proactive and integrated, it is not just about avoiding penalties but about enabling consistent, customer-focused performance across complex operations.

5.2 IT Management

IT management in Banking and Financial Services is foundational to secure, efficient service delivery and plays a critical role in innovation, compliance, and customer engagement. As institutions digitize, IT strategies must align closely with governance and risk management to prevent disruptions, ensure data protection, and support seamless customer experiences. Financial services today are not only about security and compliance but also about building digital platforms that deliver convenience, personalization, and reliability to clients.

In the Hospitality and Leisure sector, IT management similarly drives operational efficiency and guest satisfaction. Digital check-ins, IoT-enabled rooms, personalized booking platforms, and contactless services all depend on strong IT frameworks. These systems must be able to deliver memorable experiences while protecting customer data.

Although the complexity and regulatory pressure may differ, both sectors are converging on the realization that IT is a strategic asset, central to service quality, customer loyalty, and business continuity. The ability to deliver fast, secure, and personalized digital services is now a core expectation in both cases and IT management has evolved into a business function tied directly to organizational success and competitive differentiation.

References

- Cornejo, J. (2024) *Corporate Governance in the Manufacturing Industry: Compliance and Quality Assurance*, Attorney Aaron Hall. Disponível em: <https://aaronhall.com/corporate-governance-in-the-manufacturing-industry-compliance-and-quality-assurance/> (Acedido: 18 de maio de 2025).
- EU GDPR. (2018). General Data Protection Regulation. <https://gdpr.eu/>
- Hospitality Technology. (2024). The Digital Transformation of Guest Experiences. <https://hospitalitytech.com/>
- Oracle. (2024). AI in Hospitality CRM Systems. <https://www.oracle.com/>
- Managing IT systems in the manufacturing industry - explitia. (2024, September 16). Retrieved May 22, 2025, from explitia website: <https://explitia.com/blog/managing-it-systems-in-the-manufacturing-industry/>
- Baumann, B. (2025, January 6). Panorama Consulting Group. Retrieved May 22, 2025, from Panorama Consulting Group website: <https://www.panorama-consulting.com/root-causes-of-it-failures-manufacturing-industry/>
- What is predictive maintenance? A complete overview | SAP. (2022). Retrieved May 22, 2025, from SAP website: <https://www.sap.com/portugal/products/scm/apm/what-is-predictive-maintenance.html#:~:text=Predictive%20maintenance%20works%20by%20capturing,transmit%20information%20on%20equipment%20conditions>.
- Procter, A. (2024, March 14). Using AI and automation for true self-optimization | Okoone. Retrieved May 22, 2025, from Okoone website: <https://www.okoone.com/spark/strategy-transformation/using-ai-and-automation-for-true-self-optimization/#:~:text=Self%2Doptimizations%20means%20proactively%20identifying,technological%20advancements%2C%20or%20unforeseen%20events>.
- Thampy, A., & Tiwary, M. K. (2021). Local banking and manufacturing growth: Evidence from India. *IIMB Management Review*, 33(2), 95–104. <https://doi.org/10.1016/j.iimb.2021.03.013>

Group: 157

Students: 98957, 103259, 103344, 112192

Manufacturing

Selected Subdomain: Smart Manufacturing / Industry 4.0

Industry Definition:

The manufacturing industry involves the transformation of raw materials into finished goods through physical, chemical, or digital processes. *Smart Manufacturing*, a subdomain of Industry 4.0, is characterized by the integration of cyber-physical systems, IoT devices, and data analytics to enable adaptive, automated production environments. It blends operational technology (OT) with information technology (IT), requiring advanced governance models to manage complexity, security, and digital resilience.

Textual Analysis 1: Theme 1 - Business Governance and Management in Smart Manufacturing

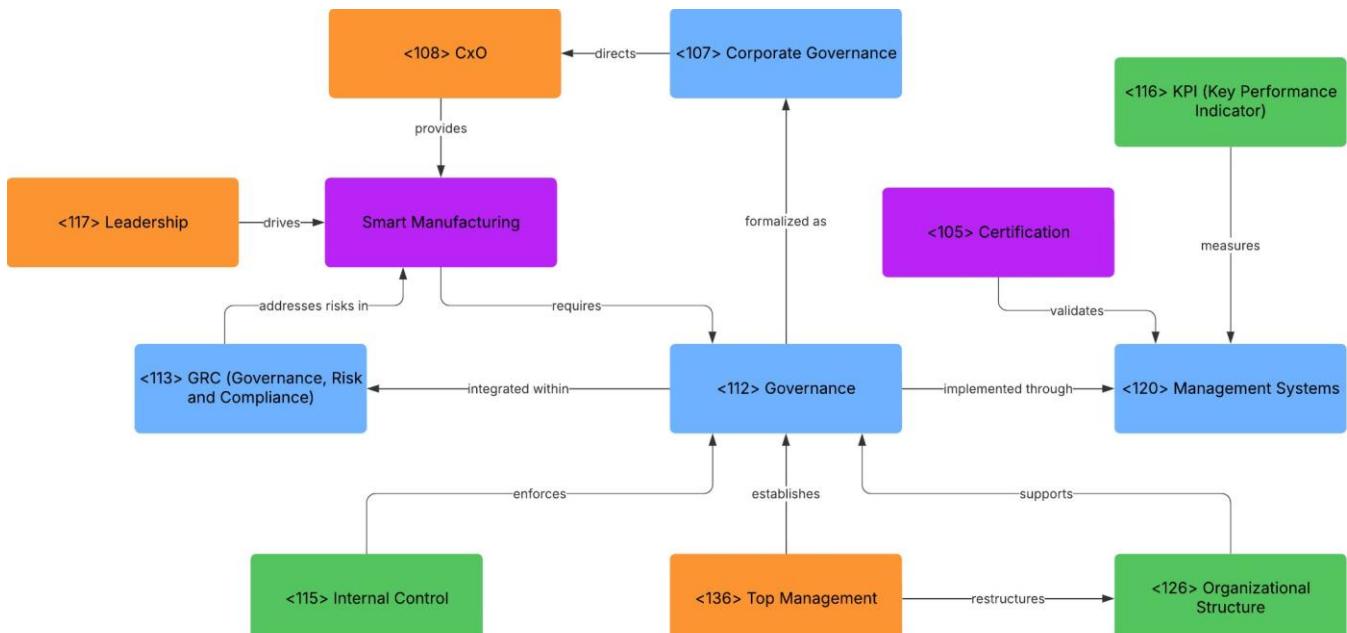
Smart Manufacturing represents a paradigm shift requiring robust <112> Governance frameworks that align digital capabilities with production requirements. The <126> Organizational Structure must evolve to eliminate silos between production and IT, while <136> Top Management sets a <122> Mission that balances technological advancement with manufacturing excellence. This transformation demands comprehensive <127> Policy frameworks addressing both production standards and digital security concerns.

Effective <117> Leadership is essential to drive cultural change as organizations integrate cyber-physical systems into existing operations. Leaders must maintain focus on <130> Quality across both physical products and digital systems that control them. The <108> CxO structure often expands to include digital specialists who bridge manufacturing expertise with technology capabilities, requiring a redefined <131> RACI matrix to clarify decision rights across these converging domains.

<115> Internal Control systems become more complex as they span physical assets and networked infrastructure. Organizations implement integrated <120> Management Systems that require <101> Audit processes evaluating both operational efficiency and digital security. Such audits verify <106> Compliance with traditional manufacturing standards and emerging cybersecurity frameworks, creating a cohesive <113> GRC (Governance, Risk and Compliance) approach that addresses the unique risk profile of connected manufacturing environments.

Smart Manufacturing requires sophisticated <116> KPI (Key Performance Indicator) frameworks measuring both production metrics and system performance. The <107> Corporate Governance structure must ensure appropriate oversight of physical and digital assets, often requiring <105> Certification against multiple standards to demonstrate

<121> Maturity in this integrated management approach. <118> Management must balance traditional industrial concerns with emerging digital priorities while maintaining <111> Ethical Values in data usage and algorithmic decision-making that affects production processes.



Textual Analysis 2: Theme 2 - IT Management in Smart Manufacturing

Smart Manufacturing environments merge operational technology with enterprise systems, creating unique management challenges. <217> ITSM practices must adapt to address both business applications and production systems, with service catalogs expanded to include <318> Operational Technology components requiring cross-domain expertise.

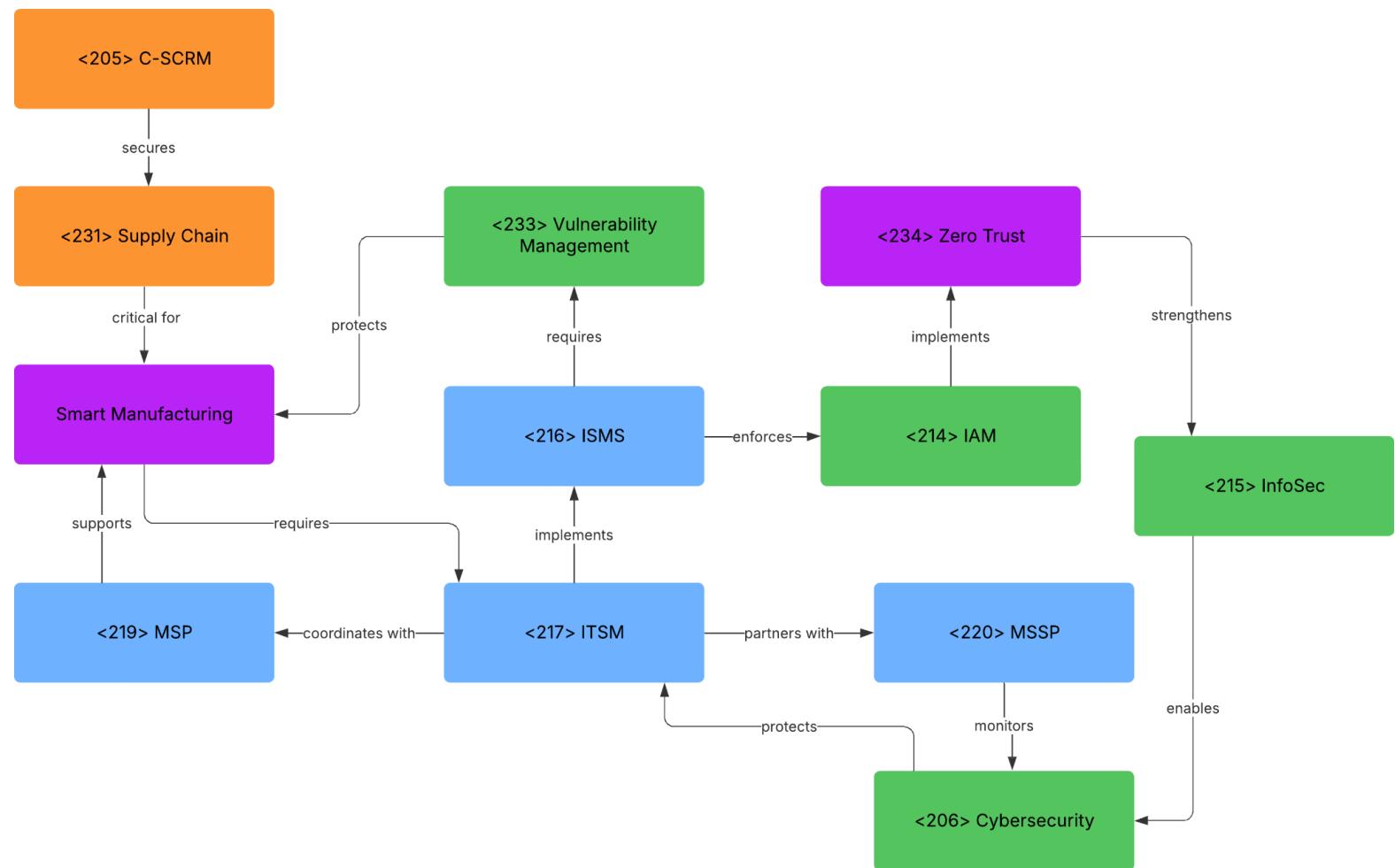
The converged landscape necessitates sophisticated <214> IAM solutions that enforce strict boundaries between business and production networks. Manufacturers often establish <219> MSP relationships for specialized OT support while maintaining <220> MSSP partnerships for security monitoring across both domains.

<216> ISMS implementations must address the extended attack surface of connected equipment. Manufacturers develop customized <233> Vulnerability Management procedures accounting for equipment lifecycle limitations, typically aligning patching windows with planned production downtime to minimize operational disruption.

Organizations implement <208> Data Privacy protections for sensitive operational information, particularly when sharing with equipment vendors. <207> Data Localization requirements influence architecture decisions for global manufacturers, while <210> Data Retention policies balance compliance with operational insights preservation.

<206> Cybersecurity controls must maintain the <202> CIA triad across both domains, with security architecture including network segmentation between business systems and shop floor equipment. <215> InfoSec teams expand to include industrial protocol monitoring, requiring specialized skills beyond traditional enterprise security.

Integration drives the need for comprehensive <205> C-SCRM approaches evaluating components throughout the <231> Supply Chain. Manufacturers require <230> SBOM documentation from vendors while adopting <234> Zero Trust principles with continuous authentication protecting critical production assets from threats and misconfigurations.



Smart Manufacturing

Manufacturing paradigm integrating digital technologies with physical production systems

Hospitality & Leisure

Selected Subdomain: Accommodation

Industry Definition:

The Hospitality and Leisure industry encompasses services designed to provide comfort, recreation, and lodging to guests. Within it, the *Accommodation* subdomain refers to businesses offering overnight stays such as hotels, hostels, and resorts focused on service quality, guest experience, and operational efficiency. This sector varies from family-owned hotels to global chains, each subject to distinct governance and compliance requirements related to health, data privacy, and service delivery.

Textual Analysis 1: Theme 1 - Business Governance and Management in Accommodation

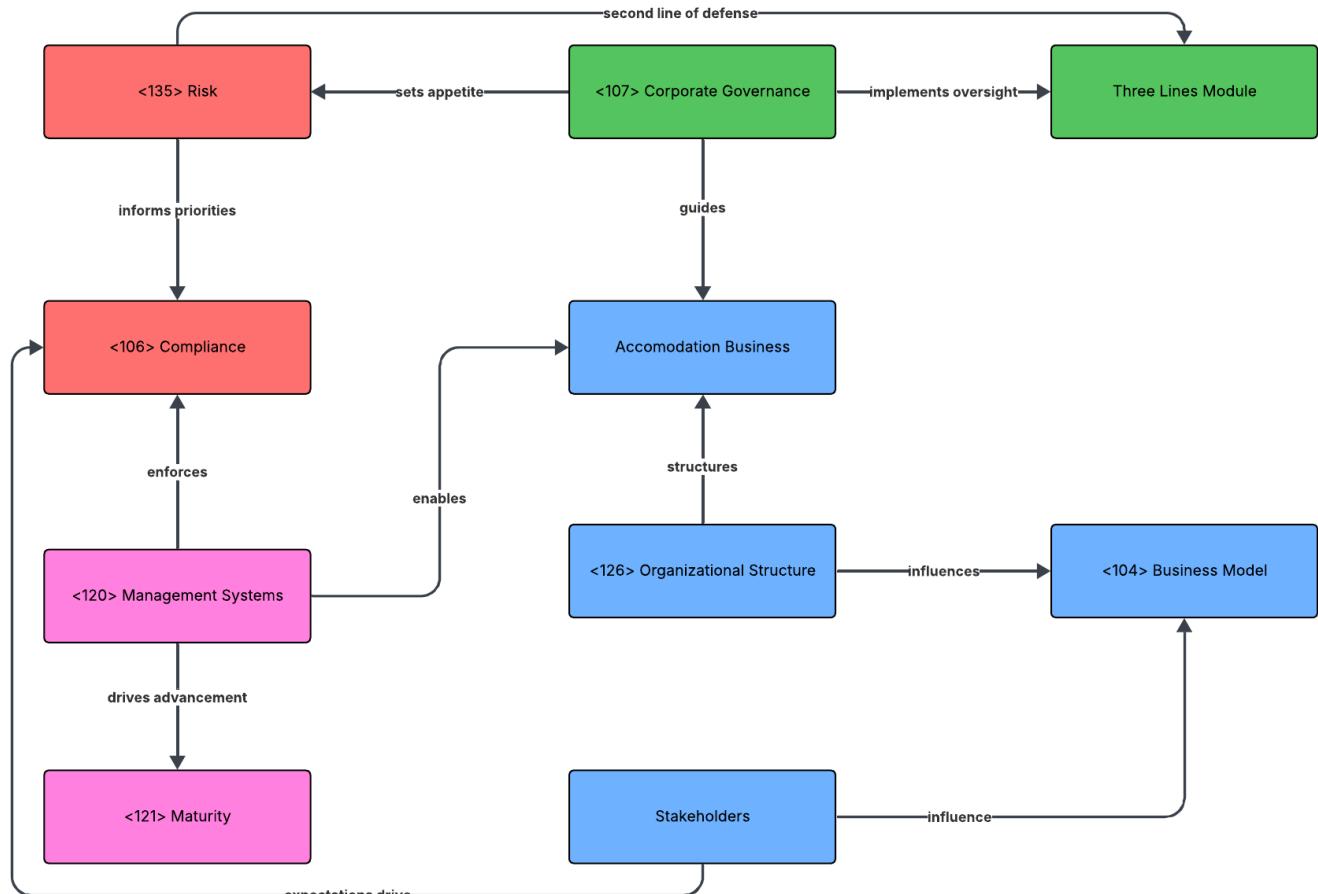
The Accommodation niche within the Hospitality and Leisure industry represents a critical component of the broader hospitality sector, characterized by its focus on guest experience and service quality. This segment operates within a complex *<112> Governance* framework that must balance consistency in service delivery with adaptability to local market conditions.

Effective *<112> Governance*, *<135> Risk*, and *<106> Compliance* in accommodation businesses requires managing diverse risks including operational disruptions, reputational damage from guest reviews, and regulatory adherence. The sector employs sophisticated *<120> Management Systems* such as Property Management Systems (PMS) to coordinate bookings, billing, and room status while ensuring operational excellence.

The industry exhibits various Organizational Models, ranging from family-owned establishments to international hotel chains with complex *<126> Organizational Structure and Models*. These businesses implement the Three Lines of Defence model to ensure proper oversight, with front-line staff managing daily operations, *<135> Risk* and *<106> Compliance* functions providing guidance, and internal *<101> Audits* offering independent assurance. This structured approach creates clear accountability across the organization, with *<112> Governance* mechanisms defining how each line operates and interacts with others to maintain effective control and *<135> Risk management*.

Accommodation businesses operate under multiple *<119> Management Frameworks* including health regulations, labor standards, and data protection laws like GDPR. Their *<104> Business Models* vary from ownership to franchise arrangements, each requiring specific Role and Responsibility Frameworks to clarify decision-making authority.

Organizations with high *<121> Maturity* levels demonstrate systematic property management practices, documented procedures, and continuous improvement cycles that enables them to deliver consistent guest experiences while adapting to changing market conditions.



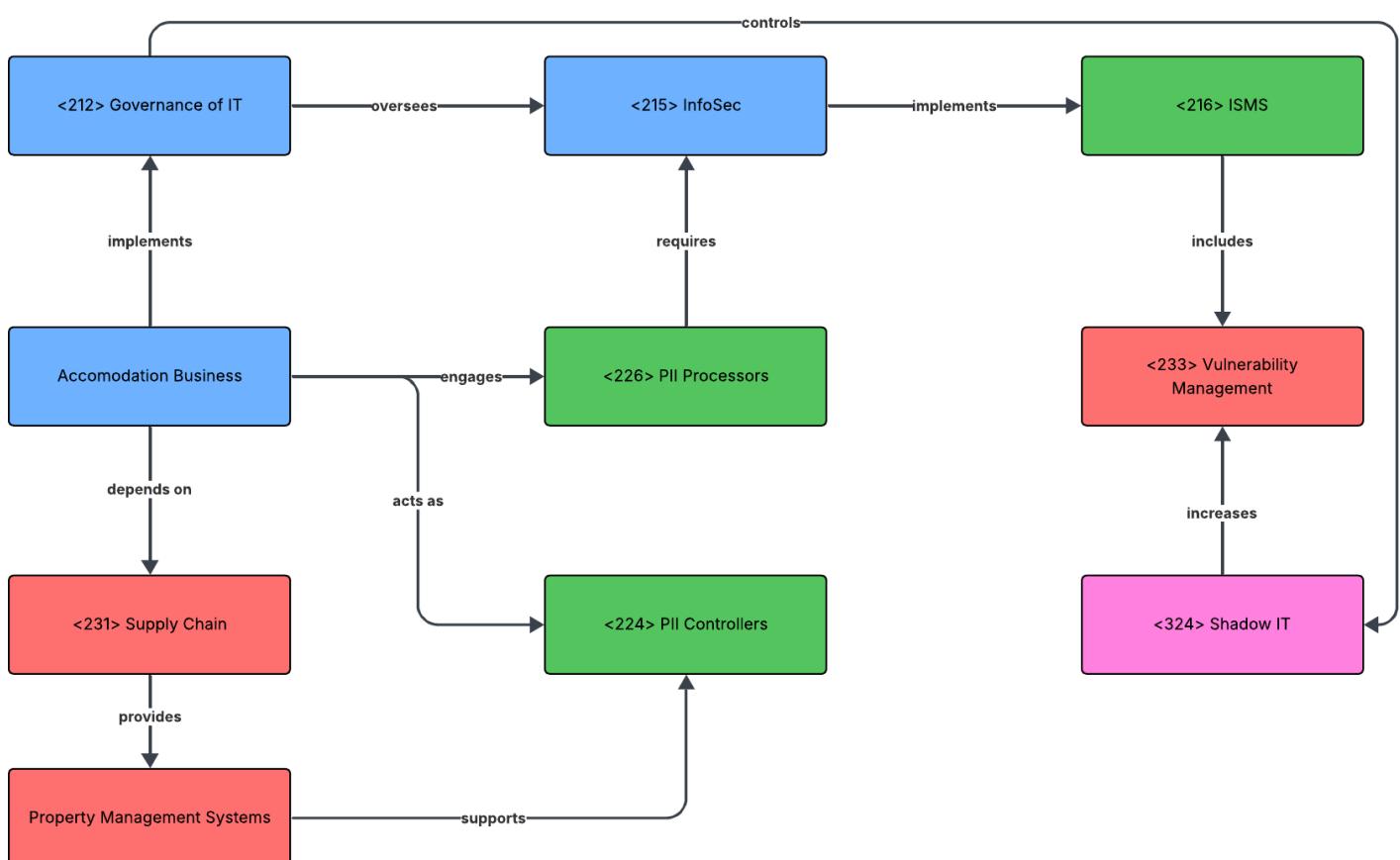
Textual Analysis 2: Theme 2 - IT Management in Accommodation

The Hospitality and Leisure industry, specifically the Accommodation niche, operates in a complex digital ecosystem that requires robust **<212> Governance of IT** to ensure service quality, guest satisfaction, and operational efficiency. Hotels and resorts manage extensive personal data through **<224> PII Controllers** and **<226> PII Processors**, making **<211> GDPR <106> Compliance** critical when handling guest information in booking systems and loyalty programs.

Accommodation businesses rely heavily on **<231> Supply Chain** relationships with Application and Platform Providers for their Property Management Systems (PMS), which serve as core software for managing bookings, billing, and room status. These systems often connect to Online Travel Agencies through Global Distribution Systems (GDS), creating complex **<205> C-SCRM** challenges as data flows through multiple **<226> PII Processors**. The sector faces significant **<135> Risks** related to **<223> PII protection**, requiring strong **<215> InfoSec** governance and implementation of **<216> ISMS** through frameworks like ISO/IEC 27001 to maintain the **<202> CIA triad** principles when handling sensitive guest information.

<324> Shadow IT presents particular challenges in accommodation businesses where staff may adopt unauthorized applications to improve guest service. Meanwhile, IT **<231> Supply-chain dependencies** through various IT providers create a potential **<233> Vulnerability Management** problem that must be solved through effective vendor and contract management.

For international hotel chains, **<221> Opt-in consent mechanisms** are essential when collecting guest data for marketing purposes, while **<132> Records Management** ensures proper handling of reservation histories and financial transactions according to regulatory requirements.



Agriculture

Selected Subdomain: Cooperative and Subsidy-Dependent Structures

Industry Definition:

Agriculture comprises activities related to crop cultivation, livestock management, and food production. The chosen subdomain, *Cooperative and Subsidy-Dependent Structures*, includes entities that operate under participatory governance models and rely on financial support from national or EU programs like the CAP. These structures are shaped by fragmented IT resources, decentralised management, and strict compliance obligations tied to land use, food safety, and environmental regulation.

Textual Analysis 1: Theme 1 - Business Governance and Management in Cooperative and Subsidy-Dependent Structures

Agricultural governance in cooperative and subsidy-dependent contexts exemplifies the challenge of aligning **<104>** business model diversity with coherent **<107>** corporate governance structures. While some entities function under cooperative principles with strong local roots, others are embedded in complex subsidy frameworks, often tied to national or supranational regimes such as the EU's CAP. These variations require governance models that balance stakeholder representation with **<103>** business continuity, particularly amid policy shifts and climate-related disruptions.

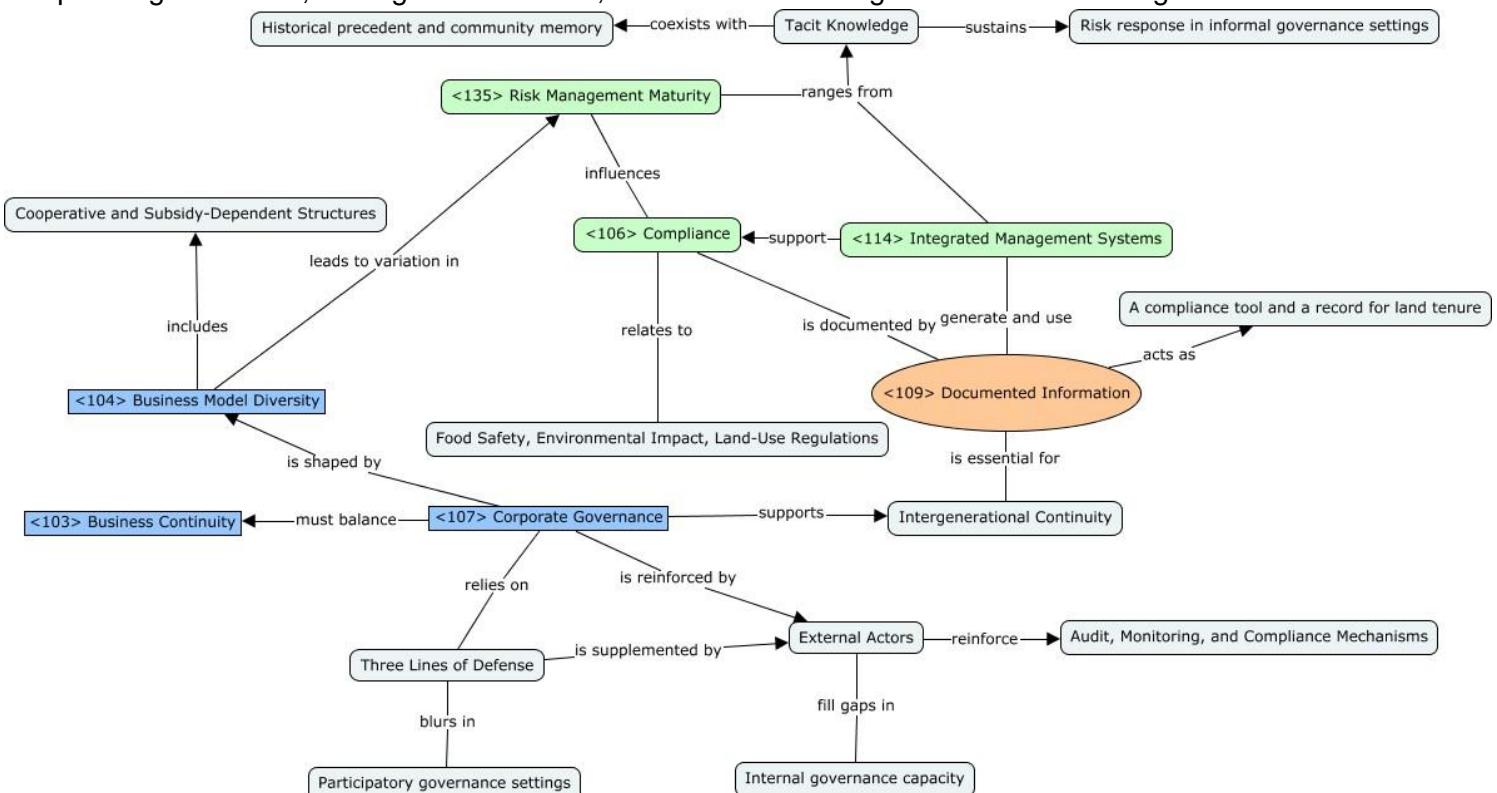
In cooperative settings, governance is typically participatory and distributed, which complicates the delineation of executive roles and weakens the distinction between oversight and operational execution. The application of the Three Lines of Defense framework is often hybrid or informal, with external actors (e.g., public agencies or NGOs) reinforcing or substituting **<101>** audit and compliance mechanisms. This is especially true for **<106>** compliance with food safety, environmental impact regulations, and land-use eligibility for subsidies.

Risk governance is conditioned by structural features of the sector: long planning horizons, seasonal exposure, and limited market liquidity. As such, **<135>** risk management maturity is uneven, with some organisations using formal

<114> integrated management systems (e.g., ISO 9001 or 14001), while others rely on tacit knowledge and historical precedent. In this context, **<109>** documented information is both a compliance instrument and a tool for sustaining intergenerational continuity, especially where land tenure is complex or contested.

Overall, governance must not only navigate legal and fiscal obligations but also reinforce collective purpose and adaptive capacity. The convergence of ecological volatility and subsidy dependency places a premium on transparent governance, strategic coordination, and resilience through institutional learning.

1



Textual Analysis 2: Theme 2 - IT Management in Cooperative and Subsidy-Dependent Structures

The architectural setup of IT systems in agriculture, particularly in cooperative or subsidy-dependent structures—must adapt to decentralised environments, fragmented resources, and compliance-heavy workflows. These systems operate with varying levels of digital maturity, often relying on Shadow IT, which refers to tools and systems deployed without formal IT oversight. These informal practices complicate integration and undermine governance mechanisms.

In low-infrastructure regions, cooperatives rarely have a dedicated architectural blueprint or reference model. The use of <229> Public Procurement mechanisms—while ensuring fairness and accountability—often leads to fragmented acquisitions that do not support long-term <220> MSSP-style integration or holistic IT strategies.

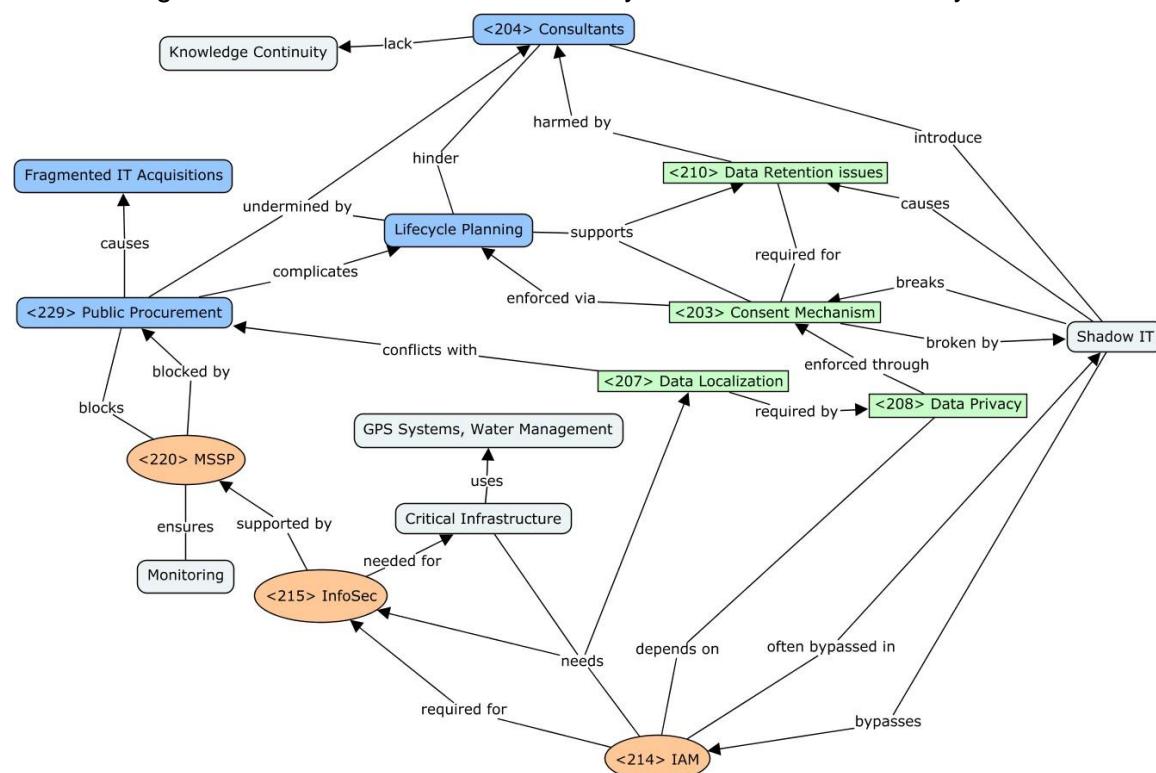
Systems are frequently externally maintained or pieced together by <204> Consultants with no embedded knowledge continuity, leading to <210> Data Retention issues. Without proper lifecycle planning, cooperatives face difficulties in enforcing <222> Opt-out or <203> Consent Mechanism requirements tied to GDPR. This is especially problematic when dealing with shared data infrastructures across CAP subsidy portals and land registries.

In terms of strategic architecture, most structures fail to incorporate <207> Data Localization constraints, despite handling location-sensitive agricultural and environmental records. Storage may reside on cloud services hosted abroad, potentially conflicting with sovereignty regulations and <208> Data Privacy expectations.

Additionally, cooperatives rarely implement <214> IAM with sufficient granularity. Multi-user environments such as Farm Management Information Systems (FMIS) often lack proper segregation of duties or audit trails, raising risks under sectoral regulations. These risks extend to supply-chain visibility where tracking systems should be aligned with <215> InfoSecprinciples but are instead governed ad hoc, or not at all.

As digital services evolve, cooperatives are increasingly considered part of Critical Infrastructure, especially when GPS-guided irrigation, environmental monitoring, and water rights management systems are involved. However, few adopt the architectural standards required to ensure resilience, redundancy, and compliance with sectoral obligations.

Effective IT management architecture in this domain must balance regulatory compliance, operational simplicity, and long-term sustainability. Applying architectural discipline demands coordination between internal roles and Vendor and Contract Management frameworks to ensure that systems evolve deliberately rather than reactively.



Comparative Analysis: Theme 1 – Business Governance and Management in Smart Manufacturing vs. Accommodation

Smart Manufacturing and Accommodation illustrate distinct approaches to **Governance**, shaped by their structural logic and digital evolution. In Smart Manufacturing, **Corporate Governance** frameworks are designed to integrate **Organizational Structures** across both IT and production domains. **Top Management** defines a **Mission** that balances technological innovation with operational stability, supported by specialized **CxO** roles such as CIO and CISO. These roles require a clarified **RACI matrix** to manage responsibilities across converging technical and business functions.

Accommodation businesses, in contrast, operate within diverse **Business Models**—ranging from independent hotels to global franchises—each requiring flexible governance mechanisms. The Three Lines of Defence model is often applied to distribute **Governance** and **Compliance** responsibilities between front-line operations, risk and control functions, and internal **Audit** structures. In larger chains, **Organizational Structures** include regional and corporate layers, requiring clearly defined **Policies** and standardized procedures.

While Smart Manufacturing prioritizes strong **Internal Control** and integrated **Management Systems**, often aligned with ISO standards (e.g., 9001, 14001), Accommodation businesses may rely more heavily on Property Management Systems and localized procedures. Maturity levels differ: manufacturing organizations aim for high **Maturity** in digital-physical alignment and security assurance, while accommodation entities demonstrate maturity through consistent service delivery and adaptability to regulatory changes.

Risk is also treated differently. In Smart Manufacturing, risk governance addresses cyber-physical threats, supply chain vulnerabilities, and operational continuity. In Accommodation, risk includes reputational exposure, regulatory non-compliance, and guest satisfaction. In both sectors, **Documented Information** supports **Integrated Management Systems** and serves as evidence of compliance and operational consistency.

Comparative Analysis: Theme 2 – IT Management in Smart Manufacturing vs. Accommodation

Smart Manufacturing and Accommodation differ significantly in their IT Management priorities due to the nature of their operations and risk exposure. In Smart Manufacturing, **ITSM** practices must integrate enterprise software with production environments, demanding service models that support both business and industrial assets. The sector requires precise **IAM** implementations to segment access between business and shop-floor networks, mitigating risks across the extended digital landscape. Additionally, manufacturers rely on **MSPs** and **MSSPs** to support OT-specific functionality and 24/7 security monitoring.

Security and compliance are addressed through robust **ISMS** aligned with industry standards, with **Vulnerability Management** processes adapted to avoid disrupting production cycles. As manufacturers engage external vendors, **C-SCRM** becomes essential, supported by **SBOM** requirements and **Zero Trust** strategies to ensure supply chain transparency and asset integrity. **Data Localization** and **Data Retention** policies are carefully considered due to global operations and regulatory exposure, especially where **Data Privacy** concerns intersect with sensitive industrial data.

In contrast, Accommodation environments emphasize **Governance** of IT for guest satisfaction, operational uptime, and trust in digital services. Core platforms such as PMS and GDS rely heavily on external providers, creating layered **Supply Chain** dependencies. Guest data is handled by **PII Controllers** and **PII Processors**, making **GDPR** compliance a key concern. **Opt-in** consent mechanisms are deployed to meet **Consent Mechanism** requirements, particularly in marketing and loyalty systems.

Both industries uphold **InfoSec** principles to protect the **CIA triad**, but their focus differs: Smart Manufacturing prioritizes architectural resilience and cybersecurity enforcement, while Accommodation focuses on data governance, privacy, and regulatory alignment in service delivery contexts.

Comparative Analysis: Theme 1 – Business Governance and Management in Smart Manufacturing vs. Agriculture

Smart Manufacturing and Agriculture reveal fundamentally different approaches to governance, shaped by technological integration in one and institutional diversity in the other. In Smart Manufacturing, governance is centralized and strategic, with clearly defined organizational structures linking IT and operational domains. Top Management drives innovation while maintaining operational resilience, establishing a clear Mission and role clarity through refined RACI frameworks. These organizations often adopt comprehensive Management Systems and standardized Policies aligned with international norms.

In contrast, Agriculture, especially in cooperative and subsidy-dependent structures—features participatory and sometimes informal governance models. Business Models range from local cooperatives to subsidy-reliant entities governed by national or EU frameworks like the CAP. Governance structures often blur the lines between management and execution, with oversight shared among internal members and external actors, including NGOs and public agencies. This decentralization complicates the formal application of models like the Three Lines of Defence and weakens the consistency of Audit and Compliance processes.

Smart Manufacturing organizations demonstrate high Maturity, reinforced by robust Integrated Management Systems (e.g., ISO 9001, 14001), which support operational excellence and digital alignment. They apply Internal Control rigorously and leverage KPIs to ensure accountability across cyber-physical systems. Agriculture, on the other hand, displays uneven maturity. While some entities adopt formal systems, others rely on tacit knowledge, with Documented Information serving both compliance and intergenerational continuity purposes, particularly in land tenure and environmental obligations.

Risk in manufacturing is linked to technological disruption, supply chain fragility, and system integrity. In agriculture, risk stems from environmental volatility, policy changes, and market uncertainty. Both sectors reflect the need for adaptable, sector-specific Corporate Governance frameworks that align stakeholder interests with strategic coordination, operational continuity, and long-term resilience.

Comparative Analysis: Theme 2 – IT Management in Smart Manufacturing vs. Agriculture

Smart Manufacturing and Agriculture exhibit distinct IT Management priorities driven by their infrastructure capabilities, operational complexity, and regulatory environments. In Smart Manufacturing, ITSM extends across enterprise and production systems, requiring specialized support from MSPs and MSSPs to ensure performance and security. IAM is essential to enforce access boundaries between digital and physical layers, supporting InfoSec objectives and maintaining the CIA triad.

To manage a growing threat surface, manufacturers implement ISMS frameworks and align Vulnerability Management procedures with production schedules to minimize disruption. Organizations also apply C-SCRM to address digital supply chain risks, requesting SBOMs to improve transparency. Zero Trust principles are increasingly adopted to secure critical infrastructure. Global manufacturers must navigate Data Localization and Data Retention requirements, especially where sensitive operational data intersects with compliance.

In Agriculture, especially within cooperative and subsidy-dependent structures, IT systems tend to be fragmented and underfunded. Many are acquired via Public Procurement, leading to inconsistent architectures and short-term planning. External Consultants often implement and maintain systems, limiting internal capacity and continuity. IAM is typically basic, resulting in poor segregation of access in shared tools like FMIS.

Compliance with Data Privacy and GDPR-related Consent Mechanisms and Opt-out processes remains uneven, particularly when data flows through CAP subsidy platforms and regional land registries. Unlike Smart Manufacturing's strategic, proactive approach, agricultural IT management is often reactive, shaped by policy shifts, funding conditions, and operational constraints. These differences underscore the importance of tailoring IT governance to industry-specific maturity, risk, and sustainability needs.

Industry 1 – Manufacturing – Multi-Site Production Facilities

Theme 1: Organizations, Governance, and Management

The manufacturing sector is defined by its operational scale and complexity, often spanning multiple geographically dispersed production sites. These facilities require tightly coordinated systems to manage production workflows, supply chains, and resource planning. Within this context, the governance of IT becomes critical, particularly when balancing centralized control with the flexibility needed for local site autonomy. The selected niche focuses on how manufacturers align systems, roles, and policies across diverse environments to maintain performance, compliance, and resilience at scale.

Multi-site manufacturers must navigate governance complexity stemming from decentralized operations. The **<104> Business Model** frequently relies on semi-autonomous production sites for regional adaptability, but strategic coherence depends on strong **<112> Governance** mechanisms to maintain efficiency, consistency, and compliance across the network.

Governance in this context is supported by **<118> Management** systems that define **<116> KPI**-based roles and responsibilities, creating clear accountability between headquarters and local operations. **<112> Governance** is formalized through frameworks like **<127> Policies**, **<128> Procedures**, and **<115> Internal Control** practices. These systems ensure standard performance and reporting across all sites, even under differing regulatory or operational conditions.

The strategic challenge lies in balancing centralized oversight with local operational flexibility. Excessive centralization may reduce responsiveness to local needs, while high autonomy risks fragmentation. Excessive centralization may reduce responsiveness to local needs, while high autonomy risks fragmentation. Effective oversight must address **<106> Compliance** issues while supporting site-level flexibility. As **<135> Risk** management grows more complex with scale, policy alignment becomes critical to prevent regulatory breaches and reputation loss.

Ultimately, governance maturity is reflected in cross-site **<120> Management System** integration, feedback loops, and alignment mechanisms that distinguish firms capable of achieving operational consistency and local adaptability.

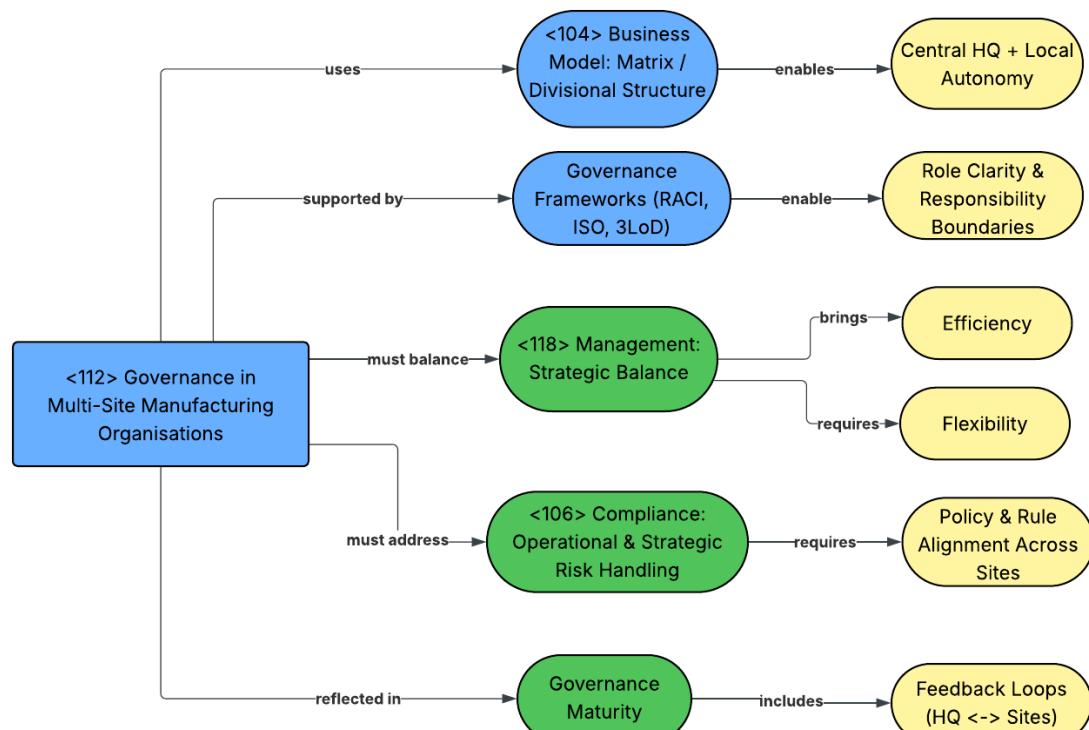


Figure 1: Conceptual Map describing Manufacturing (Multi-Site Production Facilities) from the perspective of Theme 1.

Theme 2 : Governance of IT and IT Management

In multi-site manufacturing environments, IT governance must coordinate enterprise-level systems like ERP, MES, and PLM with site-specific operational needs. Effective <212> **Governance of IT** ensures that digital infrastructure supports both strategic goals and plant-level execution, while maintaining resilience and security across sites.

The division of IT responsibilities is guided by <116> **KPI** frameworks that define access, control, and accountability. Clear <127> **Policies** and <128> **Procedures** regulate IT activities, while <115> **Internal Control** mechanisms support data integrity, access control, and system oversight. The use of shared digital platforms requires that <119> **Management Frameworks** incorporate local configuration guidelines and risk response planning.

A major governance challenge lies in managing <106> **Compliance** risks, such as <208> **Data Privacy**, downtime, and IT/OT integration, without overburdening plant-level teams. The central IT function must support local sites with aligned security protocols and standardized solutions, while enabling adaptability to local workflows, equipment, and legal conditions.

Mature IT governance is reflected in <118> **Management** structures that include cross-site feedback loops, escalation procedures, and contingency planning. This ensures operational continuity, digital security, and consistency in performance across distributed production networks.

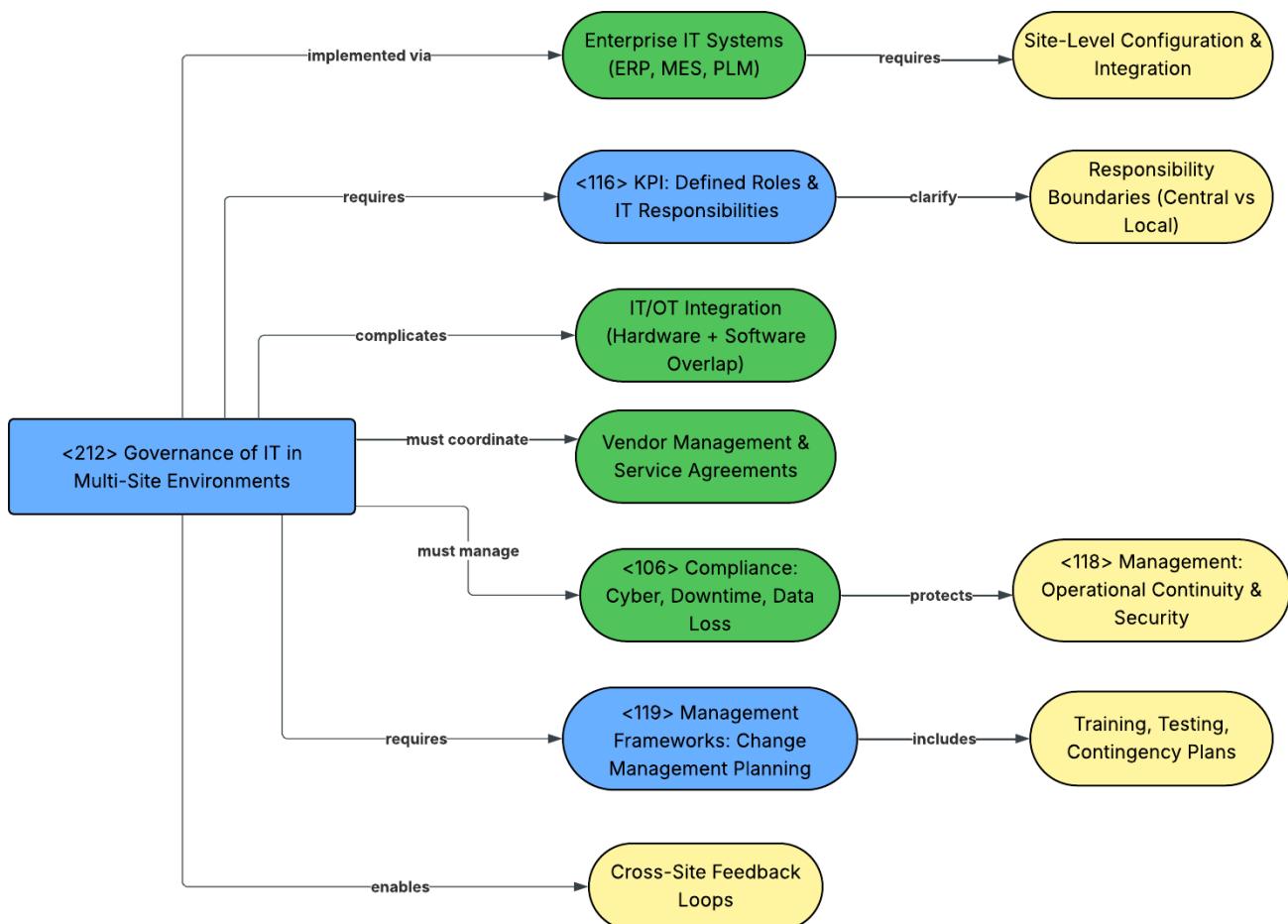


Figure 2: Conceptual Map describing Manufacturing (Multi-Site Production Facilities) from the perspective of Theme 2.

Industry 5 – Hospitality and Leisure – Franchise Models in Hospitality

Theme 1: Organizations, Governance, and Management

The hospitality industry frequently expands through franchising models, enabling rapid brand growth while relying on independently operated units. These franchise structures introduce unique governance challenges, as franchisors must ensure service consistency, digital alignment, and brand protection across legally separate entities. This niche centers on how hospitality organizations enforce operational standards and IT conformity across diverse franchisees to uphold quality, mitigate risk, and preserve brand reputation.

Franchise-based hospitality models, like global hotel chains or branded fast-food outlets, introduce a complex governance dynamic. At the heart of the business model lies a tension: the **<104> Business Model** depends on local franchisees for scalability and market penetration, yet the **<107> Corporate Governance** of the franchisor must maintain brand integrity, service consistency, and reputation. Governance is typically exercised through **<127> Policies**, brand standards, and operational **<128> Procedures**, enforced contractually.

The **<102> BoD (Board of Directors)** of the franchisor, in collaboration with high-level **<108> CxO** roles like the CEO (Chief Executive Officer) or CRO (Chief Revenue Officer), sets the strategic direction, ensuring the franchise system aligns with growth targets while mitigating risks of non-compliance or reputational harm. Mechanisms like **<101> Audits**, franchise scorecards, and **<115> Internal Control** processes serve as oversight tools.

However, **<106> Compliance** in these models is challenging due to the legal autonomy of franchisees. The franchisor must balance **<110> Due Diligence** in partner selection with continuous enforcement of standards, often through **<105> Certification** programs and structured **<118> Management** systems. Governance **<121> Maturity**, reflected in a comprehensive **<120> Management System**, distinguishes high-performing franchise networks from fragmented ones.

The semi-autonomous nature of franchises also tests **<125> Organizational Culture** alignment, where differences in local values, staffing practices, and business maturity may clash with global branding expectations. The governance challenge is thus not only structural but behavioral and relational, requiring careful stewardship across legal, cultural, and operational boundaries.

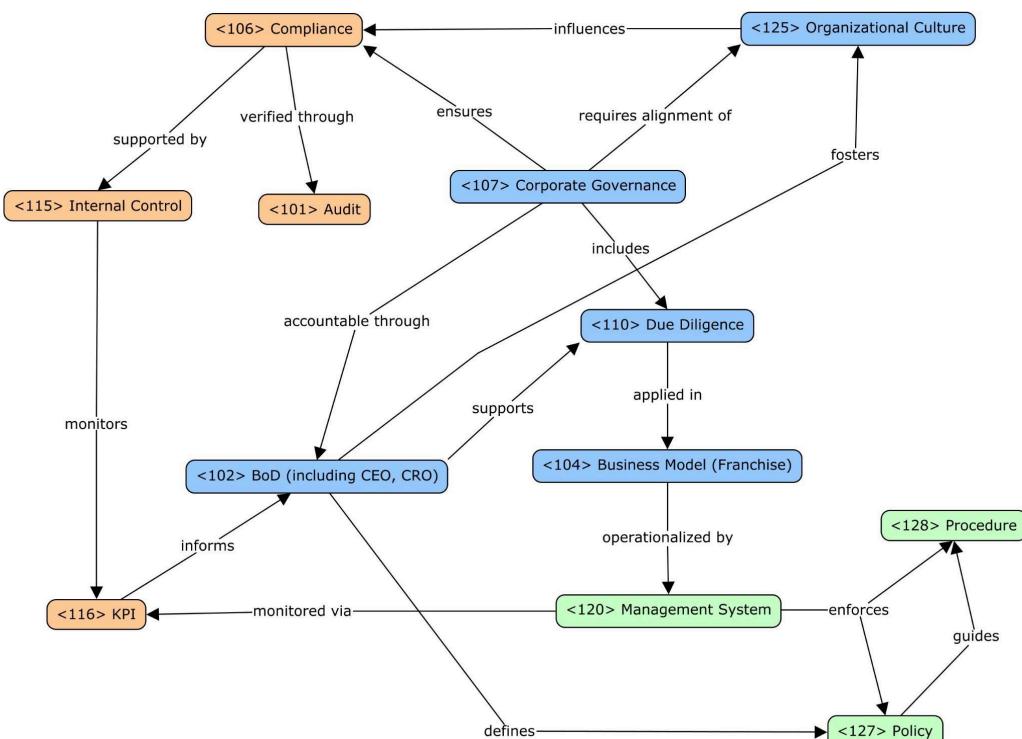


Figure 3: Conceptual Map describing Hospitality and Leisure (Franchise Models in Hospitality) from the perspective of Theme 1.

Theme 2 : Governance of IT and IT Management

In franchise hospitality, **<212> Governance of IT** plays a pivotal role in ensuring digital consistency across geographically dispersed and legally independent units. Franchisors often mandate standard platforms like **PMS** (Property Management Systems), **booking engines**, and **CRM** (Customer Relationship Management) **tools**, all of which fall under a central **<216> ISMS** (Information Security Management System) or broader **<114> IMS** (Integrated Management System). These systems are not just operational, they are strategic tools of governance.

Tensions arise between standardization and local adaptation. Franchisees may want flexibility for local innovation, yet franchisors seek **<217> ITSM** (IT Service Management) consistency to uphold uniform user experience, system security, and data integrity. Misalignment introduces vulnerabilities, particularly concerning **<206> Cybersecurity**, **<211> GDPR** (General Data Protection Regulation), and **<202> CIA Triad** (confidentiality, integrity, and availability) obligations.

The role of **<108> CxO** executives, such as the CIO (Chief Information Officer) or CISO (Chief Information Security Officer), is central to defining and monitoring IT performance and risk posture. These executives coordinate cross-border IT deployment, oversee **<219> MSPs** (Managed Service Providers) or **<220> MSSPs** (Managed Security Service Providers), and ensure the **<121> Maturity** of IT processes across all franchise sites. Technology decisions must align with franchising contracts that stipulate support terms, incident response plans, and upgrade cycles, governed by IT policy frameworks like **<119> Management Frameworks** (COBIT or ISO/IEC 38500).

Additionally, **<115> Internal Control** mechanisms such as remote dashboards, automated compliance **<101> Audits**, and patch management tools are used to verify franchisee alignment. When deviations occur, enforcement may involve **<105> Certification** suspensions or financial penalties, demonstrating how IT governance is not merely technical but contractual and regulatory.

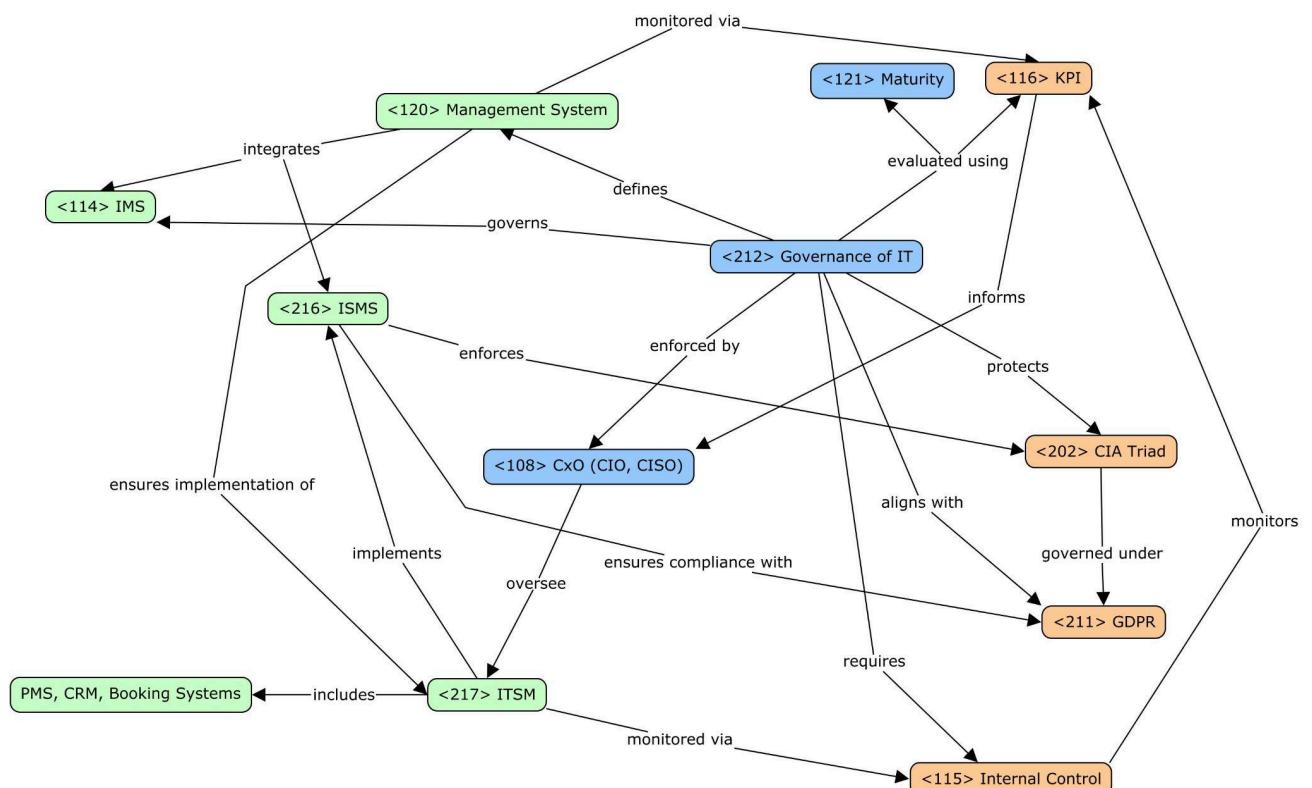


Figure 4: Conceptual Map describing Hospitality and Leisure (Franchise Models in Hospitality) from the perspective of Theme 2.

Industry 8 – Healthcare – Connected Medical Infrastructure in Hospital Systems

Theme 1: Organizations, Governance, and Management

Healthcare organizations increasingly depend on interconnected medical devices and systems that bridge clinical operations with digital infrastructure. These operational technology (OT) assets, often embedded in patient care, require careful oversight to ensure security, reliability, and regulatory compliance. This niche investigates how hospitals coordinate internal stakeholders and manage procurement, cybersecurity, and technical standards to safely integrate and govern life-critical digital infrastructure.

In hospital environments, cybersecurity-related governance must bridge the gap between clinical operations and IT. **<112> Governance** plays a vital role in clarifying risk ownership, guiding **<229> Procurement** standards, and enabling effective cross-functional coordination.

Ownership of **<135> Risk** is frequently fragmented, split between IT departments and clinical engineering teams that manage the **<318> Operational Technology** layer. To address this, hospitals must implement structured governance models that assign operational responsibility explicitly, define escalation **<128> Procedures**, and formalize collaborative decision-making structures.

<229> Procurement processes must also enforce **<228> Secure-by-Design** devices requirements, ensuring that vendors deliver equipment capable of safe integration into the hospital's existing **<206> Cybersecurity** framework.

Finally, **<310> Incident Response** plans must reflect this multidisciplinary reality: when a connected medical device is compromised, both IT and medical staff must respond cohesively. Governance must therefore support operational uptime while safeguarding patient safety through integrated oversight.

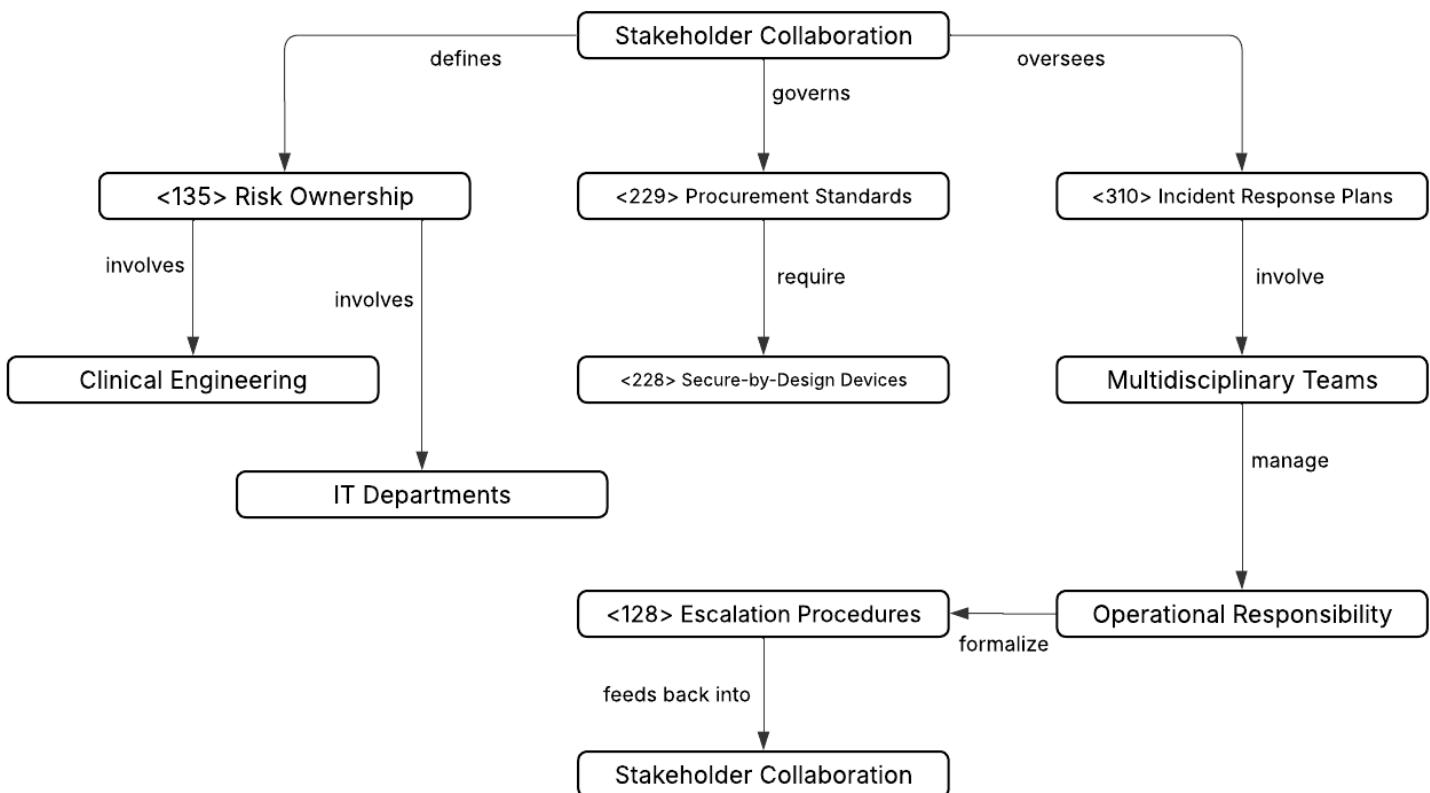


Figure 5: Conceptual Map describing Healthcare (Connected Medical Infrastructure in Hospital Systems) from the perspective of Theme 1.

Theme 2 : Governance of IT and IT Management

The integration of the <318> OT layer with hospital IT infrastructure introduces unique <212> IT Governance challenges. Unlike traditional IT systems, OT devices in healthcare often have long life cycles, lack <319> Patch Management, and were not originally designed to meet modern <206> Cybersecurity requirements.

Effective governance must ensure proper network segmentation between IT and OT environments, limiting the blast radius of potential breaches. <233> Vulnerability Management becomes more complex, requiring hospitals to track outdated firmware, legacy communication protocols, and device-specific risk profiles.

<106> Compliance with regulatory frameworks such as NIS2, IEC 62443, or national cyber laws is essential. These standards formalize <135> Risk assessments, define security controls, and mandate structured reporting in the event of incidents.

Furthermore, <212> IT Governance must address the resource and safety constraints of clinical settings by balancing <135> Risk mitigation with operational uptime. In many cases, this involves developing compensating controls and documenting <135> Risk acceptance strategies when ideal technical solutions are not feasible due to device limitations or vendor constraints.

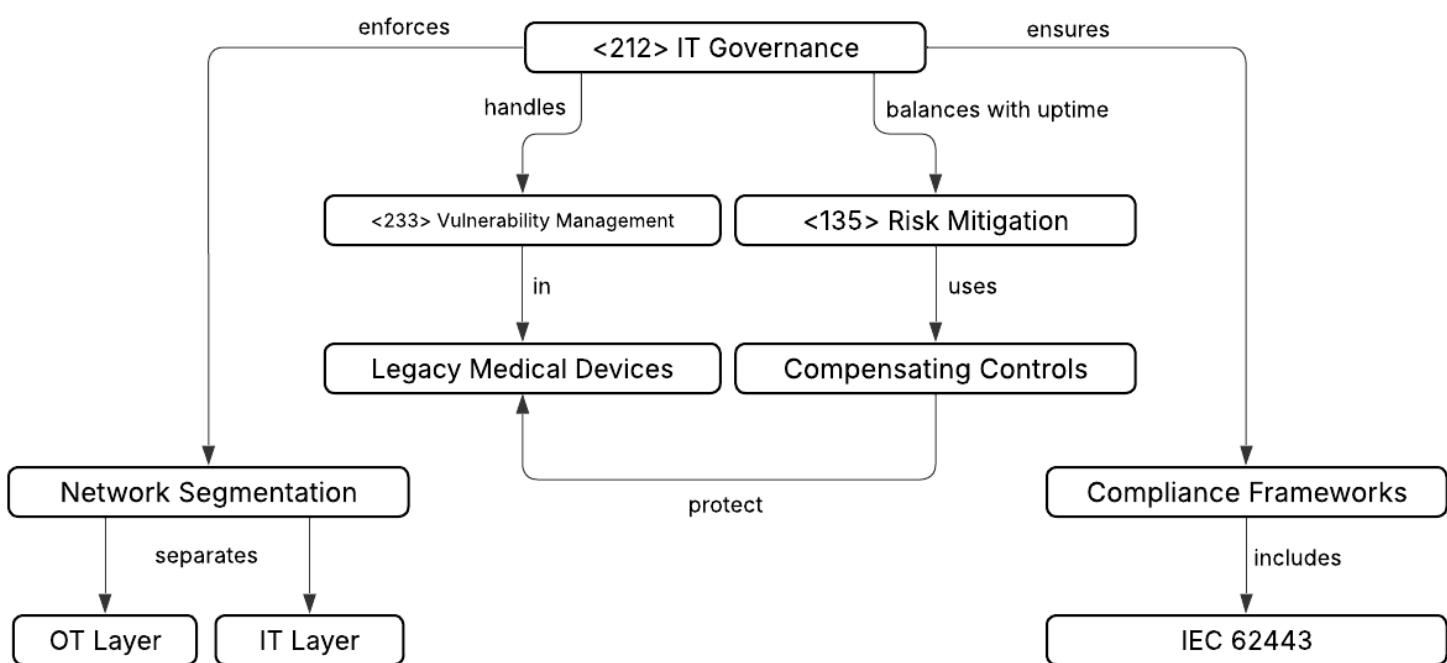


Figure 6: Conceptual Map describing Healthcare (Connected Medical Infrastructure in Hospital Systems) from the perspective of Theme 2.

Industry Comparisons

Manufacturing vs. Hospitality and Leisure

Theme 1 : Organizations, Governance, and Management

In both multi-site production manufacturing and franchise hospitality, the **<104> Business Model** relies on geographically distributed operations, yet the governance implications differ significantly. In manufacturing, facilities are typically under unified ownership or control, allowing more direct application of **<112> Governance** structures and **<118> Management** responsibilities. This enables the parent company to apply organization-wide **<120> Management Systems** and standardized **<127> Policies**, enhancing consistency across production lines.

By contrast, franchise-based hospitality operates through legally independent entities, where the franchisor governs primarily through contractual **<128> Procedures**, **<105> Certification** schemes, and brand enforcement. The **<102> BoD** and **<108> CxO** roles must balance strategic growth with **<110> Due Diligence** in franchisee selection and compliance assurance.

While both industries employ **<115> Internal Control** systems and **<116> KPI**-driven monitoring to manage operational performance, hospitality faces unique challenges in aligning **<125> Organizational Culture** and expectations across semi-autonomous partners. In manufacturing, cultural coherence is more often embedded via direct organizational control and hierarchical **<126> Organizational Structure**. Ultimately, governance **<121> Maturity** in both industries is shaped by their ability to sustain **<106> Compliance**, mitigate **<135> Risk**, and ensure performance across decentralized operations.

Theme 2 : Governance of IT and IT Management

Both industries face the challenge of aligning dispersed IT environments under unified oversight, but they differ in terms of IT ownership, stakeholder roles, and regulatory exposure. In multi-site production manufacturing, IT systems like **MES** and **ERP** are often deployed internally, coordinated under central **<212> Governance of IT**, and managed through structured **<119> Management Frameworks** such as COBIT. These systems are backed by **<114> IMS** or **<216> ISMS** implementations that emphasize resilience, uptime, and process control, particularly in environments integrating Operational Technology.

Franchise hospitality, on the other hand, operates through a model where IT platforms (**PMS**, **CRM**, **booking systems**) are either mandated or supported by the franchisor but operated locally. This introduces complexity in ensuring **<106> Compliance** with frameworks like **<211> GDPR** and maintaining control over **<215> InfoSec** requirements, particularly the **<202> CIA Triad**. Here, **<108> CxO** roles (notably CIOs and CISOs) are critical for managing third-party service providers like **<219> MSPs** or **<220> MSSPs**, and ensuring **<121> Maturity** of **<217> ITSM** practices across all franchise locations.

Both industries utilize **<115> Internal Control** mechanisms to track system compliance and risk exposure. However, hospitality must rely more heavily on **<101> Audits** and legal enforcement to ensure IT alignment, while manufacturing can execute oversight through internal processes. The core contrast lies in the degree of control and integration: manufacturing IT governance is built on ownership and standardization; hospitality IT governance is shaped by influence, contracts, and adaptation to diverse operator environments.

Healthcare vs. Hospitality and Leisure

Theme 1 : Organizations, Governance, and Management

Healthcare and hospitality both operate in complex, multi-actor environments, but differ significantly in how **<112> Governance** is structured and executed. In hospitality, **<107> Corporate Governance** is centralized within the franchisor, who sets operational **<127> Policies** and **<128> Procedures** to manage a network of legally independent franchisees. These governance mechanisms are contractually enforced, with the **<102> BoD** and **<108> CxO** roles responsible for strategic oversight. Tools like **<101> Audits** and **<115> Internal Control** are used to maintain **<106> Compliance** and performance across units.

In contrast, healthcare governance around connected medical infrastructure is more internally fragmented. Hospitals must bridge **<112> Governance** across departments like IT, clinical engineering, and medical staff, with no external contracts to impose control. The lack of clear **<135> Risk** ownership complicates decision-making, requiring the development of internal governance models that assign responsibilities, define escalation **<128> Procedures**, and ensure coordination. Unlike hospitality, which uses **<105> Certification** schemes to ensure franchisee compliance, hospitals rely on procurement governance and **<229> Procurement** standards to enforce **<228> Secure-by-Design** requirements for medical devices.

Whereas hospitality governance is shaped by legal autonomy and brand protection, healthcare governance is deeply tied to clinical safety, ethical standards, and cross-functional coordination. Both industries must manage **<125> Organizational Culture**, but the healthcare sector faces internal alignment challenges, while hospitality navigates cultural differences across independent entities.

Theme 2 : Governance of IT and IT Management

In both healthcare and hospitality, **<212> Governance of IT** is essential to control risk and ensure system reliability across distributed environments. In hospitality, franchisors enforce standard IT platforms like **PMS** and **CRM** across legally independent units using centralized **<216> ISMS** and broader **<114> IMS** frameworks. These systems are monitored through **<115> Internal Control** tools, automated **<101> Audits**, and maintained under **<119> Management Frameworks** such as COBIT or ISO/IEC 38500. The primary concerns are **<211> GDPR** **<106> Compliance**, data security, and maintaining consistent user experience across all franchisees.

Healthcare, however, presents a distinct challenge with the integration of **<318> OT** layer systems, such as networked medical devices, which often lack modern **<319> Patch Management** and complicate **<233> Vulnerability Management**. These assets are not just data-driven, they are life-critical. IT governance in this context must safeguard the **<202> CIA Triad** (Confidentiality, Integrity, Availability) while also managing clinical **<103> Business Continuity**, which has become a growing concern due to the rise in disruptive cyberattacks targeting hospital systems. Compliance with sector-specific frameworks like IEC 62443 and NIS2 is essential, but hospitals frequently face **<135> Risk** acceptance decisions when ideal security controls are unfeasible.

While hospitality IT governance relies on uniformity and centralized enforcement, healthcare governance is constrained by clinical realities, requiring coordination between IT staff, medical professionals, and **<224> PII Controllers**. In healthcare, **<206> Cybersecurity** failures can result in patient harm, not just service disruption, making IT governance not only technical but ethical and safety-critical.

Security and Management of Information Systems

Project 1: Group 167

Leonard Zerwes, Fanny Sjöström, Isa Widmaier, Onni Kivistö

May 23, 2025

Contents

1	Manufacturing	3
1.1	Theme 1: Governance, Management	3
1.2	Theme 2: IT Management	4
2	Banking and Financial Services	5
2.1	Theme 1: Governance, Management	5
2.2	Theme 2: IT Management	6
3	Agriculture and Farming	8
3.1	Theme 1: Governance, Management	8
3.2	Theme 2: IT Management	9
4	Comparisons	10
4.1	Banking and Financial Services / Agriculture and Farming Theme 1	10
4.2	Banking and Financial Services / Manufacturing Theme 1	10
4.3	Banking and Financial Services / Agriculture and Farming Theme 2	11
4.4	Banking and Financial Services / Manufacturing Theme 2	11

1 Manufacturing

Manufacturing as an industry refers to the process of transforming materials into goods using labour, machinery, tools and chemical or biological processing. The industry provides value through physical products that support infrastructure, mobility, health, energy and daily life, making it a foundational domain of economic activity. Manufacturing operations range from small-scale workshops to highly automated global production networks.

For our niche, we chose Smart Manufacturing, also referred to as Industry 4.0, which is the most modern shift in the industry towards efficient and reliable operations. It includes the integration of cyber-physical systems, industrial IoT, robotics, 3D printing, digital twins, and data-driven operations.

1.1 Theme 1: Governance, Management

Manufacturing as a sector is characterised by its integration of both physical and digital systems, precision requirements, and dependency of coordination across < 231 > supply chains. These attributes make the field highly dependent on other industries and operations within the same industry, requiring ongoing optimisation of throughput, cost, and time. Because of this in addition to the foundational value the field provides to society, the < 112 > governance in manufacturing must be held at a high standard. The industry often involves capital-intensive infrastructure and complicated machinery, increasing the need for < 106 > complying with safety and quality standards.

< 113 > GRC in manufacturing aims to fulfil the need to ensure operational continuity, product quality, safety, and regulatory compliance. As digital transformation accelerates, GRC functions must evolve to address the new < 135 > risks posed by cyber-physical integration. This includes safeguarding against < 206 > cybersecurity threats, protecting intellectual property in collaborative ecosystems, and maintaining compliance with changing global regulations regarding data protection, emissions, labor practices etc. Smart manufacturing operations that are powered by real-time data analytics and autonomous decision-making systems rely on transparent governance structures and < 109 > documented information to ensure accountability and traceability in the possible case of data breaches or operational failures.

Another key aspect of smart manufacturing is the transformation of the workforce. As automation and AI redefine roles within the industry, there is an increasing need for skilled workers who can operate, maintain, and innovate with advanced technologies. Governance should therefore take this talent gap into account through upskilling and reskilling programs to ensure an inclusive digital transition. As the role of the workforce changes, so do regulations regarding labor and ethical replacement of workers with automation and AI. GRC functions must constantly stay compliant of these rapidly evolving regulations.

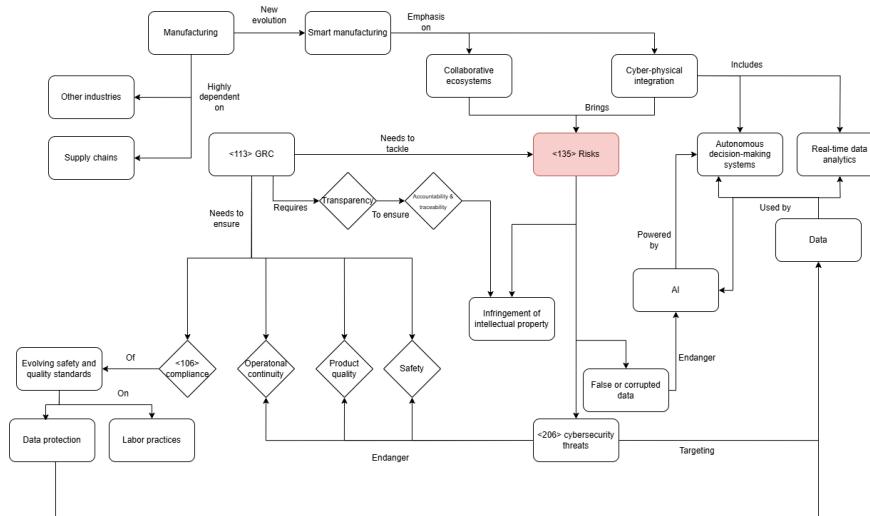


Figure 1: Concept Map for Manufacturing Theme 1

1.2 Theme 2: IT Management

Throughout the transitions of manufacturing, the technology has transitioned with it. In recent years, the use of technological innovations such as cyber-physical systems, industrial IoT, robotics, 3D printing, digital twins, and data-driven operations has become a standard. Therefore, the need for < 212 > Governance of IT and < 119 > Management Frameworks is essential for these new innovations and technologies. Industry 4.0, also referred to as Smart Manufacturing, is the manufacturing of today and demands a mature and strategic approach as the integration of IT and < 318 > Operational Technology (OT) introduces further complex environments that require proper management. It includes sensors, data analytics, < 401 > AI, and a cloud platform to optimize production. This technology is a function and a driver of value and resilience.

Increasing digitalisation of the manufacturing process causes the growth of exposure to cyber risks. A major challenge lies in the ability to exchange information while keeping < 206 > Cybersecurity high, especially given the increased attack surface introduced by these connected devices in the industry (< 233 > Vulnerability Management, < 214 > IAM). It calls for proper frameworks and standards to operate correctly, both functionally and ethically. IT managers are expected to implement frameworks and standards that protect sensitive data and ensure that systems are reliable to both technical failures and possible cyber threats. < 134 > Regulatory Frameworks are also increasingly expecting organisations to show proactive risk assessment and ethical foresight. For example, the use of AI in predictive maintenance and decision-making must comply with < 422 > Explainability standards, ensuring that algorithms do not include biases that compromise safety or quality.

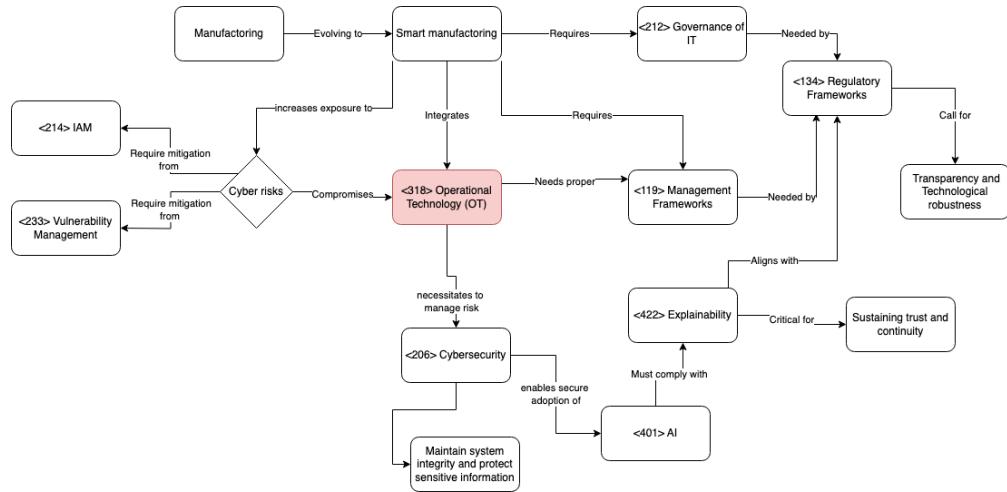


Figure 2: Concept Map for Manufacturing Theme 2

2 Banking and Financial Services

Banking and financial services are essential to the global economy, supporting credit, payments, investments, and risk management. This sector includes a wide range of institutions such as retail and commercial banks, central banks, investment firms, insurance companies, pension funds, and fintech platforms. Due to their systemic importance and potential for widespread impact, financial services are one of the most heavily regulated sectors, with strict oversight to ensure stability, security, and trust.

For our project, we chose to focus on the niche of digital payments and real-time payment rails, which are central to the evolving systems of fintech. They enable instantaneous money transfers and are transforming how transaction between consumers and businesses are made, raising new challenges in governance, compliance, and cybersecurity.

2.1 Theme 1: Governance, Management

For our niche we selected digital payments and real-time payment rails (FedNow, UPI, etc.) move money between accounts in seconds, 24/7, via ISO 20022 APIs. Their irrevocable, systemic nature demands top-tier governance, risk, and cyber-resilience.

In the real-time rails and digital-payments niche, the overarching theme of < 112 > Governance, < 118 > Management, and < 126 > Organisational structure is more than textbook theory. < 112 > Governance gives a rail its licence to operate. A board must translate public-policy aims—safe, efficient, inclusive payments—into a rule-book that every participant bank follows. Clear roles and a < 133 > regulatory body (for example, < 131 > RACI for fraud-resolution and incident escalation) prevent finger-pointing when milliseconds matter. Because funds settle irrevocably in seconds, the rail is usually designated a systemically important financial-market infrastructure; regulators therefore expect a mature Three Lines of Defence: operations teams running the switch (first line), a risk and compliance function monitoring liquidity caps and real-time AML controls (second), and an independent internal audit that tests governance effectiveness (third). A formal < 120 > management system—often built around ISO 27001/27701 for information security and ISO 20022 change-management procedures—turns board intent into day-to-day discipline. In practice this means documented processes for code promotion, key management, and service-level monitoring, all feeding continuous-improvement loops. High < 121 > maturity in such a system allows the rail to scale volumes, onboard new participants, or introduce “request-to-pay” overlays without compromising integrity; low maturity shows up as ad-hoc deployments or delayed fraud-rule updates that erode trust. Real-time rails also embody integrated governance, risk, and compliance (< 113 > GRC). < 135 > Risk management must model liquidity, operational, and cyber risk in near-real time, while §106; compliance aligns with anti-money-laundering rules, data-privacy statutes, and scheme mandates for price transparency. Effective control structures provide assurance to shareholders and wider stakeholders (merchants, consumers, fintechs, central banks) that the rail meets its public-interest mandate. Finally, < 124 > organisational culture acts as the glue. A learning-oriented, blameless post-mortem culture encourages rapid incident disclosure—critical in an environment where downtime can halt national commerce. By pairing robust formal governance with a high-maturity management system and adaptive culture, real-time payment networks can deliver on their promise of instant, ubiquitous, and safe value transfer.

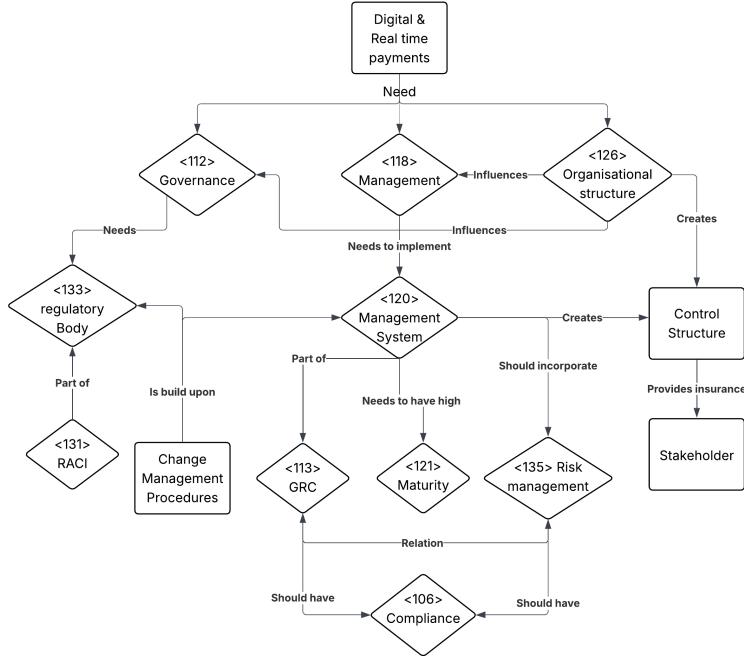


Figure 3: Concept Map for Banking and Financial Services Theme 1

2.2 Theme 2: IT Management

Digital payments and real-time payment rails are a key part of modern banking and financial services. They make it possible to pay online, through websites, apps or with contactless cards, as well as allow transferring funds with high speed across financial institutions. IT management plays a key role in ensuring that these payment platforms operate securely, reliably, and in line with strict regulatory requirements.

Real-time digital payments happen all the time around the clock and require near-zero latency. Systems need to be fast, reliable, and always available, in line with the <202> CIA triad (Confidentiality, Integrity, Availability). This is ensured e.g. by using backups and strong servers. IT management ensures this by maintaining robust infrastructure, including backups, load balancing, and failover systems to prevent interruptions and data loss.

Real-time payments cannot be reversed easily once settled, so the stakes are higher for fraud prevention and data protection. Digital payment systems handle currency and confidential information, and handling <223> Personally Identifiable Information requires strict compliance with privacy regulations such as the <211> GDPR. A successful cyberattack or data breach could lead to direct financial loss of customers, so IT management must also implement strong <206> cybersecurity measures - including firewalls, encryption, and continuous monitoring - and apply <234> Zero Trust frameworks. These are crucial methods to protect the system from fraud and breaches.

IT is also responsible for how payment and user data is stored and accessed. This includes making sure rules about data residency <208>, data retention <209>, and data privacy <210> are followed, especially when data is transferred or stored in cloud environments. Systems should be built with privacy-by-design <228> principles, where privacy and security controls are included from the very beginning of the system's development, not just added later.

Finally, digital payments depend on multiple separate parties like banks, payment gateways, card networks, and wallet apps. This adds technical risk to the <231> supply chain, so IT must make <205> Cyber Supply Chain Risk Management an IT priority. It is important to ensure that a third-party system integrates properly and safely with internal systems. IT Management needs to ensure sufficient testing for vulnerabilities, setting secure communication standards, and regularly reviewing the performance and security of external systems.

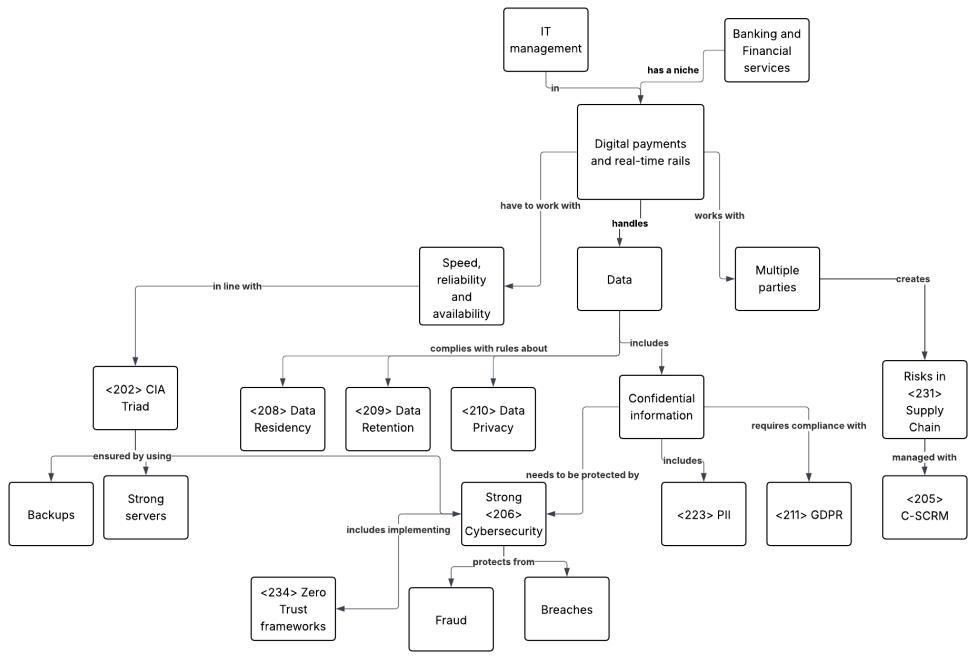


Figure 4: Concept Map for Banking and Financial Services Theme 2

3 Agriculture and Farming

Agriculture and farming are one of the oldest organised sectors of human activity, and include food production, the environment, and global trade. Climate variability, regulation, consumer expectations, and digital transformation influence this. It has evolved quickly from where it started. Through the adaptation of digital tools, such as farm management platforms that help plan, monitor and optimise farming operations, the sector is now more efficient and increasingly dependent on information systems to support strategic decision-making and sustainability.

3.1 Theme 1: Governance, Management

< 113 > (GRC) Governance, Risk and Compliance, in agriculture, are shaped by land ownership, seasonal cycles, subsidy regimes, and regulations related to food safety and the environment. It involves setting direction, making decisions and ensuring accountability. As farms increasingly adopt digital tools like farm management platforms, new forms of oversight and coordination become necessary. Traditionally, agricultural operations have remained small to medium-sized and often rely on informal or outdated systems. Today, however, many farms depend on digital platforms to support decisions, ensure regulatory compliance (< 134 > Regulatory Framework), and interact with global markets. This digital shift exposes the absence of formal governance structures and emphasises the need for clearer < 126 > Organisational Structure and better < 437 > Strategic Alignment between operational goals and technology use. In many cases like this, there are no dedicated IT or < 108 > CxO roles to oversee these systems. It blurs the line between < 112 > Governance, < 118 > Management and operations. Responsibilities for digital decisions may remain undefined, which would further increase the < 317 > Operational Risk of poor coordination and compliance failures.

In cooperatives or public programs that support farmers, governance also needs to cover standardising services, managing data reporting and < 206 > Cybersecurity. But since not all farms are at the same digital level, it's hard to manage these areas consistently. To improve this, agricultural organisations should adopt a more structured model that clearly defines who's responsible for what (< 131 > RACI), helps coordinate between different stakeholders and makes sure digital tools actually support sustainability goals and compliance requirements.

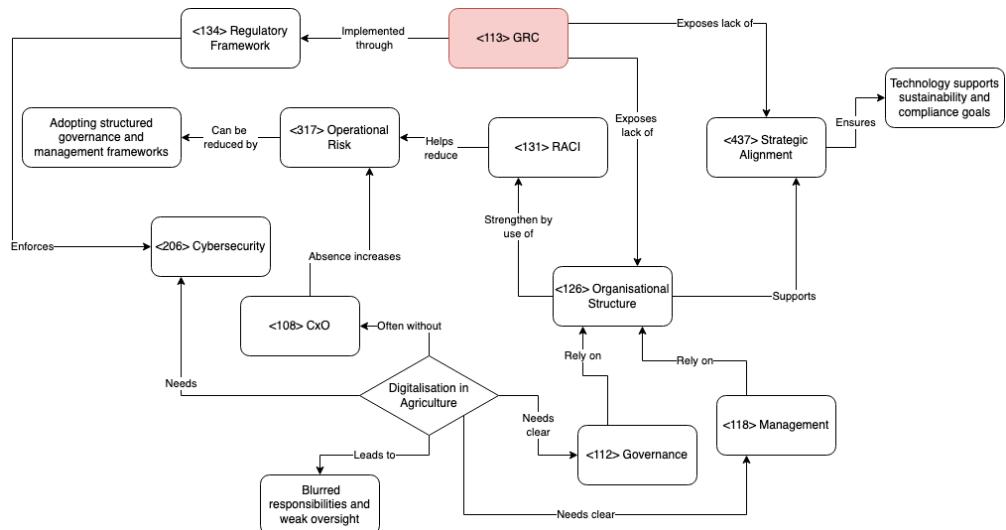


Figure 5: Concept Map for Agriculture and Farming

3.2 Theme 2: IT Management

As farm management platforms become more and more prevalent in modern agricultural operations, effective IT management becomes a critical part of enabling performance, reliability, and innovation. One challenge in IT management in farm management platforms is ensuring the integrity and security of data. Agricultural data is often collected from distributed sources in remote areas with a variable quality of connectivity, making data-based decision-making difficult if information is not exchanged efficiently, is inconsistent or in a risk of loss. When farm platforms begin to integrate with national and international < 231 > supply chains, managing the security of sensitive business data becomes increasingly important. Proper access controls, encryption and regular security < 101 > audits can help protect information against breaches or misuse.

Training and user support are also important components of IT management in this context. Farms often have low < 412 > digital maturity as farmers and agricultural workers may have varying levels of digital literacy, and the success of any platform depends on how effectively it is used in daily operations. This means that ongoing training, intuitive and accessible user interfaces, and localized support are essential. IT managers and support teams must also ensure that systems are maintained with minimal downtime in short and specific < 315 > maintenance windows, especially during critical periods like planting or harvest seasons.

Interoperability is another concern. Many farms may use a mix of proprietary hardware and software from different vendors. Without standardized data formats or APIs, integrating these tools into a cohesive platform becomes technically complex and financially difficult. IT management practices must therefore include vendor evaluation, lifecycle management, and clear strategies for system upgrades and integrations to prevent separated operations.

As many farming operations do not currently have dedicated IT departments, there is often a need to outsource IT services or form partnerships with technology providers. These collaborations can help fulfill capability gaps, but also require well-defined < 323 > service level agreements (SLAs), good < 312 > IT service continuity management (ITSCM), and data ownership policies to manage IT-related risks effectively.

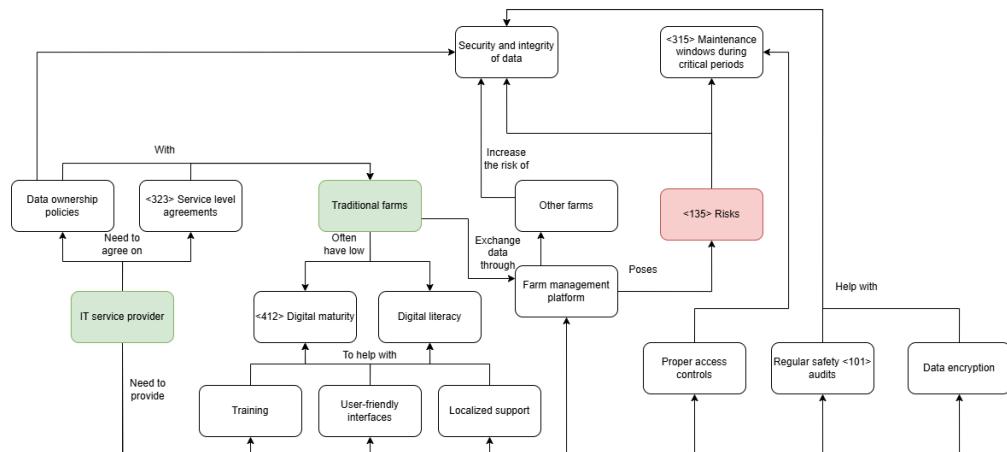


Figure 6: Concept Map for Agriculture and Farming Theme 2

4 Comparisons

4.1 Banking and Financial Services / Agriculture and Farming Theme 1

Real-time payment (RTP) rails sit at the core of systemically important financial market infrastructure. Governance is largely externalised: a central-bank licence, ISO 20022 messaging, and DORA-level operational-resilience rules give regulators direct sway over strategy. A scheme board translates policy aims (speed, safety, inclusion) into binding rulebooks, while “three lines of defence” (operations, risk/compliance, internal audit) track liquidity, sub-second sanctions screening, and minute-level recovery objectives. Management is KPI-driven and ritualised: 24 × 7 availability, < 500 ms message latency, automated end-of-day treasury sweeps, and instant incident disclosure to supervisors.

Farm-management information systems (FMIS) operate in a near-opposite context. Agriculture is fragmented; many producers are family-owned or cooperative, and regulation is dispersed across subsidies, food safety, and land-use law. Governance here is created rather than codified: the platform itself standardises data capture, embeds traceability, and pokes compliance through mobile workflows. Management remains hands-on (fine-tuning variable-rate fertiliser, syncing drone imagery, or auto-filling CAP forms). Assurance is emergent, built on open-source data models and co-op charters clarifying data ownership and API permissions, rather than statutory mandates.

Data sovereignty underscores the contrast. RTP rails minimise payload richness to reduce fraud and privacy risk; audits are continuous and penalties immediate. FMIS seeks maximal data (yield maps, soil telemetry, satellite imagery) to unlock carbon-credit revenue and parametric insurance, yet faces higher cyber-risk from patchy rural connectivity. To conclude, RTP governance is propelled by regulatory compulsion, FMIS by collective benefit; still, both niches validate the overarching theme: digital transformation succeeds only when accountability pathways and iterative management systems are explicit, whether moving money in milliseconds or growing crops by the hectare.

4.2 Banking and Financial Services / Manufacturing Theme 1

In the first comparison we saw how real-time payment (RTP) rails were steered largely from the outside-in (their governance imposed by central banks and scheme rulebooks) while farm-management platforms matured from the inside-out, using cooperative charters to fill regulatory gaps.

Smart-manufacturing platforms share RTP’s appetite for milliseconds-level precision but resemble the farms in how governance authority is distributed. A factory’s board, rather than a public supervisor, decides whether to adopt different norms or digital-twin safety protocols, and the payoff is measured in throughput and Overall Equipment Effectiveness rather than compliance fines. The exact tasks between those two niches vary a lot. Where a payment-scheme CISO worries about sub-second sanction screening and end-of-day liquidity sweeps, a plant’s Chief Digital Manufacturing Officer is balancing cyber-segmentation against the need to stream gigabytes of sensor data to an AI model that prevents a €10-million line stoppage.

Management rhythms diverge too. RTP operations run on a fixed playbook of SLAs, incident ladders and “three-lines-of-defence” audits; improvement is incremental because a single mis-routed payment can ripple through the financial system. Smart factories iterate like software teams: weekly DevOps sprints push new cobot routines or anomaly-detection models, tolerating occasional rollbacks as long as worker safety fences stay green. Payment rails pare each transaction message down to the bare essentials to reduce data exposure, whereas smart-factory platforms flood their digital twins with every sensor ping (vibration, temperature, voltage) to maximise insight. Yet both niches confirm the same cross-industry finding: digital trust rests on unmistakable lines of accountability and a management loop that can learn in real time, whether the task is shuttling euros between banks or synchronising robots during different manufacturing tasks.

4.3 Banking and Financial Services / Agriculture and Farming Theme 2

From an IT management perspective, digital payments in banking and financial services and farm management platforms in agriculture represent two very different environments, each with unique demands and constraints.

In digital payments and real-time payment rails, IT management must prioritize speed, availability, and security. Transactions occur 24/7 with near-zero latency requirements, making infrastructure reliability and cybersecurity paramount. IT teams are responsible for maintaining systems with strong encryption, continuous monitoring, and privacy compliance (e.g., GDPR). With financial data being very sensitive and transactions irreversible once processed, cybersecurity frameworks like Zero Trust, secure backups, and robust disaster recovery plans are essential. Integration with multiple external parties like banks, card networks and payment gateways requires supply chain risk management to ensure secure, reliable connections.

In contrast, IT management in farm management platforms focuses on data integrity, usability, and adaptability to low-connectivity environments. While security is still important - especially as farms integrate into broader supply chains - data collection is more geographically distributed and often subject to connectivity and hardware inconsistencies. IT managers must implement reliable data synchronization, encryption, and access controls across potentially offline or semi-connected systems. An additional challenge is the low digital maturity of many users in the agriculture sector. Effective IT management must include user training, intuitive interface design, and localized support to ensure systems are adopted and used effectively.

Another key difference lies in system interoperability and infrastructure support. Whereas digital payment systems operate within well-regulated, standardized environments, farm platforms often rely on a fragmented mix of proprietary hardware and software. This requires IT managers to emphasize vendor management, lifecycle planning, and system integration strategies. Additionally, many agricultural operations lack in-house IT departments, necessitating outsourced services managed through well-structured SLAs and continuity planning.

In summary, while digital payments focus on high security, real-time processing, and regulatory compliance, farm management IT emphasizes resilient, user-friendly systems adapted to variable conditions and interoperability. Both require strong IT leadership, but they differ significantly in technical focus, risk profiles, and user engagement strategies.

4.4 Banking and Financial Services / Manufacturing Theme 2

From an IT management perspective, both smart manufacturing and digital payments in banking and financial services rely heavily on advanced technologies, but they face distinct challenges and priorities due to the nature of their operations. Smart manufacturing, or Industry 4.0, integrates IT with Operational Technology (OT) through cyber-physical systems, IoT, AI, and data analytics to optimize production. IT management here must oversee complex environments where real-time data collection, machine learning, and automation drive efficiency and resilience. The focus is on ensuring robust IT governance and management frameworks, seamless integration of digital tools with physical systems, and maintaining cybersecurity amid growing interconnectivity and vulnerability.

In contrast, digital payments and real-time payment rails demand ultra-low latency, high availability, and uncompromising security. IT management in this sector centers on maintaining the integrity, confidentiality, and availability (CIA triad) of real-time financial transactions. Here, systems must be resilient against downtime and capable of handling sensitive user data in compliance with strict privacy laws like GDPR. Moreover, the irreversible nature of real-time payments heightens the importance of fraud prevention, zero trust security frameworks, and cyber supply chain risk management to ensure secure integration of third-party services.

While both domains require strong cybersecurity and risk management, manufacturing emphasizes the safe and ethical deployment of AI and OT integration, whereas digital payments prioritize secure, uninterrupted transaction flows and data protection. Each sector demands a tailored IT strategy aligned with its operational and regulatory environments.

Project 1

SECURITY AND MANAGEMENT OF INFORMATION SYSTEMS

Authors:

Mariana Bernardo (102665)
Filipa Araújo (102878)
Mateus Nóbrega (102838)
João Viana (103571)

Contents

1 Healthcare	2
1.1 Organizations, Governance, and Management	2
1.2 Governance of IT and IT Management	3
2 Banking and Financial Analysis	4
2.1 Organizations, Governance, and Management	4
2.2 Governance of IT and IT Management	5
3 Manufacturing	6
3.1 Organizations, Governance, and Management	6
3.2 Governance of IT and IT Management	7
4 Comparison	8
4.1 Organizations, Governance, and Management	8
4.2 Governance of IT and IT Management	9

1 Healthcare

1.1 Organizations, Governance, and Management

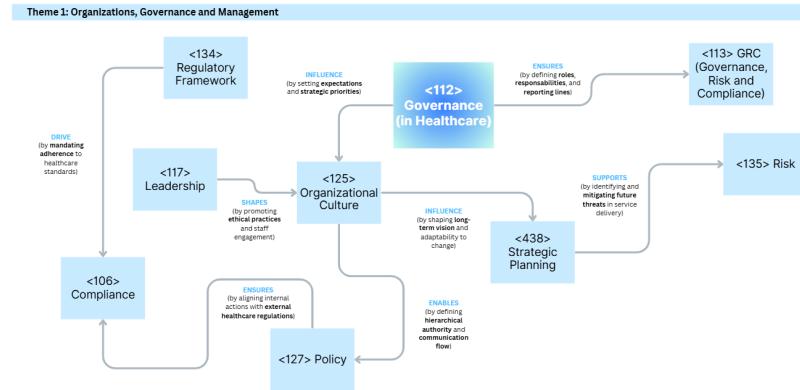


Figure 1: Concept map for Healthcare industry in Organizations, Governance, and Management

Healthcare **<112> Governance** ensures that **<127> Policy** and **<128> Procedure** address real-world challenges while maintaining a consistent, human-centered approach across the entire organization. It recognizes and integrates the distinct roles, responsibilities, and perspectives of both clinical and operational staff. The ultimate goal is to ensure that systems, tools, and protocols support, rather than hinder, the work of patients, clinicians, and staff [1].

Healthcare governance typically includes key **<117> Leadership** roles such as the Chief Executive Officer (CEO), Chief Medical Officer (CMO), Chief Nursing Officer (CNO), and the chairs of various committees, including peer review, medical executive, and credentialing committees [1].

In terms of **<126> Organizational Structure**, there are various ways to approach this and we can see some of them in the follow Table 1.

Structured Type	Key Characteristics	Advantages	Challenges	Best Fit For
Hierarchical	Top down decision	Clear chain of command	Slow response and low flexibility	Large or complex systems
Flat	Decentralized decisions	Quicker decisions and better collaboration	Unclear roles	Smaller hospitals
Functional	Departments organized by specialty	Higher specialization and operational efficiency	Poor interdepartmental coordination	Hospitals with specialized services
Divisional	Semi-independent units (e.g. pediatrics and oncology)	Patient-centered care and service flexibility	Higher costs	Large hospitals with diverse services
Matrix	Staff report to multiple managers across departments	Innovation and collaboration	Confusing authority	Healthcare organizations with complex projects (e.g. research hospitals)

Table 1: Types of Hospital Organizational Structures [3]

Healthcare organizations adopt various **<117> Leadership** styles to guide teams, drive innovation, and improve outcomes. **Transformational leadership** focuses on inspiring and motivating staff through a shared vision, encouraging growth and engagement. **Servant leadership** emphasizes empathy and support, prioritizing the well-being of team members to foster trust and collaboration. **Agile leadership** brings flexibility and quick decision-making, ideal for adapting to change in fast-paced environments. **Democratic leadership** values participation and teamwork, promoting inclusive decision-making across multidisciplinary groups. **Strategic leadership** takes a long-term, goal oriented approach, aligning team efforts with the organization's broader mission and preparing for future challenges. Each style contributes differently to organizational effectiveness depending on the context and goals [4].

1.2 Governance of IT and IT Management

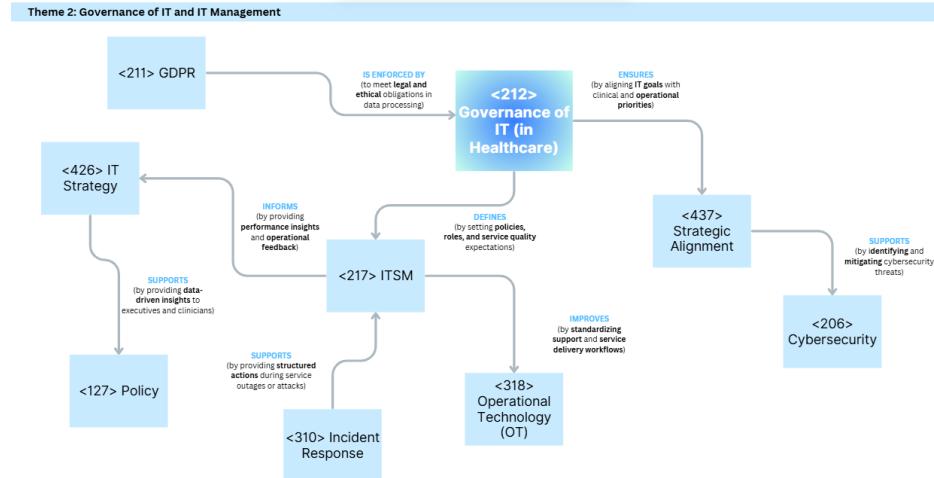


Figure 2: Concept map for Healthcare industry in Governance of IT and IT Management

The healthcare industry increasingly relies on technology to enhance efficiency and simplify operations. However, due to its sensitive nature, **<212> Governance of IT** in healthcare must be highly structured and compliant with strict regulations. This includes having a **<134> Regulatory Framework** ensuring adherence to laws that protect patient data, implementing robust risk management plans for quick response with **<2026> Cybersecurity**, and promoting transparent decision-making processes to align IT initiatives with organizational and clinical goals [5].

Technology offers numerous benefits to the healthcare industry, significantly improving patient outcomes, operational efficiency, and access to services. Some of the most impactful advantages include [6] [7]:

- **Enhanced Patient Care and Monitoring:** Wearable technologies allow physicians to monitor patients remotely, while telemedicine enables patients to receive professional medical care regardless of location, increasing convenience and continuity of care.
- **Increased Accessibility to Healthcare Services:** Technology helps providers reach underserved or remote populations, expanding the availability of healthcare and minimizing geographic barriers.
- **Improved Efficiency and Workflow in Healthcare Facilities:** With the adoption of Electronic Health Records (EHRs), healthcare professionals can quickly and securely access patient information without relying on outdated methods such as phone calls or postal mail. Additionally, automated billing systems streamline payment processes, reducing administrative delays.
- **Innovations in Treatment and Diagnosis:** Advances such as 3D printing, nanotechnology, regenerative therapies, implantable artificial organs, robotic-assisted surgeries, and AI-driven diagnostics are revolutionizing how conditions are treated and identified.
- **Data Driven Decision Making:** Real-time health analytics empower healthcare organizations to make informed decisions based on accurate and timely data, leading to improved patient care and resource management.

- **Reduce Healthcare Costs:** Virtual consultations minimize the need for travel, cutting expenses for both patients and providers. Furthermore, automation reduces administrative burdens such as claims processing, data entry, physician credentialing, and appointment scheduling.

In the healthcare industry, managing IT systems involves a critical responsibility: protecting the sensitive information patients entrust to hospitals and clinics. To ensure **<208> Data Privacy**, frameworks like the **<211> General Data Protection Regulation (GDPR)** establish rigorous standards designed to safeguard patient rights. **<211> GDPR** provides a comprehensive legal framework governing how personal health information is collected, stored, processed, and shared.

Healthcare organizations are obligated to protect various categories of patient data, including [8]:

- **Electronic Health Records (EHR):** Comprehensive medical records containing a patient's history, diagnoses, medications, treatment plans, immunizations, allergies, radiology images, and lab results.
- **Personal Identifiable Information (PII):** Data that can identify or be linked to an individual, such as names, addresses, phone numbers, and national identification or social security numbers.
- **Biometric Data:** Unique physical characteristics used for identification, including fingerprints, facial recognition data, and genetic information.
- **Insurance Information:** Details regarding a patient's health insurance policy, including policy numbers, coverage specifications, and submitted insurance claims.
- **Payment and Billing Information:** Financial records related to patient billing, payments made, and outstanding balances for healthcare services.

These categories illustrate the breadth of data under protection and highlight the importance of robust governance, **<206> Cybersecurity**, and **<106> Compliance** with regulations in healthcare IT management.

2 Banking and Financial Analysis

2.1 Organizations, Governance, and Management

<107>Corporate governance in banks involves a set of roles and processes designed to ensure strategic direction, effective risk management, and regulatory compliance. The <102>Board of Directors holds ultimate responsibility for the bank's strategy, financial soundness, and <106>compliance with legal and ethical obligations. [9] The Board defines the institution's <135>risk appetite and oversees organizational culture, including <135>risk and <106>compliance policies. Large banks strengthen this oversight through specialized committees – such as <135>risk, Audit, and Remuneration – at the Board level, as recommended by international guidelines. [10]

These committees provide focused attention on critical areas: for example, the Risk Committee monitors enterprise risk management (ERM) and supports the Chief Risk Officer (CRO), who must have independence, resources, and direct access to the Board. [10] Basel Committee principles emphasize that banks must have an independent risk function, led by a CRO with authority and unrestricted access to senior management, in order to identify, monitor, and report risks comprehensively. [10]

An integrative approach widely adopted is <112>Governance, Risk and Compliance (GRC), which unifies internal control processes to ensure business objectives are achieved within acceptable <135>risklimits and in regulatory compliance. Banks structure their three lines of defense according to the IIA model:

1st line: business and operations, managing <135>risk daily;

2nd line: <135>risk and <106>compliance functions setting frameworks, monitoring, and advising;

3rd line: Internal Audit, providing independent evaluation and reporting directly to the Board (via the Audit Committee).

[9]

The <102>Board of Directors oversees all three lines, ensuring risks are properly monitored, and that each line operates with autonomy. Coordination between these layers is crucial: clear communication and transparent reporting among management, control areas, and audit ensures there are no "grey zones" of responsibility. [9]

Another essential <112>governance component is external regulatory supervision. Banks operate in a highly regulated environment – government agencies (such as central banks and supervisory authorities) closely monitor <112>governance and control procedures. Following the 2008 financial crisis, the global response strengthened requirements for more risk-savvy boards, IT-literate members, and mandatory risk/audit committees in systemic banks. [10] Regulators act as a kind of "fourth line of defense", setting standards (e.g., Basel Principles for Effective Governance) and assessing governance through inspections and mandatory reporting. [11]

Governance failures can result in serious penalties and reputational damage – cases like the Silicon Valley Bank collapse in 2023 exposed weak <135>risksupervision (long absence of a CRO, excessive <135>risk concentration), leading to scrutiny of boards and regulators. [12] In response, banking <112>governance increasingly incorporates ESG (Environmental, Social, Governance) and <106>compliance management (e.g., stricter AML and data protection controls). In short, effective bank <112>governance today means balancing performance and <106>compliance : engaged boards, committee support, robust control structures, a healthy risk culture, and regulatory scrutiny ensure the stability and trust of the financial system. [13]

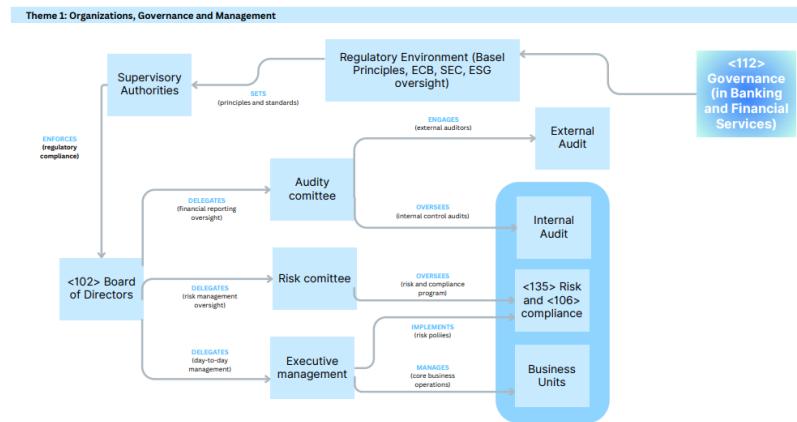


Figure 3: Concept map for Healthcare industry in Organizations, Governance, and Management

In figure 3 the conceptual map outlines <112>governance in the banking sector, highlighting the key bodies and frameworks. Light-blue blocks represent components such as the <102>Board of Directors , its specialized board committees (Audit Committee, Risk Committee), Executive Management, and control functions like Internal Audit (Third Line of Defense). It also shows external oversight by Supervisory Authorities within the broader Regulatory Environment (e.g. Basel principles, ECB, SEC regulations, ESG expectations). Arrows indicate relationships with action-oriented annotations – for example, the Board delegates certain oversight duties to committees, committees oversee audit functions, and regulators enforce <106>compliance – reflecting the “Three Lines of Defense” model (Business Units as 1st line, <135>risk and <106>compliance as 2nd line, Internal Audit as 3rd line) in bank <112>governance.

2.2 Governance of IT and IT Management

IT management in banks is structured to ensure that technology adds business value while controlling technological risks and maintaining regulatory compliance. A central principle is the strategic alignment between IT and business: IT decisions must support the bank's corporate goals. [9] Thus, many financial institutions establish high-level IT governance mechanisms, such as IT committees involving senior executives and often Board members. These committees review IT strategic plans, investment priorities, and innovation initiatives, ensuring that digitization projects (like mobile banking, analytics platforms) align with business strategy and deliver measurable benefits. [14]

IT leadership (CIO, CTO, CISO) is increasingly involved in strategic decision-making – reflecting the importance of technology for competitiveness and operational efficiency in finance. Tactically, IT management in banks includes systems governance and information security. Banks adopt recognized frameworks like COBIT 2019 to define processes, metrics, and controls aligned to business goals. The ISO/IEC 38500 standard guides Boards and executives on effective IT governance, emphasizing that governance responsibilities differ from daily management and should focus on alignment, performance, and IT risk control. [9]

These structures help ensure decisions about systems investment, architecture design, and project prioritization are made transparently and value-driven. Standards like ITIL ensure quality in IT service delivery, while enterprise architectures guide integration between legacy and modern systems. [9]

<206>**Cybersecurity** and IT risk management are now central to banking IT, given the growing threat landscape. Financial institutions are frequent cyberattack targets, leading regulators to demand robust security and operational resilience programs. New regulations, like the EU Digital Operational Resilience Act (DORA), effective in 2025, require institutions to manage ICT risks and be ready for major incidents. [15] This includes mandatory vulnerability testing, third-party <135>**risk** oversight, and incident reporting within tight deadlines.

Banks now reinforce IT risk functions, often as part of operational risk frameworks, with CISOs reporting at senior levels and updated continuity plans. Frameworks like NIST and ISO 27001/27002 guide security policies, covering everything from data protection to incident response. For resilience, standards like ISO 22301 (business continuity) ensure quick recovery from disruptions or attacks. [9]

Resilience is not treated in isolation: it's embedded in risk governance, with business impact analysis, contingency plans, and stress-testing (e.g., for payment system outages, ransomware events). Regulators now expect Boards and executives to lead on cyber risks – DORA explicitly assigns executive accountability for digital resilience, requiring <112>**governance** structures and response plans.

Sector-specific challenges include modernizing legacy systems without disrupting services – requiring careful planning, investment, and portfolio <112>**governance**. Leading banks adopt agile methods and modular architectures to boost flexibility, often inspired by successful transformations (e.g., ING's agile squads). Another challenge is balancing innovation vs. <106>**compliance**: integrating fintechs, cloud computing, or AI brings competitive advantages but also regulatory scrutiny (e.g., cloud adoption demands third-party risk governance).

Data privacy (LGPD/GDPR) and data governance (quality, integrity) are now integral to IT management. In summary, banking IT management has evolved from a technical focus to a strategic and integrated function: effective IT governance ensures technology not only keeps the bank secure and compliant but also enables business value. This requires committed leadership, solid frameworks, and continuous improvement aligned with sector goals and obligations.

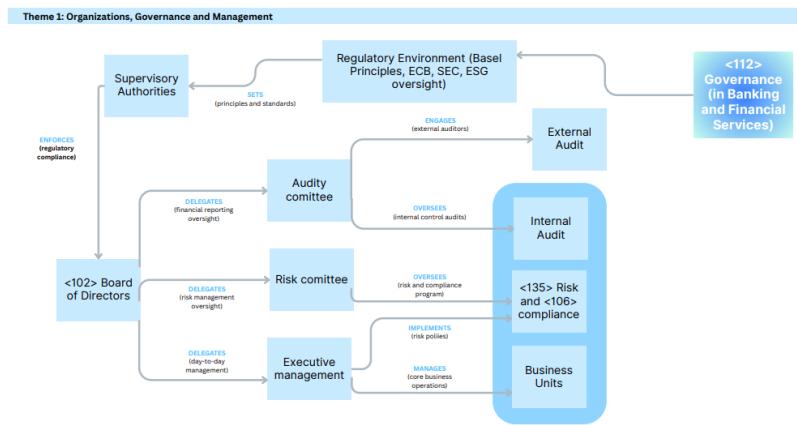


Figure 4: Concept map for Healthcare industry in Organizations, Governance, and Management

The conceptual map for IT management in the banking sector is represented in figure 4, focusing on how IT governance aligns with business objectives and regulatory requirements. Key elements include Governance of IT at the center, driving Strategic Alignment between IT and business strategy, the formulation of an IT Strategy, and its execution through IT Service Management (ITSM) processes. An Incident Response capability is included as part of operational resilience, underpinned by the <206>**Cybersecurity** program. The diagram also shows how <206>**Cybersecurity** and Operational Technology oversight are integrated into IT management. Finally, Regulatory Environment factors (like GDPR for data protection and DORA for digital operational resilience) anchor the framework by imposing compliance obligations that shape IT policies and governance structures.

3 Manufacturing

3.1 Organizations, Governance, and Management

Organizations, Governance, and Management in Manufacturing

In the manufacturing industry, effective <112> **Governance** plays a pivotal role in aligning organizational design and decision-making with the sector's operational and strategic goals. Unlike service-based industries, manufacturing governance involves navigating complex relationships between physical production systems, supply chain networks, and digital platforms [2]. At the core of this structure is multi-level <130> **Management**, where strategic, tactical, and operational layers work in tandem to ensure organizational agility and control.

One of the central principles underpinning manufacturing governance is <437> **Strategic Alignment**. This ensures that technological infrastructure—such as ERP and MES systems—and organizational processes are directly supporting long-term business goals like quality assurance, productivity, and innovation [16]. The implementation of <127> **Policies** at each level ensures cohesion in governance practices, standardizing procedures for data handling, quality control, and continuous improvement.

Regulatory adherence is another fundamental concern. Manufacturers typically operate under strict <211> **Compliance and Standards** regimes, including ISO 9001 (quality), ISO 14001 (environment), and ISO 45001 (safety), which serve as both operational frameworks and marketing differentiators [17–19]. These standards require companies to embed governance within day-to-day processes, thus enhancing transparency, auditability, and risk management.

Another important factor is the <301> **Sectoral Context**, which includes global competition, volatile supply chains, and sustainability pressures. Manufacturing organizations must adapt governance mechanisms to fit specific industrial realities, whether they produce pharmaceuticals, electronics, or heavy equipment. Global firms often establish centralized governance frameworks with local customization, enabling compliance with regional regulations while maintaining strategic coherence [20].

Moreover, digital transformation initiatives like Industry 4.0 are reshaping organizational governance. The integration of AI, IoT, and cloud platforms into production environments requires rethinking <130> **Management** roles, cybersecurity responsibilities, and innovation governance. Boards and executives are increasingly accountable for ensuring these technologies are ethically and effectively governed to deliver long-term value [21].

In summary, <112> **Governance** in manufacturing is a multifaceted discipline that integrates strategic vision, operational excellence, and regulatory accountability. Effective governance frameworks are key to navigating the sector's technical complexity and enabling sustainable, digitally driven growth.

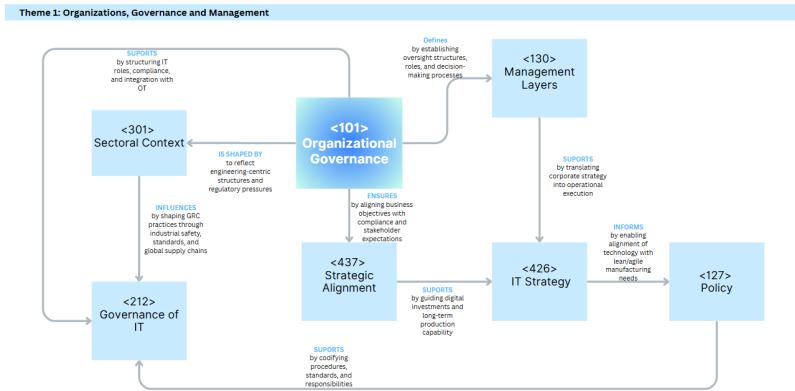


Figure 5: Concept map for Manufacturing industry in Organizations, Governance, and Management

In manufacturing, organizational governance must manage the complex intersection of corporate leadership, engineering disciplines, and operational control. Reflects the sector's focus on safety, precision, and regulatory compliance. This governance framework defines clear management layers responsible for executing strategic and operational goals, especially in capital-intensive environments.

The sectoral context, characterized by global supply chains, industrial safety standards, and long innovation cycles, greatly influences governance approaches. Management practices are informed by compliance with international standards and integration of digital capabilities, especially under Industry 4.0.

Strategic alignment ensures that manufacturing objectives are translated into actionable IT and operational strategies, supported by clear policies. Governance of IT reinforces these structures by embedding accountability, risk management, and compliance into IT-OT convergence.

3.2 Governance of IT and IT Management

The manufacturing industry increasingly relies on digital infrastructures and complex systems integration, making effective **Governance of IT** <212> essential [20, 22]. This governance ensures that technological capabilities are not only aligned with operational needs but also embedded into the company's strategic vision. It plays a critical role in overseeing systems that connect digital tools such as ERP, MES, and PLM platforms with the physical realities of production [21].

A cornerstone of this governance model is **Strategic Alignment** <437>, which ensures that IT efforts directly support business objectives such as operational efficiency, safety, and quality management. In manufacturing, aligning IT with business is not optional—it is vital to competitiveness and resilience in global supply chains [22]. **Strategic Alignment** <437> bridges the gap between engineering functions and executive priorities, enabling smarter investments in automation, robotics, and digital twins.

To implement these goals effectively, organizations rely on structured **IT Service Management** <217>. This function defines service levels, roles, and responsibilities across the IT-OT spectrum. By setting clear policies and expectations, **ITSM** <217> ensures that disruptions are minimized, service delivery is standardized, and change management is consistent [23]. One critical support mechanism is **Incident Response** <310>, which enables organizations to manage cyber threats and system failures without halting production lines. These predefined protocols are increasingly important as manufacturing environments become more connected—and thus more exposed [24].

At the heart of modern risk management in this domain is **Cybersecurity** <206>. As Operational Technology (OT) becomes networked, threats to SCADA systems, industrial controllers, and digital workflows multiply. **Cybersecurity** <206> supports **Strategic Alignment** <437> by protecting assets, ensuring compliance, and building digital trust. Without it, even the most innovative strategy could be compromised by a single vulnerability [25, 26].

The development and execution of a coherent **IT Strategy** <426> ensures that decisions around infrastructure, platforms, and tools are guided by both technical insight and business foresight. This strategy must be informed by operational feedback and framed by organizational goals. Policies, represented by **Policy** <127>, support this by formalizing governance procedures, including rules for access control, audit readiness, and data handling. These policies underpin both accountability and adaptability, two essential traits in an evolving industrial landscape [27].

Finally, strong governance depends on adherence to **Standards & Regulations** <211>, such as ISO 9001 for quality, ISO 45001 for workplace safety, IEC 62443 for OT cybersecurity, and the EU's NIS2 Directive. These frameworks are not simply checkboxes; they are integral to ensuring secure, efficient, and lawful operations, reinforcing the core goals of **Governance of IT** <212> [28, 29].

In summary, the governance of IT in manufacturing orchestrates a complex ecosystem of people, processes, and technology. Through strategic alignment, robust IT management, <206> **cybersecurity**, and regulatory compliance, manufacturing firms are better positioned to innovate securely and sustainably.

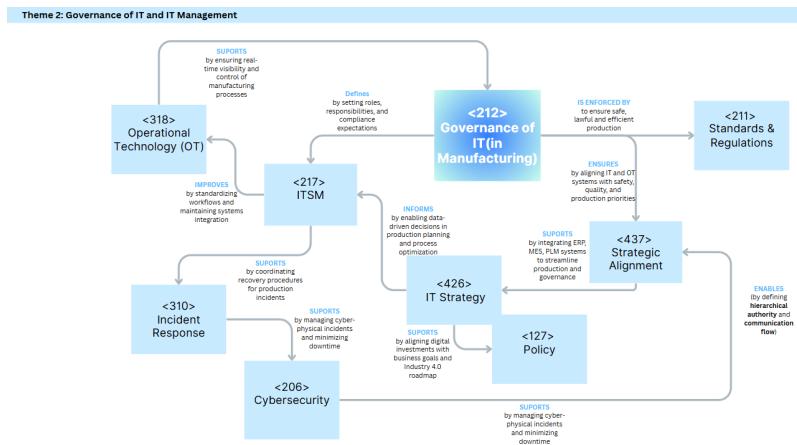


Figure 6: Concept map for Manufacturing industry in Governance of IT and IT Management

The governance of IT in manufacturing revolves around integrating digital tools and policies with operational technology (OT) to ensure resilient, efficient, and secure production. It aligns digital initiatives with core industrial priorities such as safety, throughput, and quality.

Key frameworks (ISO 9001, NIS2, IEC 62443) support structured risk management, especially where IT converges with OT in areas like Industrial IoT and SCADA systems. IT Service Management (ITSM) structures define responsibilities, enhance service quality, and reduce disruption through standardized workflows. Strategic alignment ensures digital initiatives (e.g., MES, ERP, PLM) contribute to long-term competitiveness and operational excellence.

Incident response and <206> **cybersecurity** are vital due to the increased threat surface from connected production systems. <206> **cybersecurity** supports both continuity and compliance, feeding into broader strategic IT decisions. The IT strategy ensures evolving technologies like digital twins, predictive maintenance, and analytics are embedded into the organization's roadmap.

4 Comparison

4.1 Organizations, Governance, and Management

Governance in manufacturing is heavily oriented toward operational efficiency, quality assurance, and compliance with physical safety and environmental standards. It spans the coordination of supply chains, precision in production, and adherence to international standards such as **ISO 9001** (quality), **ISO 14001** (environment), and **ISO 45001** (workplace safety). With increasing digital integration—especially under **Industry 4.0**—manufacturing governance must also manage cyber-physical risks, blending operational technology (**OT**) with **IT** systems. Here, governance includes not just traditional managerial oversight but also the secure integration of **ERP**, **MES**, and **PLM** platforms to avoid data breaches and ensure continuity of production.

In contrast, governance in banking and financial services is more abstract and regulation-intensive, reflecting the sector's critical role in economic stability. Banks and financial institutions are overseen by boards, audit committees, and compliance officers, but also by robust external regulators like the **ECB**, **EBA**, and national supervisory bodies. Risk governance emphasizes liquidity, credit exposure, and operational resilience, with rigorous stress testing and adherence to standards like **Basel III** and **DORA**. Unlike manufacturing, where physical production is paramount, finance must guard against systemic risk and financial crime while navigating digital innovation, such as fintech and algorithmic trading, which introduce unique governance challenges around transparency, customer protection, and cybersecurity.

While both finance and healthcare are highly regulated, their governance structures reflect different imperatives. Financial services focus on capital adequacy, solvency, and systemic risk mitigation. Governance is driven by a blend of internal control and external oversight, with global coordination through institutions like the Basel Committee and Financial Stability Board. Regulatory compliance in finance often hinges on precise, timely reporting and robust **cybersecurity** to protect against market contagion or data breaches.

Healthcare governance, meanwhile, must address an intricate web of clinical accountability, patient rights, ethical oversight, and data privacy. While financial failures threaten economic systems, governance failures in healthcare can directly harm human lives. Compliance involves not only financial and operational considerations but also rigorous protection of sensitive health data under GDPR and the proposed European Health Data Space (**EHDS**). Governance here must coordinate across providers, payers, and regulators, ensuring continuity of care, medical safety, and equitable access. The integration of digital health records, telemedicine, and **AI**-driven diagnostics adds complexity, demanding governance that is both technically proficient and ethically grounded.

Thus, while both sectors share a need for strong governance frameworks, finance prioritizes systemic resilience and investor protection, whereas healthcare governance is shaped by ethical responsibility, patient safety, and public trust. The former is guided by economic logic, the latter by social and clinical imperatives

4.2 Governance of IT and IT Management

Management in manufacturing is fundamentally oriented around the coordination of physical processes, supply chains, and production systems. It involves a blend of engineering oversight, operations planning, and human resource coordination to ensure throughput, product quality, and safety. Manufacturing managers must integrate **Lean** or **Six Sigma** principles to reduce waste and defects while adapting to rapid technological change, especially in smart factories. Their environment is defined by tangible assets—machinery, labor, raw materials—and the efficient conversion of inputs into finished goods, often requiring close attention to shift scheduling, maintenance cycles, and compliance with safety standards.

In contrast, management in banking and financial services revolves around the stewardship of intangible assets: capital, data, risk, and customer trust. Managers in this sector are less concerned with physical flows and more focused on regulatory compliance, financial performance, and digital innovation. They oversee departments such as risk, compliance, lending, wealth management, or digital platforms, with **KPIs** centered on returns, customer acquisition, and operational resilience. Strategy and decision-making rely on financial modeling, market analysis, and regulatory frameworks rather than production metrics. Furthermore, management here must navigate frequent policy changes and technological disruption from **fintech**, making agility and strategic foresight key traits.

While both banking and healthcare operate in high-stakes, tightly regulated environments, management responsibilities differ significantly due to their core missions. Financial services management is focused on optimizing profitability, ensuring compliance, and managing market risks. Managers prioritize metrics such as cost-income ratios, asset growth, and risk-weighted capital adequacy. Digital transformation is a key priority, with executives managing large **IT** investments and cyber resilience strategies. Their leadership is driven by shareholder expectations and competition within global financial ecosystems.

Healthcare management, however, must balance financial sustainability with care delivery and ethical responsibility. Managers in hospitals, clinics, or public health bodies are tasked not only with budgets and staffing but also with ensuring patient safety, treatment quality, and service accessibility. They coordinate with clinical staff, regulators, and **IT** teams to maintain smooth and compliant operations while supporting outcomes like reduced readmission rates or improved patient satisfaction. Decision-making often involves trade-offs between cost efficiency and clinical value. Additionally, healthcare managers must handle systemic challenges like aging populations, staff shortages, and digitization, all under intense public and political scrutiny.

In essence, while finance managers are primarily stewards of capital and compliance in a fast-moving market, healthcare managers are orchestrators of multidisciplinary systems where success is measured not only in costs saved but lives improved.

References

- [1] Lynne Rinehimer. Healthcare governance & why it matters, January 2025. Accessed: 2025-05-22.
- [2] Information systems management and security: A glimpse of industries. Internal Course Material, 2025. Course document covering governance, risk, and digital strategy across various industries.
- [3] Organimi. Hospital organizational structure – how it works & examples, 2024. Accessed: 2025-05-22.
- [4] Jameson Lee. The importance of it management style in healthcare, 2024. Accessed: 2025-05-22.
- [5] Chris Davis. It governance: A guide for healthcare professionals, 2024. Accessed: 2025-05-22.
- [6] Rachna Kumar. 6 pros of technology in healthcare, 2024. Accessed: 2025-05-23.
- [7] Tedisel Medical. The importance of technology in healthcare, 2024. Accessed: 2025-05-23.
- [8] Kiteworks. Gdpr compliance checklist for healthcare: Patient data protection best practices, 2024. Accessed: 2025-05-23.
- [9] Information systems management and security: Lecture notes. Internal Course Material, 2025.
- [10] Corporate governance principles for banks - executive summary, 2023. Accessed: 2025-05-22.
- [11] Isabella Arndorfer and Andrea Minto. The “four lines of defence model” for financial institutions. *Financial Stability Institute Occasional Paper*, 2015.
- [12] Silicon valley bank: Key takeaways and questions for board risk oversight., 2023. Accessed: 2025-05-22.
- [13] Harun R Khan. It governance and it strategy: Board’s eye view, 2015.
- [14] It governance and management manual, 2017. Accessed: 2025-05-22.
- [15] Dora compliance 2025 - what you need to know, 2025. Accessed: 2025-05-22.
- [16] Gartner. The business value of strategic it alignment, 2022. Accessed: 2025-05-23.
- [17] Iso 9001:2015 - quality management systems — requirements, 2015. Accessed: 2025-05-23.
- [18] Iso 14001:2015 - environmental management systems — requirements, 2015. Accessed: 2025-05-23.
- [19] Iso 45001:2018 - occupational health and safety management systems, 2018. Accessed: 2025-05-23.
- [20] McKinsey & Company. Smart governance in global manufacturing, 2023. Accessed: 2025-05-23.
- [21] Deloitte. Reimagining governance in the age of industry 4.0, 2023. Accessed: 2025-05-23.
- [22] Gartner. The business value of strategic it alignment, 2022. Accessed: 2025-05-23.
- [23] ServiceNow. What is itsm?, 2024. Accessed: 2025-05-23.
- [24] Sectrio. Cybersecurity compliance in manufacturing: A complete guide, 2023. Accessed: 2025-05-23.
- [25] FortifyData. Manufacturing cybersecurity risks management, 2023. Accessed: 2025-05-23.
- [26] NIST. Cybersecurity framework 2.0 draft, 2023. Accessed: 2025-05-23.
- [27] Gartner. It policy management best practices, 2024. Accessed: 2025-05-23.
- [28] ISA. Iec 62443: Industrial cybersecurity standard, 2022. Accessed: 2025-05-23.
- [29] NCC Group. Nis2: What you need to know, 2024. Accessed: 2025-05-23.

Agriculture and Farming Industry

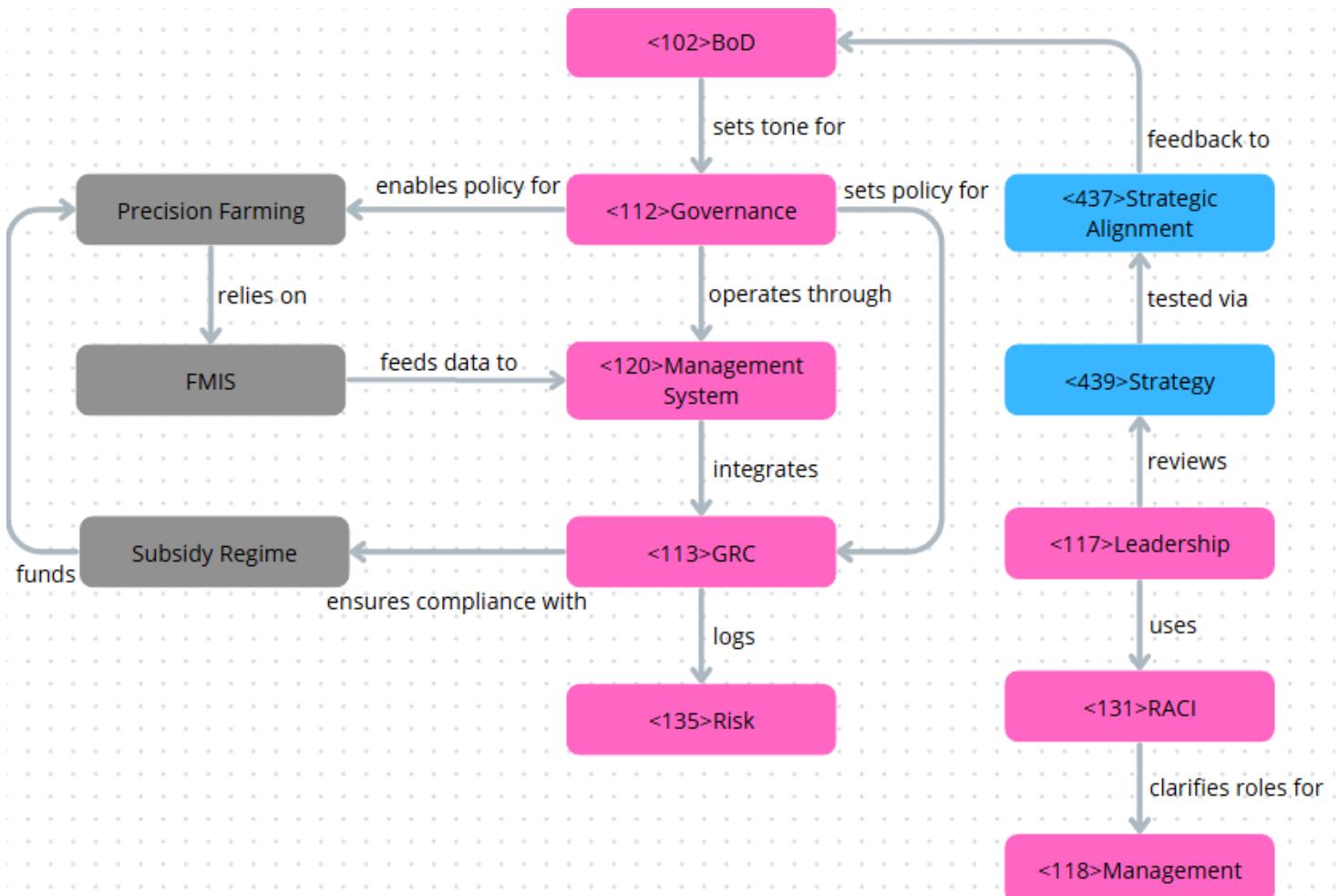
This industry is characterized here as the interconnected set of activities that transform land, water, seeds, and livestock into marketable food and bio-based raw materials—spanning field operations, input supply, data-driven advisory services, storage, and first-stage processing. Because “agriculture and farming” can mean subsistence plots, high-tech vertical farms, or global grain traders, our focus narrows to **precision crop-farming cooperatives** (co-ops): producer-owned entities that deploy digital tools (FMIS, IoT sensors, drone imagery) to raise yields and meet regulatory, environmental, and market demands.

Organizations, Governance, and Management lens (niche: Precision Crop Farming)

Boards (<102> BoD) in precision-farming co-ops must steer crops and code at once. They install a <120> Management System that links subsidy rules, food-safety tests, and carbon targets to daily drone flights recorded in the FMIS (Farm-Management Information System). A slim <113> GRC layer sits inside that system, keeping objectives, audits, and risk logs together.

<117> Leadership publishes a <131> RACI so agronomists, tech vendors, and compliance officers know who changes sensors and who signs subsidy reports. The board reviews <439> Strategy each season and checks it in <437> Strategic Alignment sessions to be sure new tools advance Precision Farming goals rather than create silos.

All moves are tracked by <118> Management and scored in dashboards; if <135> Risk starts to climb—weather, prices, or cyber—the board brings in training or outside help. This loop lets the co-op adopt AI seed maps and drone imagery without losing oversight or trust.



Precision Farming - Data-driven optimisation of seeding, fertiliser and pesticide use.

FMIS - Farm-Management Information System that stores field data, drone imagery, and compliance records.

Subsidy Regime - EU CAP and similar schemes that tie funding to compliance metrics.

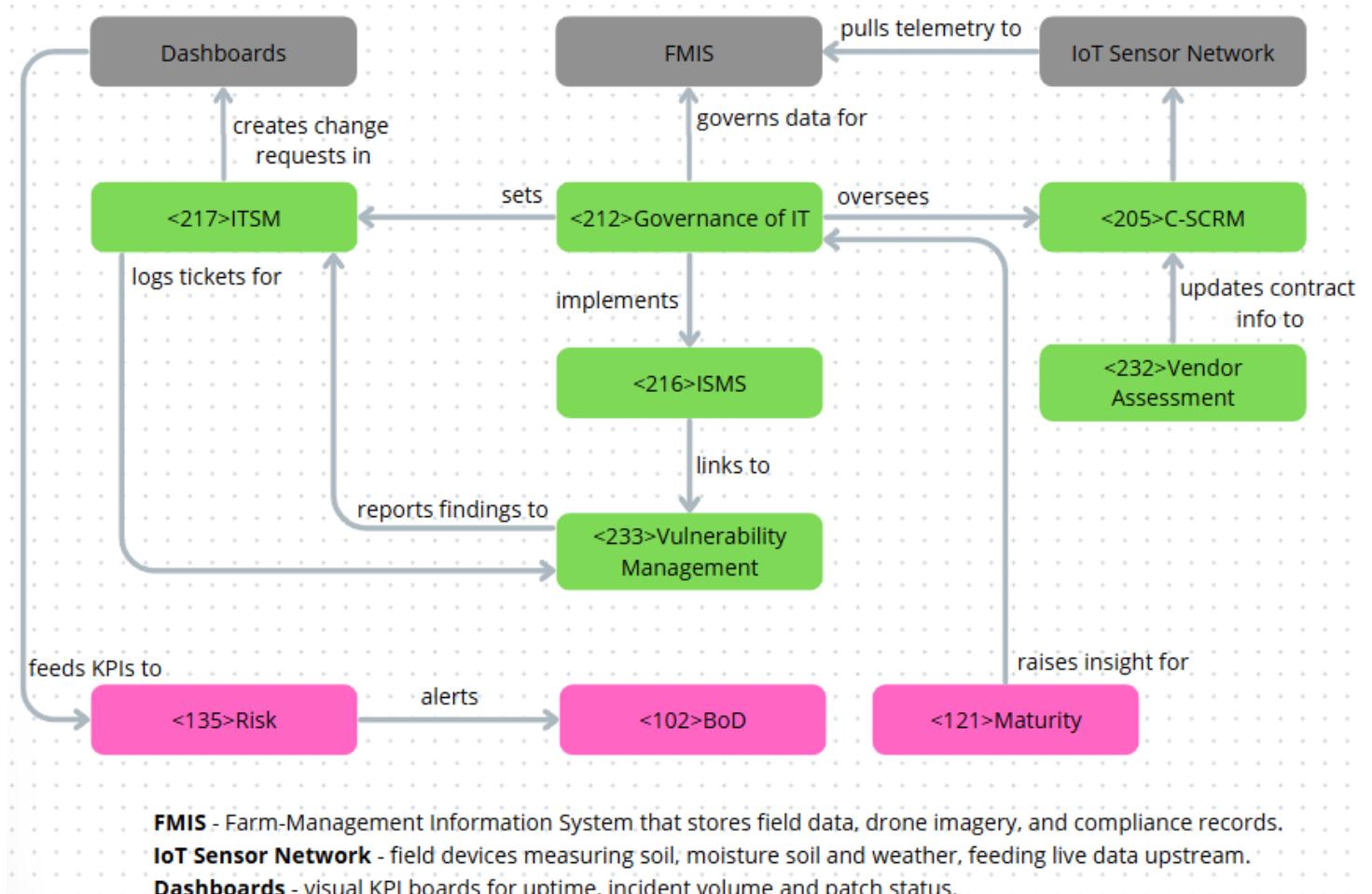
Governance of IT and IT Management lens (niche: Precision Crop Farming)

Precision Farming depends on two core platforms: the IoT Sensor Network in the fields and the central FMIS in the office. A solid <212> Governance of IT framework keeps both safe, legal, and useful.

The board approves an <216> ISMS that sets data-security rules for drones, gateways, and cloud stores. A service-level <217> ITSM process logs incidents, changes, and asset life cycles so broken sensors or bad firmware are fixed before harvest.

Most devices come from small Ag-Tech Vendors. <205> C-SCRM and <232> Vendor Assessment check code updates and contract terms, while <233> Vulnerability Management scans gateways for weak passwords. Findings loop back into <217> ITSM tickets.

<212> Governance of IT also maps data flows to help the privacy officer run a DPIA when new drone imagery is added, and it links farm <116>KPIs to dashboards, so leaders see if uptime targets slip. Continuous reviews raise <121> Maturity and keep <135> Risk within appetite, letting the co-op add AI crop models without losing control.



Healthcare Industry

The healthcare sector is highly regulated and increasingly reliant on digital systems such as electronic health records, telemedicine, and data platforms. It includes hospitals, clinics, insurers, and public health authorities, all aiming to provide safe, efficient, and compliant care. In Portugal, both public and private actors operate within this space, creating a dual governance structure. This setup affects how digital coordination, data responsibilities, and regulatory compliance are managed across systems and institutions.

Organizations, Governance, and Management lens (niche: Dual Governance in Portuguese eHealth)

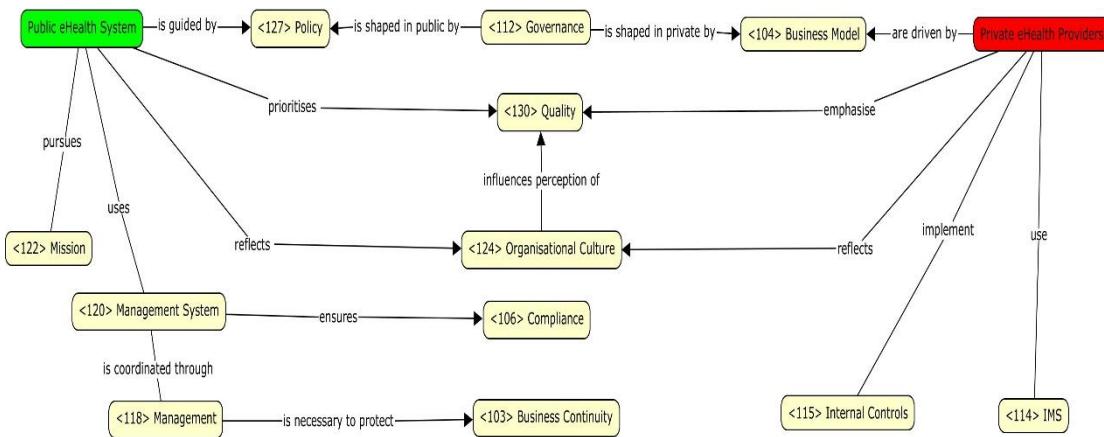
Portugal's eHealth sector exhibits dual <112> Governance, where distinct public and private actors operate under different logics: state-led models aim for universal care, while private providers follow market-based <104> Business Models. This structural split creates contrasting priorities in management, oversight, and values.

Public eHealth systems, coordinated by entities such as SPMS, pursue a clear <122> Mission of universal access, guided by national <127> Policy and supported by high <121> Maturity. Structured <120> Management Systems ensure <106> Compliance, reinforced through <105> Certification and periodic <101> Audit. <111> Ethical Values such as equity and accountability are central to the legitimacy of public governance models.

Private providers, in contrast, emphasize responsiveness, innovation, and differentiation. Strategic control is exercised through <108> CxO roles operating within flexible <126> Organizational Structures. In the private sector, use of <115> Internal Controls and <114> IMS varies widely, typically shaped by internal objectives rather than regulatory requirements.

Perceptions of <130> Quality also diverge. Public systems prioritize standardised access and equitable outcomes, whereas private actors focus on patient experience and service differentiation. These contrasting goals reflect underlying differences in <124> Organisational Cultures and governance logic.

The result is fragmentation in <113> GRC. Bridging both models requires interoperable standards and harmonized <118> Management strategies. This is essential not only to ensure <103> Business Continuity but also to deliver equitable care and maintain public trust in hybrid healthcare landscape.



Governance of IT and IT Management lens (niche: Dual Governance in Portuguese eHealth)

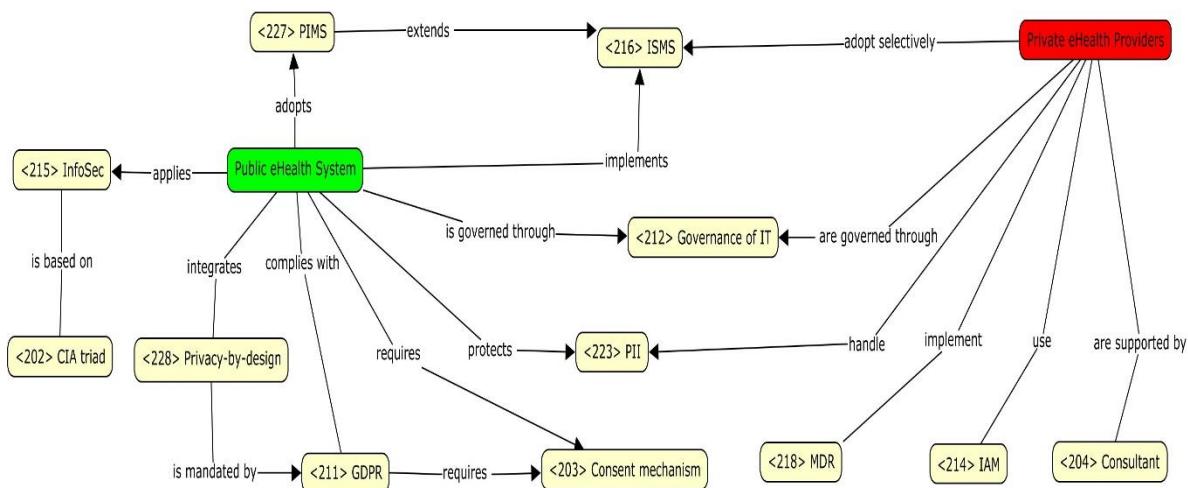
Portuguese eHealth exhibits dual <212> Governance of IT, where public and private providers manage information and technology systems under distinct operational models.

Public health entities such as SPMS adopt structured frameworks like <216> ISMS and <227> PIMS to protect <223> PII and ensure compliance with <211> GDPR. These systems are built around <215> InfoSec principles, namely confidentiality, integrity, and availability (<202> CIA triad), and are supported by mandatory <203> Consent mechanisms and <228> Privacy-by-design, which embed data protection into technical and organizational processes.

Private e-Health providers, on the other hand, follow more flexible and strategy-driven IT management approaches. While some apply <216> ISMS and seek support from <204> Consultants, adoption levels vary depending on internal risk tolerance. Security measures such as <214> IAM and <233> Vulnerability Management are implemented selectively, and outsourcing to <219> MSPs or <220> MSSPs is common, particularly for services like <218> MDR.

This divergence creates challenges in integration, risk sharing, and assurance. Addressing these issues requires improved coordination on <232> Vendor Assessment, investment in shared <205> C-SCRM capabilities, and mutual understanding of <231> Supply Chain risks. Regulatory constraints such as <207> Data Localization and <209> Data Residency further complicate alignment across sectors.

Achieving effective dual IT governance in healthcare depends on a consistent baseline of security maturity and collaborative management of digital risk and resilience.



Manufacturing Industry

The manufacturing industry encompasses the process of converting raw materials, components, or parts into finished goods using labor, machinery, tools, and chemical or biological processing. It is characterized by systematic production methods aimed at producing large volumes of standardized products efficiently and consistently.

Organizations, Governance, and Management lens (niche: Pharmaceutical Manufacturing)

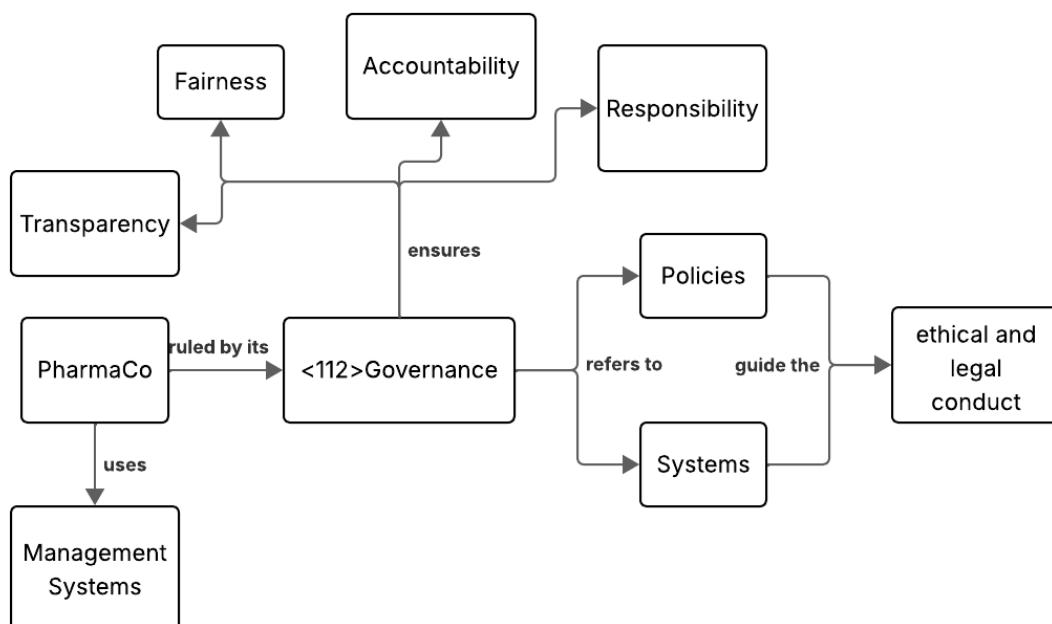
This industry plays a vital role in the economy by creating tangible products that meet consumer, commercial, and industrial needs. Manufacturing ranges across various sectors including automotive, electronics, textiles, food and beverages, pharmaceuticals, etc.

If we take on the example of PharmaCo, its <112>governance refers to the policies and systems that guide the ethical and legal conduct of pharmaceutical companies, ensuring accountability, transparency, fairness, and responsibility. It's a crucial aspect of managing a pharmaceutical business, particularly considering the significant impact these companies have on public health and societal well-being.

Pharmaceutical companies are ruled by strict regulatory oversight and global quality standards, leading to the <112>governance and management being particularly formalized and multilayered. Organizations must operate under Good Manufacturing Practices (GMP) and national/internation legislation.

Some key aspects of its governance are:

- <111>Ethical Conduct: Establishing clear guidelines and codes of conduct for employees and partners, promoting ethical decision-making and preventing misconduct.
- <106>Compliance: Adhering to relevant regulations and industry standards, including those related to drug development, manufacturing, and marketing.
- Stakeholder Engagement: Fostering transparency and open communication with investors, patients, and the public.
- Risk Management: Identifying and mitigating potential risks related to drug safety, efficacy, and ethical practices.
- Accountability: Ensuring that executive leadership and boards are held accountable for company performance and ethical conduct.
- Transparency: Publicly disclosing relevant information, including financial data, research findings, and potential conflicts of interest



Governance of IT and IT Management lens (niche: Pharmaceutical Manufacturing)

Pharmaceutical manufacturing integrates IT governance and IT management as core enablers of regulatory compliance, data integrity, and product traceability. The convergence of cyber-physical systems, regulatory scrutiny, and digital tools necessitates sector-specific adaptations of governance frameworks.

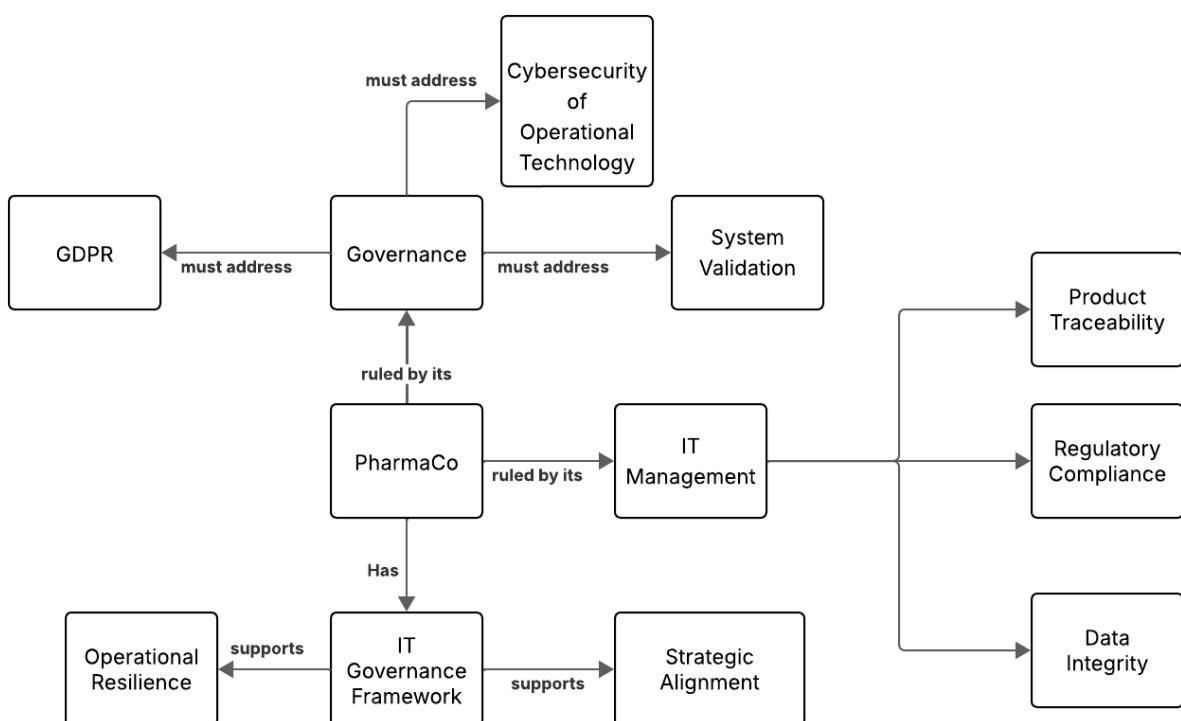
Key dimensions:

- Governance of IT Risk: Governance must address system validation, cybersecurity of operational technology (IEC 62443), and privacy under regulations like GDPR.
- IT Governance Frameworks: Frameworks such as COBIT, ISO/IEC 38500, and ITIL are tailored to support both operational resilience and strategic alignment with regulatory goals.
- Information Governance: Ensuring data integrity across systems like LIMS, EBR, and ERP is essential to prevent regulatory breaches and support audits (e.g., CFR 21 Part 11 compliance).
- Vendor and Contract Management: With reliance on IT service providers and cloud-based platforms, clear roles, audit rights, and security requirements must be embedded in contracts.

Industry-Specific Challenges:

- Hybrid Governance Across IT/OT: Integration between IT systems and OT platforms (e.g., SCADA, PLCs) requires unified oversight that blends safety, compliance, and security principles.
- Traceability and Chain-of-Custody: Governance structures must ensure that each stage of digital records (from raw materials to patient delivery) is transparent and tamper-proof.
- Board-Level Involvement: In high-risk environments, governance of IT is not delegated solely to CIOs but requires visibility and sponsorship from the executive and regulatory affairs leadership.
- Auditability and Digital Trust: Pharmaceutical firms must proactively demonstrate system integrity through frequent audits, continuous monitoring, and digital forensics capabilities.

Governance of IT in the pharmaceutical sector is not just about optimizing technology but about safeguarding public health, ensuring scientific integrity, and preserving trust in the regulatory ecosystem.



Comparisons from the perspective of Organizations, Governance, and Management

Precision crop-farming (Agriculture and Farming) vs Pharmaceutical Manufacturers (Manufacturing)

Governance set-up - Farming co-ops rely on a member-elected <102> BoD and a <120> Management System that welds subsidy rules, food-safety tests, and carbon targets to field routines in the FMIS. Their <113> GRC is lightweight but must cover climate, price, and cyber risk (<135>). Pharma firms operate under multilayer <107> Corporate Governance: an independent board, quality-assurance committees, and strict Good Manufacturing Practice audits. Compliance (<106>) is formal, spanning global regulators and continuous inspection.

Leadership and role clarity - Co-ops publish a <131> RACI so agronomists know who fixes sensors; decision cycles follow seasons and cooperative votes. Pharma assigns roles through SOPs, with <111> Ethical Values codes guiding all staff. Executives (<108> CxO) face personal liability for misconduct.

Strategic alignment - Farm boards review <439> Strategy each season and test it in <437> Strategic Alignment sessions to avoid siloed tech investments that clash with Precision Farming goals. Pharma strategy changes slowly—pipeline timelines and GMP validation freezes architecture for years, but portfolio reviews focus on patent cliffs and supply resilience.

Risk posture and maturity - Agriculture accepts high environmental volatility; its <121> Maturity varies, and risk is capped by insurance and public subsidies. Pharma's risk lens centers on patient safety and product recalls; mature quality systems and layered documentation (<109>) narrow variance but raise overhead.

Stakeholder engagement - Co-ops dialogue with members and local buyers; transparency is informal. Pharma must engage investors, regulators, clinicians, and patients, publishing trial data and financials.

Result: agriculture governance is adaptive and community-driven; pharma governance is formal, compliance-heavy, and globally standardised—each reflecting its unique risk, regulation, and ownership structures.

Dual Governance in Portuguese e-Health (Healthcare) vs Precision crop-farming (Agriculture and Farming)

Governance logic - Public e-Health bodies work under a state mandate for universal access (<122> Mission) and tight <127> Policy control; private clinics answer to market-based <104> Business Models. Precision co-ops anchor governance in member ownership; their <102> BoD balances yield, subsidy, and carbon targets.

Management systems - Hospitals rely on layered <120> Management Systems with routine <101> Audits, GMP-like <105> Certification, and strong <106> Compliance tracking. Co-ops run a lean IMS that hinges on FMIS data and a compact <113> GRC; formality is lower but seasonally reviewed.

Leadership & structure - In e-Health, <108> CxO roles manage large bureaucracies; public side uses rigid hierarchies, private side favours agile <126> Organisational Structures. Farming co-ops keep small staff; <117> Leadership issues a <131> RACI so agronomists, vendors, and compliance officers see clear hand-offs.

Culture & ethics - Public e-Health stresses <111> Ethical Values such as equity; private e-Health highlights innovation and service differentiation. Co-ops foster communal <124> Organisational Culture - shared risk and profit - while adopting precision-tech mindsets.

Risk & maturity - Healthcare risks center on patient safety and data privacy; high <121> Maturity is enforced by regulators. Farming risks cover weather, market swings, and cyber; maturity is uneven and cushioned by subsidies.

GRC integration - e-Health suffers from fragmented <113> GRC between public and private actors; co-ops struggle with lightweight GRC that may miss cyber threats. Both sectors need interoperable standards to bridge gaps and secure <103> Business Continuity.

Result: Healthcare shows high formal maturity yet suffers coordination gaps between public and private actors; farming co-ops keep agile, community-driven governance but risk cyber and compliance blind spots. Both must tighten interoperable GRC standards to sustain trust and business continuity as digital tools spread.

Comparisons from the perspective of Governance of IT and IT Management

Healthcare Industry vs Manufacturing Industry

In both the manufacturing and healthcare industries, the governance of IT plays a critical role, in different contexts and with unique challenges.

In the manufacturing sector, IT governance focuses on ensuring operational continuity, product quality, safety, and regulatory compliance, especially given the industry's reliance on both Operational Technology (OT) and Information Technology (IT). The manufacturing environment often faces risks such as cyberattacks targeting industrial control systems and data loss, necessitating strong governance frameworks to protect sensitive production data and proprietary designs. Compliance frameworks, such as ISO 9001 for quality management and IEC 62443 for cybersecurity, play a key role in shaping governance practices. The industry's push toward Industry 4.0 emphasizes the integration of digital technologies like IoT, AI, and robotics into manufacturing processes, further increasing the complexity of IT governance.

On the other hand, healthcare governance of IT is shaped by a complex web of ethical considerations, privacy regulations, and operational demands. Given the sensitive nature of health data, the governance of IT in healthcare must prioritize patient safety, data privacy, and regulatory compliance, with frameworks like the GDPR and national health laws dictating strict data protection measures. Additionally, healthcare IT systems, such as electronic health records (HER) and telemedicine platforms, are integral to patient care and must be carefully governed to ensure interoperability, security, and accuracy across diverse healthcare settings. The governance of IT in healthcare is also concerned with maintaining high standards of clinical governance, ensuring that IT systems support the delivery of high-quality care while safeguarding against cyber threats and data breaches.

While both industries face increasing digitalization and cyber risks, the healthcare sector places a stronger emphasis on privacy and patient care, requiring a more stringent regulatory approach. In contrast, manufacturing is more focused on operational continuity, efficiency, and the integration of digital technologies into physical production processes. These differences highlight the distinct governance needs of each industry, influenced by their respective regulatory environments, operational models, and strategic priorities.

Healthcare Industry vs Agriculture and Farming Industry

Healthcare and Agriculture both depend on digital systems, but their approach to **Governance of IT** differs in structure and intent.

The Healthcare industry is shaped by strict regulatory demands. It uses structured frameworks such as **ISMS** and **PIMS** to protect **PII**. These are based on **InfoSec principles**, especially the **CIA triad**. Governance is supported by **Consent mechanisms** and **Privacy-by-design**, ensuring that privacy is embedded in both systems and processes. Risk control includes formal **Vendor Assessment** and the use of **Vulnerability Management** to manage security exposures across systems.

In Agriculture, particularly in Precision Crop Farming, governance focuses on system reliability and vendor coordination. It integrates IoT sensor networks and FMIS platforms under a unified **Governance of IT** model. A board-approved **ISMS** defines rules for drones, gateways, and cloud data. Operational continuity is maintained using **ITSM** to track incidents, changes, and asset status. Since devices often come from small Ag-Tech vendors, the sector relies on **C-SCRM** and **Vendor Assessment** to review code and contracts. **Vulnerability Management** is applied to detect misconfigurations and feed back into **ITSM** processes.

In summary, Healthcare governance is compliance-oriented and focused on protecting sensitive data. Agriculture governance is performance-oriented and geared toward operational stability and vendor oversight. Both industries rely on strong IT management, but they prioritize different outcomes based on their sector context.

Security and Management of Information Systems

Group 234

Alessandro Costa Campagna - 106751 • Diogo Alexandre Moreira Henriques - 102780
Isabela Pereira de Ornelas - 102703 • José Santos Corte - 103210

Index

Governance in the Energy and Utilities Industry.....	1
Textual Analysis.....	1
Structural Mapping.....	1
IT Management in the Energy and Utilities Industry.....	2
Textual Analysis.....	2
Structural Mapping.....	2
Governance in Retail and Digital Commerce Industry.....	3
Textual Analysis.....	3
Structural Mapping.....	3
IT Management in Retail and Digital Commerce Industry.....	4
Textual Analysis.....	4
Structural Mapping.....	4
Governance in Transport and Logistics.....	5
Textual Analysis.....	5
Structural Mapping.....	5
IT Management in Transport and Logistics.....	6
Textual Analysis.....	6
Structural Mapping.....	6
Comparative — Governance.....	7
Comparison 1: Energy vs Retail.....	7
Comparison 2: Transport vs Retail.....	7
Comparative — IT Management.....	8
Comparison 3: Energy vs Transport.....	8
Comparison 4: Retail vs Transport.....	8

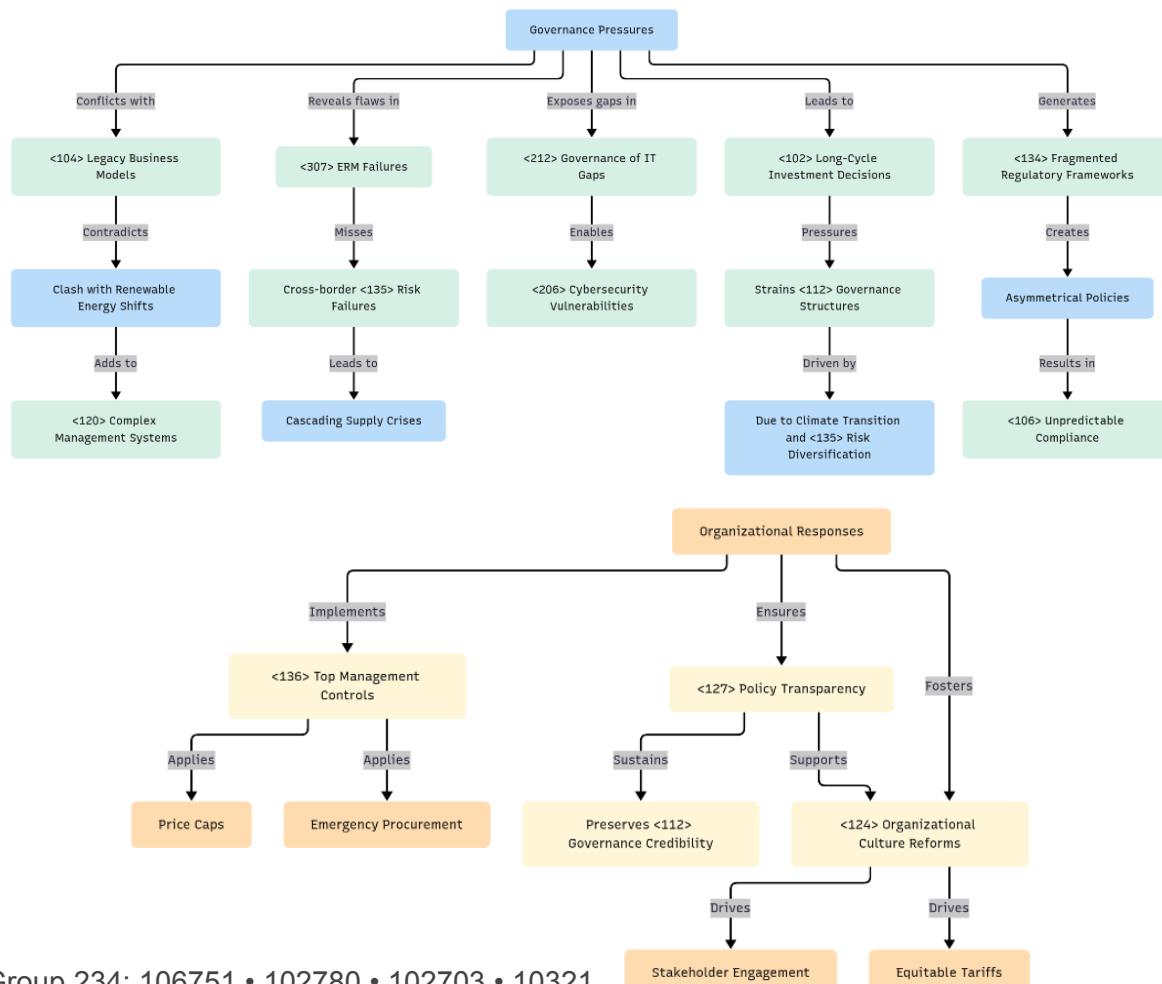
Governance in the Energy and Utilities Industry

Textual Analysis

This industry is fundamentally characterized by its dual role as both an economic engine and a critical public service provider, creating unique governance tensions between commercial and societal objectives. The energy sector operates under complex governance conditions due to its essential nature and infrastructure dependence. Boards manage competing priorities, including ensuring supply security, enabling green transitions, and maintaining affordability. With public accountability and state ownership, governance often involves regulatory agencies and adherence to EU directives like the Clean Energy Package and the Green Deal.

Governance frameworks are structured to enhance resilience, particularly against risks such as cyberattacks, climate disruptions, and geopolitical instability. Risk management encompasses cybersecurity, climate risks, and market volatility. Board members and executives are required to balance long-term infrastructure investment with environmental and digital innovation goals. The shift toward renewable and distributed energy models further increases stakeholder complexity. These dynamics require transparent, long-term governance models capable of coordinating across infrastructure, policy, and innovation.

Structural Mapping



IT Management in the Energy and Utilities Industry

Textual Analysis

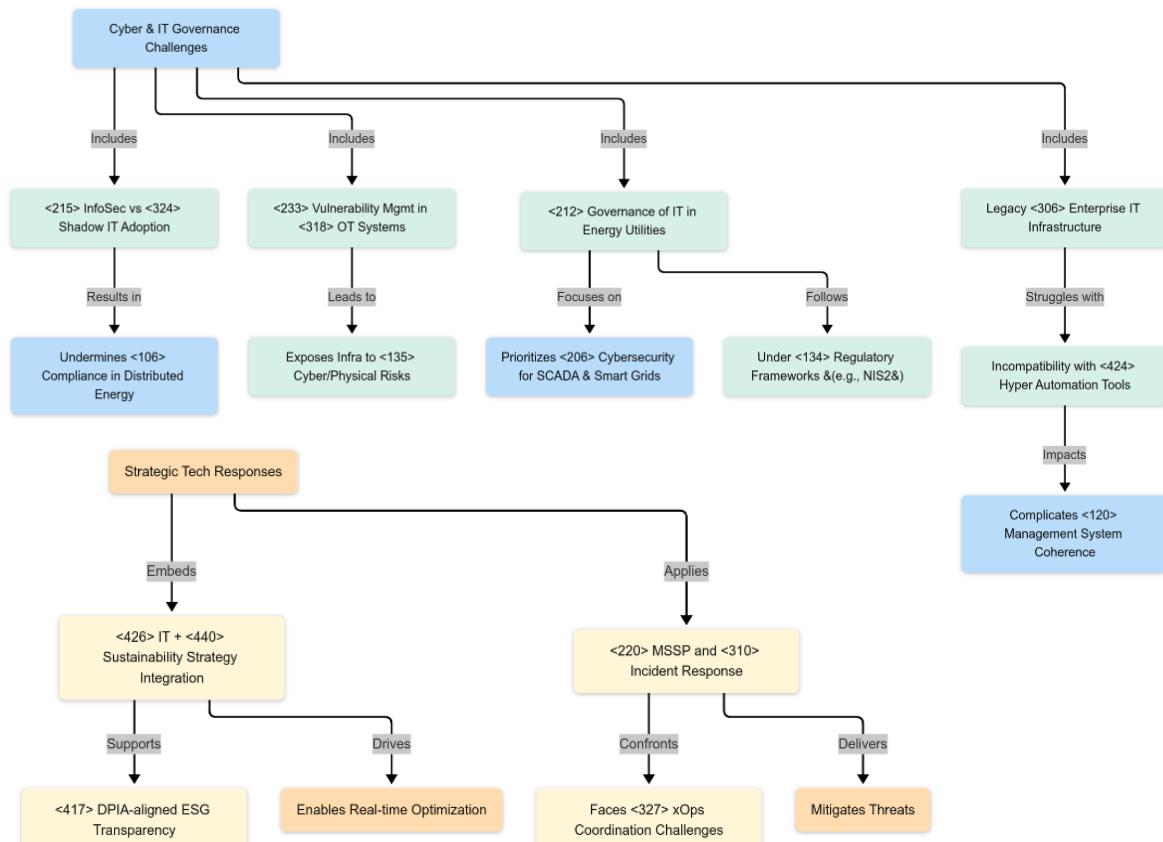
This industry is defined by its critical infrastructure dependencies, where IT management directly impacts national energy security and the clean energy transition. IT governance in the energy and utilities sector is fundamentally shaped by the need to ensure operational continuity, regulatory compliance, and infrastructure security. Core operational systems—such as SCADA, smart meters, and grid automation platforms—are critical assets requiring robust cybersecurity protections against cyberattacks, physical disruptions, and system failures.

EU directives like NIS2 and the EU Cybersecurity Act impose stringent resilience and incident response obligations on energy providers, framing IT as a critical national security concern.

As digital transformation accelerates, the sector faces growing complexity. Emerging technologies such as AI-driven forecasting, predictive maintenance, and distributed energy control platforms must interoperate with legacy systems. This hybrid environment requires IT leaders to manage both operational technology (OT) and information technology (IT) domains, ensuring security, interoperability, and regulatory alignment.

Furthermore, IT strategy must support broader sustainability and decarbonization goals by enabling real-time energy optimization, data transparency for ESG reporting, and consumer engagement through smart billing and demand response systems.

Structural Mapping



Governance in Retail and Digital Commerce Industry

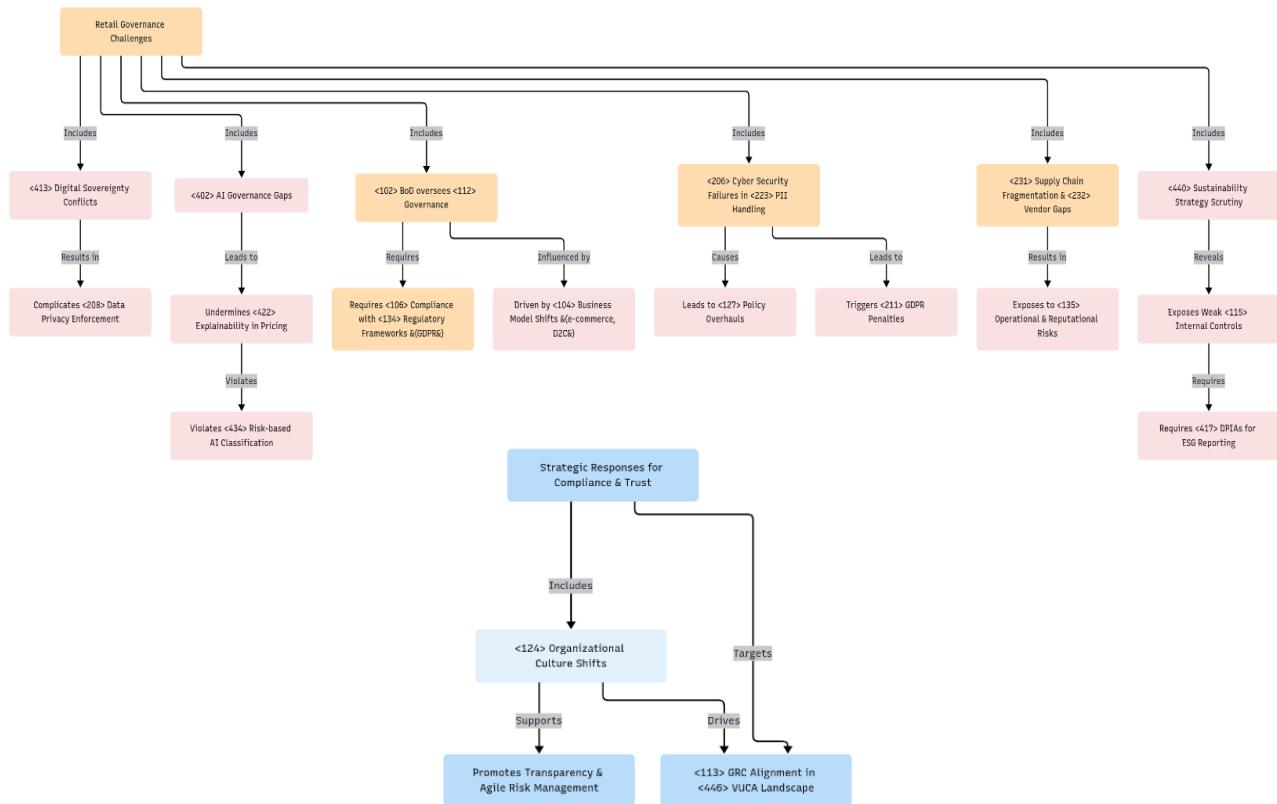
Textual Analysis

This industry is characterized by its unprecedented digital-physical convergence, where governance must simultaneously manage traditional retail operations while navigating complex platform ecosystems and data-driven business models. Retail governance faces unique challenges due to the sector's transformation into a global, platform-driven, and data-intensive ecosystem. Boards and executives must balance operational agility with compliance to multilayered regulatory frameworks such as GDPR, the Consumer Rights Directive, and the Digital Services Act. The complexity increases with hybrid models that combine brick-and-mortar stores, e-commerce, marketplaces, and direct-to-consumer brands.

Governance involves oversight of supply chains, vendor relationships, data protection, pricing transparency, and customer experience. Key risks include operational disruptions, reputational damage from poor service or regulatory breaches, cyber threats in payment and customer data systems, and compliance across diverse jurisdictions.

Strategic governance must adapt to challenges in platform dependency, data sovereignty, algorithmic accountability, and sustainability claims. Successful governance emphasizes transparency, agile risk management, and long-term brand stewardship within a dynamic regulatory and competitive landscape.

Structural Mapping

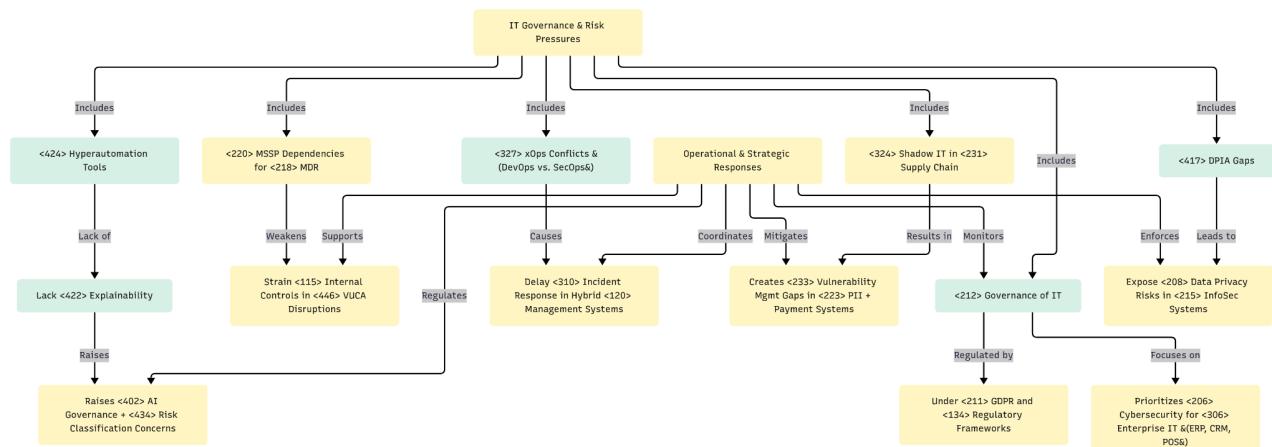


IT Management in Retail and Digital Commerce Industry

Textual Analysis

This industry is characterized by its hyper-connected digital ecosystem where IT governance directly impacts customer trust, regulatory compliance, and competitive differentiation. IT management in retail and digital commerce is defined by the necessity to secure complex omnichannel infrastructures while enabling digital transformation that enhances customer experience and operational efficiency. Critical systems include ERP, CRM, POS/ePOS, digital marketing platforms, and recommendation engines. The hybrid environment, combining legacy and modern headless commerce architectures, poses integration challenges. Security priorities focus on protecting payment systems, customer data, and fraud prevention under strict GDPR and Digital Services Act mandates. The rise of platform ecosystems and third-party service dependencies introduces vulnerabilities and governance gaps. IT leaders must manage data interoperability, real-time analytics, and system scalability while ensuring compliance and resilience. Emerging technologies like AI-driven personalization and dynamic pricing require robust controls to prevent ethical and operational risks. Incident response and recovery protocols align with evolving EU digital resilience frameworks.

Structural Mapping



Governance in Transport and Logistics

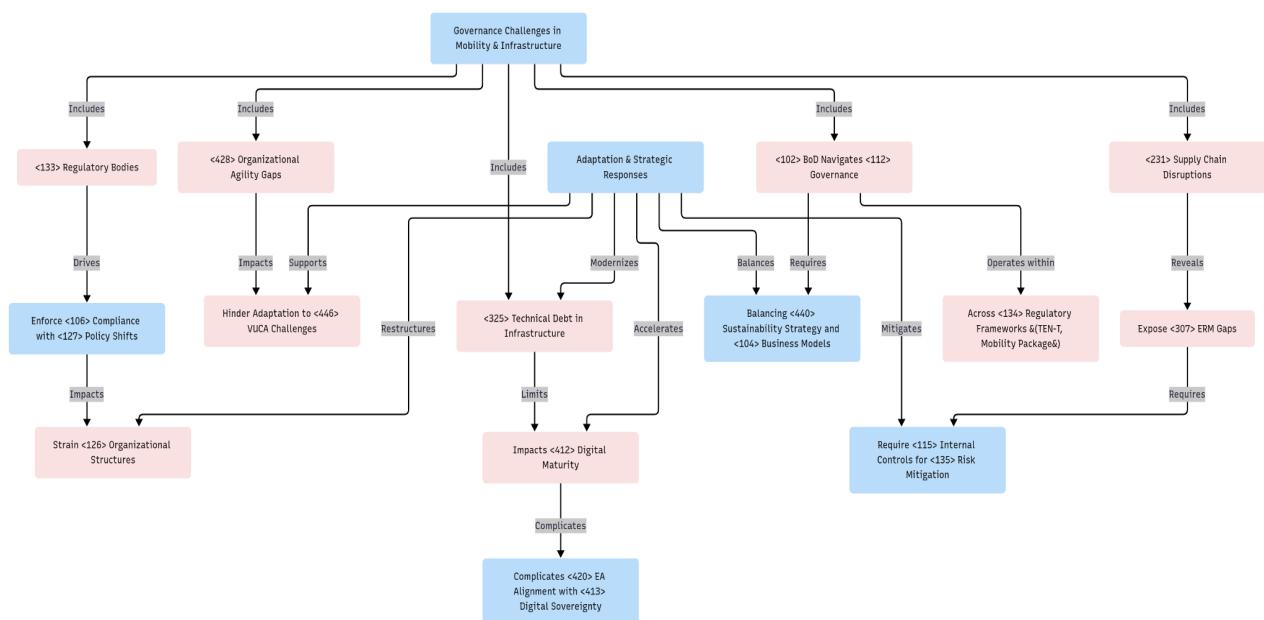
Textual Analysis

This industry is characterized by its complex interdependencies between physical infrastructure, regulatory frameworks, and technological innovation. Governance in the transport and logistics sector is multi-layered, involving coordination between infrastructure management, public mobility planning, and service delivery oversight. Many entities operate through public-private partnerships and are guided by regional, European, and international frameworks such as TEN-T, the EU Mobility Package, and the Sustainable and Smart Mobility Strategy.

Board-level governance must balance priorities such as service reliability, cost-efficiency, environmental sustainability, and user satisfaction. The sector is exposed to a broad spectrum of risks, including operational disruptions (accidents, delays), regulatory shifts (emissions, labor rights), and geopolitical tensions affecting freight and cross-border logistics.

Effective governance models must accommodate long asset life cycles, engage with regional and national planning bodies, and adapt to evolving labor standards, digital transparency obligations, and environmental targets. These dynamics require long-term, resilient governance strategies capable of coordinating across infrastructure, compliance, and innovation.

Structural Mapping



IT Management in Transport and Logistics

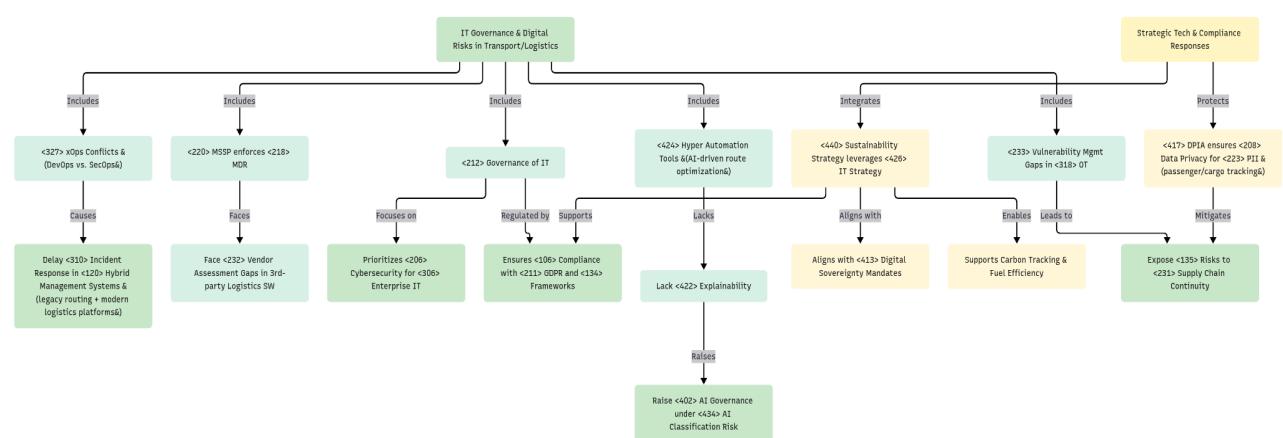
Textual Analysis

This industry is defined by its critical reliance on real-time data integration across multiple stakeholders, from fleet operators to customs agencies, creating unique IT management challenges. IT governance in the transport and logistics sector is driven by the need for real-time coordination, operational efficiency, and secure data exchange across complex networks. Core systems form the digital backbone of the modern supply chain.

CIOs are tasked with managing a hybrid environment where emerging technologies must integrate with legacy infrastructure. Interoperability is a key governance concern, requiring seamless communication between transport operators, customs authorities, and end-users. Regulatory compliance places added responsibility on IT leaders to secure personal and freight data, especially in passenger transport and e-commerce delivery platforms.

Cybersecurity risks are escalating, with threats targeting connected vehicles, routing systems, and coordination platforms. As a result, IT governance must enforce strong resilience standards, vendor accountability, incident response protocols, and continuous performance monitoring. Digital strategy also plays a critical role in supporting sustainability and through data-driven route optimization.

Structural Mapping



Comparative — Governance

Comparison 1: Energy vs Retail

Governance in the Energy sector is characterized by long-term planning, regulatory oversight, and a strong focus on infrastructure resilience. The <102> Board of Directors (BoD) is responsible for aligning strategy with national policy and <134> regulatory frameworks, ensuring compliance through formal mechanisms such as <123> Management System Standards (e.g., ISO standards) and structured <119> management frameworks. Key governance activities include <110> due diligence, <103> business continuity planning, and engagement with <133> regulatory bodies. The emphasis is on public accountability and operational stability, often supported by structured risk assessments and <201> Business Impact Analysis.

In contrast, governance in the Retail sector is more agile and market-driven. Retail boards focus on short-term performance, consumer satisfaction, and brand competitiveness. While compliance and ethical practices remain important, governance is less formalized and more decentralized. <113> GRC systems are integrated into business performance tools and adapted to support innovation and rapid decision-making. The retail governance model prioritizes adaptability, with <116> KPIs linked to sales, loyalty, and digital engagement rather than infrastructure or long-term public interest.

Comparison 2: Transport vs Retail

Governance in the transport sector is centered on safety, regulatory compliance, and infrastructure efficiency. The <102> Board of Directors (BoD) must navigate complex <134> regulatory frameworks related to public safety, environmental impact, and logistics coordination. Governance practices emphasize long-term planning, <110> due diligence in infrastructure investments, and <103> business continuity in the face of operational disruptions. To ensure consistency and compliance, organizations apply formal <119> management frameworks and <123> management system standards (such as ISO 39001 for road traffic safety). The sector also addresses operational risk, resilience, and interoperability across regions, often in partnership with public authorities. As mobility services become more data-driven, <113> GRC systems are evolving to include <208> Data Privacy, cybersecurity, and sustainability concerns.

In contrast, Retail governance focuses on flexibility, customer experience, and rapid decision-making. The <102> BoD is more concerned with brand differentiation, market responsiveness, and innovation. Governance is more decentralized and fluid, aiming to enable agile operations and quick product or service adaptations. While <106> compliance and ethical conduct are still relevant, they are more closely tied to consumer protection, sourcing standards, and digital privacy regulations. Retail increasingly integrates <114> IMS to align marketing, IT, and operations around unified brand and performance goals. As operations digitize, <107> Corporate Governance practices are expanding to include oversight of data ethics, personalization, and digital accountability, ensuring strategic growth aligns with responsible innovation.

Comparative — IT Management

Comparison 3: Energy vs Transport

The Energy sector's IT management is built around the stability and protection of critical infrastructure. Core systems such as SCADA are central to monitoring and controlling energy distribution, requiring robust <212> Governance of IT and adherence to <206> cybersecurity regulations such as NIS2. Energy organizations often implement formal <119> management frameworks and <123> Management System Standards to ensure compliance and operational resilience. Due to the high-risk nature of grid operations, IT assets are managed with a focus on <103> business continuity and <135> risk mitigation. <115> Internal controls and structured <217> ITSM practices are widely adopted to maintain system availability, data integrity, and national security interests.

In contrast, the Transport sector prioritizes IT systems that support logistics coordination, fleet visibility, and real-time operational decision-making. Fleet management platforms, route optimization tools, and sensor-integrated vehicles form the core of transport IT. Regulatory frameworks such as eFTI (electronic Freight Transport Information) mandate the digitalization and sharing of transport data across borders, requiring compliance with data governance and interoperability standards. While <212> Governance of IT remains relevant, transport IT governance tends to be more distributed and business-aligned. <208> Data privacy and information flow are key concerns, especially in multimodal and international logistics contexts. As a result, transport IT strategy leans toward flexibility, visibility, and cross-platform integration rather than infrastructure resilience.

Comparison 4: Retail vs Transport

The Retail sector's IT landscape is shaped by consumer interaction, personalization, and data governance. Technologies such as CRM systems, e-commerce platforms, and electronic point-of-sale (ePOS) systems are governed under frameworks that emphasize <208> Data Privacy, user experience, and digital consent mechanisms such as <221> opt-in. Retail organizations implement <212> Governance of IT with a focus on marketing analytics, customer profiling, and compliance with <211> GDPR. IT governance is often embedded within marketing and sales functions, and ethical concerns around data usage are increasingly central. As such, the sector prioritizes transparency, <106> compliance, and the ethical use of <223> PII (Personally Identifiable Information) to sustain consumer trust.

In the Transport sector, IT management is driven by operational efficiency and the secure handling of logistical and regulatory data. Systems used include fleet tracking, route optimization, and customs data processing, which must adhere to standards for <208> Data Privacy and international data sharing. <212> Governance of IT supports the coordination of multiple stakeholders—such as freight operators, port authorities, and customs agencies—under unified platforms, often guided by regulations like eFTI. While <211> GDPR compliance is also required, the focus is more on structured data exchange and <103> business continuity. Unlike retail, where IT supports engagement and personalization, transport IT emphasizes safety, traceability, and operational reliability across complex supply chains.

P1

SGSI 2024/2025

102082	Simão Sanguinho
102779	João Mestre
103252	José Pereira
103560	Miguel Benjamim
104010	Antonio Oliveira

Industries.....	2
Energy and Utilities.....	2
Organizations, Governance, and Management.....	2
Governance of IT and IT Management.....	3
Retail and Digital Commerce.....	4
Organizations, Governance, and Management.....	4
Analysis of Omnichannel Retail for Consumer Electronics.....	4
Concept Map.....	4
Governance of IT and IT Management.....	5
Analysis.....	5
Concept Map.....	5
Hospitality and Leisure.....	6
Organizations, Governance, and Management.....	6
Governance of IT and IT Management.....	7
Industry Comparisons.....	8
Organizations, Governance, and Management.....	8
Energy and Utilities vs Retail and Digital Commerce.....	8
Hospitality and Leisure vs Energy and Utilities.....	8
Governance of IT and IT Management.....	9
Energy and Utilities vs Retail and Digital Commerce.....	9
Hospitality and Leisure vs Retail and Digital Commerce.....	9

Industries

Energy and Utilities

Organizations, Governance, and Management

Analysis of Distribution System Operators

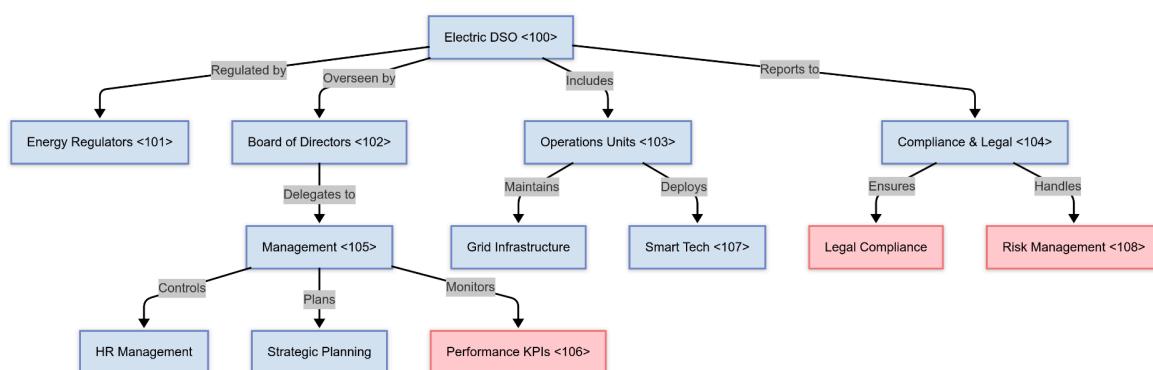
Electric Distribution System Operators <100> manage regional and local power distribution networks under strict regulatory oversight by Energy Regulators <101>. Their structures typically combine geographic divisions with central functional areas, including Operations Units <103>, Compliance & Legal <104>, and Strategic Planning coordinated through Management <105>. A Board of Directors <102> oversees strategic decisions, supported by committees focused on Risk Management <108>, sustainability, and finance.

These organizations operate within regulated frameworks that dictate performance targets, investment levels, and service reliability standards. National regulators such as ERSE or Ofgem <101> play a critical role in shaping DSO <100> priorities. Internally, Management <105> focuses on maintaining Grid Infrastructure, optimizing resources, and incorporating Smart Tech <107> innovations. Key performance indicators such as SAIDI and SAIFI, tracked under Performance KPIs <106>, help monitor service continuity.

Compliance & Legal <104> teams ensure adherence to legal standards <104> and manage enterprise risks <108>. Asset management is increasingly supported by digital tools for predictive maintenance and smart grid upgrades.

DSOs <100> also face mounting pressure to integrate low-carbon technologies like solar panels, electric vehicles, and smart meters. This drives the need for stronger coordination between technical operations <103> and Strategic Planning <105>. Governance structures must balance regulatory compliance <104>, operational efficiency <103>, and long-term transformation goals.

In this context, DSOs <100> operate as both utility providers and digital infrastructure managers. Their success depends on agile governance from the Board <102> and well-aligned Management systems <105> capable of adapting to energy transition demands while maintaining high service quality tracked through KPIs <106>.



Governance of IT and IT Management

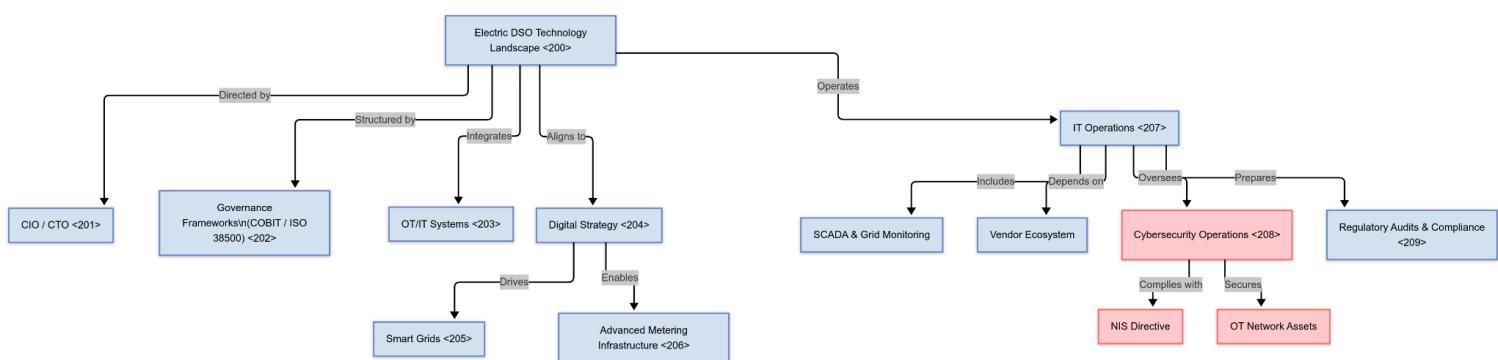
Analysis of Distribution System Operators

In modern Electric Distribution System Operators <200>, the technology landscape is governed by a structured and integrated approach that aligns leadership, strategic planning, and operations. IT governance is directed by senior roles such as the CIO / CTO <201> and structured around formal governance frameworks like COBIT and ISO 38500 <202>, which help ensure regulatory compliance, performance alignment, and effective decision-making.

At the core of this governance is the integration of OT/IT Systems <203>, enabling capabilities such as Smart Grids <205> and Advanced Metering Infrastructure <206>. These technologies form the digital backbone of modern DSOs <200>, supporting real-time grid management, energy consumption tracking, and automated fault detection. A clearly defined Digital Strategy <204> guides this evolution, ensuring that infrastructure investments support operational efficiency and long-term resilience.

IT Operations <207> serve as the functional core, encompassing critical systems such as SCADA & Grid Monitoring, as well as an ecosystem of external vendors <207>. These vendors supply essential tools and services, meaning vendor management is a key component of IT oversight. Operations also include Cybersecurity Operations <208>, which is no longer treated as a separate function but as a fully integrated layer governed by both compliance needs and operational risk. DSOs <200> must meet regulatory obligations under the NIS Directive <208> and are responsible for securing OT Network Assets <208> from emerging cyber threats.

Finally, Regulatory Audits & Compliance <209> are built into IT governance, ensuring that security measures, operational integrity, and data privacy are continuously monitored and validated. Together, these elements form a tightly integrated system that enables DSOs <200> to operate safely, efficiently, and in alignment with energy transition goals.



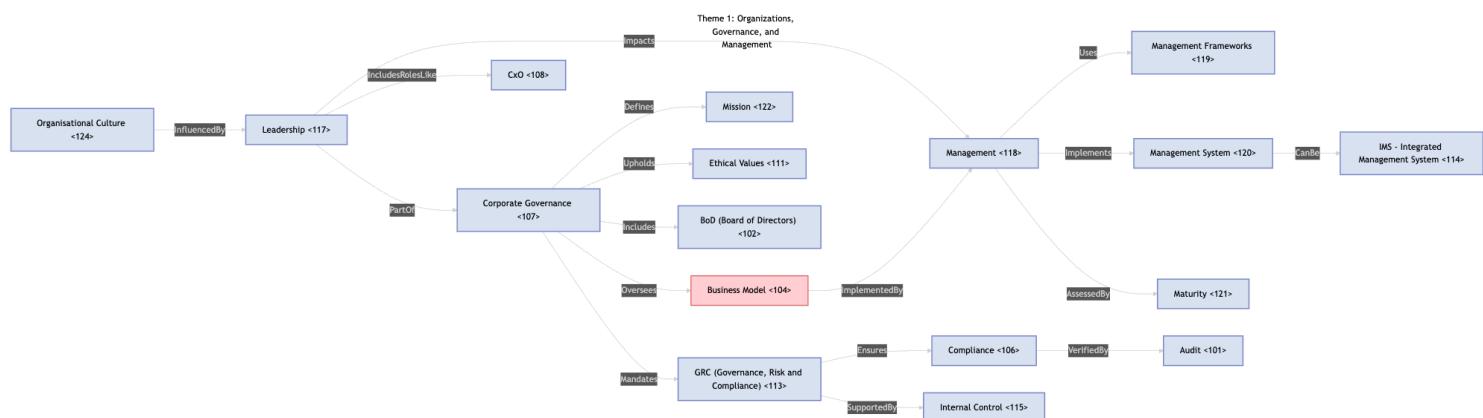
Retail and Digital Commerce

Organizations, Governance, and Management

Analysis of Omnichannel Retail for Consumer Electronics

In the competitive sphere of omnichannel consumer electronics retail, a well-defined structure for organizations, governance, and management is crucial. Corporate Governance <107>, typically spearheaded by the BoD (Board of Directors) <102>, sets the foundational direction. This involves articulating a clear Mission <122> and upholding core Ethical Values <111>. It ensures the Business Model <104> is strategically designed to create, deliver, and capture value effectively, while also considering diverse stakeholder interests.

Effective Management <118> translates this strategic vision into operational reality. This is achieved by employing suitable Management Frameworks <119> to guide activities and implementing robust Management Systems <120>—potentially an IMS - Integrated Management System <114>—to ensure consistent execution and quality. The overall organizational Maturity <121> in these systems and processes is a key determinant of success and adaptability. A critical pillar supporting this is a comprehensive GRC (Governance, Risk and Compliance) <113> strategy. This framework ensures strict Compliance <106> with relevant legal and regulatory obligations. It also embeds proactive risk-aware practices, supported by effective Internal Control <115> mechanisms and regular Audits <101> to verify efficacy. Finally, the prevailing Organisational Culture <124> (or <125>), shaped significantly by Leadership <117>, plays an indispensable role in fostering an environment conducive to achieving strategic goals and driving necessary organizational change and technological adoption. Key CxO <108> roles are central to this leadership.

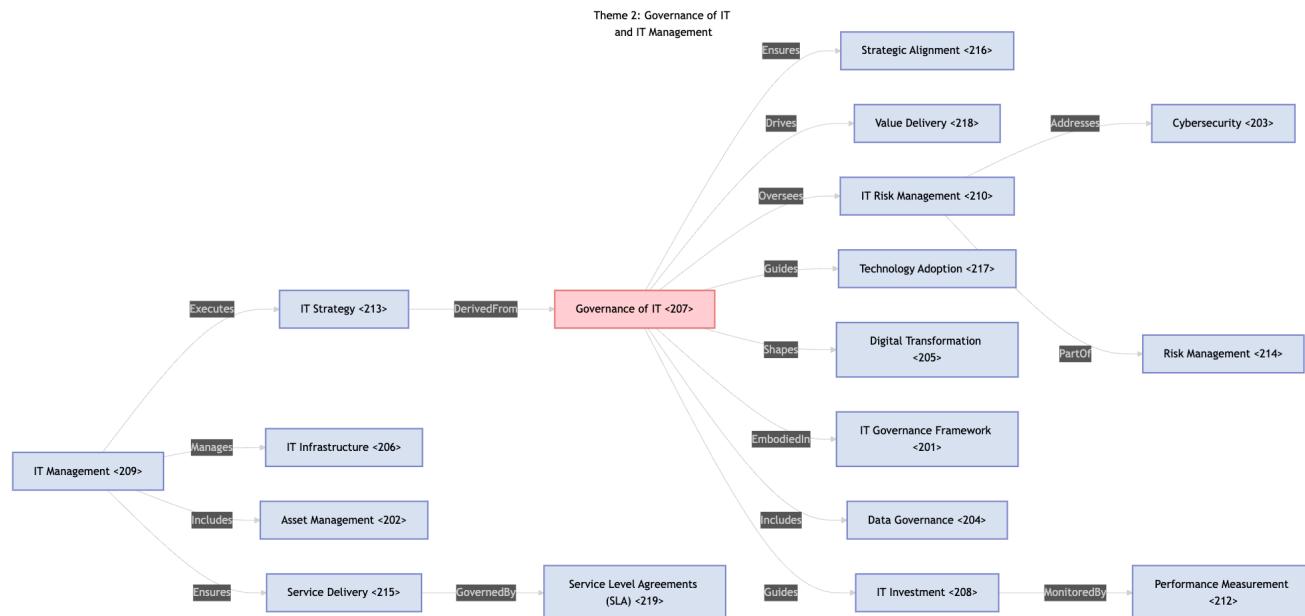


Governance of IT and IT Management

Analysis of Omnichannel Retail for Consumer Electronics

In the technology-centric domain of omnichannel electronics retail, robust Governance of IT <207> is indispensable. Its core purpose is to ensure that all information technology efforts are in strict Strategic Alignment <216> with overarching organizational objectives. This involves directing IT resources towards achieving maximum Value Delivery <218>—enhancing efficiency and competitive advantage—while diligently overseeing IT Risk Management <210> (which includes managing IT Risk <211>) to safeguard digital assets and operational integrity. This governance also guides Technology Adoption <217> and the path of Digital Transformation <205>.

Effective IT Management <209> is responsible for the execution of the IT Strategy <213>. This encompasses the planning, development, operation, and continuous improvement of IT systems and services, including IT Infrastructure <206> and Asset Management <202>. Key activities include managing essential business applications to support customer engagement, ensuring resilient Service Delivery <215> (often governed by Service Level Agreements (SLA) <219>), and adopting established methodologies for IT service processes. Within the scope of IT governance, particular emphasis is placed on maintaining stringent Cybersecurity <203> measures, which forms a critical part of broader Risk Management <214>. Furthermore, robust Data Governance <204> practices are essential for managing data assets and supporting adherence to legal and regulatory obligations. Strategic IT Investment <208> decisions must also be carefully governed to ensure they yield the intended benefits, with ongoing Performance Measurement <212> to track results. Comprehensive guiding structures, sometimes referred to as an IT Governance Framework <201>, can provide a valuable structure for overseeing enterprise IT. Ensuring Resilience <215> is a fundamental operational imperative.



Hospitality and Leisure

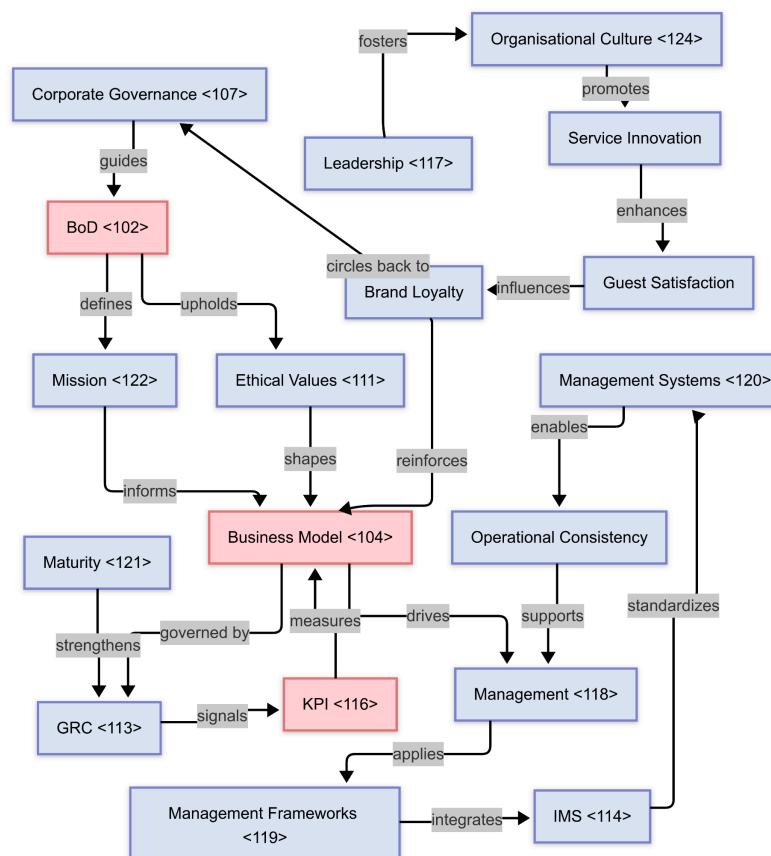
Organizations, Governance, and Management.

Analysis of large hotel chains

A well-structured governance and management approach is essential for delivering consistent, high-quality guest experiences across widespread operations. Corporate Governance <107> provides the strategic foundation, defined and directed by the BoD <102>. They articulate a clear Mission <122> and uphold essential Ethical Values <111>, which shape the brand's public image and internal accountability structures. These values influence the design of the Business Model <104>, which seeks to balance profitability with value creation across service offerings and customer segments.

Operational effectiveness is driven by capable Management <118> using structured Management Frameworks <119> and coordinated Management Systems <120>, often unified under an Integrated Management System <114>. These tools translate strategic direction into consistent delivery across properties. A comprehensive Governance, Risk and Compliance <113> approach ensures Compliance <106> with legal, ethical, and operational requirements, backed by robust Internal Control <115> mechanisms. These systems are regularly assessed through Audits <101>, with KPIs <116> providing real-time insights into performance metrics like occupancy and revenue per available room.

Sustainable success depends on the organization's Maturity <121> in deploying these systems and adapting to change. Leadership <117> plays a critical role here—guiding not just execution, but shaping an Organisational Culture <124> that promotes service innovation and guest-centric thinking. This interconnected framework—linking governance, risk, operations, and culture—supports resilience and long-term competitive advantage.



Governance of IT and IT Management

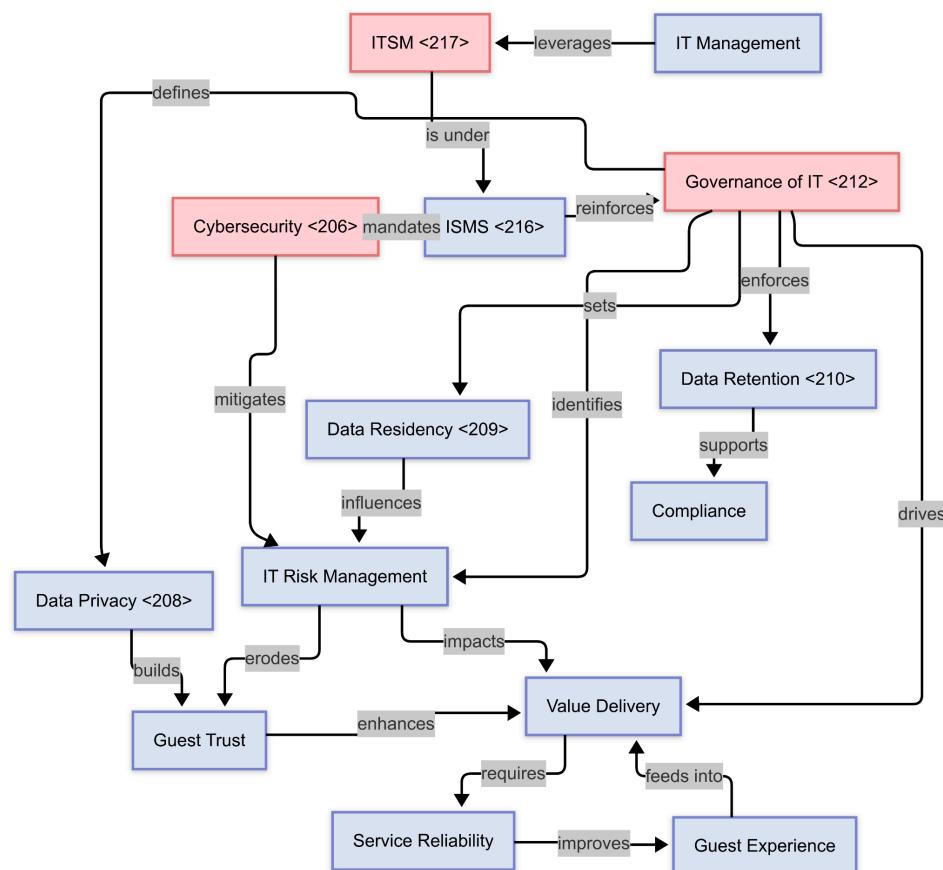
Analysis of large hotel chains

Governance of IT <212> sets out who makes decisions about technology and establishes the rules everyone follows to keep systems running smoothly . It makes sure that all digital tools—from online booking engines to guest-facing mobile apps—work toward clear business goals without unexpected risks getting in the way.

Part of this work is looking after guest information. Strong Data Privacy <208> policies protect personal details and define how they can be used . Data Residency <209> rules make sure data stays in approved locations so it follows local laws , while Data Retention <210> schedules determine how long records are kept to meet legal or operational needs . Together, these measures build trust and keep the chain on the right side of regulations.

On a day-to-day basis, IT teams follow ITSM <217> practices to log issues, manage changes, and deliver services consistently . An ISMS <216> wraps around these practices to oversee information-security processes, from detecting incidents to learning from them . A solid Cybersecurity <206> approach—backed by monitoring and response plans—helps prevent outages and keeps guest services available without interruption .

As part of their digitization initiatives, hotel chains are adding small but impactful improvements—like faster self-service kiosks, mobile key check-in, and more intuitive booking screens—that slot neatly into existing governance and risk-management frameworks. These targeted changes boost efficiency and make stays more convenient, all while keeping control firmly in place.



Industry Comparisons

Organizations, Governance, and Management

Energy and Utilities vs Retail and Digital Commerce

National energy providers vs global e-commerce platforms

Energy utilities operate in a heavily regulated environment with formal, top-down **Governance** structures. Oversight is driven by **Regulatory bodies**, guided by strict **Regulatory frameworks**, and monitored through **Internal Controls** and regular **Audits**. These organisations often have hierarchical **Organizational Structures**, with governance tied to public service obligations and **BoD** oversight. Governance maturity **Maturity** is typically high, emphasizing risk mitigation **Risk** and long-term planning.

Retail and digital commerce companies, such as Amazon, operate under dynamic market conditions. Governance focuses on agility, innovation, and customer responsiveness. These firms use flexible **Management Frameworks**, real-time **KPIs**, and data-driven **Management Systems**. Their **Governance** prioritizes fast decision-making, digital risk **Risk** controls, and investor confidence. Compliance **Compliance** is integrated into operations but often more decentralized than in utilities.

In summary, utilities emphasize stability and compliance, while digital commerce values adaptability and speed, reflecting differences in **Maturity** and strategic governance priorities.

Hospitality and Leisure vs Energy and Utilities

Chain restaurants vs regional energy providers

Chain restaurants often rely on centralized **Policies** and standard **Procedures**, but their local execution introduces variability. Governance structures tend to be less formal, with moderate **Maturity**. Compliance **Compliance** focuses on health and safety, monitored by **Audits** and **Certifications**. Governance is operationally focused and influenced by local managers more than structured boards.

In contrast, energy utilities maintain structured, formal **Governance** aligned with regulatory expectations. They use clear **RACI models**, mature **GRC systems**, and robust oversight through their **BoD**. Their **Organisational Culture** is risk-averse and safety-focused, reflecting public accountability and long-term infrastructure needs.

Restaurants need flexible governance to adapt quickly, while utilities prioritize predictability and control. These differences show contrasting levels of governance maturity **Maturity** and strategic focus across industries.

Governance of IT and IT Management

Energy and Utilities vs Retail and Digital Commerce

National energy providers vs global e-commerce platforms

Energy and utilities are often characterized by a highly regulated environment and long-term infrastructure projects, whereas retail and digital commerce entities operate in fast-moving markets with frequent innovation cycles and direct consumer engagement.

In the energy utilities sector, governance structures are tightly aligned with regulatory mandates and national energy policies. Companies like EDP must comply with rigorous [Governance of IT](#) standards to maintain operational stability and meet public service obligations. Risk is managed with comprehensive [BIA](#) assessments and stringent [InfoSec](#) frameworks to ensure continuity and reliability of energy supply.

By contrast, digital commerce platforms such as Amazon operate with more dynamic and customer-centric governance models. IT Management here focuses on scalability, speed, and seamless user experience, relying heavily on cloud infrastructure and AI-powered analytics. Governance in this sector is agile, with continuous integration of [Data Privacy](#), [GDPR](#) compliance, and [Consent Mechanisms](#) into customer data operations. These firms lead in [Privacy-by-design](#) and have high [MSSP](#) and [MDR](#) integration to handle cybersecurity threats. Their strategic alignment of IT is driven by predictive data models and [ITSM](#) best practices, enabling rapid adaptation to market trends. Unlike energy utilities, their digital risk posture is proactive, emphasizing real-time monitoring and supply chain agility through robust [Supply Chain](#) governance.

Hospitality and Leisure vs Retail and Digital Commerce

Hotel chains vs global e-commerce platforms

Hospitality enterprises such as Marriott or Accor manage diverse operational environments that blend physical service delivery with digital engagement. These organizations face significant challenges in harmonizing [IT Governance](#) across geographies while ensuring [Data Privacy](#) and compliance with [GDPR](#) in customer-facing systems. Strong [IAM](#) policies and [InfoSec](#) practices are essential to protect [PII](#) during reservations, payments, and loyalty program interactions. Their governance approach often includes risk controls such as [BIA](#) and [ISMS](#) to support business continuity during service disruptions or cyber incidents.

In contrast, retail and digital commerce platforms manage vast, cloud-native ecosystems with real-time data collection and algorithmic decision-making. These firms face more intensive [Cybersecurity](#) challenges due to the scale and variety of data transactions. Governance maturity is typically higher due to embedded [Privacy-by-design](#) principles and automated [Opt-in](#) consent mechanisms. While hospitality emphasizes customer experience and operational uptime, retail prioritizes scalability, with governance models focused on [Vulnerability Management](#) and supplier risk assessment.

Group Work 1

Security and Management of Information Systems - 2025

Hyunseo Kim (115478)

Jiseung Choi (115651)

Camila Melendez (115587)

Samuel Lee Cordon (112860)

Energy and Utilities - Governance

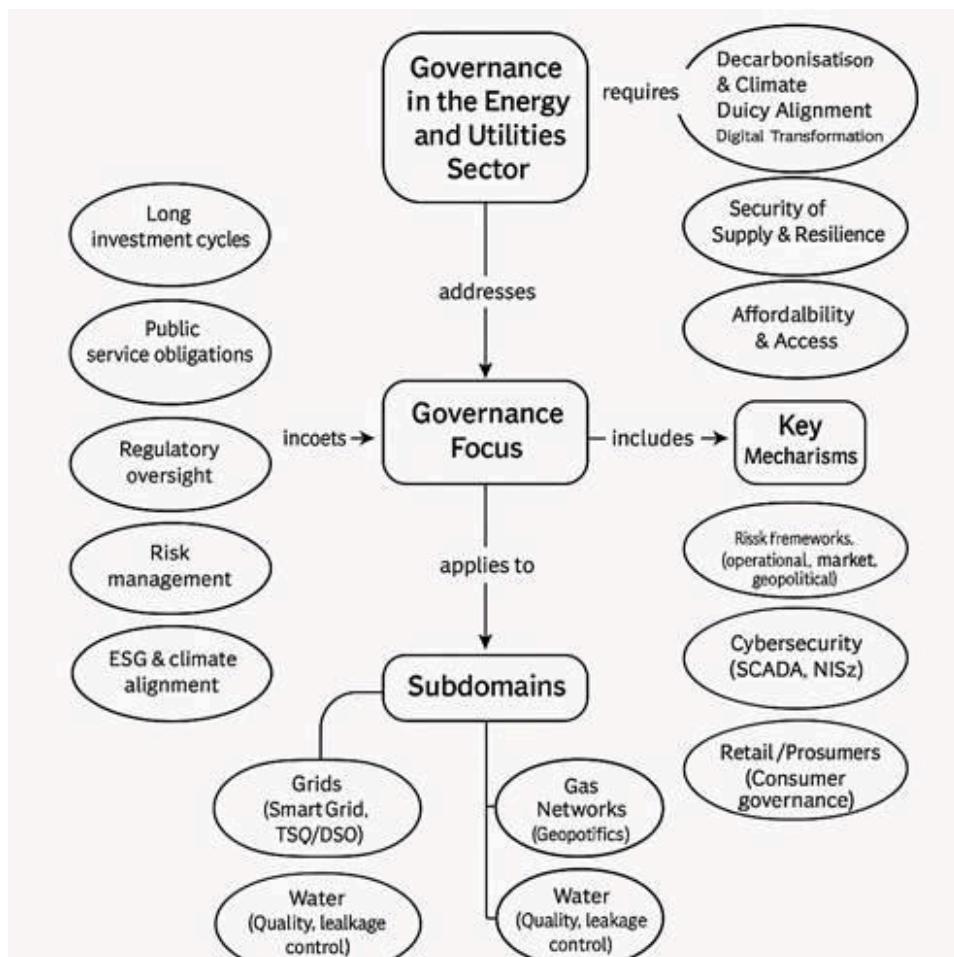
The energy and utilities sector delivers essential services like electricity, gas, and water, demanding robust governance to ensure reliability, safety, and sustainability. Governance must balance long-term infrastructure planning with short-term risk management, while aligning with evolving climate and digital policies.

Modern governance involves:

- Strategic oversight by boards;
- Compliance with complex environmental and market regulations;
- Risk controls against outages, price shocks, and cyber threats;
- Cyber/IT governance, especially for smart systems (e.g. SCADA, meters).

European governance frameworks (e.g. Green Deal, Clean Energy Package) emphasize decarbonisation, consumer empowerment, and interoperable systems, with NIS2 addressing cyber risks in critical infrastructure.

Across subdomains—electricity, gas, water, heating, retail—governance adapts to sector-specific risks and public needs. Increasingly, ESG reporting and stakeholder engagement shape how companies are held accountable, especially as energy becomes more digital, decentralised, and decarbonised.



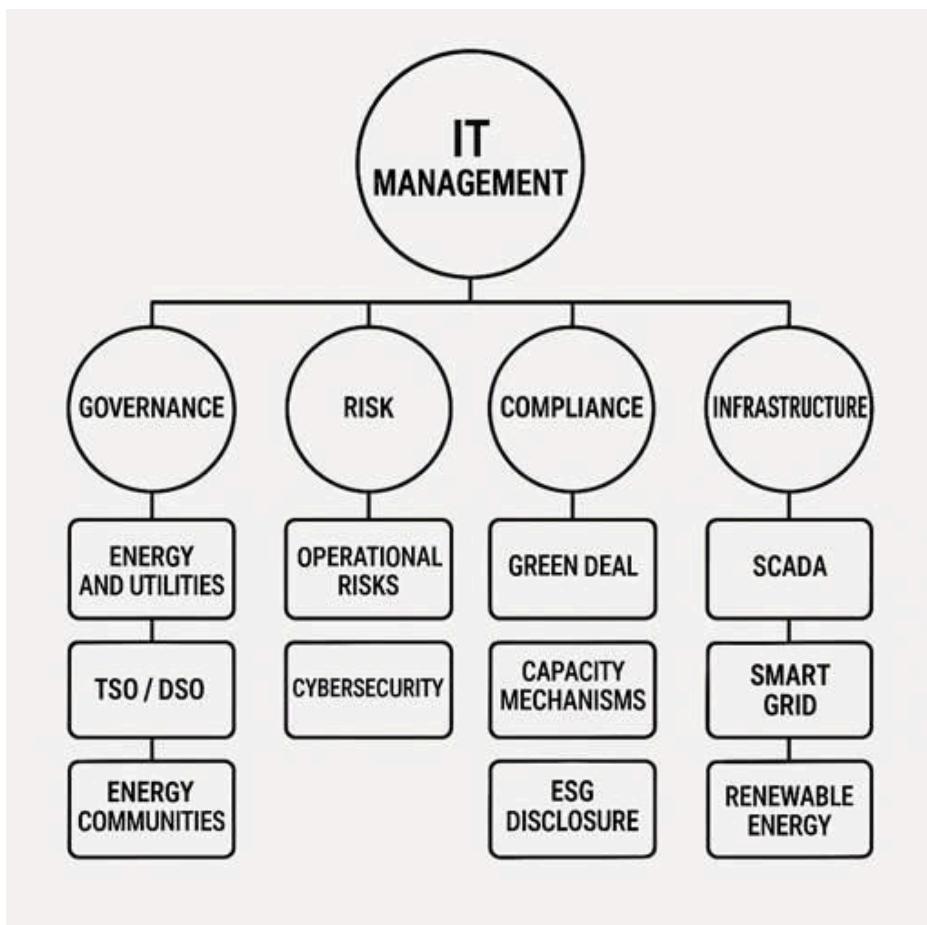
Energy and Utilities - IT management

In the energy and utilities sector, IT management plays a central role in enabling reliable operations, regulatory compliance, and digital innovation. As systems modernise, the convergence of IT and operational technology (OT)—like SCADA, sensors, and smart meters—demands integrated, secure, and resilient IT governance.

Key IT priorities include:

- Cybersecurity: With critical infrastructure at stake, sector-wide adherence to directives like NIS2, and standards such as ISO 27001, is essential.
- Data Management: Utilities must manage large volumes of data for grid balancing, predictive maintenance, billing, and ESG reporting.
- Digital Platforms: From energy trading systems to customer portals, modern IT supports real-time transactions and user engagement.
- AI & Analytics: Used in demand forecasting, system optimisation, and fault detection, AI boosts efficiency and sustainability.
- Cloud and Edge Computing: These technologies enable scalable, distributed energy control and support real-time system visibility.

Effective IT management in this context relies on structured frameworks (e.g., ITIL, COBIT) to ensure reliability, security, and alignment with evolving digital strategy and regulation.



Retail and Digital Commerce - Governance

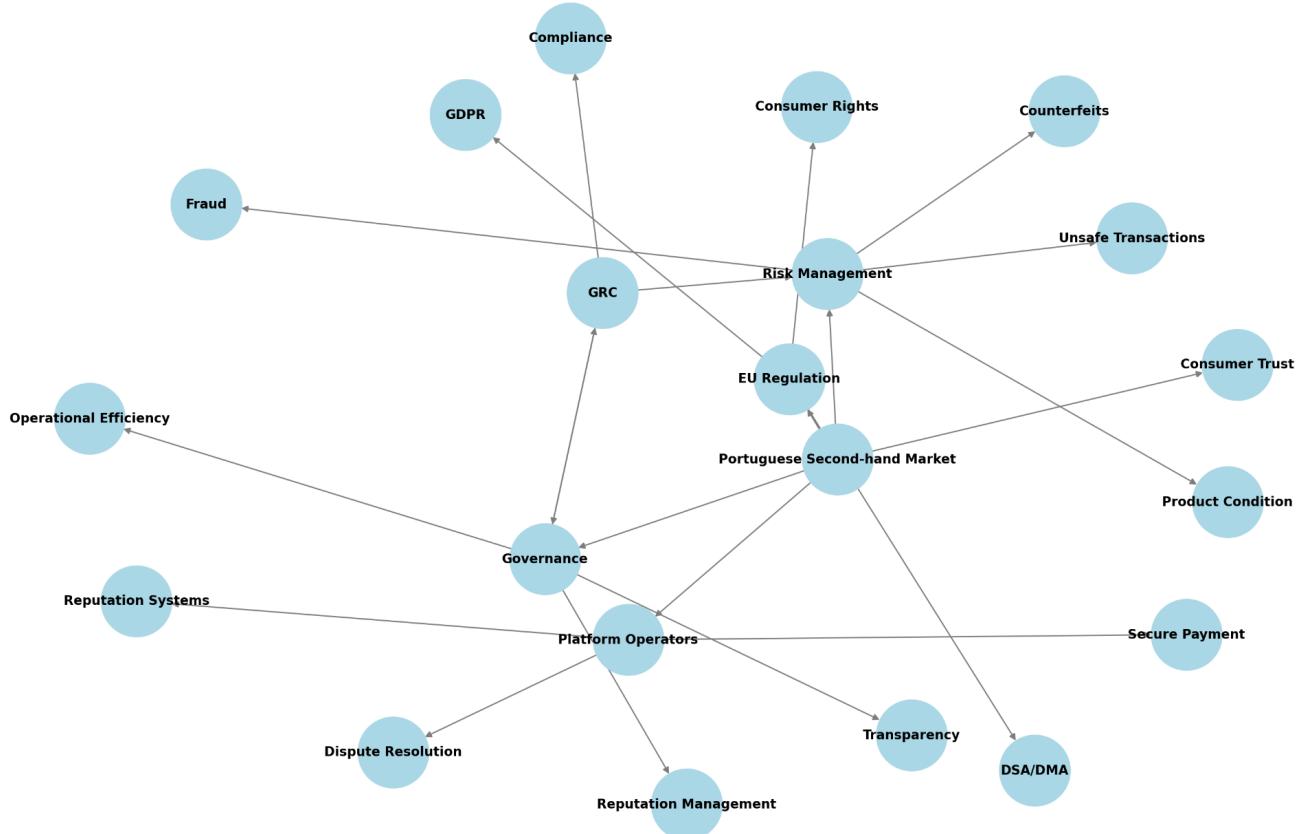
Portugal's second-hand market includes a mix of traditional and digital formats. Common forms are **C2C transactions** via platforms like **OLX**, **CustoJusto**, and **Facebook Marketplace**, enabling direct item exchanges. **Physical shops** such as **Humana** focus on second-hand clothing with social and environmental goals. **Flea markets** like **Feira da Ladra** offer informal, community-based trading. Recently, apps like **Vinted** have gained popularity among younger users, emphasizing fashion resale and convenient shipping.

Given the specific characteristics of second-hand trade, the necessity for a robust governance system that secures market participants' trust and enhances transparency is even more pronounced.

Governance is closely linked to managing operational risks and complying with relevant laws and regulations. As a member state of the European Union (EU), Portugal is significantly influenced by various EU regulatory frameworks. Therefore, entities operating second-hand trading platforms or conducting related businesses must strictly adhere to GDPR regulations regarding the protection of user personal data and EU directives concerning consumer rights. As noted in the document, businesses (B2C) specializing in selling second-hand goods have minimum obligations regarding quality and product description, albeit perhaps at a different level than for new products, and establishing internal processes and policies for this is also a crucial part of Governance. Furthermore, if a platform grows beyond a certain size, it may become subject to platform regulations such as the EU's Digital Services Act (DSA) or Digital Markets Act (DMA), and understanding and preparing for these is also within the domain of Governance.

Risks inherent to the second-hand market, such as discrepancies in product condition, counterfeit goods transactions, fraud risks, and unsafe transaction methods, must be managed through an effective Governance system. Platform operators should establish reliable reputation systems, secure payment methods (e.g., escrow), and clear procedures for resolving disputes to ensure users can transact with confidence.

Concept Map: Governance in the Portuguese Second-hand Market



Retail and Digital Commerce - IT Management perspective

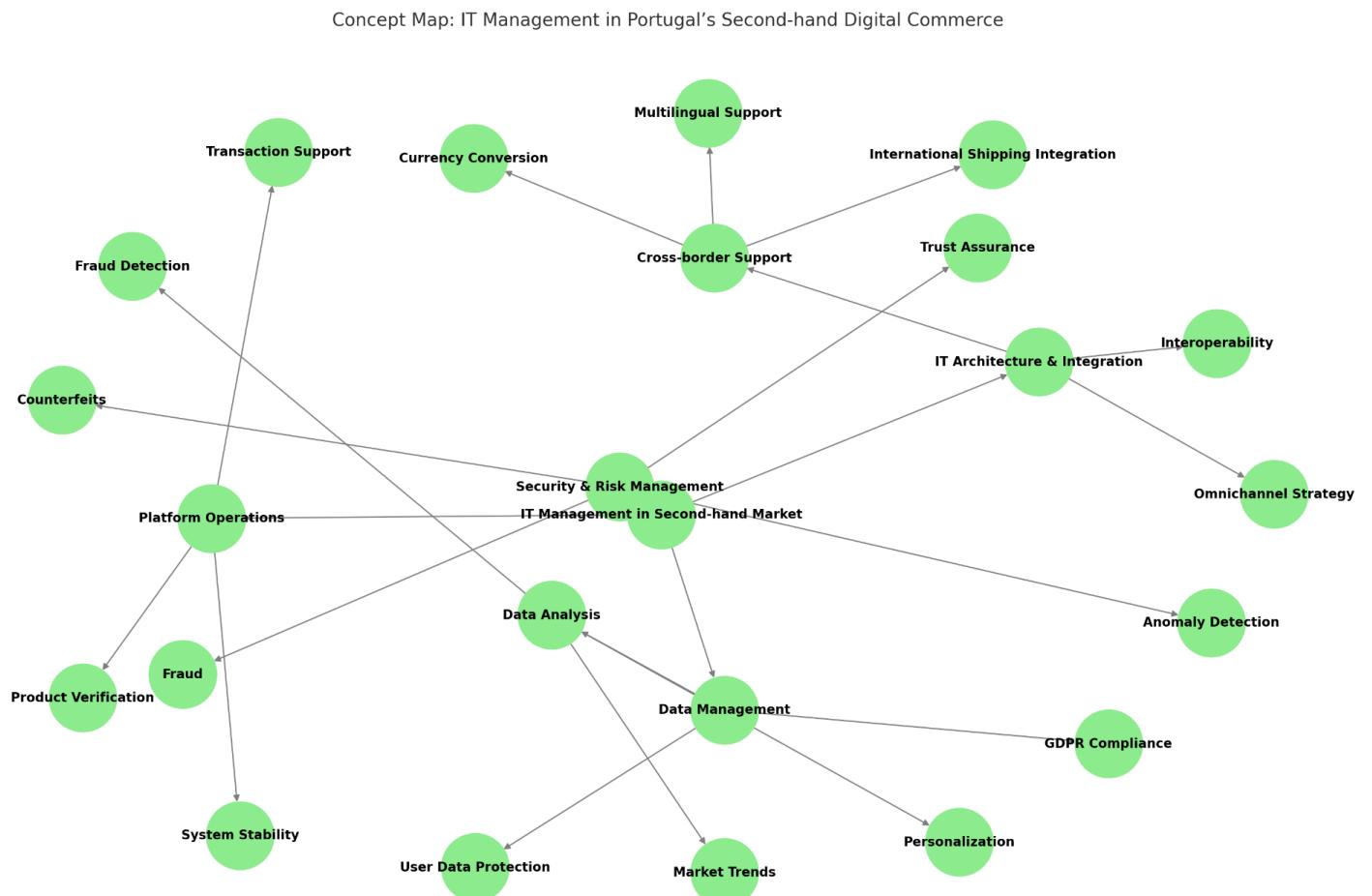
From an IT Management perspective, the second-hand retail and digital commerce market in Portugal involves several complexities. At the core of this market are digital platforms, which serve as the infrastructure connecting buyers and sellers and supporting the entire transaction process. A primary task of IT Management is to ensure that these platforms operate stably and efficiently. Especially in second-hand transactions, accurate product condition descriptions and authenticity verification are vital, requiring IT systems to provide supporting functionalities.

Data management is another core area for IT Management. Vast amounts of data, including user profiles, transaction history, product information, and search patterns, are generated during platform operation. Under EU regulations like GDPR, securely collecting, storing, and processing this data, and rigorously complying with user personal data protection obligations, is a critical responsibility of IT Management. Furthermore, IT systems

are utilized for data analysis to identify market trends, provide personalized recommendations, and detect potential fraudulent transactions.

The Portuguese second-hand market features a coexistence of large international platforms such as OLX and Vintered alongside local and specialized platforms, which presents considerations regarding IT architecture and interoperability. For platforms specializing in specific categories or adopting omnichannel models linking online and offline, designing and implementing IT solutions optimized for each business model is crucial. Additionally, in the cross-border trading environment of the EU, technical complexities arise, including multilingual support, currency conversion, and integration with international shipping systems, necessitating an efficiently managed IT infrastructure.

Finally, risks inherent to the second-hand market (e.g., fraud, counterfeits) demand the establishment of robust security and risk management systems. The IT management team must minimize these risks and ensure user trust through measures like enhanced transaction monitoring systems and anomaly detection systems.



Agriculture and Farming - Governance

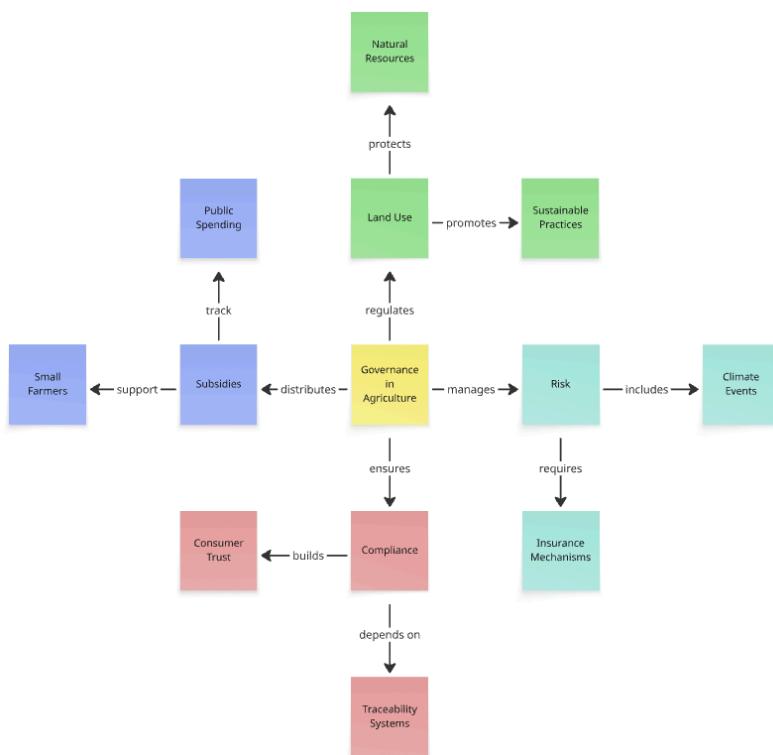
The agriculture and farming industry is one of the oldest organised sectors in human history, but today it operates within a much more complex system. Governance in this field has to balance traditional practices with modern challenges like climate change, digital transformation, and global trade. Because the sector includes both small family-run farms and large multinational agribusinesses, governance structures need to be flexible enough to address very different needs.

Modern governance in agriculture involves:

- **Land use and environmental regulation:** Making sure farming practices align with sustainability goals, biodiversity protection, and water/soil conservation.
- **Risk management:** Preparing for weather events, disease outbreaks, and market volatility that can threaten productivity and livelihoods.
- **Compliance with food safety and health standards:** Ensuring traceability from farm to fork, especially important for consumer trust and legal requirements.
- **IT and digital governance:** Managing technologies like precision agriculture, satellite monitoring, and farm management systems, while also supporting smaller producers who may still rely on informal tools.
- **Subsidy and policy oversight:** Tracking government aids and ensuring fair access, especially in places with major public programs like the EU's Common Agricultural Policy (CAP).

Across its different subdomains (crop and animal farming, agroforestry, processing, and agricultural finance) governance also needs to address broader strategic issues like adapting to climate risks, ensuring land tenure transparency, and integrating sustainability into production methods.

So, governance in agriculture isn't just about following rules. It's about helping a diverse and essential industry evolve, stay resilient, and meet growing global demands.



Agriculture and Farming - IT Management

The agriculture and farming industry has become increasingly dependent on digital tools and data-driven processes. As farms and agribusinesses face challenges like climate change, food security, and global supply chain pressures, effective IT management is becoming central to operations, planning, and sustainability.

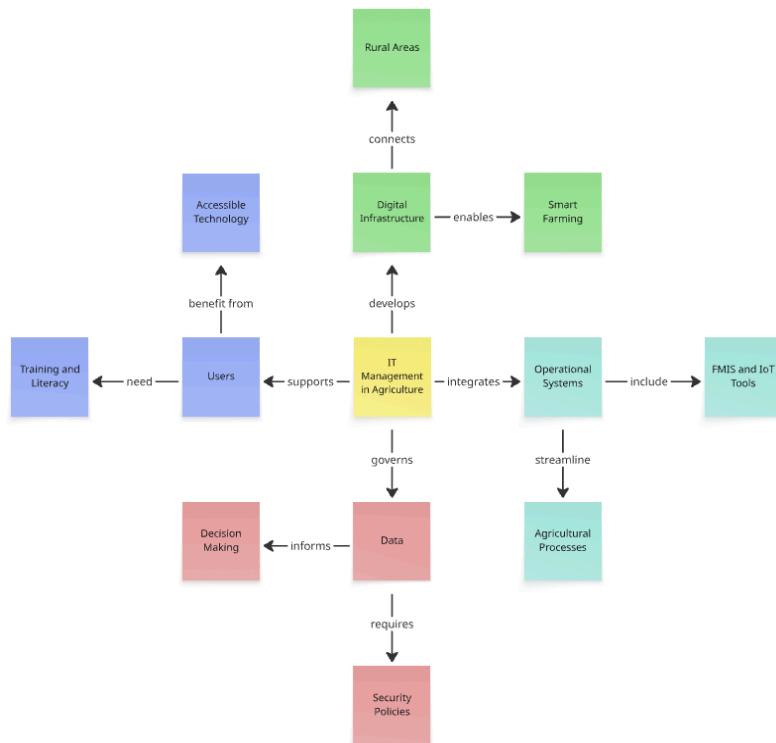
Unlike highly digitised industries, agriculture presents a unique mix of high-tech innovation and low-tech realities. IT management must navigate a wide spectrum of needs: from small farms using basic spreadsheets to large agribusinesses running advanced analytics and AI tools.

IT management in agriculture includes:

- **Infrastructure management:** Deploying and maintaining reliable networks, especially in rural or remote areas with limited connectivity.
- **System integration:** Linking various platforms like Farm Management Information Systems (FMIS), precision agriculture tools, and supply chain software.
- **Data governance:** Managing farm data securely and ethically, especially as more operations depend on cloud platforms and IoT sensors.
- **User support and digital literacy:** Helping farmers and rural cooperatives use technology effectively, often with limited training or resources.

IT managers in this sector also have to think strategically: choosing the right tools, scaling systems for different farm sizes, and making sure data collected from the field actually leads to useful decisions.

Overall, IT management in agriculture is about more than just keeping systems running. It plays a key role in transforming how food is grown, processed, and delivered, making the sector more resilient, efficient, and future-ready.



Comparison from a governance perspective

Energy and Utilities vs. Retail and Digital Commerce

Governance within Energy and Utilities meticulously balances long-term infrastructure planning with immediate risk mitigation. Strategic oversight is stringent, driven by extensive compliance requirements, exemplified by EU frameworks such as the Green Deal and NIS2 directive. For instance, regulations mandate strict adherence to cybersecurity practices protecting critical infrastructure. Conversely, Retail and Digital Commerce governance concentrates predominantly on safeguarding consumer trust through robust data protection and transaction transparency, leveraging mechanisms such as GDPR compliance and platform-specific regulations like the EU's Digital Services Act (DSA). The governance here is consumer-centric, illustrated by reputation systems and dispute resolution mechanisms fundamental to platforms like OLX and Vinted.

Energy and Utilities vs. Agriculture and Farming

Governance in Energy and Utilities is characterized by structured regulatory compliance focusing heavily on sustainability and cyber resilience, shaped by policy frameworks such as the EU Clean Energy Package. For example, stringent environmental governance requirements guide the decarbonization of utilities. Agriculture governance, however, demands a broader, more adaptive approach due to sectoral diversity—ranging from small family farms to large agribusinesses. Regulations like the EU Common Agricultural Policy (CAP) exemplify governance mechanisms tailored to manage environmental sustainability and market volatility, balancing traditional practices with contemporary digital and environmental standards.

Retail and Digital Commerce vs. Agriculture and Farming

Retail and Digital Commerce governance primarily addresses consumer protection, data governance, and risk mitigation of transactional fraud, as observed in platforms like Vinted, which emphasize authenticity verification and secure payments. Agriculture governance, by contrast, spans wider concerns including sustainability, biodiversity protection, and compliance with food safety standards (e.g., CAP standards). It must integrate diverse operational realities, from digitally advanced agribusinesses employing precision farming to smaller traditional operations still adapting to digital governance frameworks.

Energy and Utilities vs. Retail and Digital Commerce (Alternative Angle)

Energy and Utilities governance heavily emphasizes stakeholder accountability through mandated ESG reporting and transparency in operational practices, particularly vital given their critical societal role. Retail and Digital Commerce, meanwhile, fosters governance that directly engages consumers and relies significantly on reputational transparency mechanisms. Platforms like OLX manage customer relationships through transparent transactional practices and feedback-driven reputational systems, whereas Energy and Utilities navigate more formalized regulatory environments and stakeholder engagements.

Comparison from IT Management perspective

Energy and Utilities vs. Retail and Digital Commerce

In Energy and Utilities, IT management integrates operational technology (OT) systems like SCADA and smart meters, focusing on secure, resilient operations aligned with stringent compliance standards such as ISO 27001. Cybersecurity practices are crucial, as evidenced by adherence to the NIS2 directive. Retail and Digital Commerce IT management prioritizes real-time consumer-facing platforms, data analytics, and secure transactional processes. Platforms like Vinted leverage advanced data analytics to enhance user experience, implement secure payment systems, and perform sophisticated fraud detection, reflecting a distinct set of operational priorities and technological implementations.

Energy and Utilities vs. Agriculture and Farming

Energy and Utilities IT management displays high uniformity and sophistication, characterized by extensive cybersecurity measures, real-time analytics, and stringent compliance with regulatory standards. Utilities employ advanced integrated systems to manage critical infrastructure reliably. Conversely, Agriculture and Farming IT management varies significantly across technological adoption levels, ranging from small farms utilizing basic data entry to large-scale agribusinesses employing advanced precision agriculture technologies like satellite monitoring and IoT systems. The emphasis in agriculture is often more pragmatic, managing technological adaptation across diverse resource availability and infrastructure limitations.

Retail and Digital Commerce vs. Agriculture and Farming

IT management in Retail and Digital Commerce emphasizes platform reliability, consumer data security, and efficient transaction processing, supported by analytics and cybersecurity systems evident in platforms such as OLX, which prioritize fraud prevention and secure consumer interactions. Agriculture IT management is driven by practical considerations such as rural connectivity, scalable technology solutions, and data-driven decision-making tools adapted for varied farming scales. This approach accommodates infrastructure variability, from rural network deployments to advanced IoT-driven solutions for predictive farming.

Energy and Utilities vs. Agriculture and Farming (Alternative Angle)

IT management in Energy and Utilities is dictated by comprehensive regulatory requirements and operational resilience standards, ensuring consistency and uniform compliance. The implementation of cybersecurity frameworks and operational technology management (e.g., SCADA systems) exemplifies this standardized approach. Conversely, IT management in Agriculture and Farming addresses substantial variability, focusing on pragmatic adaptation to diverse operational scales and technological capabilities. The agriculture sector requires flexible, scalable solutions, illustrated by the widespread yet varied adoption of Farm Management Information Systems (FMIS) and precision agriculture tools, adapting to varying degrees of digital maturity and infrastructure readiness.

Project Deliver 1

Security and Management of Information Systems



Sofia Maria Arauz - 115442

Sofia Garcia Ruiz - 115453

Francisco Quian Blanco - 115588

Maria Agustina Sanguinetti - 115524

Index

Index.....	1
Task.....	2
Energy and Utilities: Organizations, Governance, and Management.....	3
Textual Analysis.....	3
Conceptual Map.....	3
Energy and Utilities: Governance of IT and IT Management.....	4
Textual Analysis.....	4
Conceptual Map.....	4
Retail and Digital Commerce: Organizations, Governance, and Management.....	5
Textual Analysis.....	5
Conceptual Map.....	5
Retail and Digital Commerce: Governance of IT and IT Management.....	6
Textual Analysis.....	6
Conceptual Map.....	6
Healthcare: Organizations, Governance, and Management.....	7
Textual Analysis.....	7
Conceptual Map.....	7
Healthcare: Governance of IT and IT Management.....	8
Textual Analysis.....	8
Conceptual Map.....	8
Organizations, Governance, and Management Comparison.....	9
Governance of IT and IT Management Comparison.....	10

Task

What: Each group will get 3 industries (to be assigned by academia) and must deliver a report, in a PDF file, describing and comparing the industries from the perspectives of the first two themes (Governance; IT Management), each analysis comprising:

- (60% = 3 industries × 2 themes × 10%) For each of the 3 industries, create 2 pages:
 - Each page should include a conceptual map and a textual analysis.
 - Each page should focus on one of the two themes (i.e., one theme per page per industry).
- (40% = 4 × 10%) Create 2 additional pages, each containing 4 half-page comparisons:
 - Each half-page compares two industries from the perspective of one of the two themes (freestyle format).
 - Note: One industry will need to appear in two different comparisons.

Industries

- Energy and Utilities
- Retail and Digital Commerce
- Healthcare

Energy and Utilities: Organizations, Governance, and Management

Textual Analysis

The Energy and Utilities sector is critical for public health, economic development, and national security, and therefore operates under tight regulatory and governance frameworks. Traditionally structured as state-run monopolies, the sector has evolved into a complex landscape of privatized and semi-regulated actors. This transformation demands robust <113>GRC practices and alignment between <117>Leadership structures and public policy objectives, especially concerning sustainability, affordability and energy security.

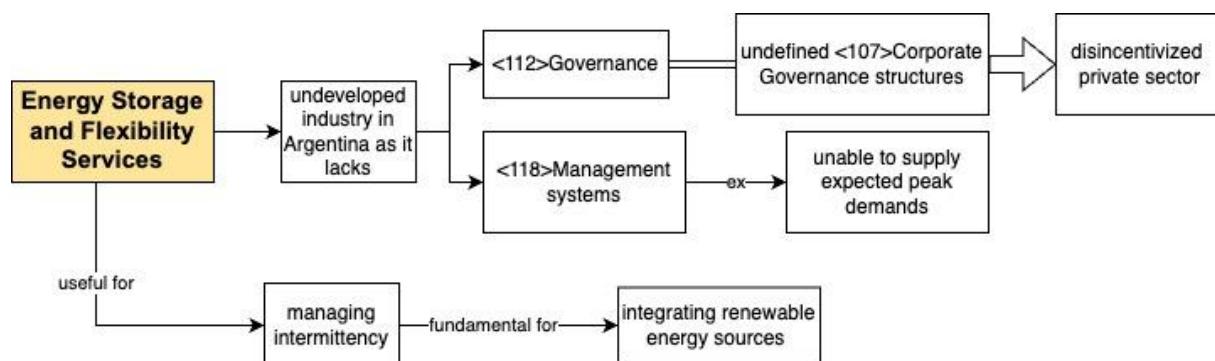
A particularly strategic and emerging subdomain is **Energy Storage and Flexibility Services**, especially in the context of **Argentina**. As the country integrates more renewable energy sources, managing intermittency becomes essential. However, Argentina lacks a mature regulatory and governance framework for storage. There is no dedicated legal classification for storage systems, and the role of actors providing demand-side flexibility remains undefined. This governance gap creates uncertainty for investors, limits innovation, and reduces the system's ability to adapt to new challenges.

In this context, analysing the governance and management of flexibility and storage services in Argentina allows us to understand how the absence of tailored <107>Corporate Governance structures and <118>Management systems can hinder systemic transformation. Beyond regulatory clarity, the subdomain urgently requires the development of integrated <118>Management capabilities: from designing operational workflows and technical interoperability protocols, to managing distributed assets in real time and coordinating between public and private actors.

For example, every summer, Argentina experiences record-breaking peaks in electricity demand—each year higher than the last—yet the system continues to lack the flexibility and planning capacity to respond effectively. The lack of scalable storage infrastructure to supply this peak demand results in blackouts and emergency load-shedding. This recurring mismatch between predictable demand and available supply highlights a failure in strategic <118>Management, not just in infrastructure deployment but also in long-term planning and <135>Risk mitigation.

In sum, the strategic development of Energy Storage and Flexibility Services in Argentina hinges not only on technological or regulatory advances, but on the creation of coherent organizational structures, robust governance mechanisms, and effective <118>Management systems. Without integrated planning, cross-sector coordination, and institutional prioritization, the sector will remain reactive rather than resilient—unable to scale innovations or secure long-term energy stability.

Conceptual Map



Energy and Utilities: Governance of IT and IT Management

Textual Analysis

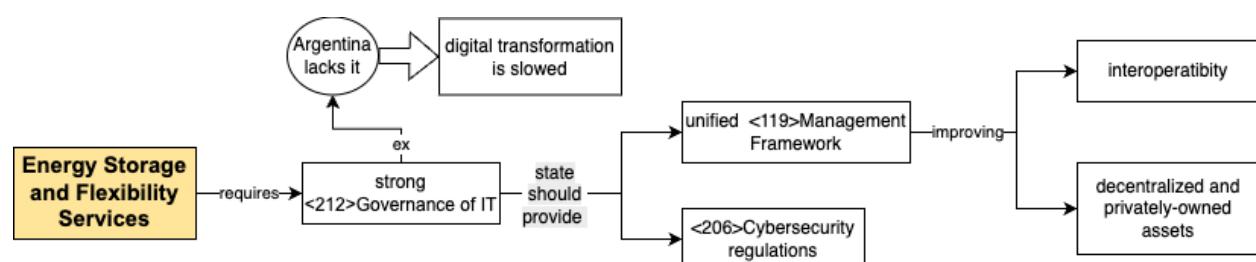
The Energy and Utilities sector operates in a highly regulated environment where information systems, <206>Cybersecurity, and digital alignment are becoming central to <112>Governance. As the sector integrates more distributed energy resources (DERs) like solar panels, electric vehicles, and batteries, the need for robust <212>Governance of IT frameworks intensifies. Digital platforms are now critical for real-time monitoring, load forecasting, and grid balancing, which introduces new risks and demands on information integrity and system resilience.

Within this context, we focus on the niche of **Energy Storage and Flexibility Services in Argentina**. This subdomain supports grid stability and energy transition through battery storage, demand-side response, and virtual power plants (VPPs). These systems are increasingly governed by IT-intensive infrastructures, requiring secure, interoperable, and trustworthy information systems to function effectively. And their proper functioning is critical, not just for technical performance, but for national stability. In an economy as fragile as Argentina's, energy disruptions can paralyse production lines and reinforce the country's image of instability among investors, deepening mistrust and slowing economic growth.

Nonetheless, in Argentina, the <212>Governance of IT in this area is still emergent and fragmented. There is no unified <119>Management Framework ensuring the alignment between technical architectures and energy policy, and <206>Cybersecurity regulations for decentralized assets (like home batteries or aggregators) remain underdeveloped. The lack of data standards and integration platforms also impairs the sector's capacity to scale flexibly while safeguarding grid stability.

This subdomain exemplifies the <212>Governance of IT challenges in critical infrastructure. As Argentina advances toward decarbonization and grid modernization, governing IT systems becomes a strategic necessity. The sector must align digital platforms with national energy goals while ensuring the security and integrity of information flows across decentralized and privately-owned assets. Interoperability, data standardization, and <135>Risk management are increasingly central as the system grows more reliant on real-time data and automated control. These dynamics highlight the urgent need for robust <212>Governance of IT frameworks to support both technological innovation and national energy resilience.

Conceptual Map



Retail and Digital Commerce: Organizations, Governance, and Management

Textual Analysis

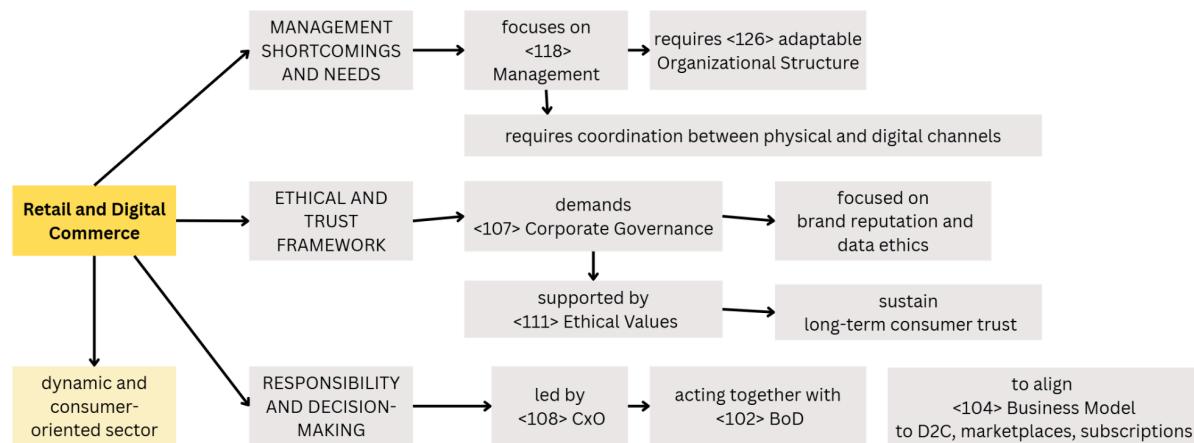
Retail and Digital Commerce operates in a fast-paced, consumer-driven environment shaped by platform business models and intensive data use. Governance frameworks must balance innovation with consumer trust, regulatory compliance, and ethical standards.

Corporate Governance^{<107>} in this sector is increasingly concerned with brand reputation, data ethics, and agile risk management. Executive leadership (CxO^{<108>}) oversees not just supply chains and logistics, but also digital platforms, marketing, and consumer engagement. GRC^{<113>} structures address diverse challenges, from GDPR compliance to algorithmic fairness in IT systems.

Governance in Retail and Digital Commerce requires integrated oversight across physical and digital operations. Boards of Directors^{<102>} and Management^{<118>} teams collaborate to ensure strategic agility while safeguarding consumer data, cybersecurity, and sustainability targets. Ethical Values^{<111>} and transparent communication are central to maintaining long-term consumer loyalty and stakeholder trust.

The sector often operates with highly dynamic Organizational Structures^{<126>}, including platform ecosystems, marketplaces, and omnichannel strategies. These structures must be flexible to respond to shifting consumer preferences and technological trends, while aligning with evolving Business Models^{<104>} such as direct-to-consumer and subscription-based commerce.

Conceptual Map



Retail and Digital Commerce: Governance of IT and IT Management

Textual Analysis

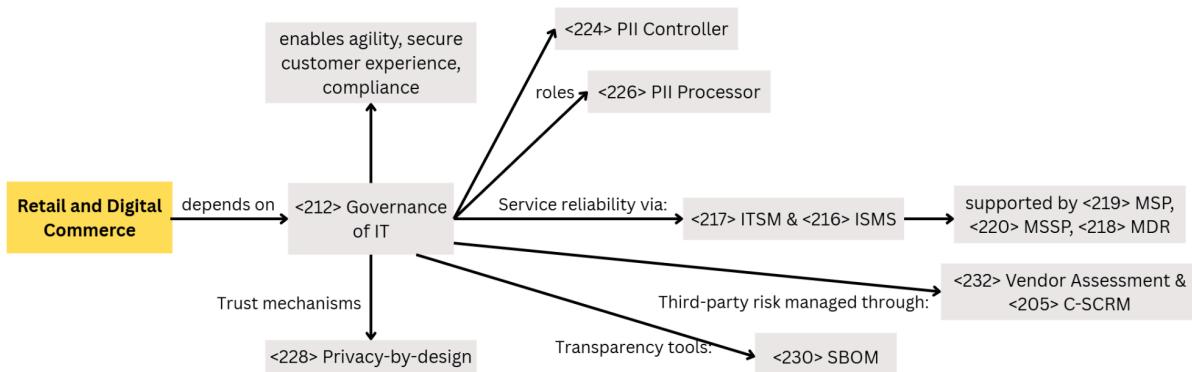
In Retail and Digital Commerce, IT governance^{<212>} focuses on enabling business agility, secure customer experiences, and compliance with data regulations. As organizations handle large volumes of PII (Personally Identifiable Information)^{<223>}, governance frameworks must integrate Data Privacy ^{<208>}, GDPR (General Data Protection Regulation)^{<211>}, and Data Retention^{<210>} requirements, using clear roles like PII Controllers^{<224>} and Processors^{<226>}.

ITSM (IT Service Management)^{<217>} and ISMS (Information Security Management System)^{<216>} ensure the reliable delivery and security of services. Retailers often rely on MSPs (Managed Service Providers)^{<219>}, MSSPs (Managed Security Service Providers)^{<220>}, and MDR (Managed Detection and Response)^{<218>} to monitor systems and address cyber threats. IAM (Identity and Access Management)^{<214>} is essential to control access to sensitive customer and operational data, supported by Zero Trust^{<234>} models that assume no implicit trust within networks.

Retail governance must also manage risks from third parties through Vendor Assessment^{<232>} and C-SCRM (Cybersecurity Supply Chain Risk Management)^{<205>}, especially when using cloud services or digital platforms. Transparency is supported by tools like SBOMs (Software Bill of Materials)^{<230>}, which document software components and their origins.

To maintain consumer trust, retailers implement Privacy-by-design^{<228>} principles, using compliant Consent Mechanisms^{<203>} such as Opt-in^{<221>} and Opt-out^{<222>}. These mechanisms ensure lawful data processing and enhance customer transparency and control.

Conceptual Map



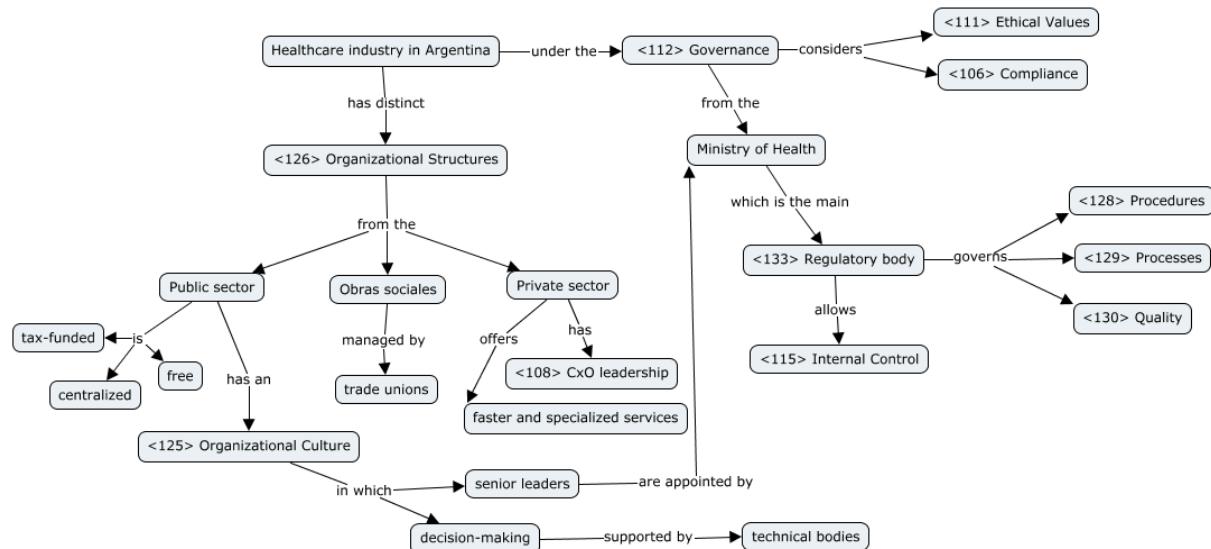
Healthcare: Organizations, Governance, and Management

Textual Analysis

In Argentina, the healthcare industry consists of the public sector, social security/union-run insurance (obras sociales) and the private sector. Public healthcare is tax-funded, centralized and free. Obras Sociales are managed by trade unions and are compulsory for workers. The private sector offers faster access and more specialized services. All systems operate within distinct <126> Organizational Structures, reflecting their sources of funding, management, and service delivery. All are under the <112> Governance from the Ministry of Health which also serves as the main <133> Regulatory body. <111> Ethical Values and <106> Compliance with national directives are taken into account. A clear <134> Regulatory framework governs <128> Procedures, <129> Processes and the overall <130> Quality of services while also allowing <115> Internal Control mechanisms.

In the public industry, the <125> Organizational Culture is shaped by a structure in which senior leaders are appointed by the government while decision-making is also supported by technical bodies and public institutions. In contrast, <102> BoD or corporate-style <108> CxO leadership is more typical in the private healthcare sector, where management practices tend to follow market-oriented models.

Conceptual Map



Healthcare: Governance of IT and IT Management

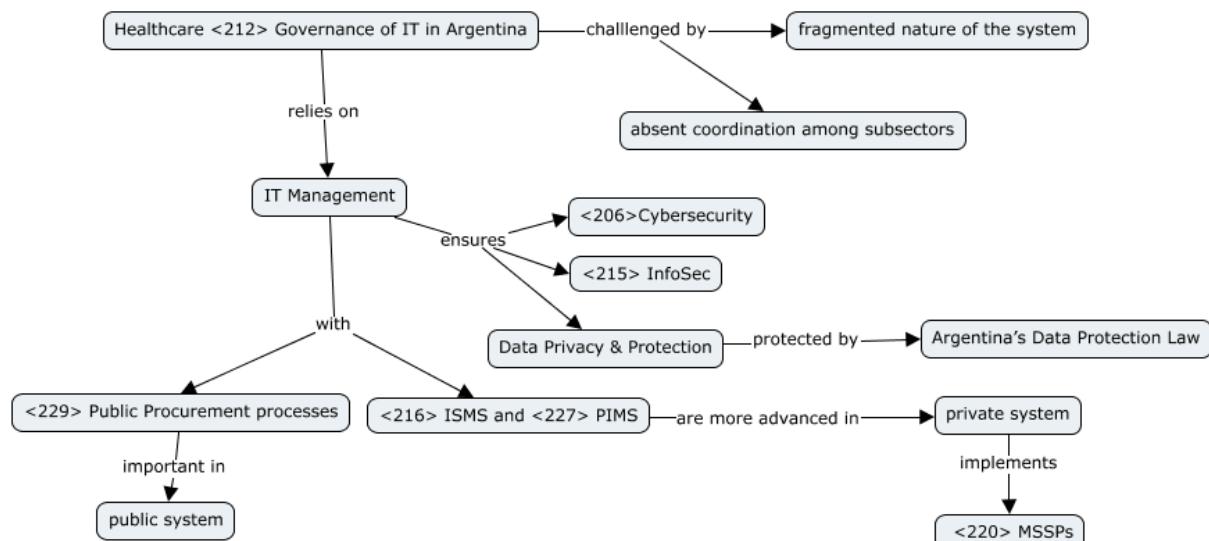
Textual Analysis

Healthcare <212> Governance of IT in Argentina remains a challenge due to the fragmented nature of the system. Each federal province has autonomy over its public health policies and regulations, which leads to variations in service delivery and challenges the alignment of national and provincial health information systems. In addition, the lack of coordination among the three subsectors complicates building an integrated and standardized national health information system.

<206> Cybersecurity and <215> InfoSec measures are less robust in the public sector due to limited resources and funding. In contrast, the private sector is more advanced in both <216> Information Security Management Systems (ISMSs) and <227> Privacy Information Management Systems (PIMSSs) often implementing <220> Managed Security Service Provider (MSSPs), while the public sector relies on slower <229> Public Procurement processes. This can complicate the implementation of critical IT and security infrastructure.

<223> PII in health records is protected by Argentina's Data Protection Law which incorporates <208> Data Privacy, <210> Data Retention, and <228> Privacy-by-design principles.

Conceptual Map



Organizations, Governance, and Management Comparison

Energy & Utilities - Retail and Digital Commerce

The governance and management of Energy Storage and Flexibility Services differ significantly from those in Retail and Digital Commerce due to the nature of their services and stakeholders.

Energy operates within critical infrastructure, requiring strong ^{<107>} Corporate Governance and ^{<113>} GRC to manage ^{<135>} Risk and ensure grid reliability. ^{<126>} Organizational Structures are typically hierarchical, and ^{<323>} SLAs are precise, reflecting high accountability. ^{<136>} Top Management aligns with national policy, focusing on stability and regulatory coordination.

Retail and Digital Commerce, in contrast, moves quickly and is driven by consumer demand and data. Governance here emphasizes brand integrity, ^{<106>} Compliance with privacy laws like ^{<211>} GDPR, and ethical use of consumer data. ^{<108>} CxO roles lead agile operations, integrating logistics, platforms, and customer experience through flexible ^{<126>} structures.

Ultimately, both sectors require robust ^{<112>} Governance and ^{<118>} Management, but while energy emphasizes control and resilience, retail prioritizes speed, innovation, and consumer trust. Their frameworks must reflect these distinct pressures to remain effective.

Healthcare - Energy & Utilities

Healthcare and Energy & Utilities in Argentina reflect divergent evolutions in ^{<112>} Governance and ^{<118>} Management. Healthcare shows higher institutional maturity, with clearly defined ^{<126>} Organizational Structures, enforced ^{<134>} Regulatory frameworks, and embedded ^{<106>} Compliance. Central oversight by the ^{<133>} Regulatory body ensures stable ^{<128>} Procedures and ^{<115>} Internal Control, especially in the public and *obras sociales* subsystems.

Energy & Utilities, particularly in storage and flexibility, lacks comparable coherence. There is no defined ^{<107>} Corporate Governance for new actors, nor a consistent ^{<113>} GRC approach. This leaves the sector exposed to ^{<135>} Risk during peak demand events and limits innovation due to regulatory uncertainty.

The difference lies in institutional grounding: healthcare is built on decades of centralized planning and public accountability, which foster procedural solidity. Energy, having transitioned from public monopoly to hybrid market, still lacks a clear ^{<122>} Mission and struggles with fragmented ^{<120>} Management Systems. While healthcare may face bureaucratic inertia, it operates within a stable governance environment. Energy, by contrast, is more dynamic but lacks the governance depth to scale or adapt.

Ultimately, healthcare's structure allows for coordination, but not always flexibility; energy's flexibility exists in theory, but not in managed practice. Bridging these gaps requires tailored ^{<119>} Management Frameworks that fit sector-specific constraints and opportunities.

Governance of IT and IT Management Comparison

Energy and Utilities - Retail and Digital Commerce

In both industries, <212>Governance of IT is essential but shaped by their unique challenges. In the selected subdomain of Energy Storage and Flexibility Services, technology is critical for real-time consumption monitoring, ensuring reliable supply, and managing storage systems. This makes <438>Strategic Planning and rigorous <135>Risk Management vital to maintain grid stability and prevent failures that, when these services are relied upon by public institutions, could have national level consequences.

In contrast, Retail and Digital Commerce focus heavily on managing and protecting large volumes of sensitive user and transaction data. Compliance with privacy regulations and robust <206>Cybersecurity are paramount, as breaches can severely damage customer trust and disrupt <103>Business Continuity. Beyond security, delivering a smooth user experience—through performance optimization and leveraging recovered user data to offer personalized products—is another critical area requiring strong Governance of IT. Without it, consumers will quickly turn to competitors that better meet their needs.

Then, although the risk profiles differ, both sectors require strong, adaptive <212>Governance of IT. The growing digitalization and technological dependency demand frameworks that integrate <118>Management, control, and <437>Strategic Alignment to support reliable and scalable operations.

Healthcare - Retail and Digital Commerce

Healthcare and Retail in Argentina reflect two distinct approaches to <212> Governance of IT, shaped by their institutional logic. Healthcare is marked by fragmentation and reactive implementation—provincial silos and uneven funding hinder <216> ISMS and <206> Cybersecurity, especially in the public sector. Retail, by contrast, embeds IT governance as a driver of business agility, deploying <217> ITSM, <214> IAM, and <234> Zero Trust as standard practice.

Retail's control over <223> PII is proactive: clear <224> PII Controller and <226> PII Processor roles, <228> Privacy-by-design, and <203> Consent Mechanisms support strong <211> GDPR compliance and consumer trust. Healthcare shares these legal foundations but lacks the operational maturity to enforce them uniformly. As a result, Retail treats data as an asset; Healthcare often sees it as liability.

Retail also excels in third-party risk management through <232> Vendor Assessment and <205> C-SCRM, while healthcare relies on slower <229> Public Procurement, limiting its responsiveness to digital threats. This contrast reflects not only different resources, but fundamentally different cultures: one built for competition, the other for stability.

Ultimately, while Retail governs IT for speed and trust, Healthcare remains constrained by legacy governance structures. Closing this gap demands more than technology—it requires strategic coherence and institutional reform.

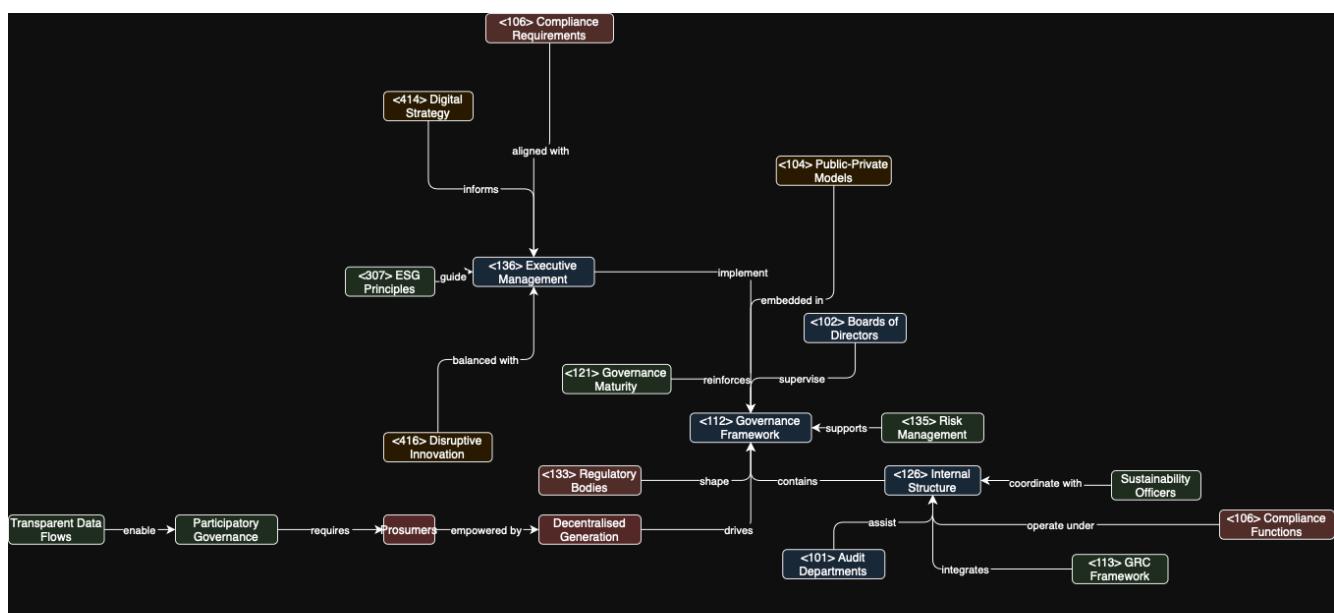
SGSI 2025 – Group 246 - Project Part 1

Industries: Energy and Utilities & Utilities | Transport and Logistics & Logistics | Banking and Financial Services & Financial Services

1. Energy and Utilities and Utilities

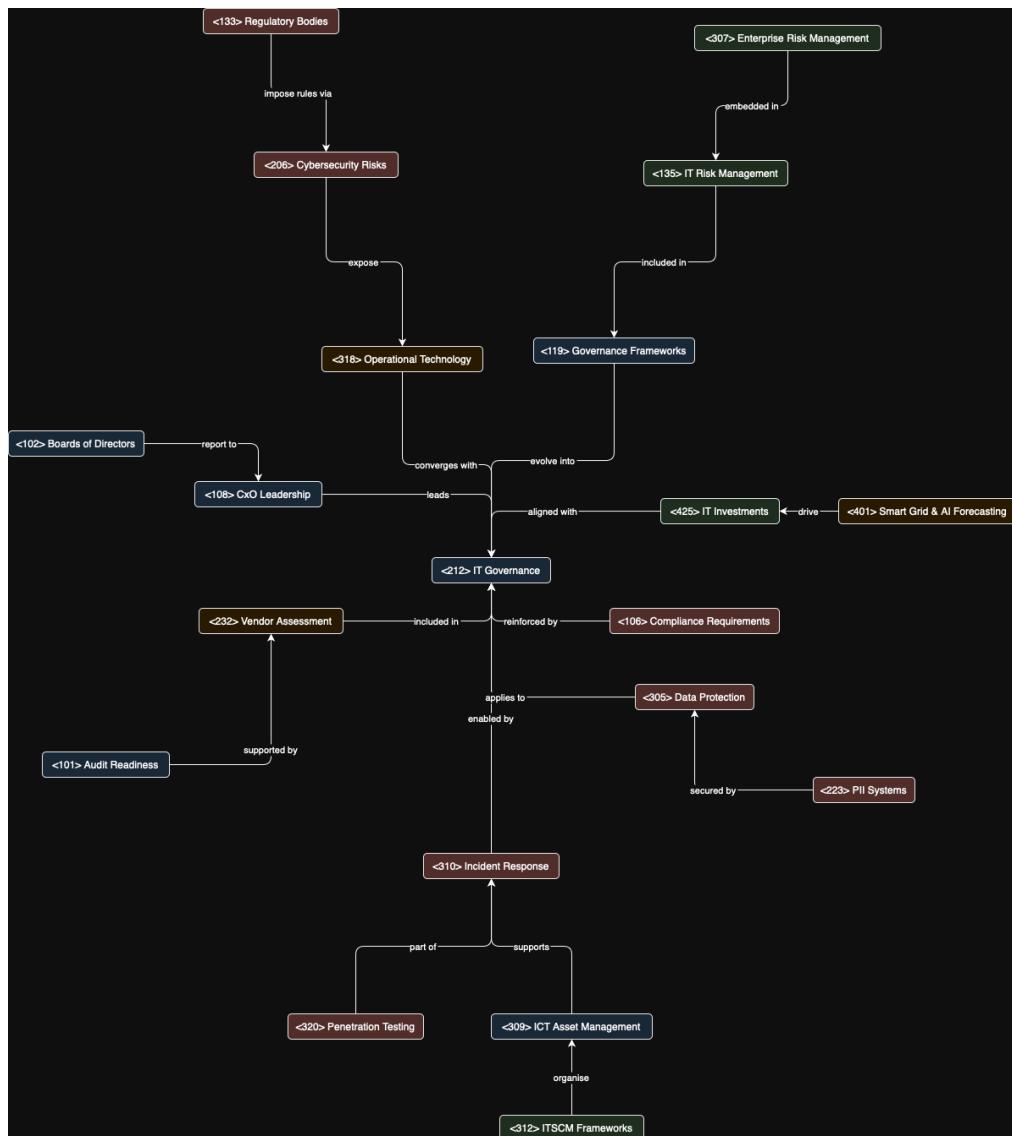
Theme 1: Organisations, Governance, and Management

The energy and utilities sector is shaped by a complex interplay of regulatory, environmental, and infrastructural factors. Organisations in this sector operate within a tightly controlled governance <112> framework that spans national governments, EU institutions, and international regulatory bodies <133>. The governance <112> model is structured around balancing three core goals: security of supply, affordability, and sustainability. In Europe, public-private hybrid business models <104> dominate, with significant state ownership in some areas (e.g., grid operators) and growing private-sector investment in renewables. Governance maturity <121> is generally high due to the critical nature of services and long investment cycles. Boards of Directors <102> and executive management <136> teams must navigate trade-offs between disruptive innovation <416> (e.g., smart grids, hydrogen) and compliance <106> (e.g., emissions targets, NIS2 obligations). Risk <135> management structures are robust, accounting for operational failures, market volatility, and geopolitical uncertainty. Organisational strategies are increasingly informed by ESG principles and digital strategy <414> imperatives. The internal organisational structure <126> of energy firms typically includes multiple compliance <106> functions, audit <101> departments, and sustainability officers working together under a GRC <113> framework. As the sector transitions toward decentralised generation and consumer empowerment (prosumers), governance <112> models are being reshaped to incorporate participatory mechanisms and transparent data flows.



Theme 2: Governance of IT and IT Management

Governance of IT <212> in the energy and utilities sector has become a cornerstone of operational and strategic resilience. Traditionally dominated by physical asset management and operational technology (OT) <318>, the sector is undergoing digital transformation through the integration of information technology systems such as SCADA, customer portals, and smart meter networks. The convergence of OT and IT introduces significant cybersecurity <206> risks, prompting regulatory bodies <133> to impose strict controls (e.g., NIS2 Directive, ISO/IEC 27001, IEC 62443). Governance frameworks <119> are evolving to integrate IT risk <135> management into broader enterprise risk management (ERM) <307> structures, often led by CxO <108> roles like CISOs and CIOs, who sit at executive or BoD <102> levels. IT governance <212> also encompasses vendor assessment <232>, procurement of critical software and hardware, and audit <101> readiness. There is increasing pressure to align IT investments <425> with environmental goals, especially through smart grid optimisation, AI <401>-based demand forecasting, and digital twin technologies. Incident response <310>, penetration testing <320>, and ICT asset management <309> are essential components of ITSCM <312> frameworks. Data protection <305> is also critical, especially in systems that handle PII <223>. As the energy transition accelerates, IT governance <212> must ensure that digital innovation supports compliance <106>, cost-efficiency, and infrastructure security.



2. Transport and Logistics and Logistics

Theme 1: Organisations, Governance, and Management

The transport and logistics sector is built on an intricate web of operational processes, infrastructure networks, and cross-border dependencies. Governance [\[112\]](#) structures vary widely across subdomains—from heavily regulated aviation and rail sectors to more agile road and last-mile delivery services. Organisations often operate under multilayered regulatory frameworks [\[134\]](#) involving EU policy (e.g., TEN-T, Sustainable and Smart Mobility Strategy), national regulatory bodies [\[133\]](#), and local municipalities. Key governance [\[112\]](#) actors include infrastructure owners, service operators, audit [\[101\]](#) and safety bodies, and compliance [\[106\]](#) teams. Top Management [\[136\]](#) is typically tasked with aligning safety, punctuality, and sustainability goals within complex stakeholder environments. Governance challenges include coordinating long-term infrastructure investments with evolving digital capabilities and shifting public policy objectives, such as carbon neutrality and inclusive mobility. Operational risk [\[317\]](#) is a significant concern, with disruptions caused by traffic, weather, geopolitical events, or system outages. As intermodal and platform-based logistics gain traction, governance [\[112\]](#) frameworks must adapt to real-time coordination needs, public-private partnerships, and documented information [\[109\]](#) sharing mandates. Organisational culture [\[124\]](#) is being reshaped by the adoption of disruptive innovation [\[416\]](#), electric fleets, and automation technologies. Governance maturity [\[121\]](#) differs widely by geography and subdomain but is generally improving due to increased standardisation and strategic focus on resilience and digital integration.



Theme 2: Governance of IT and IT Management

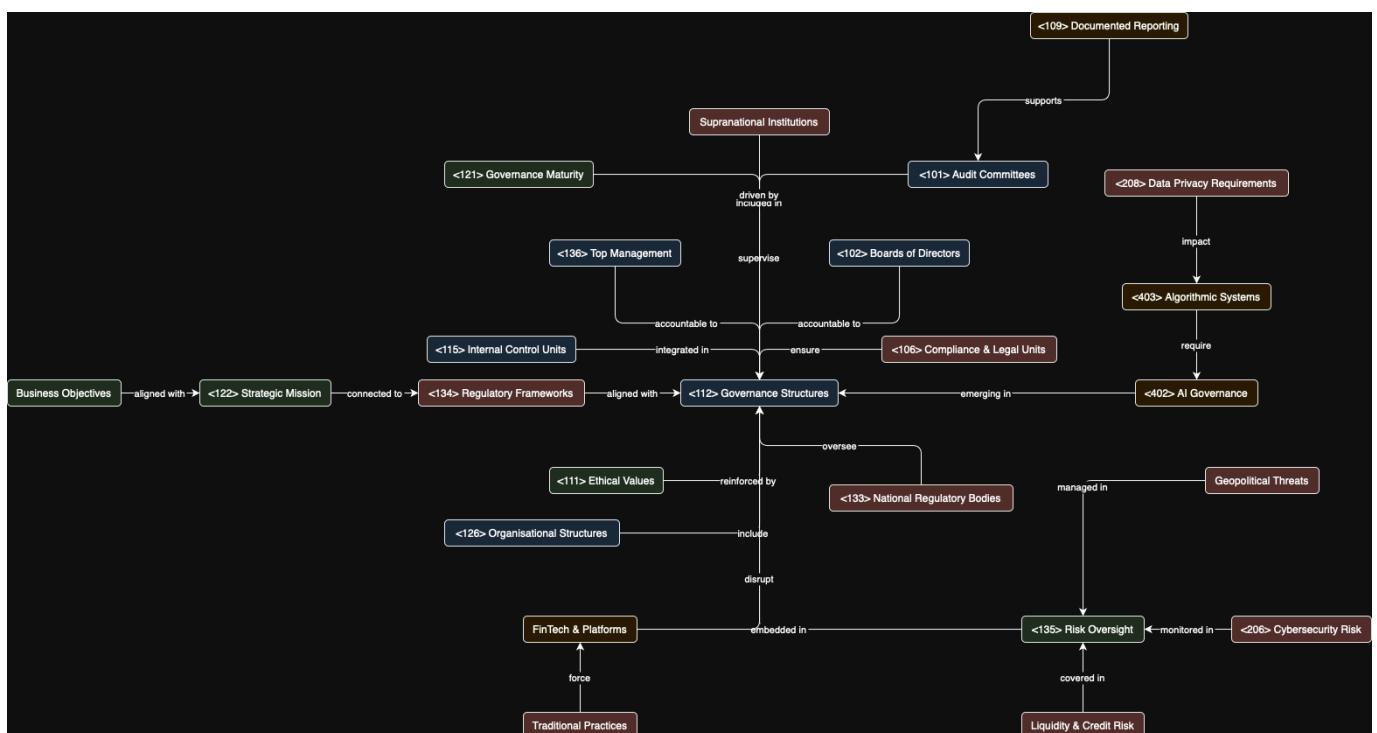
IT governance <212> in transport and logistics is defined by the need for interoperability, cybersecurity <206>, and performance optimization across a vast digital infrastructure. Key systems include fleet telematics, logistics management platforms, ticketing systems, and real-time passenger information tools. Governance frameworks <119> are typically structured around CxO <108>-led teams that coordinate across business units, compliance <106> functions, and IT operations management (ITOM) <311>. Cybersecurity <206> governance has become a top priority, especially with the rise of IoT devices, remote fleet monitoring, and data-sharing ecosystems. Regulatory compliance <106> is anchored in the GDPR <211>, eFTI Regulation, and sector-specific transparency mandates. Zero Trust <234> architectures are increasingly adopted to counter risks from diverse vendor ecosystems and third-party platforms. Logging <314>, patch management <319>, and service level agreements (SLAs) <323> are tightly integrated into IT operations. IT governance <212> maturity in the sector varies, with aviation and large logistics providers often leading in digital integration and incident response <310> readiness. Strategic alignment <437> between IT and business goals is essential to support innovations such as predictive maintenance, automated warehousing, and platform integration. As urban and intermodal mobility platforms expand, IT governance <212> must balance agility with accountability and data protection <305>.



3. Banking and Financial Services and Financial Services

Theme 1: Organisations, Governance, and Management

The banking and financial services industry is one of the most tightly governed sectors globally. Governance <112> structures are institutionalised and highly formalised, reflecting the sector's systemic importance and exposure to financial, reputational, and operational risk <135>. Boards of Directors <102> and Top Management <136> are accountable to national regulatory bodies <133>, supranational institutions (e.g., ECB, EBA), and shareholders. The governance <112> model typically includes audit <101> committees, risk <135> oversight, internal control <115>, and legal <106> units. Governance maturity <121> is extremely high, driven by compliance <106> with frameworks like Basel III/IV, MiFID II, AML/KYC, and Solvency II. Ethical values <111> and fiduciary responsibility are core principles reinforced by frequent audits <101> and documented information <109> reporting. Risk <135> management is embedded in all organisational structures <126>, covering liquidity risk, credit exposure, cybersecurity <206>, and geopolitical threats. Structures vary across retail, commercial, and investment banking but all must align strategic mission <122>, business objectives, and regulatory framework <134> compliance. Emerging challenges include ESG reporting, AI governance <402>, and adapting BoD <102> competencies for digital transitions. FinTech entrants and platform-based financial services add complexity, requiring banks to revise traditional governance practices to incorporate algorithmic systems <403>, partnerships, and data privacy <208>.



Theme 2: Governance of IT and IT Management

IT governance <212> in banking is driven by compliance <106>, operational resilience, and the criticality of financial infrastructure. Banks operate under multi-tiered IT governance <212> frameworks involving COBIT, ISO 27001, GDPR <211>, PSD2, and DORA. CxO <108> roles like CIO, CISO, and DPO frequently report to the BoD <102>, reflecting the strategic role of IT. Governance structures must ensure the CIA triad <202> (confidentiality, integrity, availability) of systems like core banking, identity access management (IAM <214>), and fraud prevention. Shadow IT <324>, technical debt <325>, and third-party outsourcing (e.g., XaaS <326>) pose governance challenges. Cybersecurity <206> involves layered defenses, vulnerability management <233>, and penetration testing <320>. Strategic IT planning includes Open Banking and Financial Services, AI <401> credit scoring, and real-time fraud analytics. Vendor assessment <232> and contractual oversight are critical due to reliance on MSSPs <220> and cloud providers. ITSCM <312> ensures service continuity amid cyberattacks or system failures. DORA enforces structured incident response <310> and resilience testing. As embedded finance and RegTech <433> advance, IT governance <212> must balance innovation with transparency, explainability <422>, and compliance <106>.



Comparative Analysis (Theme 1: Organisations, Governance, and Management)

Comparison 1: Energy and Utilities vs. Banking and Financial Services

Both industries operate within highly formalised governance frameworks [<112>](#), but their drivers and structures differ substantially.

Energy and Utilities governance is often shaped by public policy, state involvement [<104>](#), and infrastructure-heavy business models [<104>](#). Strategic priorities revolve around long-term planning, risk [<135>](#) mitigation (especially for operational and geopolitical risks), and sustainability strategy [<440>](#). The presence of Top Management [<136>](#) and BoD [<102>](#) ensures balance between innovation (e.g. disruptive technologies [<416>](#)) and stability.

In contrast, Banking and Financial Services is governed through an intricate and legalistic architecture. The sector is deeply anchored in regulatory frameworks [<134>](#), with Boards of Directors [<102>](#), CxO [<108>](#) roles, and compliance [<106>](#) units maintaining stringent oversight. The governance maturity [<121>](#) is among the highest across industries, with established practices like audit [<101>](#), internal control [<115>](#), and risk [<135>](#) committees.

While both sectors exhibit strong formal governance, banking focuses on ethical values [<111>](#) and fiduciary duty, whereas energy aligns more with infrastructure resilience and environmental mandates.

Comparison 2: Banking and Financial Services vs. Transport and Logistics

Banking and Financial Services prioritizes systemic risk [<135>](#) containment, legal accountability, and institutional transparency. Its governance is structured with layered internal control [<115>](#) systems and regular audit [<101>](#) oversight. Regulatory compliance with frameworks like MiFID II and Basel III ensures consistent, traceable operations. Oversight by BoD [<102>](#) and CxO [<108>](#) roles reinforces a highly formalised model focused on risk mitigation, ethical standards, and financial stability.

By contrast, Transport and Logistics operates through multi-actor coordination [<112>](#), involving municipalities, national regulators, and private operators. This creates a more fragmented yet agile governance structure focused on operational risk [<317>](#), service continuity [<103>](#), and cross-border logistics. Governance is often decentralised and must adapt to disruptions, infrastructure variability, and public-private dynamics.

While banking governance relies on regulatory rigidity and inward-looking risk controls, transport governance emphasizes organisational agility [<428>](#) and outward responsiveness. Both sectors manage governance complexity, but their focus diverges: banking protects financial systems, while transport ensures physical movement and network resilience.

Comparative Analysis (Theme 2: Governance of IT and IT Management)

Comparison 3: Energy and Utilities vs. Transport and Logistics

Energy and Utilities IT governance is centered around resilience and compliance <106> with frameworks like NIS2 and ISO/IEC 27001. It involves managing OT <318>/IT convergence across critical infrastructure (e.g., SCADA systems), using tools like patch management <319>, incident response <310>, and vendor assessment <232>. The focus is on continuity <312>, cybersecurity <206>, and protecting PII <223>.

In Transport and Logistics, IT governance supports performance optimization in real-time. Core systems include logistics platforms, fleet tracking, and passenger info systems. IT governance revolves around Zero Trust <234>, SLAs <323>, and data protection <305> for efficient, secure data flow. While governance maturity <121> is uneven, large operators lead in digital strategy <414> and alignment <437> with business needs.

Both sectors face the challenge of integrating digital and physical systems, but while energy focuses on infrastructure safety, transport emphasizes speed, modularity, and uptime.

Comparison 4: Banking and Financial Services vs. Energy and Utilities

Banking IT governance is driven by regulatory compliance <106>, data integrity, and fraud prevention. It operates within a tightly structured environment shaped by frameworks such as COBIT, GDPR <211>, and DORA, which establish the operational and security requirements for financial institutions. CxO <108> roles—specifically CIOs, CISOs, and DPOs—hold strategic and operational responsibilities under the oversight of the BoD <102>, ensuring that IT aligns with both risk and business objectives. Core focuses include data protection <305>, identity and access management (IAM) <214>, and cybersecurity <206>, implemented through layered controls such as penetration testing <320>, vulnerability management <233>, and continuous incident response <310> protocols. The banking sector is also a frontrunner in adopting AI <401> for fraud analytics, predictive threat modeling, and real-time transaction monitoring, giving it a competitive edge in both security and innovation.

In contrast, Energy and Utilities IT governance is primarily concerned with the protection and continuity of critical infrastructure. The sector faces additional complexity from legacy operational technology (OT) <318> systems and the technical challenges of OT/IT convergence. Its governance models are built around resilience, regulatory adherence (e.g., NIS2), and structured ITSCM <312> to mitigate the risks of physical system failure. Key priorities include robust ICT asset management <309>, vendor oversight through vendor assessment <232>, and maintaining compliance <106> with infrastructure-specific security directives. While digital maturity is progressing, the sector's transformation is often constrained by long investment cycles and public policy dependencies. Compared to banking, energy governance is less agile but deeply focused on systemic stability, making digital innovation a gradual, risk-controlled process.

1 Industry 2 - Energy and Utilities

1.1 Governance

The **Energy and Utilities sector** spans electricity, gas, water, oil and gas extraction, renewables (e.g., wind, solar, hydrogen), and energy storage, operated by public, private, or hybrid entities under strict regulation. **Governance**¹¹² must balance long-term investments, infrastructure reliance, and the need for secure, affordable, and sustainable energy.

Executives adopt integrated **GRG (Governance, Risk, Compliance)**¹¹³ frameworks to manage:

- **Operational Risks**³¹⁷: Outages, equipment failures, SCADA^{2.4.2} cyberattacks.
- **Market Risks**¹³⁵: Price volatility, supply chain disruptions.
- **Regulatory Risks**¹³⁵: Climate policy changes (e.g., EU Green Deal^{2.4.7}), procurement shifts.
- **Geopolitical Risks**¹³⁵: Dependency on foreign pipelines and critical minerals.

Compliance¹⁰⁶ includes health and safety, environmental licensing, emissions, GDPR²¹¹, tariffs, consumer protection, and cybersecurity.

In the EU, governance is shaped by the Clean Energy Package, Renewable Energy Directive, and Network Codes, promoting energy-climate planning, cross-border interoperability, and ESG disclosure^{2.4.8}. Operators align with IEA, IRENA, IEC, and ISO standards to balance local obligations with global decarbonization.

TSOs and DSOs^{2.4.3} govern digital assets—smart meters, trading platforms, asset software—under resilience and regulatory targets.

Energy Communities^{2.4.4}, as local prosumer groups, raise governance challenges: distributed generation, fair participation, and integration with central grids under EU rules.

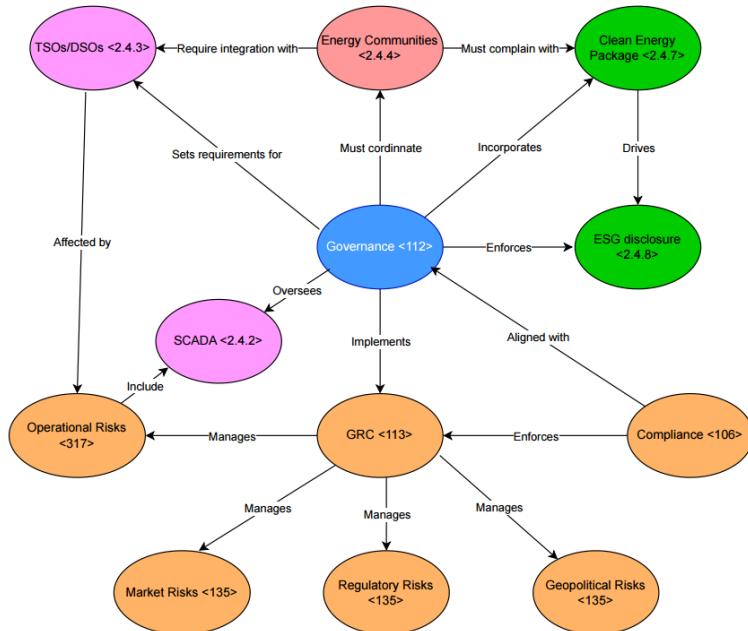


Figure 1: Conceptual map for governance(Energy and Utilities)

1.2 IT Management

IT Management in the **Energy and Utilities sector** brings together Information Technology (IT) and Operational Technology (OT) under unified governance, applying frameworks like COBIT, ITIL, and IEC 62443 to ensure cybersecurity, service continuity, and industrial control.

- **SCADA platforms^{2.4.2}**: Enable real-time monitoring and control of generation, transmission, and distribution infrastructure.
- **Smart Grid infrastructures^{2.4.1}**: Integrate smart meters, analytics platforms, and decentralized energy resource management (e.g., rooftop solar, battery storage).
- **Energy Trading Platforms and Customer Portals**: Demand high availability and robust cybersecurity due to their exposure and critical functions.

Compliance¹⁰⁶ with the EU Cybersecurity Act and NIS2 Directive^{2.4.5} requires the implementation of incident response teams³¹⁰, network segmentation, security audits, and data governance frameworks. These ensure alignment with GDPR²¹¹, maintain data integrity, and support regulatory reporting obligations.

Capacity mechanisms^{2.4.6} play a vital role in managing supply-demand imbalances, incentivizing generation reliability during peak periods, and maintaining grid stability in the context of renewable energy variability.

AI-powered applications support predictive maintenance, load forecasting, and the management of **Energy Communities^{2.4.4}**, enhancing efficiency and resilience.

Strategic **digital transformation** efforts aim to integrate distributed energy resources, hydrogen infrastructure, and the electrification of heating and transport into cohesive digital platforms. These initiatives are tracked via KPI dashboards¹¹⁶ to ensure alignment with decarbonization goals and capacity planning targets.

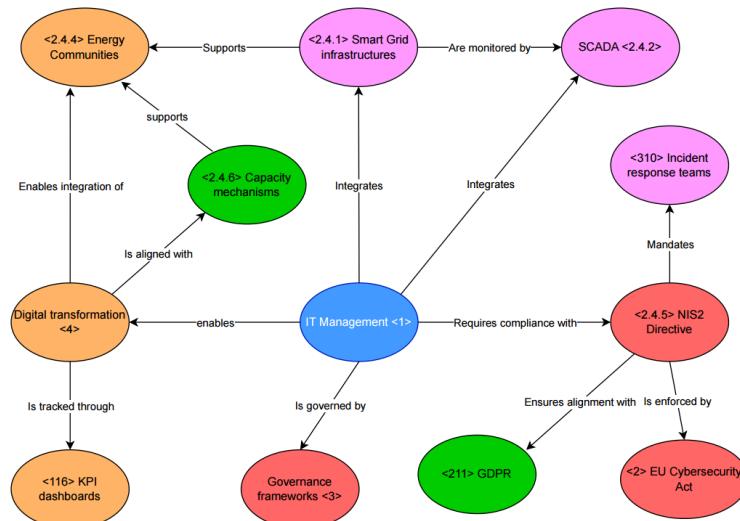


Figure 2: Conceptual map for IT management(Energy and Utilities)

2 Industry 4 - Transport and logistics

2.1 Governance

Governance in the transport and logistics sector involves balancing long-term infrastructure planning with the day-to-day demands of operating across multi-modal and cross-border networks. **Corporate Governance**¹⁰⁷ provides the strategic foundation for decision-making, where **Boards of Directors**¹⁰² establish direction and oversight, and **CxOs**¹⁰⁸ operationalise governance through large-scale project and service delivery. Given the sector's interconnection across regions and countries, regulatory harmonisation is crucial. Frameworks like the EU's TEN-T policy set the foundation for integrated infrastructure, while **Compliance**¹⁰⁶ ensures adherence to safety protocols, emissions controls, and information-sharing standards. These obligations are verified through structured audits and performance reviews.

Governance is not only structural — it is cultural. **Organisational Culture**¹²⁴ plays a central role in aligning public service objectives with private operational efficiency, especially within public-private partnerships. **Due Diligence**¹¹⁰ supports this alignment by proactively identifying and mitigating risks related to environmental challenges, labour conditions, and geopolitical instability. To manage these complex dynamics, organisations implement **GRC systems**¹¹³ that integrate governance, risk management, and compliance into a unified framework.

More digitally mature actors in the sector employ **Maturity models**¹²¹ to evaluate and improve governance structures, supported by internationally recognised **Management Frameworks**¹¹⁹ like ISO 37000. Additionally, **Regulatory Frameworks**¹³⁴ from global authorities such as ICAO (aviation) and IMO (maritime) influence governance strategies — particularly concerning emissions targets, digital logistics, and safety certifications. Ultimately, governance in this sector must go beyond control and compliance; it must foster trust, adaptability, and innovation. As digital platforms and data-sharing systems become central to logistics operations, strong governance is what enables resilience and public accountability in a globally interconnected and rapidly evolving environment.

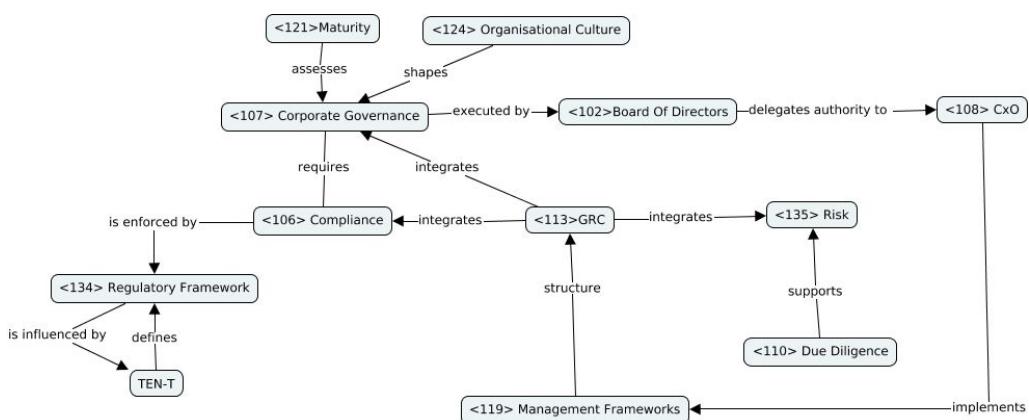


Figure 3: Conceptual map for Governance(Transport and logistics)

2.2 IT Management

In the transport and logistics sector, **Governance of IT**²¹² plays a pivotal role in aligning digital systems with business priorities such as operational efficiency, real-time visibility, and security in the transport and logistics sector. It provides strategic direction for **IT Operations Management**³¹¹, which handles the performance and integration of critical technologies like **Operational Technology (OT)**³¹⁸ — including vehicle telematics, logistics platforms, and warehouse automation systems. Given the sector's increasing dependence on interconnected systems, the risk of cyber threats is significant. As a result, **Cyber Resilience**³⁰³ is essential to protect infrastructure and maintain service continuity. This requires robust **Incident Response**³¹⁰ capabilities and consistent **Patch Management**³¹⁹ to close vulnerabilities and respond to disruptions.

The EU's eFTI Regulation is accelerating digital transformation by mandating the use of structured, interoperable **Documented Information**¹⁰⁹ to support electronic freight transport information exchanges. To meet this requirement, organisations must adopt **Management Frameworks**¹¹⁹ that ensure standardisation, scalability, and compliance across their IT environments. Tools such as Logistics Management Systems (LMS) and Fleet Telematics are now central to real-time operations and data-driven decision-making, but they require effective governance to function securely and legally. This responsibility falls largely to **CxOs**¹⁰⁸, who must ensure that these systems align with regulatory obligations and internal risk policies.

Effective IT Management in this sector goes far beyond deploying technology — it enables cross-border coordination, enforces regulatory compliance, and turns IT infrastructure into a competitive asset. As logistics networks become more digitised and integrated, strong governance is what enables organisations to respond to disruptions, optimise routes, protect customer data, and meet sustainability and transparency goals in an increasingly connected and fast-moving environment.

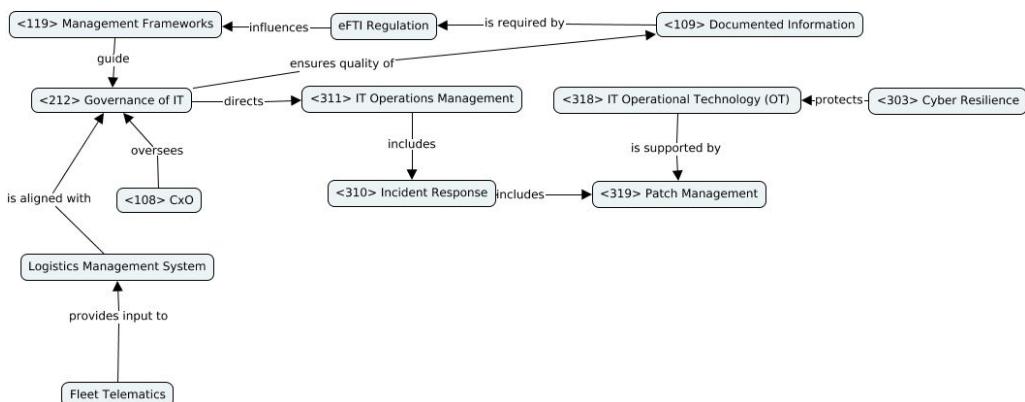


Figure 4: Conceptual map for IT management(Transport and logistics)

3 Industry 7 - Agriculture and Farming

3.1 Governance

Governance in agriculture balances sustainability, food safety, and economic resilience in a sector that ranges from smallholders and cooperatives to multinational agribusinesses. At its foundation, **Corporate Governance**¹⁰⁷ defines how decisions are made and objectives are structured to meet internal goals and external obligations. Regulatory expectations are shaped by **Regulatory Frameworks**¹³⁴ like the EU's Farm to Fork Strategy, which set standards for pesticide usage, emissions control, animal welfare, and ethical sourcing. These frameworks require strict **Compliance**¹⁰⁶, which is enforced through operational controls and third-party audits.

A well-structured **GRG (Governance, Risk, and Compliance)**¹¹³ model enables agricultural organisations to coordinate their responses to **Risk**¹³⁵ factors such as crop failure, price shocks, or climate volatility. Within this model, **Due Diligence**¹¹⁰ plays a vital role in managing risks tied to public subsidies, land stewardship, and reputational integrity, while also helping ensure coordination among multiple stakeholders, from producers to regulators.

Certification schemes¹⁰⁵ — including Global G.A.P., organic standards, and ISO 22000 — reinforce **Governance**¹¹² through requirements for traceability, documentation, and accountability. These mechanisms improve trust across the supply chain and support access to premium markets. Emerging technologies like blockchain are also being tested to increase traceability and transparency, particularly in export chains.

Cultural factors are equally significant. **Organisational Culture**¹²⁴, especially within cooperatives and community-based models, shapes how governance is enacted on the ground. Shared values such as sustainability and fairness influence how decisions are made collectively and how compliance is prioritised. In this evolving landscape, mature governance systems go beyond regulatory box-ticking — they align agricultural practices with long-term environmental goals, digital innovation, and growing public demand for ethical and transparent food systems.

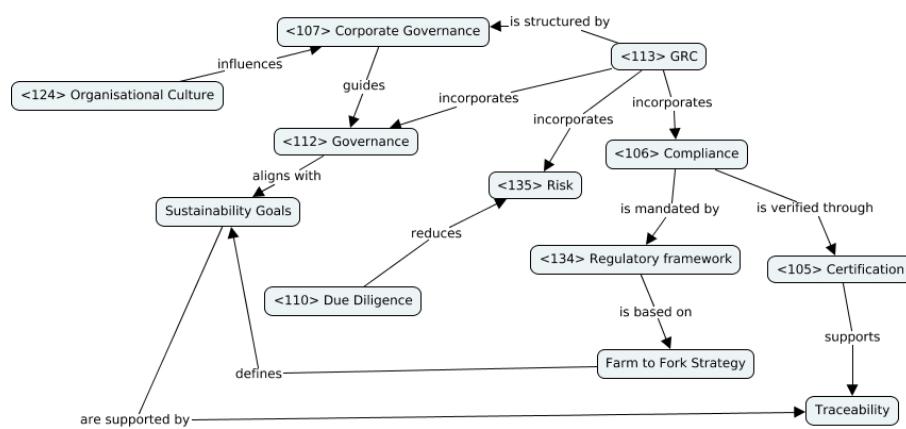


Figure 5: Conceptual map for Governance(Agriculture and Farming)

3.2 IT Management

Digital tools are reshaping agriculture, with **Governance of IT**²¹² ensuring that systems like sensors, automation, and cloud platforms align with sector goals such as yield optimisation, regulatory compliance, and environmental sustainability. A defining feature of smart farming is the use of **Operational Technology (OT)**³¹⁸, including drones, irrigation controllers, and soil sensors, to power **Precision Agriculture**. These technologies gather real-time data to optimise inputs like water and fertiliser, reduce waste, and predict threats such as pests or drought.

To keep these systems functional and secure, **IT Operations Management**³¹¹ is critical, especially across rural landscapes with varying infrastructure. Its stability is supported by **ITSM frameworks**²¹⁷ that standardise service quality and uptime. As digital agriculture becomes more connected, ensuring privacy and compliance is key. Tools like **Traceability Systems** help farms track products and inputs across the value chain, while **Consent Mechanisms**²⁰³ and **Data Protection**³⁰⁵ safeguard sensitive data collected from farmers, landowners, or supply chain partners.

Meeting food safety and sustainability goals also requires alignment with **Certification standards**¹⁰⁵ such as ISO 22000, which demand audit-ready digital systems. Meanwhile, increased reliance on cloud platforms and external tech providers highlights the need for **Cybersecurity Supply Chain Risk Management (C-SCRM)**²⁰⁵ to prevent service disruption and data breaches. To bring all these elements together, many farms and co-operatives are adopting **Integrated Management Systems (IMS)**¹¹⁴ that combine IT governance, food safety, and environmental controls into a single operational framework. While digital maturity remains uneven across the sector, public funding, EU policy, and innovation hubs are accelerating adoption. Long-term success depends not just on the tools used, but on the governance structures, cybersecurity capabilities, and strategic alignment that ensure those tools serve broader agricultural, economic, and environmental objectives.

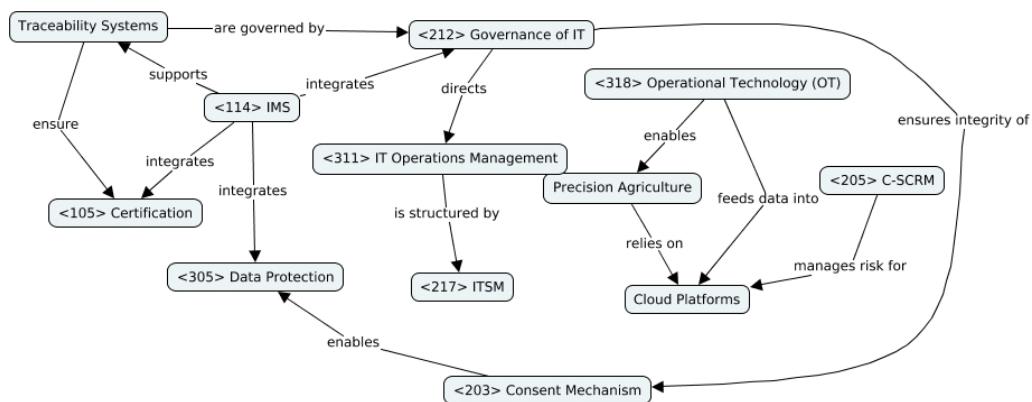


Figure 6: Conceptual map for IT management(Agriculture and Farming)

4 Industries comparison

4.1 Governance

Industry 2 vs Industry 4

Governance in the Energy and Utilities sector focuses on long-term infrastructure, regulatory compliance, and energy resilience. It spans electricity, gas, water, renewables, and storage, operating under integrated GRC (Governance, Risk, Compliance)¹¹³ frameworks. Key risks include Operational³¹⁷ (e.g., SCADA^{2.4.2} cyberattacks), Market¹³⁵, Regulatory¹³⁵ (e.g., EU Green Deal^{2.4.7}), and Geopolitical¹³⁵. Compliance¹⁰⁶ involves safety, GDPR²¹¹, and environmental regulations. EU policies like the Clean Energy Package and Network Codes promote sustainability and ESG disclosure^{2.4.8}. TSOs and DSOs^{2.4.3} manage smart grids, while **Energy Communities**^{2.4.4} introduce governance challenges in distributed generation and grid integration.

Governance in the Transport and Logistics sector emphasizes agility and cross-border coordination across road, rail, maritime, and air. It is structured through Corporate Governance¹⁰⁷, led by Boards¹⁰² and CxOs¹⁰⁸, and guided by policies like TEN-T. GRC¹¹³ systems, Due Diligence¹¹⁰, and Compliance¹⁰⁶ on emissions, safety, and data are key. Governance maturity is supported by Maturity Models¹²¹ and frameworks like ISO 37000¹¹⁹, alongside sector-specific regulations¹³⁴ from ICAO and IMO.

In summary, **Energy and Utilities** governance centers on infrastructure and sustainability, while **Transport and Logistics** prioritizes interoperability, digital transformation, and adaptive risk management.

Industry 4 vs Industry 7

Governance in both agriculture and transport sectors provides a framework for managing complexity, risk, and compliance, though their priorities differ. Agriculture governance focuses on sustainability, food safety, and ethical sourcing, guided by Corporate Governance¹⁰⁷ and Regulatory Frameworks¹³⁴ like the EU's Farm to Fork Strategy. Compliance¹⁰⁶ is ensured through audits and Certification Schemes¹⁰⁵, while GRC models¹¹³, Risk Management¹³⁵, and Due Diligence¹¹⁰ support land stewardship and subsidies. Organisational Culture¹²⁴ influences governance, especially in cooperatives.

Transport governance centers on infrastructure, efficiency, and cross-border coordination. Corporate Governance¹⁰⁷ is structured around Boards¹⁰² and CxOs¹⁰⁸, aligned with frameworks like TEN-T and global regulations¹³⁴ (ICAO, IMO). Compliance¹⁰⁶ ensures safety and emissions standards, while Due Diligence¹¹⁰ mitigates geopolitical and labor risks. Maturity Models¹²¹, ISO 37000¹¹⁹, and GRC systems¹¹³ refine governance strategies in an increasingly digital landscape.

In summary, agriculture governance prioritizes ethical sourcing and sustainability, while transport governance focuses on integration, scalability, and innovation.

4.2 IT Management

Industry 2 vs Industry 7

Both industries rely on IT and Operational Technology (OT³¹⁸) to drive efficiency, ensure security, and align with regulatory frameworks, but their focus and challenges differ significantly.

Energy and Utilities prioritize **real-time control and cybersecurity**, integrating **SCADA platforms**^{2.4.2} for infrastructure monitoring and **Smart Grid infrastructures**^{2.4.1} for decentralized energy management. Compliance with **EU Cybersecurity Act**¹⁰⁶ and **NIS2 Directive**^{2.4.5} necessitates strong security measures, including **incident response teams**³¹⁰ and **network segmentation**. **Capacity mechanisms**^{2.4.6} ensure supply-demand balance amid renewable energy variability, while **AI-powered applications** improve predictive maintenance and load forecasting.

Agriculture and Farming, on the other hand, emphasize **Precision Agriculture and sustainability**, leveraging **Operational Technology (OT)**³¹⁸ like **drones, irrigation controllers, and soil sensors** to optimize inputs and reduce waste. Compliance with **Certification standards**¹⁰⁵ such as ISO 22000 ensures food safety, while **Traceability Systems** track products across the value chain. Cybersecurity is also crucial, with **Cybersecurity Supply Chain Risk Management (C-SCRM)**²⁰⁵ preventing service disruptions and **Consent Mechanisms**²⁰³ safeguarding sensitive farm data.

While digital transformation is a shared goal, Energy & Utilities integrate **capacity planning via KPI dashboards**¹¹⁶, **hydrogen infrastructure**, and **electrification efforts**, whereas Agriculture focuses on **Integrated Management Systems (IMS)**¹¹⁴, **data protection**³⁰⁵, and **regulatory compliance**. Ultimately, both sectors depend on **strategic IT governance**, but their implementation varies based on industry-specific risks, operational needs, and sustainability goals.

Industry 4 vs Industry 7

Governance of IT²¹² is vital in agriculture and transport and logistics, ensuring efficiency, compliance, and digital transformation.

Agriculture leverages Operational Technology (OT³¹⁸) like soil sensors, drones, and irrigation controllers for precision farming. IT Operations Management³¹¹ and IT Service Management (ITSM) frameworks²¹⁷ standardize service quality, while Traceability Systems, Consent Mechanisms²⁰³, and Data Protection³⁰⁵ ensure data security. Compliance with ISO 22000¹⁰⁵ mandates audit-ready systems, while Cybersecurity Supply Chain Risk Management (C-SCRM²⁰⁵) prevents disruptions. Integrated Management Systems (IMS¹¹⁴) unify IT governance with food safety and environmental oversight.

Transport and logistics emphasize real-time visibility and automation. IT Governance²¹² secures fleet telematics and logistics platforms, reinforced by Cyber Resilience³⁰³, Incident Response³¹⁰, and Patch Management³¹⁹. Compliance with the eFTI Regulation requires structured Documented Information¹⁰⁹, while Management Frameworks¹¹⁹ enhance scalability. Logistics Management Systems (LMS) and Fleet Telematics drive data-driven decision-making, with oversight from high-level executives (CxOs¹⁰⁸).

While agriculture focuses on sustainability and food safety, transport prioritizes speed, security, and operational efficiency. Both industries rely on governance, cybersecurity, and innovation for digital progress.

Energy and Utilities: Smart Grid Infrastructure

Theme 1: Organizations, Governance & Management

The energy industry manages essential services like electricity, gas, and water. It includes both centralized and decentralized systems, combining traditional infrastructure with smart technologies and renewable sources.

Energy companies <104> Business Model is moving from a centralized system to a more flexible, modern “smart grid.” This means they no longer just produce electricity and send it to customers. Now, they must manage a network of partners, like people who generate their own solar power or companies that run EV charging stations.

<102> BoD must make decisions that ensure <103> Business Continuity, balancing keeping the lights on, protecting the environment, and keeping prices affordable. These decisions are more complex now and rely on up to date <109> Documented Information.

Inside the organization, traditional engineers must now work with IT experts and data analysts. The <112> Governance of the company must bring all these groups together. They also must report on new <135> Risks, like <206> Cybersecurity, and meet sustainability <111> Ethical Values.

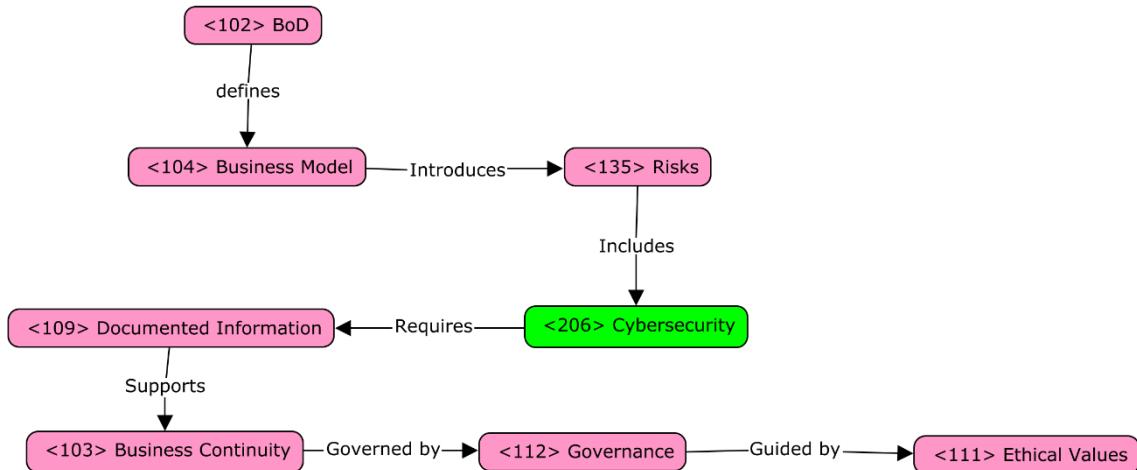


Figure 1 - Concept Map for Energy and Utilities: Smart Grid Infrastructure (Theme 1)

Theme 2: Governance of IT & IT Management

Smart grids use lots of connected devices and sensors that constantly send data, which requires a strong <212> Governance of IT. <217> ITSM must ensure that IT and operational systems (like SCADA) must work together safely. To manage this complexity, companies use <113> GRC standards.

Because these systems are part of national infrastructure, companies must check their suppliers carefully, <232> Vendor Assessment, and make sure all systems are secure. The board must understand and manage <206> Cybersecurity risks too.

They also need to double-check that their software and data models work correctly, through <101> Audits, and often get <105> Certifications for the systems they use, making sure they follow <211> GDPR. This helps prevent failures like blackouts and builds trust in smart-grid technology.

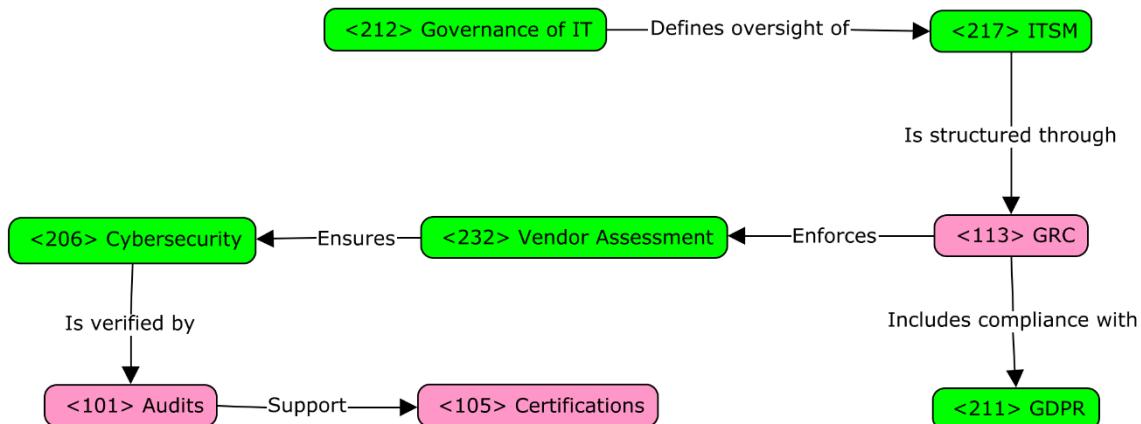


Figure 2 - Concept Map for Energy and Utilities: Smart Grid Infrastructure (Theme 2)

Transport and Logistics: Fleet Electrification and Telematics

Theme 1: Organizations, Governance & Management

The transport and logistics industry covers the movement of goods and people across road, rail, sea, and air. It includes shipping companies, fleet operators, and urban mobility platforms. Increasingly data-driven, it relies on systems like telematics and automation.

Transport companies switching to electric vehicles (EVs) aren't just buying new trucks, they're changing how their whole **<104> Business Model**. This involves new costs, staff training, building charging stations, and working closely with energy providers and local governments, which requires a whole new **<114> IMS**.

The **<102> BoD** must coordinate across many partners and decide on a new **<119> Management Framework** to deal with new **<135> Risks**, like running out of battery mid-delivery or not having enough chargers. These changes also affect long-term planning and investment.

Because EVs are connected and send data, companies must also think about **<127> Policy** regarding **<208> Data Privacy**. For example, they need a set of **<128> Procedures** on how to use driver tracking data responsibly. And they need **<308> Failover** plans in case digital tools fail, to ensure **<103> Business Continuity**.

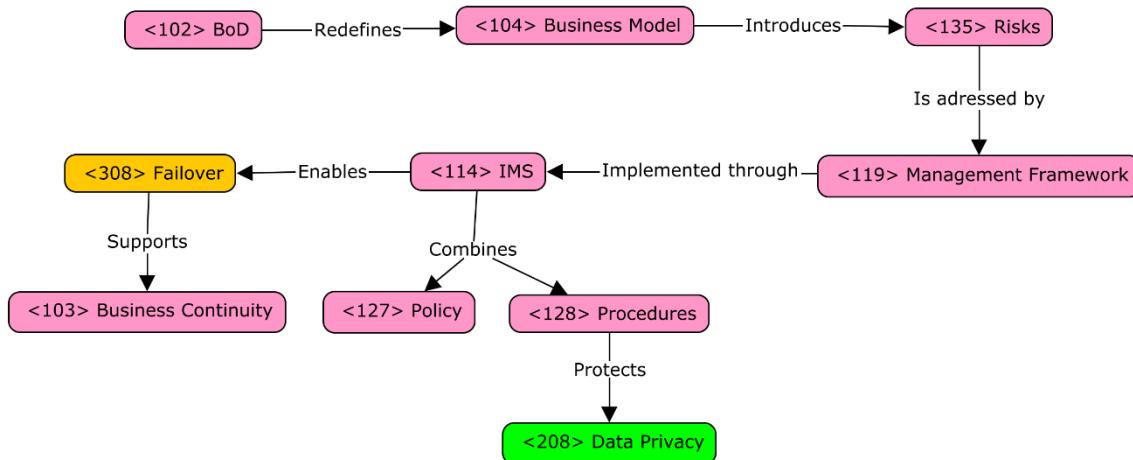


Figure 3 - Concept Map for Transport and Logistics: Fleet Electrification and Telematics (Theme 1)

Theme 2: Governance of IT & IT Management

Modern fleets use telematics, as in systems that collect real-time data about vehicles. This includes GPS, battery levels, and driver behavior. Companies must follow strict rules to protect this data, especially under laws like <211> GDPR.

IT managers need to make sure all the technology works well together and is safe, through a robust <217> ITSM. This relies on a proper <212> Governance of IT, which should include clear control over who can access what information.

They must also keep track of updates and <206> Cybersecurity for apps and devices. A strong <216> ISMS is needed, tied with <232> Vendor Assessment, to ensure all the used tools are <105> Certified to show they're reliable. If something goes wrong, like a cyberattack on a charging station, it can stop the whole fleet.

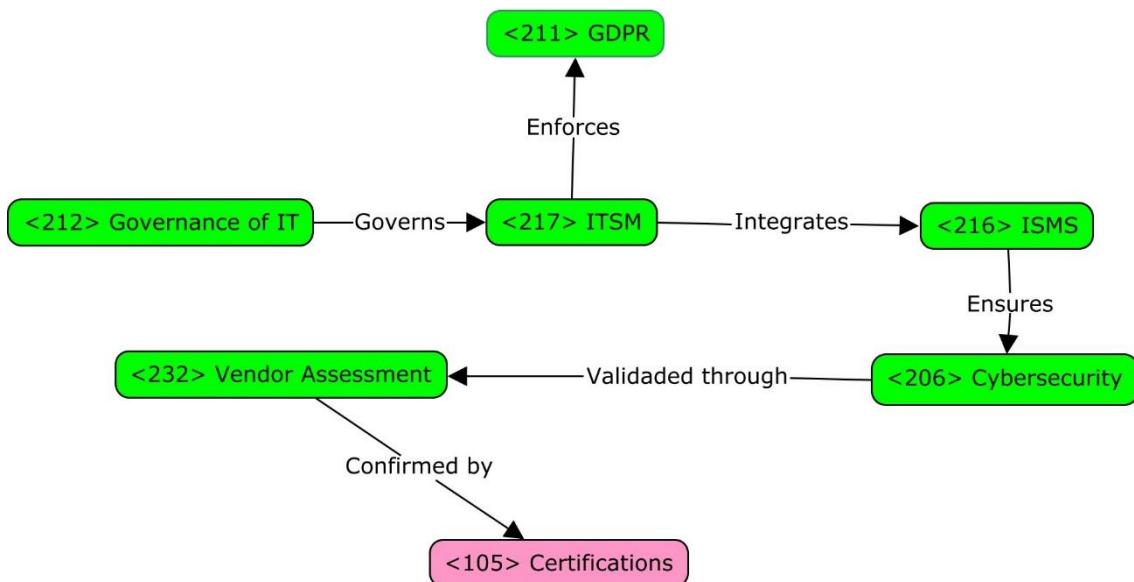


Figure 4 - Concept Map for Transport and Logistics: Fleet Electrification and Telematics (Theme 2)

Healthcare: Remote Patient Monitoring

Theme 1: Organizations, Governance & Management

Healthcare includes services and systems that prevent, diagnose, and treat health conditions. It spans hospitals, insurers, pharmaceutical firms, and digital health providers. It is highly regulated and ethically sensitive, requiring coordination across clinical care, technology, and data management, both in-person and remotely.

Remote Patient Monitoring lets patients use devices at home that share their health data (like heart rate or blood pressure) to doctors. This can help people stay out of the hospital, but it requires a change to the **<119> Management Frameworks** of the healthcare industry.

Hospitals and clinics must work closely with device makers, app developers, and cloud providers, doing their **<110> Due Diligence**. The **<102> BoD** is responsible for making sure everything runs safely and follows **<111> Ethical Values**.

This also changes how doctors work, they must trust automated alerts and decide what to do based on data they get without seeing their patients. Good **<112> Governance** requires a **<131> RACI**, and **<135> Risks**, like data leaks or bad readings should be clearly managed.

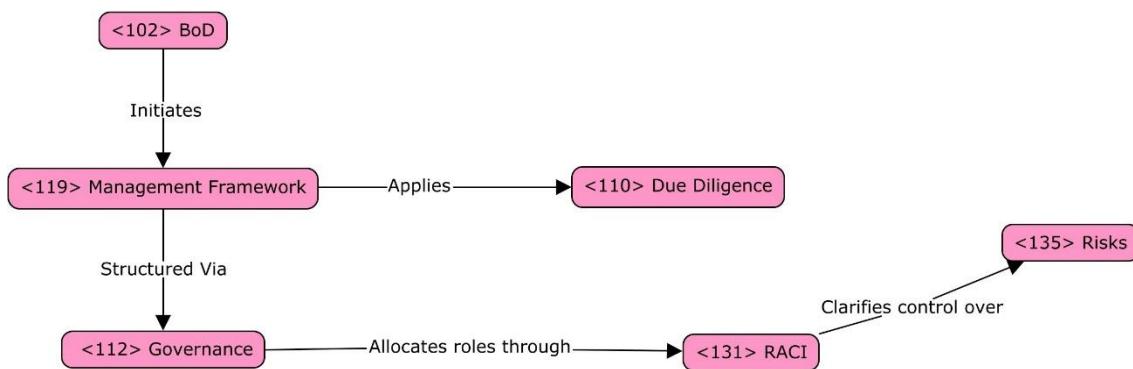


Figure 5 - Concept Map for Healthcare: Remote Patient Monitoring (Theme 1)

Theme 2: Governance of IT & IT Management

Health data is highly sensitive, due to its <223> PII nature and <217> ITSM must be designed to ensure <228> Privacy-by-design. This means encrypting data, controlling access, and making sure it's used correctly.

To make sure different systems (like hospital records and wearable devices) can talk to each other, healthcare providers use <214> IAM mechanisms. They also <101> Audit the systems regularly.

<108> CIOs must manage the full life cycle of these technologies, including updates, support, and even removing devices safely. All of this must follow clear rules, because mistakes could put patient safety at risk.

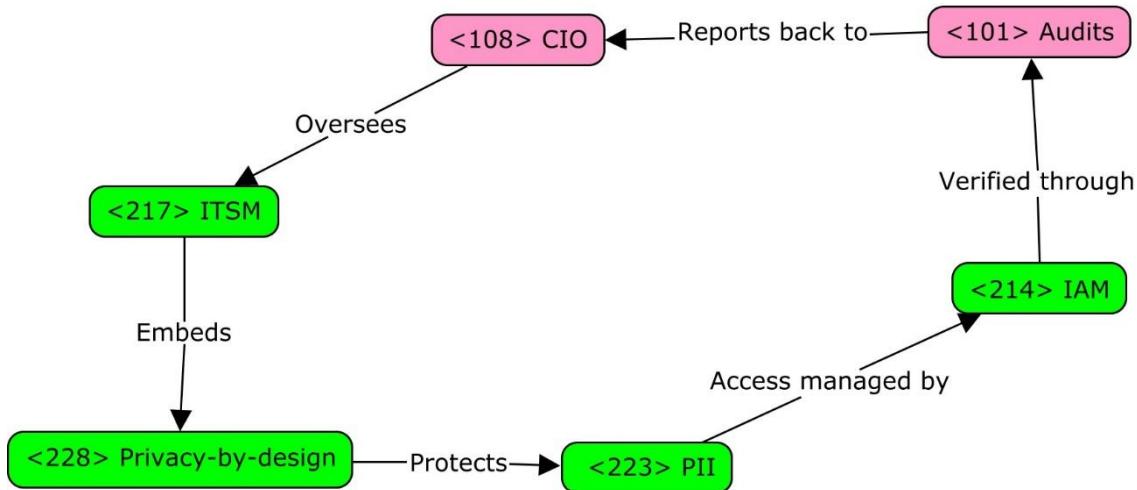


Figure 6 - Concept Map for Healthcare: Remote Patient Monitoring (Theme 2)

Energy and Utilities vs. Transport and Logistics - Organizations, Governance & Management

Both smart energy grids (Energy and Utilities) and electrified fleets (Transport and Logistics) push companies to rethink their <120> Management System and <112> Governance structures.

In the energy sector, the <102> BoD used to focus on a handful of large power plants. Now, they must manage thousands of smaller sources like rooftop solar panels, home batteries, and EV chargers, while keeping energy clean, affordable, and reliable within the new <104> Business Model. Likewise, fleet managers must work with charging stations for their vehicles, vehicle makers, and local regulators to meet rules like low-emission zones, turning logistics into a complex ecosystem.

Both sectors rely on clear <109> Documented Information to share data like <135> Risks assessments and performance metrics. Their key difference lies in the focus, energy <112> Governance deals with long-term national planning and ensuring <103> Business Continuity, while transport <112> Governance focuses on the daily operations, keeping the vehicles operational and making deliveries on time.

Energy and Utilities vs. Healthcare - Organizations, Governance & Management

Smart grids (Energy and Utilities) and remote patient monitoring (Healthcare) both require a change to their <104> Business Model and improvements to their <120> Management System, demanding an overhaul of their <107> Corporate Governance.

In energy, <102> BoDs must shift from just selling electricity to managing and optimizing many different energy sources, while upholding <103> Business Continuity in the face of cyber threats. In healthcare, the leadership must oversee a hybrid care system, where patients' home devices send vital signs back to the hospitals.

Both sectors wrestle with new <135> Risks, such as power outages or connection problems, that can be mitigated by rigorous <110> Due Diligence on third-party vendors. <109> Documented Information and transparency become crucial, energy companies share grid performance data, and healthcare must record patient-consent processes and health outcomes. Yet their ethical focus is different, energy cares about system-wide fairness and availability, while healthcare centers on each person's data privacy and autonomy.

Transport and Logistics vs. Healthcare – Organizations, Governance & Management

Electrified fleets (Energy and Utilities) and remote patient monitoring (Healthcare) both require broader [Governance](#), with complex external networks. Logistics [BoD](#) must now manage relationships with charging stations operators and telematics-software providers. In healthcare, [BoD](#) must oversee medical device manufacturers and cloud service providers.

Both sectors need strong [Ethical Values](#), transport companies must use the data they collect from their drivers fairly and healthcare providers must protect patient's private data. Both rely on [Business Continuity](#) frameworks that anticipate charging-network failures or device connectivity outages, and use [Documented Information](#) to record incident responses. Their shared challenge is balancing operational efficiency with trust, whether its preserving delivery schedules or ensuring safe, equitable patient care.

Energy and Utilities vs. Transport and Logistics – Governance of IT & IT Management

In the face of [Governance of IT & IT Management](#), both energy and transport sectors face the challenge of combining IT and OT (Operational Technology) in a framework that integrates [GRC](#) and [IMS](#). In energy, this means bringing together SCADA systems, smart meters and analytics into one [Risk management](#) setup. For fleet operators it means connecting vehicles systems, like CAN-bus, with cloud-based telematics under one system.

Each sector has different [Compliance](#) needs: Energy companies must follow rules set by the regulators for the [Cybersecurity](#) of critical infrastructures, while transport companies must comply with [GDPR](#) and eFTI rules for [Data Privacy](#) and digital freight. Both must perform [Vendor Assessment](#), to ensure the vendors have a strong [Vulnerability Management](#) and have their hardware and software [Certified](#). Regular [Audits](#) verify firmware integrity on smart devices or over-the-air update pipelines for EV ECUs. In each case, [Governance of IT](#) directly underpins physical safety, whether preventing blackouts or keeping fleets rolling smoothly.

Energy and Utilities

Organizations, Governance, and Management

The **Energy and Utilities sector**—encompassing electricity, gas, water, and emerging renewable sources—faces increasing governance pressures due to its role in national resilience, climate policy, and infrastructure modernisation. Many organisations are aligning their enterprise-wide **<112> Governance** structures with **ISO 37000**, reinforcing principles of transparency, sustainability, and long-term value creation across critical systems.

At the apex, **<102> Boards of Directors (BoD)** are directly engaged in shaping **strategies** that address climate targets, grid reliability, and public accountability. These strategies often rely on **<131> RACI** role models to manage complex relationships between **Transmission System Operators (TSOs)**, **Distribution System Operators (DSOs)**, private contractors, and state regulators—ensuring clear accountability throughout the ecosystem.

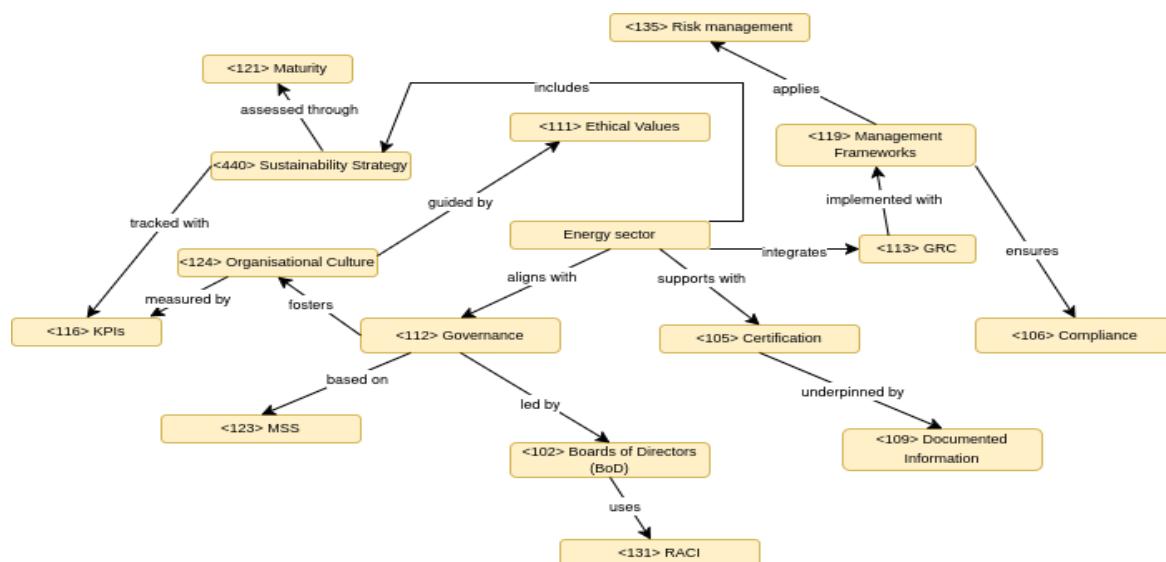
Integrated **<113> GRC (Governance, Risk, and Compliance)** capabilities are central to sector operations. Organisations deploy domain-specific **<119> Management Frameworks**, such as **ISO 31000** for structured **<135> Risk management** across supply disruptions, cyber threats, and infrastructure ageing, and **ISO 37301** to ensure **<106> Compliance** with environmental, safety, and procurement obligations. The **Three Lines of Defence** model is widely used to delineate assurance responsibilities across operational, management, and audit layers.

<105> Certification to internationally recognised **<123> MSS (Management System Standards)** like **ISO 14001** (environmental management), **ISO 55001** (asset management), and **ISO 27001** (information security) is a sector norm—underpinned by well-maintained **<109> Documented Information** systems. These certifications not only strengthen risk controls but also support robust **<103> Business Continuity** planning against grid failures, cyberattacks, or extreme weather events.

External pressures stem from tightening **<134> Regulatory Frameworks**, geopolitical energy dependencies, and binding **ESG** expectations. As a result, **<440> Sustainability Strategy** has become a board-level priority, with formal tracking of emissions, water usage, and energy efficiency through auditable KPIs and mandatory disclosures.

Finally, leading organisations are embedding **<111> Ethical Values** into decision-making and reinforcing a sustainability-oriented **<124> Organisational Culture**—monitored through **<116> KPIs** and **<121> Maturity** assessments.

Concept Map



Energy and Utilities

Governance of IT and IT Management

This sector includes providers of electricity, gas, water, and renewable energy—where digital systems are critical for infrastructure management, service continuity, and regulatory compliance. Technologies like smart meters, SCADA platforms, and AI-driven forecasting support both real-time control and long-term planning. The digital scope spans legacy OT systems and modern IoT networks. Our analysis focuses on organisations with structured IT governance addressing risks in cyber-physical systems and regulatory alignment.

<102> Boards of Directors are increasingly involved in technology oversight, integrating <112> governance of IT with sustainability and resilience strategies. This includes aligning digital initiatives with climate policy and infrastructure reliability. <108> CxO roles, including CIOs and CISOs, operate under <131> RACI models that clarify responsibilities across operators, IT, and compliance teams.

To manage complexity, energy firms apply <119> management frameworks such as ISO 31000 for <135> risk management and ISO/IEC 27001 for cybersecurity. These are part of broader <123> MSS structures that also include ISO 55001 for asset integrity. This ensures <106> compliance and operational control are systematic, auditable, and adaptable.

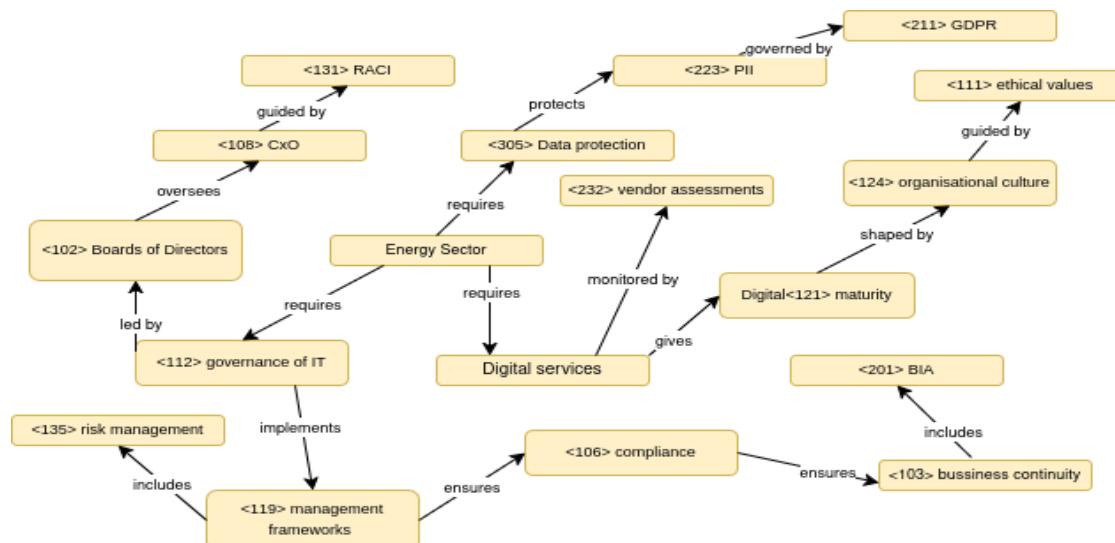
<109> Documented information procedures govern system logs, access controls, and maintenance. These are unified through <114> IMS, which integrates quality, safety, and IT management. <103> Business continuity plans include <201> BIA and disaster recovery for grid failures, cyber incidents, and extreme weather.

<305> Data protection is essential. From grid telemetry to customer records, managing <223> PII is subject to <211> GDPR and increasingly to <207> data localisation laws. Cloud adoption and remote access raise privacy and jurisdictional concerns.

Digital services outsourced to <220> MSSPs and technology vendors require oversight through <232> vendor assessments and <323> SLA monitoring. Growing <205> cyber supply chain risk drives stricter third-party governance and security reviews.

Internally, digital maturity relies on people and culture. <213> HR-led initiatives enhance cybersecurity awareness and align skills with <121> maturity goals. A resilient <124> organisational culture promotes reliability, embedding <111> ethical values into how digital infrastructure is managed and secured.

Concept Map



Hospitality and Leisure

Governance

This industry encompasses a diverse range of businesses dedicated to travel, lodging, entertainment, and recreation, including hotels, resorts, casinos, and theme parks. It is characterised by high customer interaction, dynamic market demand, and exposure to reputational and operational risks. Our focus is on organisations operating across multiple jurisdictions with mature governance frameworks, balancing guest experience, brand integrity, and regulatory compliance in a landscape increasingly shaped by digital transformation and sustainability imperatives.

<102> Boards of Directors are increasingly involved in shaping long-term strategies around guest safety, environmental performance, and ethical sourcing. Governance frameworks use **<131> RACI-based role definitions** to clarify accountability across franchises, service partners, and supply chains.

<113> GRC practices are integrated into operations through sector-relevant **<119> management frameworks**. ISO 37301 ensures **<106> compliance** in areas like licensing and food safety, while ISO 31000 supports **<135> risk management** around service disruption, hygiene, or supplier issues. Many hotel groups use the **<1.10> Three Lines of Defence model** to structure risk and assurance roles.

<105> Certification is a strategic differentiator. Leading brands adopt **<123> MSS** such as ISO 22000 (food safety), ISO 14001 (environment), and ISO 9001 (quality), backed by **<109> documented information** systems. These also support **<103> business continuity** in crises like pandemics or IT failures.

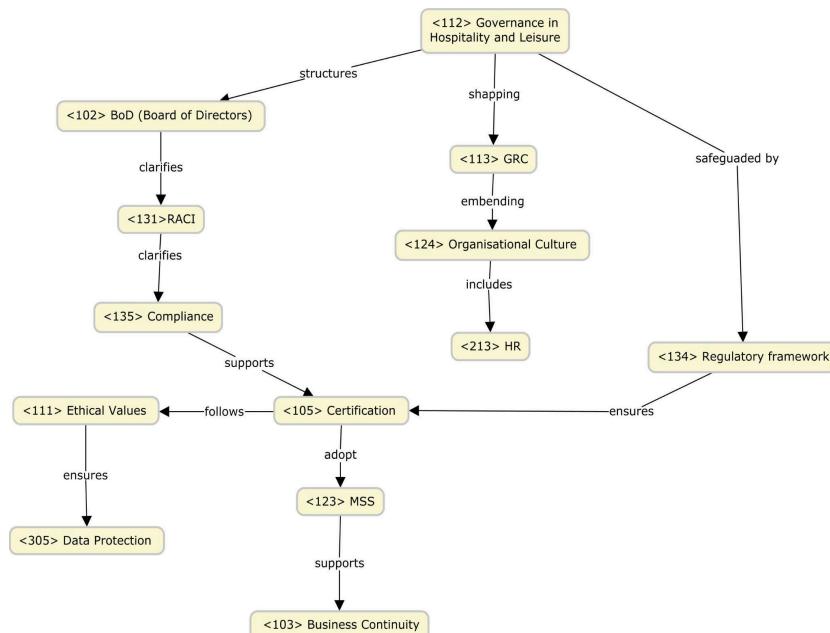
External pressures come from **<133> regulatory bodies**, ESG frameworks, and **<305> data protection** rules—especially in loyalty programs and digital platforms. **<440> Sustainability strategy** is now embedded in governance, with metrics like energy use and emissions reported at board level.

<124> Organisational culture is key in hospitality, where employee conduct directly impacts guest experience. Governance includes **<213> HR-led ethics** programs, DEI training, and **<111> ethical values** embedded in daily operations. These are tracked through **KPIs** and **<121> maturity assessments**.

Digitalisation adds complexity—especially with **<205> cyber supply chain risks** and **<207> data localisation** concerns in global platforms. Leaders are responding with **<232> vendor assessments** and stronger cybersecurity governance to protect data and ensure continuity.

Governance in this sector is no longer just about compliance—it's a strategic function enabling resilience, brand trust, and service excellence.

Concept Map



Hospitality and Leisure

IT Management

This industry includes businesses in lodging, travel, and entertainment—such as hotels, cruise lines, and theme parks—where IT systems are essential to operations and guest experience. From booking engines to IoT-enabled facilities, technology supports real-time service delivery. The scope spans legacy systems and new technologies like cloud, mobile, and data-driven personalization. Our analysis focuses on organisations with centralised IT governance, addressing challenges in cybersecurity, scalability, and digital resilience.

<102> Boards of Directors are increasingly involved in technology oversight, integrating **<112> governance of IT** into broader business strategy. This includes aligning technology initiatives with guest-centric service models and brand standards. **<108> CxO leaders**, such as CIOs and CTOs, operate under **<131> RACI**-based structures that clarify accountability for technology infrastructure, digital services, and innovation pipelines.

To manage complexity, many operators adopt **<119> management frameworks** like ITIL and COBIT, often formalised through **<123> MSS** such as ISO/IEC 20000 (**<313> ITSM**) and ISO/IEC 27001 for **<215> information security**. These systems ensure that **<106> compliance**, risk, and service management are integrated, documented, and auditable. In parallel, **<135> risk assessments** address threats such as system downtime, data loss, and cyberattacks—frequent concerns in globally distributed operations.

<109> Documented information procedures support everything from service logs and user access protocols to asset inventories and backup plans. These are often embedded in **<114> IMS** (Integrated Management Systems), which unify security, quality, and operational controls. To ensure resilience, **<103> business continuity** plans now incorporate **<201> BIA** and **<308> failover capabilities**, especially for high-dependency systems like PMS (Property Management Systems) or guest-facing mobile apps.

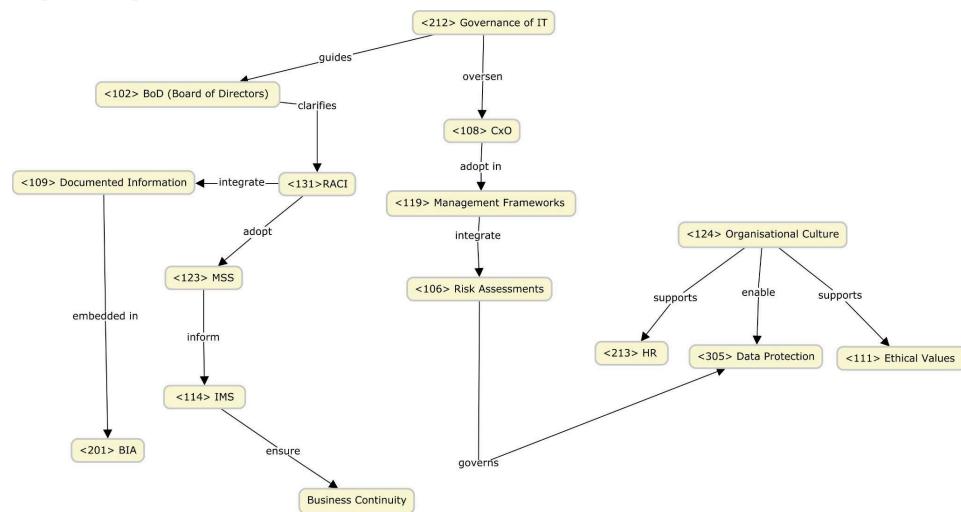
<305> Data protection is another priority. From booking platforms to loyalty programs, the handling of **<223> PII** is governed by frameworks like **<211> GDPR**. Technologies are increasingly evaluated for compliance with **<207> data localisation** laws and privacy-by-design principles, particularly in cloud environments.

Outsourced IT services—ranging from cloud hosting to cybersecurity—require robust oversight. **<232> Vendor assessments** are used to evaluate **<220> MSSPs** and **<219> MSPs**, ensuring they meet agreed **<323> SLAs** and internal control standards. The growing awareness of **<205> cyber supply chain** risk has led to more structured procurement and third-party management practices.

Internally, the success of IT Management also depends on people and culture. **<213> HR-driven initiatives** help build digital capability across hotel operations, from training staff on phishing awareness to ensuring alignment with **<121> maturity** targets. A strong **<124> organisational culture** supports these efforts, embedding **<111> ethical values** into how technology is used, secured, and improved.

In this context, IT Management in hospitality is not simply about systems—it is about delivering trust, resilience, and innovation in every guest interaction.

Concept Map



Banking and Financial Services

Organizations, Governance, and Management

This industry comprises institutions managing money, credit, payments, and risk, including retail and investment banks, insurers, and fintechs. It is characterised by multi-layered regulation, operational risk sensitivity, and strategic reliance on IT infrastructure. Our focus is on regulated financial entities operating across jurisdictions with mature governance systems and compliance-intensive operations.

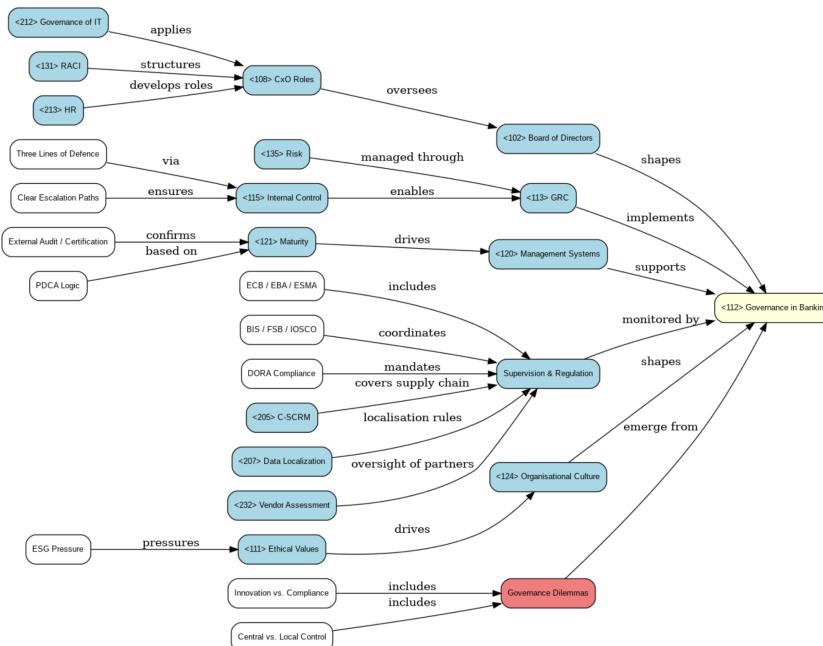
Banking and financial services operate within one of the most advanced and tightly regulated governance environments in the SGSI landscape. These institutions are anchored in **classical corporate governance models** (<107>, <112>) that emphasise structural separation between governance, management, and operations (1.7). At the apex, **Boards of Directors** (<102>) provide strategic oversight through dedicated risk, audit, and compliance committees, with escalating access to key **CxO roles** (<108>)—notably the CRO, CISO, and CCO—who are frequently embedded into governance through <131> RACI-based role mapping and clear escalation protocols.

Governance, Risk, and Compliance (<113>) functions are not siloed but deeply embedded into institutional architecture. Frameworks such as COSO and ISO 31000 serve as the operational baseline for <104> **risk management**, while <115> **internal controls** are implemented through the Three Lines of Defence model (1.10), facilitating control layering and auditability. Certified <120> **management systems** like ISO 37301 (compliance) and ISO 27001 (security) reflect an evolved compliance posture, measurable through <121> **maturity** levels and tracked through structured PDCA cycles. These systems are reinforced by <105> **threat-informed** certification logic and maintained with robust <109> **documented** information procedures to ensure transparency, continuity, and readiness for external assurance.

Externally, the governance environment is subject to multi-tiered supervision. National authorities (e.g., Banco de Portugal), EU supervisory bodies (ECB, EBA, ESMA), and global standard-setters (BIS, FSB, IOSCO) operate through a layered model of oversight, formalised via the Single Supervisory Mechanism (SSM). Regulation has expanded to include digital operational resilience (DORA), third-party risk, <232> **vendor assessment**, <205> **cyber supply chain** risk management (C-SCRM), and <207> **data localisation requirements**—making operational and IT risk a front-line regulatory concern. These supervisory layers are increasingly coordinated through <208> **regulatory compliance frameworks**, which serve as both obligation and strategic lever.

Culture is no less critical. <124> **Organisational Culture** and <111> **Ethical Values** are recognised as soft-controls with material operational implications, shaping tone-from-the-top, employee conduct, and internal compliance climate. These are further structured by <122> **values-based governance** principles and embedded in **HR training structures** (<213>) that define conduct standards across jurisdictions. The interplay between internal culture and regulatory expectation is increasingly scrutinised in formal supervisory dialogues.

Concept Map



Banking and Financial Services

Governance of IT and IT Management

This industry includes institutions responsible for financial intermediation, such as banks, insurers, and digital finance providers. It is characterised by reliance on complex, high-stakes IT systems that underpin everything from payments to regulatory reporting. The scope includes both traditional infrastructures and cloud/fintech integration, shaped by heavy compliance requirements. Our analysis focuses on regulated actors operating under centralised IT governance models and sector-specific cybersecurity standards.

In the banking sector, IT governance is highly mature and deeply integrated into strategic oversight. Institutions apply the principles of **<212> Governance of IT**, often guided by standards like ISO/IEC 38500, to ensure alignment between IT strategy, business risk, and regulatory obligations. IT governance is treated not only as a technical function but as a pillar of institutional resilience.

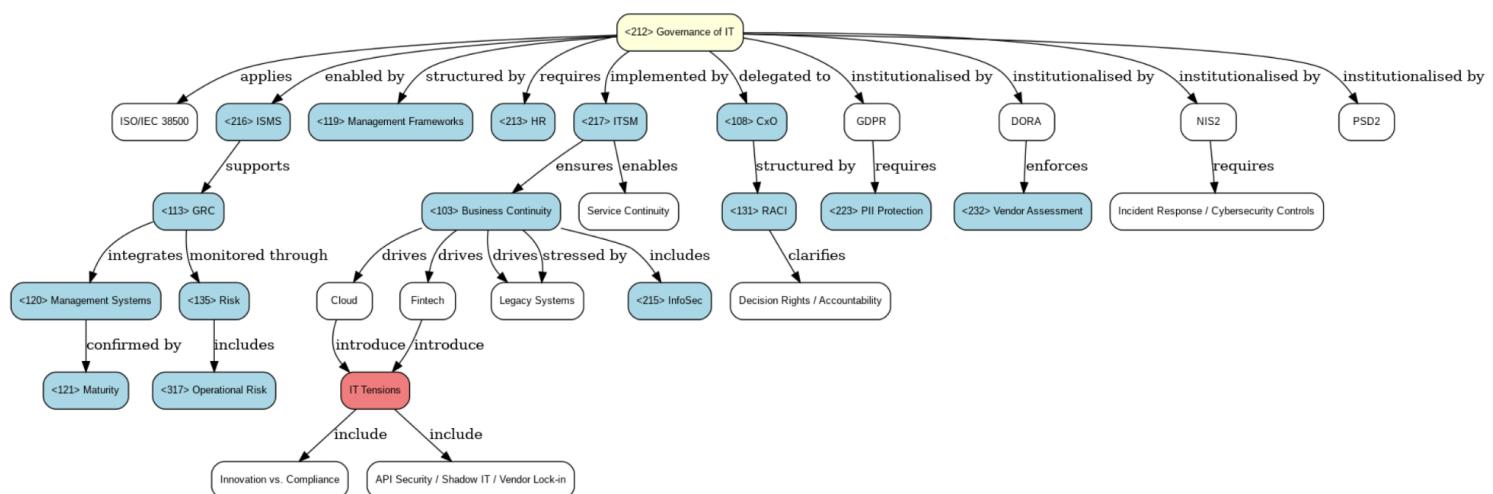
Banks operate in a risk-intensive IT environment, with core systems underpinning payment processing, customer data, and algorithmic decision-making. To manage this complexity, institutions adopt certified **<120> Management Systems**, especially **<216> ISMS** (ISO/IEC 27001) and frameworks like COBIT or NIST CSF, enabling structured IT controls and board-level visibility.

CxO roles in IT—particularly the CIO, CISO, and increasingly the Chief Data Officer—play central roles in balancing innovation, security, and compliance. These roles are supported by formal IT governance structures and clear decision rights (2.3–2.5), with frequent reporting to executive committees and the board. IT governance is intertwined with **<113> GRC**, with cyber risk now a standing item on board agendas.

Compliance pressures like GDPR, PSD2, NIS2, and DORA shape IT management priorities. These influence data governance, vendor risk, encryption, access control, and incident response protocols. IT operations are guided by **<217> ITSM frameworks** (e.g., ITIL), ensuring service delivery, change management, and uptime consistency.

Banks face governance challenges in managing legacy infrastructure, integrating cloud and fintech platforms, and handling emerging threats (e.g., AI bias, API exposure). IT maturity varies across subdomains, but overall, the sector exhibits high alignment between IT capabilities, regulatory risk, and **business continuity** (**<103>**). As such, banking offers a reference case for IT governance in complex, regulated industries.

Concept Map



Organizations, Governance, and Management

Energy and Utilities vs. Banking and Financial Services

Governance Structures:

- Energy and Utilities: Operates under hybrid ownership (state/private) due to natural monopoly status, with governance prioritizing long-term infrastructure stability and environmental compliance (e.g., EU Green Deal). Regulatory bodies enforce strict oversight on tariffs and grid resilience (Regulatory framework).
- Banking and Financial Services: Features centralized, hierarchical governance, with boards and audit committees ensuring solvency and market integrity. External supervision (e.g., SSM, EBA) is multi-layered to mitigate systemic risks.

Risk Management:

- Energy: Focuses on risks like grid outages (operational) and geopolitical supply disruptions, managed via BIA and redundancy planning (Redundancy).
- Banking: Combats operational risks (e.g., cyberattacks, liquidity crises) through ERM and stress testing (Basel III/IV).

Compliance:

- Energy: Aligns with decarbonization policies (e.g., Renewable Energy Directive) and NIS2 for cybersecurity.
- Banking: Adheres to DORA for digital resilience and AML/KYC for fraud prevention (Compliance).

Leadership:

- Energy: Leadership balances affordability and sustainability (e.g., smart grid investments).
- Banking: CxOs (CxO) drive digital transformation (e.g., AI-driven fraud detection) while maintaining customer trust.

Banking and Financial Services vs. Hospitality and Leisure

Governance Models:

- Banking: Rigid, compliance-driven governance with standardized organizational structures (e.g., SSM oversight).
- Hospitality: Decentralized, franchise-heavy models prioritizing local adaptability and brand consistency (Corporate Governance).

Risk Profiles:

- Banking: Systemic risks (Operational Risk) like cyber threats demand Vulnerability Management.
- Hospitality: Reputational risks (e.g., negative reviews) and supply chain disruptions require agile organisational agility.

Compliance:

- Banking: Heavy compliance with GDPR and MiFID II for data and market integrity.
- Hospitality: Focused on health/safety (e.g., HACCP) and GDPR for guest data, but enforcement is fragmented.

Governance of IT and IT Management

Energy and Utilities vs. Hospitality and Leisure

IT Governance:

- Energy: Governance of IT centers on SCADA and smart grids, enforcing Zero Trust for critical infrastructure.
- Hospitality: IT prioritizes PMS and OTA platforms, with weaker ISMS adoption and reliance on MSPs.

Digital Transformation:

- Energy: Leverages AI for demand forecasting and OT resilience (e.g., predictive maintenance).
- Hospitality: Uses Hyperautomation for bookings but faces Technical Debt from legacy systems.

Regulatory IT Demands:

- Energy: Complies with NIS2 and EU Cybersecurity Act for grid security.
- Hospitality: Limited to GDPR; lacks sector-specific IT regulations.

Banking and Financial Services vs. Energy and Utilities

IT Infrastructure:

- Banking: High-performance Enterprise IT Infrastructure for real-time transactions (e.g., CIAM).
- Energy: OT dominates (e.g., grid sensors), with Redundancy ensuring uptime.

RegTech and Compliance:

- Banking: RegTech automates AML/KYC checks and Incident Response.
- Energy: Uses SBOM for supply chain audits and Vulnerability Management for ICS.

Innovation:

- Banking: AI for fraud detection (Explainability) and Digital Wallets.
- Energy: AI optimizes renewable integration but lacks AI governance frameworks.

Resilience:

- Banking: Failover systems for payment platforms.
- Energy: Redundancy in physical/digital grid layers.

SGSI PROJ 1

Group 268

Eduardo Pedrosa ist103600

Pedro Letra ist103622

João Ferreira ist103680

Bernardo Meireles ist103378

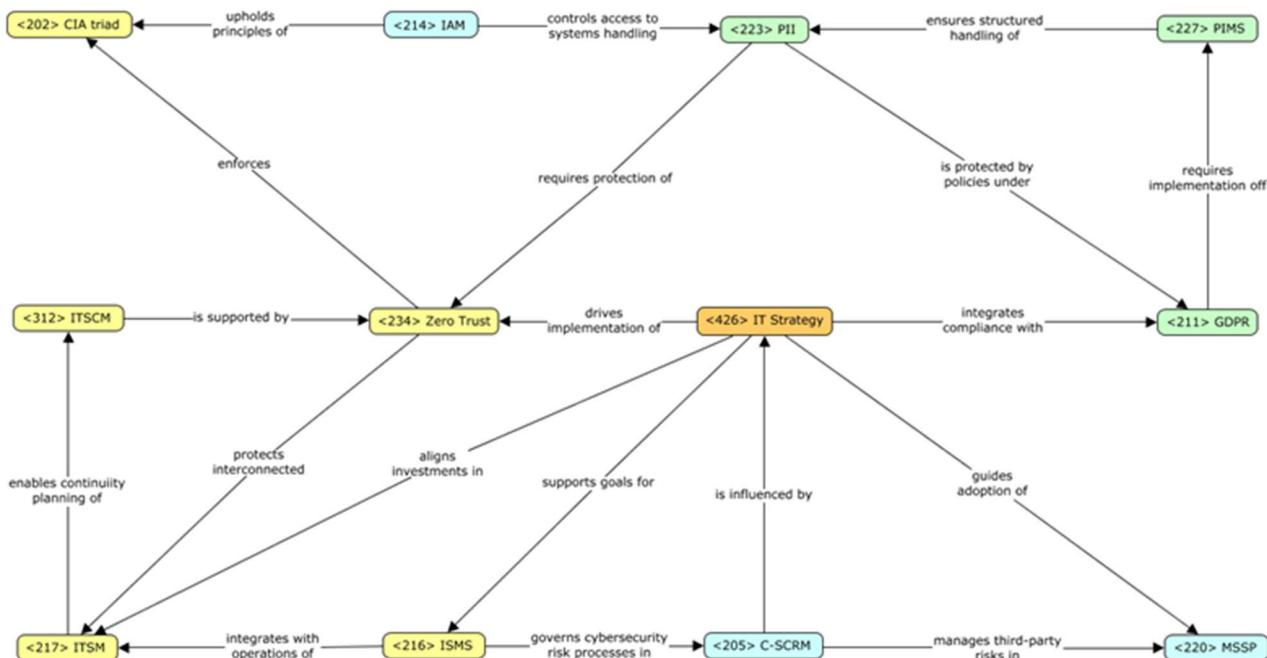
André Teodósio ist99889

Energy and Utilities (2) - IT Management

The Energy and Utilities industry depends on resilient and secure technology operations to support essential services like electricity, gas, and water. To manage critical infrastructure and ensure service continuity, organizations adopt <217> ITSM, <216> ISMS, and <312> ITSCM. These frameworks support operational reliability, regulatory alignment, and rapid response to disruptions, particularly across systems like SCADA and smart grids. As <318> Operational Technology (OT) merges with IT environments, the industry faces heightened cyber risk, making <202> CIA triad principles and <234> Zero Trust models vital to safeguard both legacy and digital assets.

Energy firms operate in a complex risk landscape shaped by <205> C-SCRM, geopolitical tensions, and EU regulations such as the NIS2 Directive and the Green Deal. With smart meters and customer platforms generating large volumes of <223> PII, <106> Compliance with <211> GDPR, <208> Data Privacy, and <227> PIMS becomes essential. This is reinforced by secure access protocols through <214> IAM and proactive <232> Vendor Assessment to mitigate third-party exposure.

The integration of distributed energy resources, the need for real-time monitoring, and decarbonisation goals are accelerating digital transformation across the sector. As a result, many utilities rely on <220> MSSP partnerships for advanced threat detection, while aligning their <426> IT Strategy with climate policy, innovation targets, and cyber-resilience priorities.



Healthcare (8) - IT Management

Healthcare IT environments are among the most complex and risk-sensitive, due to the existence of sensitive personal data, regulatory pressure (e.g., <211> GDPR, HIPAA) and the importance of service continuity. Strong IT Management is essential to support medical workflows and ensure that the underlying technology infrastructure is reliable and resilient.

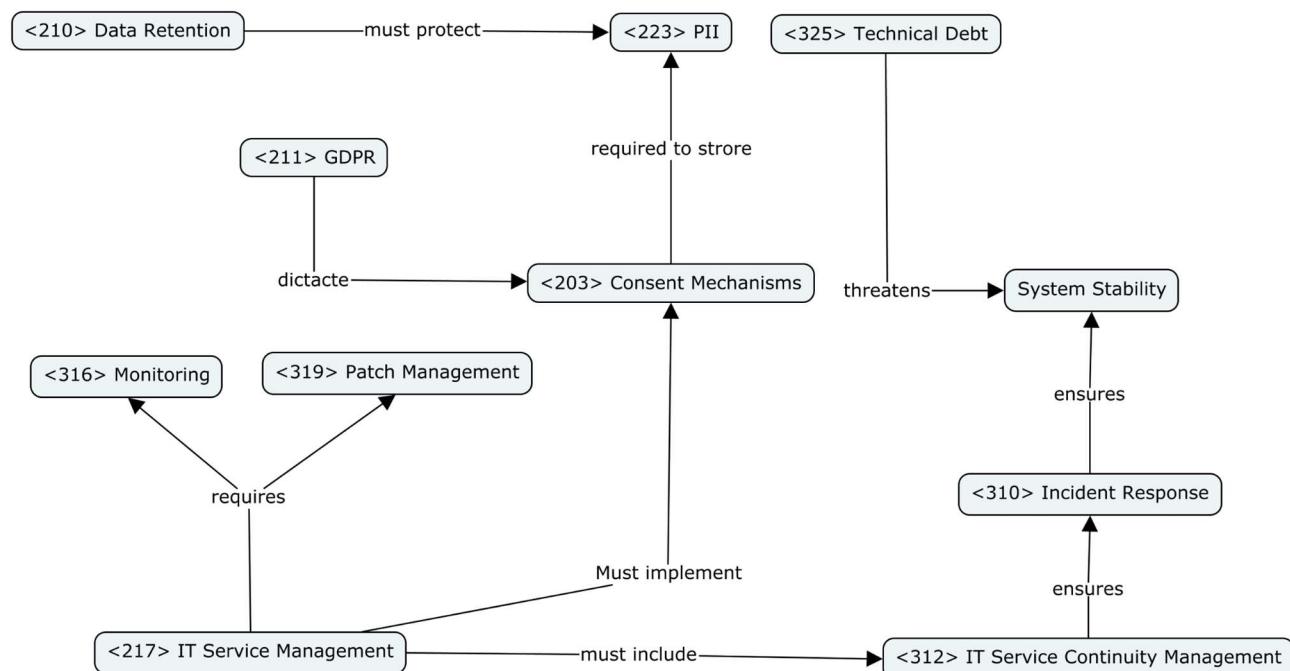
A major challenge is sustaining effective <217> IT Service Management. Hospitals depend on integrated, always-available systems, yet many still face fragmented practices—limited incident response, poor documentation, and unclear service ownership—possibly leading to delays in care, miscommunication, and heightened risk during disruptions.

Mature IT management includes robust <312> IT Service Continuity Management strategies to recover from outages safely, along with proactive <319> Patch Management and <316> Monitoring to reduce vulnerabilities and detect issues early, since even short outages or data inconsistencies can directly impact treatment quality and patient safety.

Lifecycle management is another key concern, as changes like software updates or cloud migrations must be coordinated with clinical needs. Without proper change management with long-term impact in mind, <325> technical debt can build up and compromise system stability.

Data management is equally critical. Hospitals handle large volumes of <223> PII, and IT must ensure secure, compliant storage, access, and processing—through strong access controls, <223> consent mechanisms, and <210> Data retention policies.

Ultimately, effective healthcare IT management demands disciplined coordination among IT teams, clinicians, and external partners. It requires treating IT as a critical service—monitored, maintained, and continuously improved to support patient care at all times.



Healthcare (8) - Governance

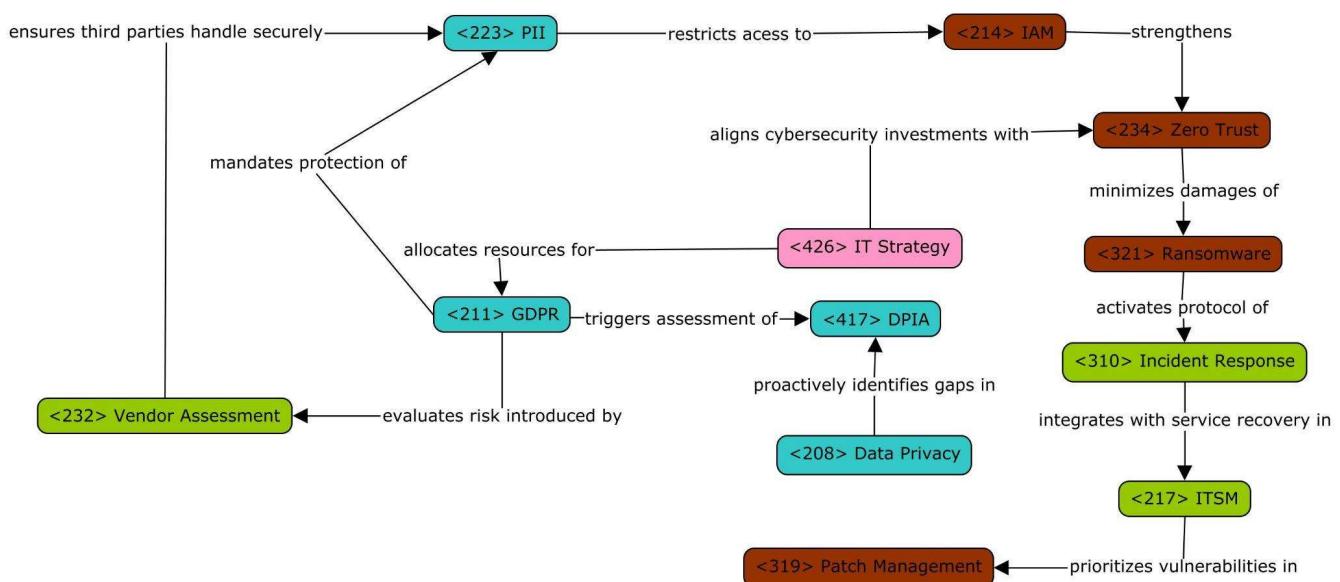
Healthcare is the sector that has the responsibility of the maintenance of the critical lifeline services, the protection of sensitive customer records, and the fulfillment of the compliance obligations. The professional conduct of the executive teams directs rightful decisions to be made on time, so the laws and regulations implementation such as the General Data Protection Regulation (GDPR) <211> and the continued operational resilience are allowed.

An effective information security framework ensures protection of PII and privacy <223> data, while <208> initial. At first, the health sector used the lower layers of the networks and data reps, and the failures to prevent unauthorized access to medical records led to the introduction of <214> IAM. This was further confirmed by the <234> Zero Trust model, which in addition to protecting against operators launching attacks like <320> ransomware.

<217> IT service management is central to supporting uninterrupted clinical operations. Unlike other sectors focused mainly on system security, healthcare prioritizes <310> incident response to minimize disruptions to patient care. Consistent <319> patch management and proactive <316> monitoring ensure that systems remain functional and <215> data security is upheld. Aging IT systems often lead to data loss and reduced treatment quality, reinforcing the need for up-to-date infrastructure.

To reduce risks tied to third-party vendors, thorough <232> vendor assessments are essential—whether they provide cloud services or medical devices. When implementing AI-based diagnostics and digital tools, ensuring safety, ethics, and public trust depends on measures like <417> Data Protection Impact Assessments (DPIAs).

At its core, healthcare security isn't just about rules: it protects patient trust and supports continuous care delivery. By aligning <426> IT strategy with clinical needs, healthcare organizations can stay compliant while still advancing through innovation.

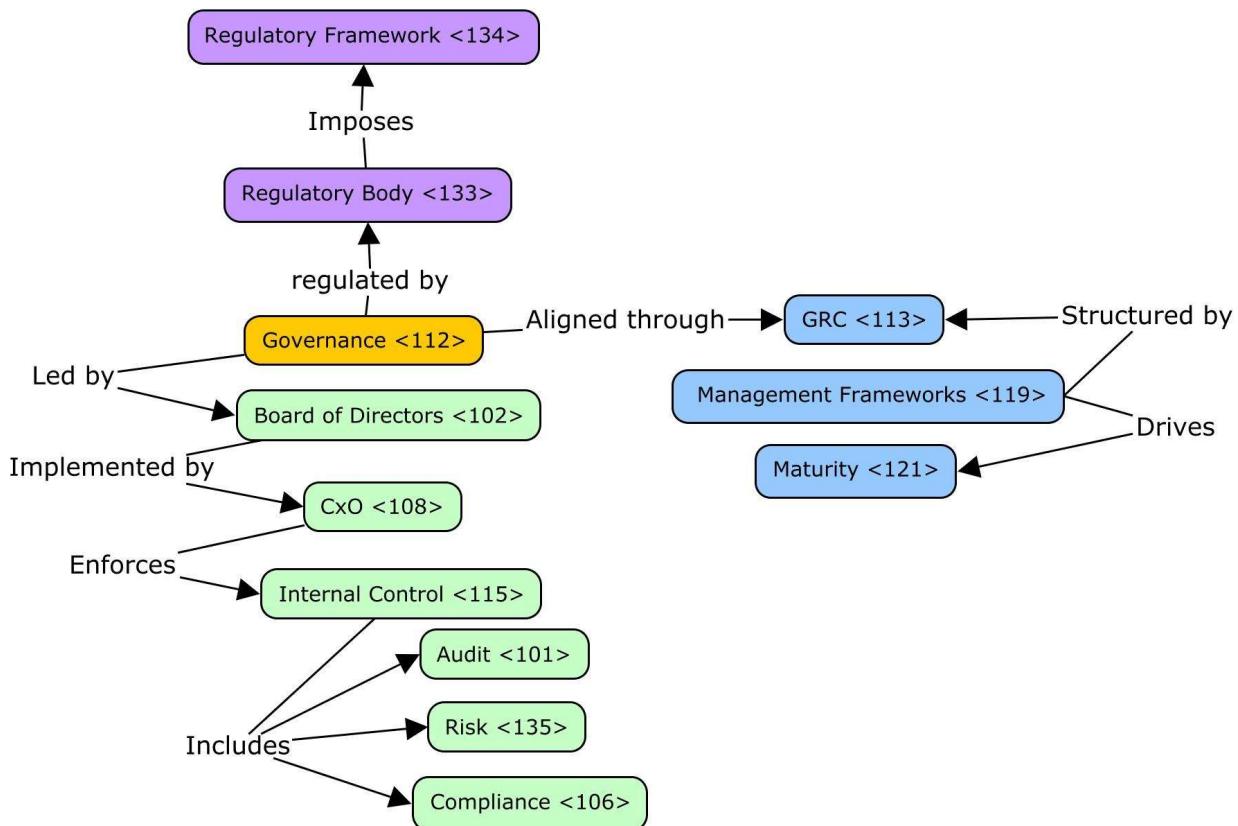


Banking and Financial Services (6) - Governance

Governance **<112>** in the Banking and Financial Services (BFSI) industry is a tightly regulated, multilayered system that balances internal accountability with external regulatory compliance **<106>**. Internally, governance **<112>** is led by the Board of Directors (BoD) **<102>** and high-level executives (CxOs **<108>**), who establish strategic priorities, enforce internal control **<115>** systems, and ensure compliance **<106>** with legal and operational requirements. Functions such as audit **<101>**, risk **<135>**, and compliance **<106>** are formalised and embedded in the governance structure, reflecting a high level of maturity **<121>** demanded by the sector's systemic significance.

Externally, BFSI institutions are supervised by regulatory bodies **<133>** including national authorities (e.g., Banco de Portugal), European entities like the ECB, EBA, ESMA, and global regulatory frameworks **<134>** like Basel III/IV and the Financial Stability Board (FSB). These bodies ensure adherence to capital, liquidity, operational risk, and digital oversight, reinforced under regulations like DORA and AML/KYC.

To align IT and enterprise governance, management frameworks **<119>** such as COBIT and ISO 38500 are used to define roles, responsibilities, and decision-making mechanisms. The use of integrated GRC **<113>** frameworks ensures alignment across governance, risk **<135>**, and compliance **<106>** efforts. In BFSI, governance **<112>** is not simply a legal obligation, it is a value driver ensuring operational resilience, strategic alignment, and long-term stakeholder trust.



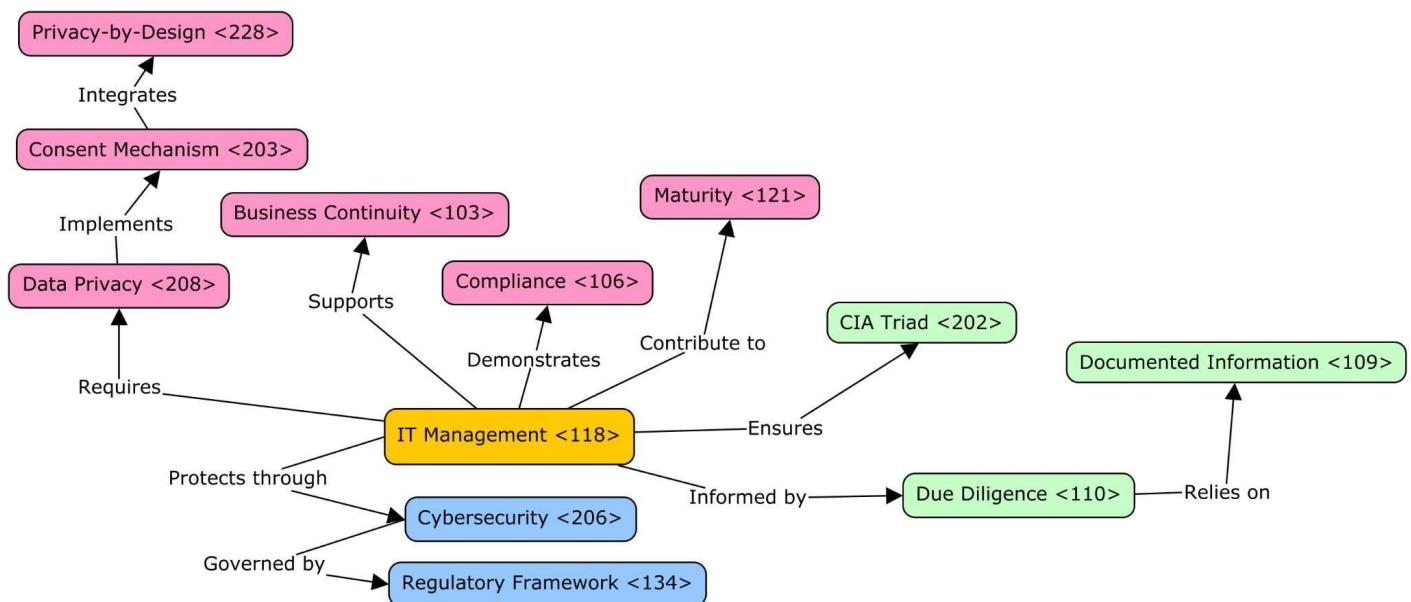
Banking and Financial Services (6) - IT Management

In the BFSI sector, IT management <118> is a strategic function critical for business continuity <103>, cybersecurity <206>, and sustainable innovation. Strategic alignment is led by CxOs <108>, especially the CIO, who ensure technology supports the institution's business model <104>. Tools like COBIT guide <212> Governance of IT and control, while ITIL standardises service operations such as change management, incident handling, and service delivery.

Resilience and security are essential given BFSI's systemic exposure. Concepts like the CIA triad <202> (Confidentiality, Integrity, Availability) are fundamental to digital infrastructure. In parallel, audits <101> and KPI <116> tracking ensure transparency and performance accountability. Regulations like GDPR, DORA, and Basel frameworks require demonstrable control and compliance <106> across digital services.

Vendor management is another key domain. Many financial firms rely on external technology providers, cloud infrastructure, or managed services. Therefore, due diligence <110> and documented information <109> are critical to maintain operational integrity and meet regulatory framework <134> expectations.

Frameworks such as IMS <114> help unify IT, security, compliance, and performance into one cohesive system. Ultimately, effective IT management in BFSI combines strategic foresight, technical governance, and institutional maturity <121> to enable adaptive, compliant, and secure financial ecosystems.



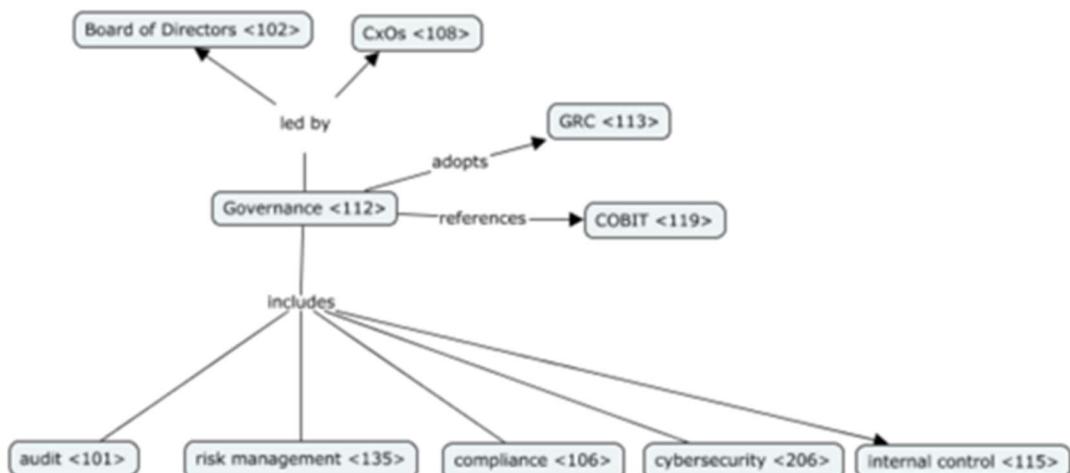
Energy and Utilities (2) - Governance

Governance <112> in the Energy and Utilities sector operates through a multi-layered structure where the Board of Directors <102> and senior executives (CxOs <108>) establish strategic priorities balancing security of supply, affordability, sustainability, and digital innovation. Internal governance functions including audit <101>, risk management <135>, compliance <106>, cybersecurity <206>, and internal control <115> are formalized at the C-level and embedded within dedicated committees to manage long investment cycles and critical service dependencies through continual oversight and reporting.

Risk <135> is segmented into four core domains: operational (SCADA/ICS failures, OT cyberattacks), market (energy-commodity price volatility, supply-chain constraints), regulatory (evolving decarbonization targets, grid-code updates), and geopolitical (import dependencies on critical minerals and fuel). Each feeds into executive risk dashboards that inform budgeting, capital allocation, and contingency planning.

Externally, operators face oversight by national regulators and EU bodies under frameworks such as the Clean Energy Package, Electricity and Gas Directives, Renewable Energy Directive, EU Cybersecurity Act, and NIS2 Directive. These mandate integrated energy-and-climate planning, emissions reporting, cybersecurity controls, and cross-border interoperability. International coordination occurs via the IEA, IRENA, IEC/ISO standards, and UNFCCC climate-finance mechanisms, requiring governance models that adapt to varying regulatory maturity <121> and infrastructure age across jurisdictions.

To align technology governance with strategic and regulatory demands, firms adopt integrated GRC <113> platforms and reference frameworks such as COBIT <119> and ISO/IEC 38500, while sector-specific standards like IEC 62443, ISO/IEC 27019, and NERC CIP provide detailed controls for SCADA, smart-grid deployments, energy-trading platforms, customer-facing portals, and ICT Asset Management <309> software. This integrated approach ensures coherent policies across IT and OT domains, enabling robust incident response, vulnerability management, and continuous compliance <106> monitoring.



Energy and Utilities (2) vs Healthcare (8) - IT Management

The Energy and Utilities and Healthcare industries differ in IT priorities but face similar challenges in <306> Enterprise IT Infrastructure and <215> InfoSec. The first industry focuses on securing <318> Operational Technology, like SCADA systems under <206> Cybersecurity frameworks such as NIS2, using <230> SBOM and <205> C-SCRM for <231> Supply Chain risks. On the other hand, the second industry emphasizes <208> Data Privacy and <211> GDPR compliance for <223> PII, leveraging <227> PIMS and <417> DPIA.

Both sectors combat <321> Ransomware differently: Energy and Utilities prioritizes <303> Cyber Resilience for grids, while Healthcare focuses on <310> Incident Response for patient data.

Shared hurdles include <325> Technical debt and <326> XaaS adoption, with Energy using hybrid clouds for <314> Logging and Healthcare relying on cloud EHRs. <234> Zero Trust is key for <214> IAM in both sectors. But it is important to note that the Energy and Utilities industry ties <426> IT Strategy to sustainability objectives, whereas the Healthcare industry pursues <412> Digital Maturity through <401> AI integration. Both manage <323> SLAs commitments and <324> Shadow IT risks, united by the need for robust <216> ISMS and <217> ITSM practices.

Healthcare (8) vs BFSI (6) - IT Management

Healthcare IT prioritizes continuous availability and patient safety. Strong <217> ITSM and <312> IT Service Continuity Management (ITSCM) planning are critical to prevent and quickly respond to disruptions that could directly affect patient care. With high volumes of sensitive <223> PII, compliance with <211> GDPR and HIPAA is non-negotiable.

In contrast, BFSI IT management emphasizes resilience, control, and trust. Frameworks like ITIL and COBIT guide service delivery, while <206> cybersecurity and <103> Business Continuity are tightly enforced through audits, KPIs, and regulatory compliance (e.g., DORA, Basel). <114> IMS helps unify IT with governance and risk functions.

Both sectors demand mature, context-aware IT practices—healthcare for operational immediacy, BFSI for systemic stability and compliance.

Healthcare (8) vs BFSI (6) - Governance

In the <101> Audit-driven Banking and Financial Services Industry (BFSI) and the mission-critical <122> Mission-oriented Healthcare sector, besides the Governance is the one that decides the actions to be done, the inherent <135> Risk and the regulatory compliance <106> are other major issues. But, services provided and the nature of data determine the actual differences in the priorities, frameworks, and pressures.

<112> Governance in the BFSI sector is deeply linked with <102> BoD oversight, <136> Top Management direction and implemented <115> Internal Control mechanisms. Organizations follow unified <113> GRC frameworks so as to keep through <117> Leadership, <439> Strategy, and <135> Risk management the reference from one side in line with the requirements from <133> Regulatory bodies such as the ECB, EBA, and local financial authorities. The use of <116> KPI metrics and <119> Management Frameworks has enhanced performance and ensured a good <121> Maturity level, especially to survive digital transformation and market turbulence.

In contrast, Healthcare relies on <112> Governance to safeguard patient trust, <208> Data Privacy, and system continuity <103>. While <106> Compliance with standards like <211> GDPR and sector-specific laws are vital, governance is equally driven by <111> Ethical Values and <122> Mission to "do no harm." Governance efforts focus on <215> InfoSec, <216> ISMS, and <227> PIMS to protect <223> PII, with a strong emphasis on <310> Incident Response and <233> Vulnerability Management.

Energy and Utilities (2) vs Banking and Financial Services (6) - IT Management

Energy and Utilities and Banking and Financial Services both rely on robust <306> Enterprise IT Infrastructure and stringent InfoSec <215> controls. Energy focuses on securing OT environments including SCADA and smart-grid telemetry under NIS2 and sector-specific frameworks, while Finance centers on high-availability core banking systems, payment gateways, and digital channels. Both sectors combat software supply-chain risks via SBOM <230> and C-SCRM <205> practices—Energy to manage firmware in IIoT devices, Finance to vet third-party fintech libraries.

Ransomware <321> resilience differs between sectors: Energy invests in cyber-resilience <303> for grid recovery and island-mode fail-over, whereas Finance emphasizes incident response <310> playbooks and fast-track forensic analysis. Shared challenges include Technical Debt <325> and XaaS <326> adoption—Energy uses hybrid-cloud logging <314> to centralize OT/IT telemetry, Finance migrates to micro-services for elasticity—while both grapple with Shadow IT <324>.

A unified shift to Zero Trust <234> and robust IAM <214> underpins both industries, yet Energy's IT strategy <426> is driven by sustainability and grid-optimization goals, while Finance pursues digital maturity <412> through AI-driven <401> risk analytics. Both mandate clear SLAs <323> and an integrated ISMS <216> alongside mature ITSM <217> practices to ensure service continuity and regulatory compliance <106>.



TÉCNICO LISBOA

Security and Management of Information Systems
2024/2025

P1 - Governance & IT Management

Authors:

Martim Moita de Abreu (98956)
Franisco Pereira de Oliveira (99939)
Gonçalo Pereira Correia (105788)
Jakub Dominik Grabski (112980)

martim.abreu@tecnico.ulisboa.pt
francisco.p.oliveira@tecnico.ulisboa.pt
goncalopcorreia.12@gmail.com
jakub.grabski@tecnico.ulisboa.pt

Group 278

1 Agriculture and Farming

1.1 Governance

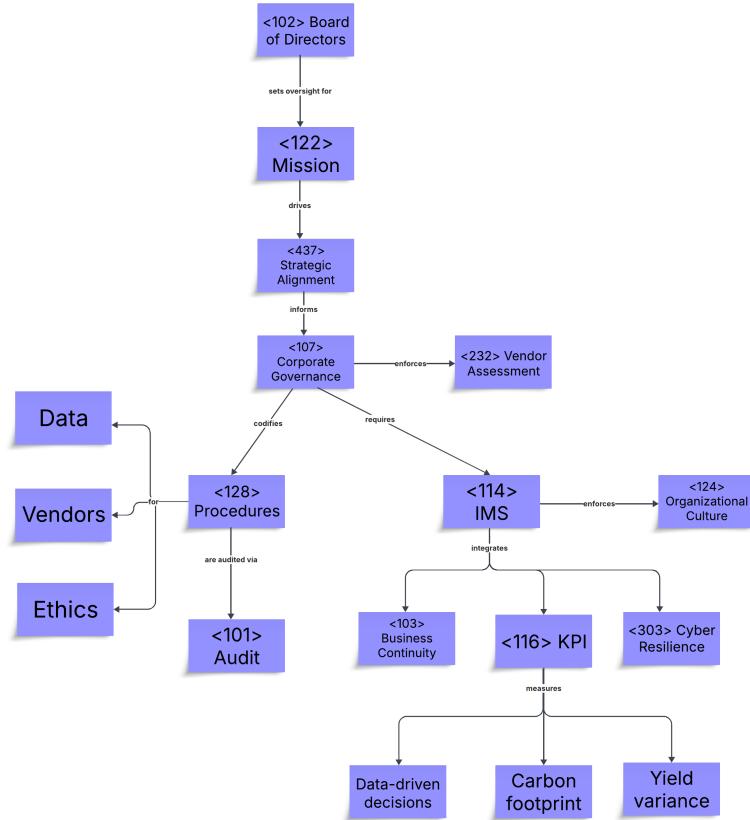


Figure 1: Concept Map 1.

The shift of the agricultural sector towards digitization - through precision sensors, autonomous machinery, and data platforms—demands robust Governance **<112>** to ensure that technology investments serve both productivity and sustainability. At the apex, the Board of Directors **<102>** must articulate a clear Mission **<122>** that balances yield maximization with environmental stewardship. This requires a formal Corporate Governance **<107>** — combining corporate policies and Procedures **<128>** for data ownership, privacy, and vendor oversight. Embedding an Integrated Management System **<114>** unifies agronomic, financial, and IT controls, enabling transparent decision making between senior leadership and field operations. A strong Organizational Culture **<124>** encourages cross-functional collaboration and ethical use of farmer data, while periodic Audits **<101>** and Vendor Assessments **<232>** validate compliance with performance and sustainability criteria. The board should also sponsor a Business Continuity **<103>** program and Cyber Resilience **<303>** exercises, integrating climate-risk scenarios (e.g., drought, flood) and cyberattack simulations to test response protocols. By aligning the governance construct with strategic goals - enabled through Strategic Alignment **<437>** and monitored via KPIs **<116>** such as carbon footprint reduction and data-driven yield improvements - farm enterprises can foster stakeholder trust, regulatory compliance, and long-term resilience.

1.2 IT Management

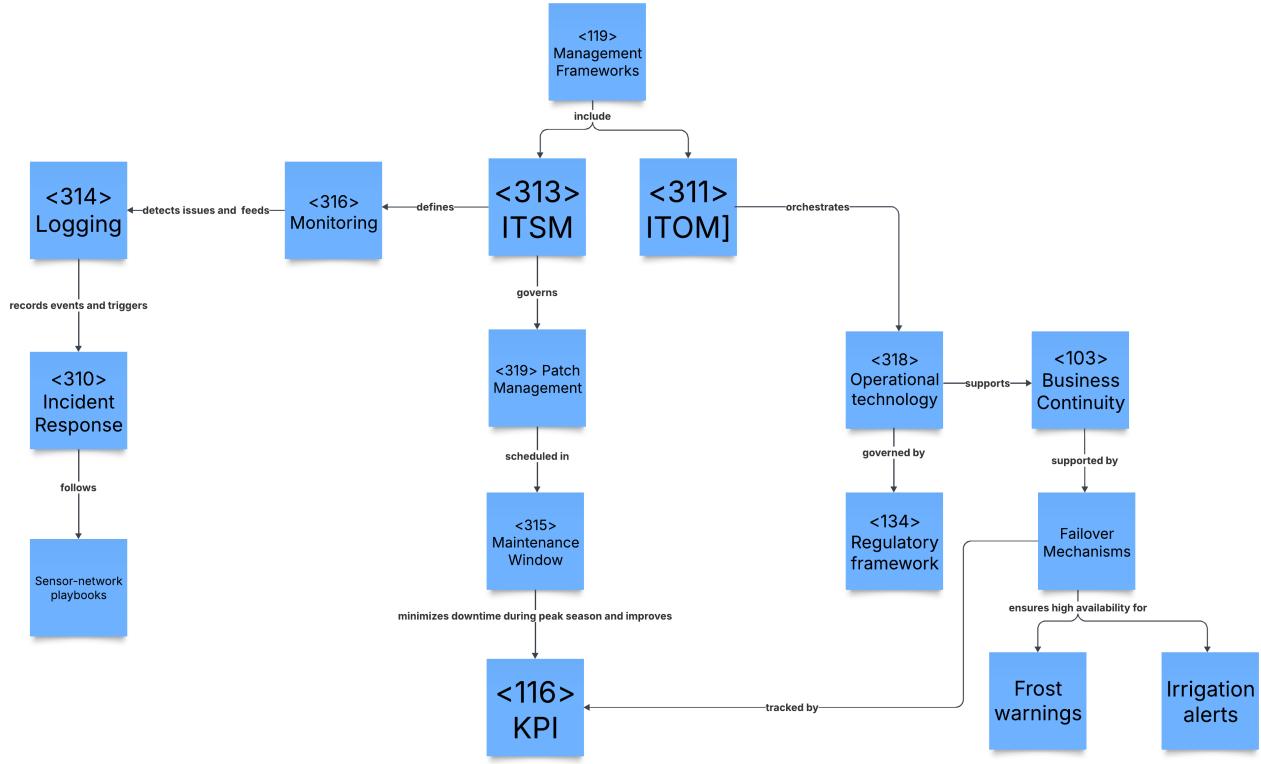


Figure 2: Concept Map 2.

Precision-farming's reliance on sensors, drones, and analytics demands a strong Governance of IT <212> framework to align digital tools with agronomic goals. At the top, the Board of Directors <102> must ratify a clear Strategic Alignment <437> between tech investments and sustainability targets, embedding oversight into an overarching Corporate Governance <107> that codifies roles, policies, and controls.

Underpinning this, documented Processes <129> and Procedures <128> govern the data lifecycle—from Data Privacy <208> and GDPR <211> compliance through Data Residency <209> restrictions to secure Vendor Assessments <232> of IoT and cloud providers. A robust GRC <113> capability integrates Cybersecurity <206> standards—defining approval workflows for firmware updates, encryption requirements, and third-party risk reviews—while periodic Audits <101> verify adherence.

Formalizing IT Service Management <313> within this governance structure ensures that change requests e.g., firmware or AI-driven irrigation schedules follow an approved Change Control process, with security sign-off and documented Configuration Management <129>. Embedding a mature Risk Orientation <135> means conducting Business Continuity <103> and Cyber Resilience (<303>) exercises that test recovery from sensor-network outages or ransomware attacks.

By linking these elements—board-level strategy, GRC, data governance, vendor oversight, and risk testing—agricultural enterprises can transform technology from a tactical add-on into a governed, accountable, and resilient pillar of modern farming.

2 Energy and Utilities

2.1 Governance

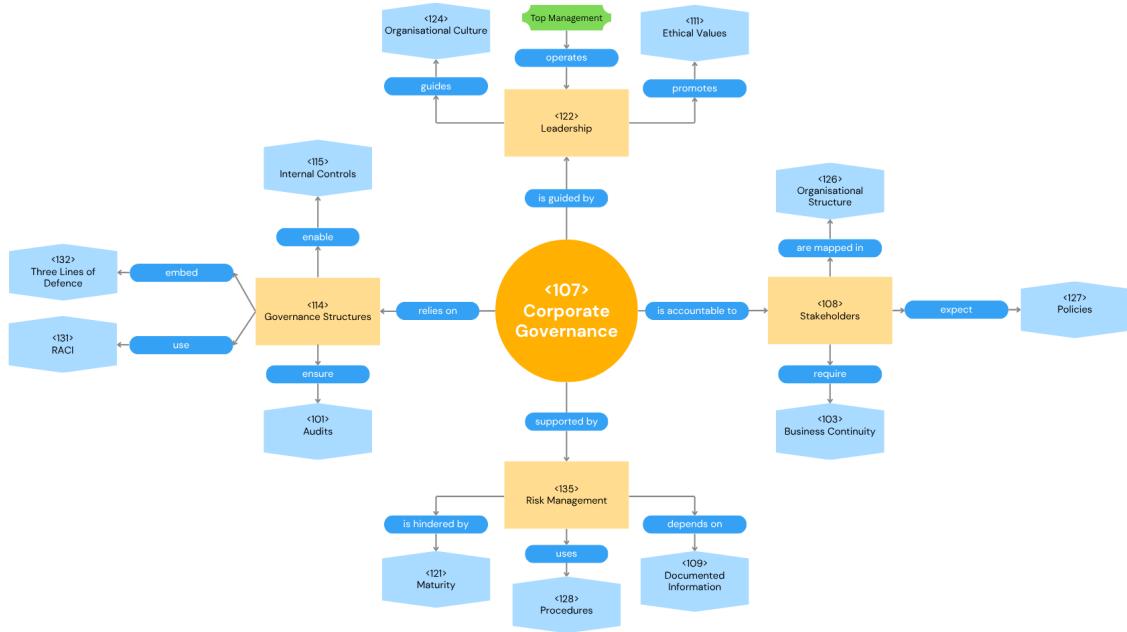


Figure 3: Concept Map 3.

The governance of energy and utility organisations requires robust, transparent, and accountable structures due to their role as critical infrastructure. Sound <112> Governance must go beyond formal oversight, embedding principles of <111> Ethical Values, <106> Compliance, and <135> Risk management into all strategic layers.

A recurring weakness is the lack of integrated <120> Management Systems, which results in fragmented processes and poor alignment between <107> Corporate Governance and operational delivery. Without consistent <127> Policies, <128> Procedures, and traceable <109> Documented Information, many organisations lack the mechanisms needed for timely and informed decision-making.

The absence of clear <131> RACI structures obstructs accountability, particularly during disruptions requiring rapid coordination between business and technical actors. This is further exacerbated when <124> Organisational Culture is risk-averse or hierarchical, limiting transparency and collaboration.

Legacy structures and public ownership often correlate with low <121> Maturity, limiting proactive adoption of <123> MSS or modern <119> Management Frameworks such as COBIT or ISO/IEC 27001. Consequently, <115> Internal Controls are underutilised, and Board-level <102> BoD visibility into digital risks remains superficial.

To build resilience, governance should adopt a systemic approach supported by <101> Audits, enforce role clarity through <126> Organisational Structure, and empower <136> Top Management to drive mission-aligned <122> Leadership.

2.2 IT Management

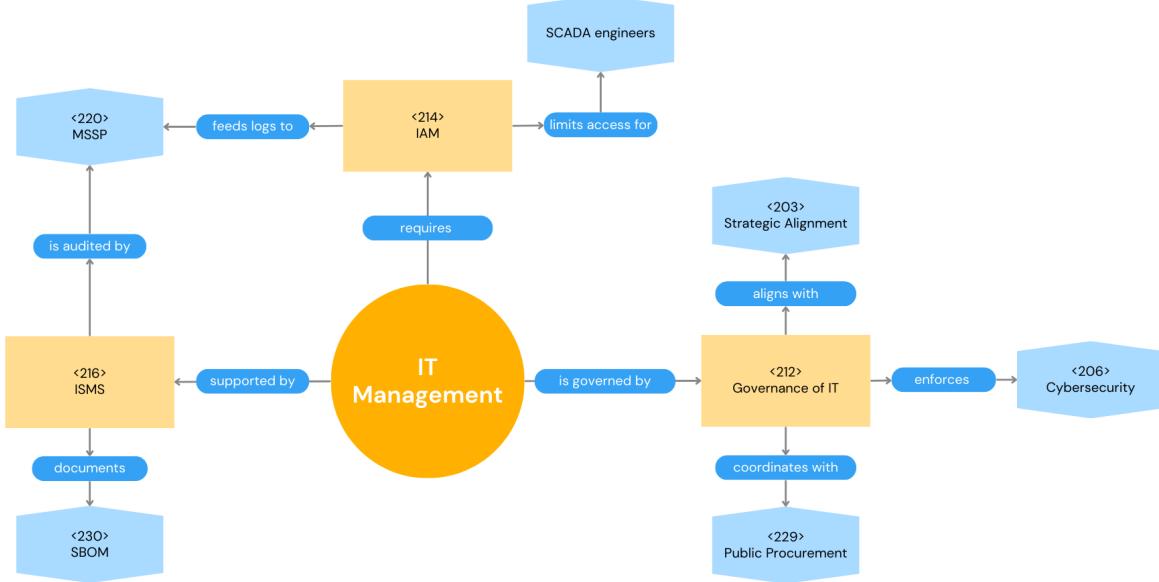


Figure 4: Concept Map 4.

The Energy & Utilities sector depends on a hybrid estate of supervisory-control (SCADA), edge sensors, and market-IT platforms. Board-level **<212>** Governance of IT therefore sits alongside traditional risk committees, ensuring that every digital decision supports security-of-supply mandates and decarbonisation targets. A first maturity signal is a functioning **<203>** Strategic Alignment mechanism: road-maps for smart-grid or hydrogen roll-outs must flow from national energy policy into IT investment gates and budget cycles.

Regulated status drives a certified **<216>** ISMS, extending ISO 27001 controls into OT enclaves. The ISMS links policy to practice by enforcing continuous **<206>** Cybersecurity risk treatment, supplier scrutiny through **<205>** C-SCRM, and documented mitigation for vulnerabilities unique to ageing turbine firmware. Access boundaries are governed by **<214>** Identity & Access Management, segmenting dispatcher consoles, market traders, and field-maintenance crews under least-privilege rules.

When incidents occur, a sector-specific **<215>** Incident Response play-book—tested in coordination with grid operators—activates within NIS 2’s one-hour disclosure window. Lessons learned feed back into the ISMS and into board dashboards, closing the governance loop that lecture 2 emphasises. Procurement is another lever: **<229>** Public Procurement clauses now oblige vendors to provide SBOMs and to accept joint red-team testing before any OT upgrade is commissioned.

Accountability remains central. Utilities assign a CIO and CISO but also nominate an OT-focused Chief Engineer to satisfy three-lines-of-defence expectations. These role boundaries, tracked in **<211>** GDPR registers for smart-meter data, ensure that cyber-physical risk is owned, audited, and reported without friction between operational and market silos.

3 Healthcare

3.1 Governance

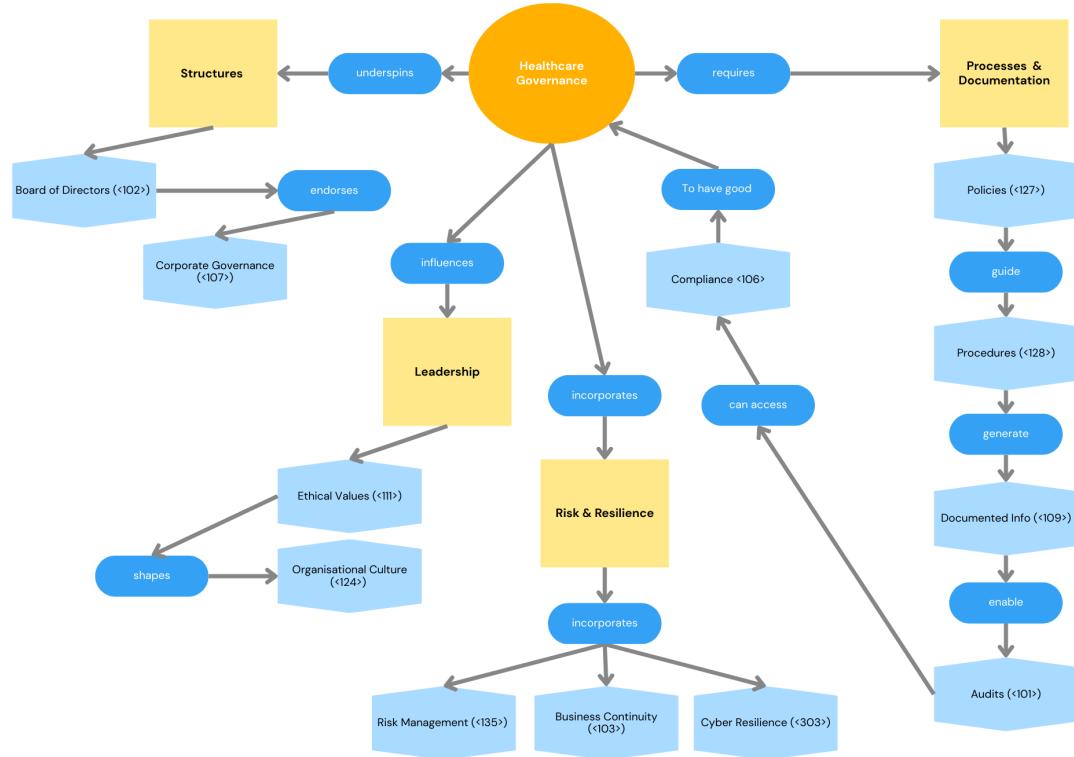


Figure 5: Concept Map 5.

The governance of the healthcare sector demands robust, transparent, and accountable structures given its status as critical infrastructure. Effective governance **<113>** must extend beyond formal oversight to embed Ethical Values **<111>**, Compliance **<106>**, and Risk Management **<135>** across all strategic layers—from the Board of Directors **<102>** down to frontline clinical teams. A recurring weakness is the lack of an Integrated Management System **<114>**, resulting in fragmented processes and misalignment between Corporate Governance **<107>** and actual care delivery. In the absence of consistent Policies **<127>**, documented Procedures **<128>**, and traceable Documented Information **<109>**, healthcare organizations lack the real-time insights required for timely, informed decision-making. The absence of clear RACI structures **<131>** obstructs accountability, especially during crises such as IT outages or disease outbreaks, when rapid coordination between clinical, technical, and vendor stakeholders is critical. This challenge is exacerbated when Organizational Culture **<124>** is hierarchical or risk-averse, limiting transparency and interdisciplinary collaboration. To build resilience and patient trust, healthcare governance should adopt a systemic approach supported by regular Audits **<101>**; codify Business Continuity **<103>** and conduct Cyber Resilience exercises **<303>**. Defining a clear Organisational Structure **<126>** to drive mission-aligned Leadership **<122>** is an essential step toward delivering safe, efficient, and patient-centered care.

3.2 IT Management

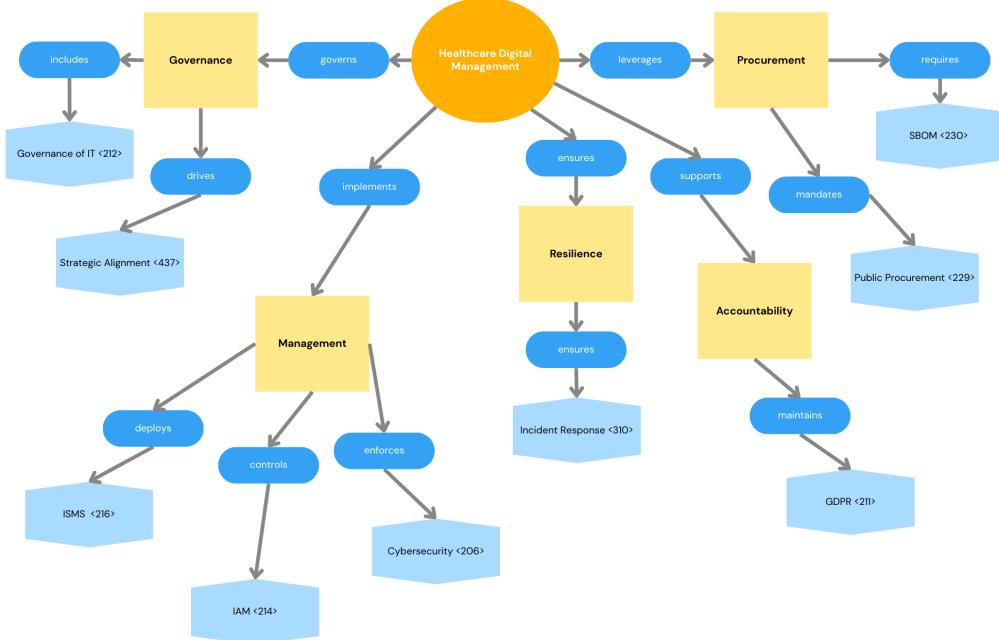


Figure 6: Concept Map 6.

The healthcare sector's IT estate spans electronic health records, AI-driven diagnostic tools, and integrated administrative systems. Board-level Governance of IT <212> ensures every IT decision upholds patient safety and regulatory mandates. A primary maturity indicator is a functioning Strategic Alignment <437> mechanism: digital roadmaps for EHR upgrades or tele-ICU roll-outs must flow from clinical strategy into IT investment approvals and budget cycles. Regulatory requirements drive a certified ISMS <216> (ISO 27001), extending controls into clinical networks and connected medical devices. The ISMS translates policy into practice by enforcing continuous Cybersecurity <206> risk treatment, supplier assessment via C-SCRM, and documented mitigation plans for vulnerabilities in legacy imaging systems. Access boundaries are enforced by IAM <214>, segmenting physicians, administrative staff, and third-party vendors under least-privilege principles. When breaches or outages occur, a tailored Incident Response <310>—tested in coordination with data-privacy officers—activates under NIS 2's one-hour notification window. Post-incident reviews feed insights back into the ISMS and board dashboards, closing the governance loop. Procurement is another strategic lever: Public Procurement <229> clauses now require device vendors to supply SBOM <230> and undergo joint red-team exercises before clinical deployment. Clear role definitions underpin accountability. Healthcare organisations appoint a CIO and CISO alongside a Chief Medical Information Officer to satisfy three-lines-of-defence expectations. These role boundaries, tracked in GDPR registers <211> for patient data, ensure digital risks are owned, audited, and reported seamlessly across clinical, operational, and market silos.

4 Comparisons

Governance (Agriculture&Farming VS Energy&Utilities):

Agriculture's governance of digital systems often remains informal: farm owners delegate technology decisions ad hoc, lacking a formal Governance Framework <107> or documented Procedures <128> for data collection and vendor oversight. By contrast, Energy & Utilities embed digital strategy into their corporate Mission <122> and employ an Integrated Management System <114> that unifies risk, compliance, and operations under board-mandated controls. Utilities conduct regular Audits <101> and rigorous Vendor Assessments <232>—reviewing SLAs, cybersecurity posture, and resilience metrics—ensuring that SCADA suppliers meet clear performance thresholds. Farms, however, seldom engage their Board of Directors <102> in technology governance, nor do they run structured Business Continuity <103> or Cyber Resilience <303> exercises, leaving them vulnerable to sensor network failures or supply-chain disruptions. Energy firms' mature Governance Culture <124> yields documented escalation paths and stakeholder transparency; agriculture's informal culture impedes cross-farm learning and slows adoption of best practices. To close this gap, agri-enterprises should codify digital oversight into a formal Governance Framework <107>, adopt periodic Audits <101>, and involve senior leadership in Strategic Alignment <437> between tech investments and sustainability goals.

IT Management (Agriculture&Farming VS Healthcare):

In Agriculture, digital governance is informal: farms often lack a formal Governance of IT <212> framework and have no clear Strategic Alignment <437> between tech investments and agronomic goals. By contrast, Healthcare embeds its digital roadmap into enterprise strategy, with the Board of Directors <102> sponsoring a robust Corporate Governance <107> that codifies Processes <129> and Procedures <128> for data privacy <208>, vendor assessment <232>, and cybersecurity <206>.

Agriculture typically handles firmware updates and sensor deployments on an ad hoc basis. Healthcare, however, operates under mature IT Service Management <313> disciplines: they maintain a CMDB and integrate Monitoring <316> and Logging <314> into their GRC <113> capability.

To align with best practices, Agriculture must formalize its Governance of IT <212> by adopting a documented Corporate Governance <107>, defining Strategic Alignment <437>, and embedding ITS <313> processes, such as Vendor Assessments <232>, and Cybersecurity <206> reviews—into its operational DNA.

Governance (Healthcare VS Agriculture&Farming):

In the <113> governance framework of healthcare, board-level oversight by the Board of Directors <102> embeds Ethical Values <111>, Compliance <106> and Risk Management <135> across all strategic layers. Yet many organisations lack an Integrated Management System <114>, leading to fragmented processes and misalignment between Corporate Governance <107> and care delivery. Without consistent Policies <127>, Procedures <128> and traceable Documented Information <109>, real-time decision-making falters; the absence of RACI structures <131> and a hierarchical, risk-averse Culture <124> further impedes accountability. To strengthen resilience and trust, boards mandate regular Audits <101>, codify Business Continuity <103> plans, run Cyber Resilience <303> exercises, and enforce mission-aligned Leadership <122> through a clear Organisational Structure <126>. In the <112> governance model of agriculture, board governance <102> begins with a clear Mission <122> that balances yield maximisation and environmental stewardship. Formal Corporate Governance <107>—backed by Policies and Procedures <128>—and an Integrated Management System <114> unify agronomic, financial, and IT controls. A collaborative Organisational Culture <124> underpins ethical data use, while periodic Audits <101> and Vendor Assessments <232> validate performance and sustainability criteria. To prepare for climate-driven disruptions, boards sponsor Business Continuity <103> programmes and Cyber Resilience <303> drills. Finally, Strategic Alignment <437> and KPIs <116> (e.g., carbon-footprint reduction, yield improvements) translate governance into measurable long-term resilience.

IT Operations Management (Energy&Utilities VS Healthcare):

In the <212> Governance of IT hierarchy of *Energy & Utilities*, board-level oversight is driven by national-infrastructure mandates: transmission-system operators, regulators, and ministries demand verifiable control of <206> Cybersecurity for SCADA and smart-grid assets. Utilities therefore embed a formally certified <216> ISMS that ties OT patch windows to grid codes and NIS 2 reporting. Role scoping is handled through granular <214> IAM that separates market-IT users from control-room engineers, while supplier firmware is tracked in a mandatory <230> SBOM. Procurement cycles are public-tender-heavy; the CIO must align road-maps with <229> Public Procurement law before any cloud or sensor refresh.

Healthcare shares the same foundational building blocks yet applies them to a patient-safety lens. Hospital boards still adopt <212> Governance of IT, but strategic authority is split with clinical governance committees. The <216> ISMS emphasises <207> Data Privacy and 72-hour GDPR breach duties rather than grid-code resilience, and medical-device vendors must supply a <233> Vulnerability Management statement before software is accepted onto a ward network. Identity control via <214> IAM is clinician-centric (single-sign-on, prox-cards), and change freezes are negotiated around surgery lists, not power-load curves. Procurement remains regulated but is brokered through framework agreements instead of grid-operator tenders, and <229> Public Procurement clauses stress HIPAA/GDPR conformance over NIS 2.

Segurança e gestão de Sistemas de Informação, Instituto Superior Técnico

Vicente Gomes (99135), Margarida Almeida (102769),
 Afonso Matos (103479), Henrique Caroço (103860)

1 Industry 3 - Retail and Digital Commerce

Retail and Digital Commerce is the industry that connects products and services to consumers through both physical stores and online platforms, using digital technologies to manage everything from inventory and payments to customer relationships and personalized marketing.

1.1 Connection of industry 3 to the Theme 1 - Organisations, Governance, and Management.

The **Retail and Digital Commerce** industry is characterized by the integration of physical retail operations with digital platforms, enabling a smooth consumer experience both in-store and online. Businesses in this sector use technology to enhance customer engagement and operational efficiency, with strategies such as optimized inventory management, personalized marketing, and the use of omnichannel approaches, to ensure consistency and convenience both online or in person.

Effective < 112 > Governance in retail and digital commerce is a must in today's world. As these crucial areas continue to expand, governance must know how to balance operational agility with long-term brand value and < 231 > Supply Chain responsibility. This also involves responsible data use, ethical marketing, and vendor < 118 > Management, all across interconnected systems.

< 117 > Leadership roles (especially boards, CIOs, and CISOs) play a key role in managing operations that go from physical stores to digital platforms, and even hybrid architectures. These leaders are tasked with essential tasks, such as aligning customer experience, < 305 > Data Protection, and agile logistics. With that, many different types of < 135 > Risk arise, which must not be overlooked to prevent escalation. < 317 > Operational Risk, reputational, cyber and < 106 > Compliance risks are key types in these industries that leaders must have in mind for every decision made, in order to avoid major consequences.

Digital platforms add further governance challenges. Retailers depend on third-party ecosystems (like marketplaces and social media) that are out of their control - this introduces issues such as data sovereignty and algorithmic accountability. These types of platforms also introduce tools like the ERP, CRM, and ePOS, requiring governance to ensure data integrity and ethical practices in this new environment.

Strategically, governance also involves adapting to evolving customer expectations. This includes practices which reinforce new values, such as inclusivity and sustainability.

With all this, compliance is strongly regulated by frameworks, to avoid wrongdoings. In the EU, the < 211 > GDPR, Consumer Rights Directive, the DSA and DMA create a layered environment. These regulations inspect customer rights and platform accountability, making sure businesses follow the legal standards.

To conclude, governance in retail and digital commerce is about responsible leadership in a volatile, ever-changing digital environment.

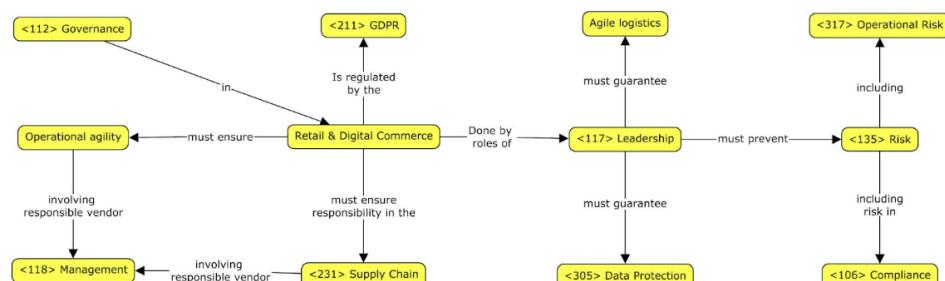


Figure 1: Concept map for Industry 3 - Organisations, Governance, and Management.

1.2 Connection of industry 3 to the Theme 2 - Governance of IT and IT Management.

Information Technology (IT) is crucial to modern retail and digital commerce, making possible a seamless integration of physical and digital operations. Nowadays, IT systems are the foundation of both <438> Strategic Planning and daily operations.

Key IT systems include the Enterprise Resource Planning (ERP) for inventory and logistics, Customer Relationship Management (CRM) for loyalty and engagement, and Point of Sale (POS/ePOS) for transaction processing. Effective IT <118> Management ensures these systems operate in a secure and cohesive fashion.

Retail increasingly operates in complex digital ecosystems, like third-party marketplaces, social media platforms, and app stores. As these platforms are out of the control of the retailer, new challenges emerge around data sovereignty, third-party <135> Risk, and algorithmic transparency. IT leaders must be aware of these emerging challenges while maintaining <115> Internal Control and data integrity.

With all this, many different retail subdomains emerge, with ranged offerings and demands. Omnichannel retail combines digital and physical, requiring seamless data and <129> Process integration; Pure-play e-commerce focuses on scalability, speed, and cost-per-acquisition; DTC brands rely on narrative, community, and personalisation. Marketplace sellers, meanwhile, operate on third-party platforms, limiting infrastructure control. With all these new models, the traditional Brick-and-mortar retailers must evolve, in order to compete with the other more advanced subdomains.

In relation to <439> Strategy, IT management must ensure <231> Supply Chain responsibility, customer <305> Data Protection, and the application of sustainability policies. As digital commerce keeps constantly evolving, IT becomes a key driver of innovation, <106> Compliance, and customer trust.

To conclude, IT management is essential for retail and digital commerce businesses to remain competitive, while assuring resilience and regulatory alignment in an ever-changing digital landscape.

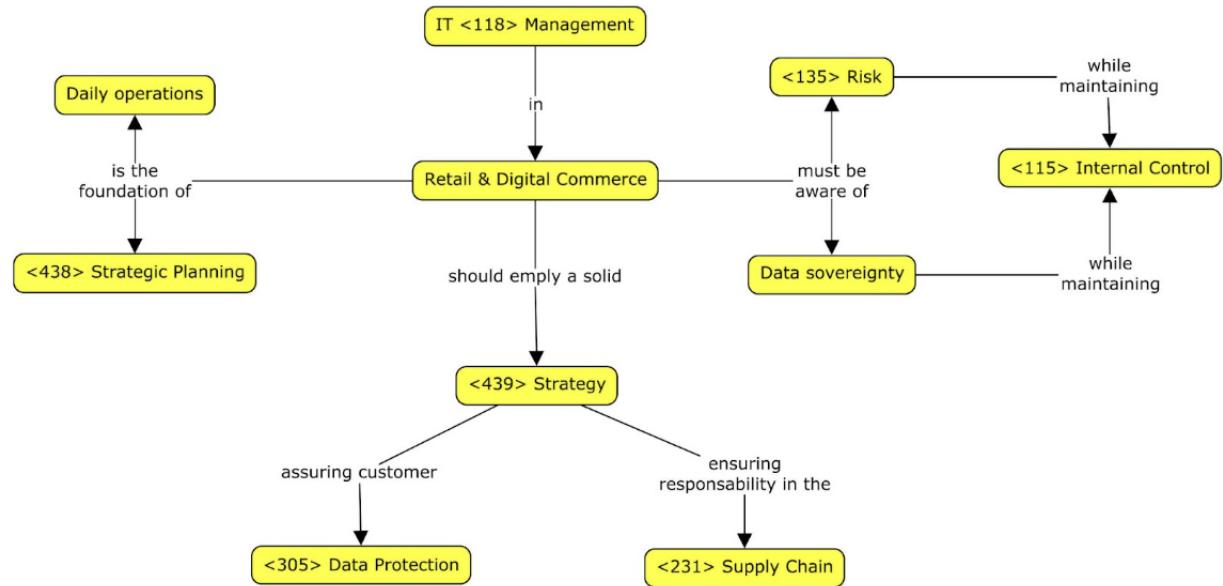


Figure 2: Concept map for Industry 3 - Governance of IT and IT Operations.

2 Industry 4 - Transport and Logistics

The **Transport and Logistics industry** encompasses a broad ecosystem responsible for moving goods and people through interconnected systems such as road, rail, air, and maritime networks. It is characterized by its operational complexity, reliance on infrastructure, and critical role in enabling global trade and economic stability.

2.1 Connection of industry 4 to the Theme 1 - Organisations, Governance, and Management.

The Transport and Logistics industry operates under complex < 112 > governance systems to direct, control, and ensure accountability. Governance coordinates critical functions like infrastructure maintenance, safety management, and supply chain resilience. The < 102 > BoD sets < 127 > policies balancing efficiency, < 106 > compliance, and < 111 > ethical values.

A core element of governance is < 113 > GRC, which integrates capabilities to achieve objectives, manage uncertainty, and ensure compliance with extensive < 134 > regulatory frameworks. The industry faces multidimensional < 135 > risk profiles, including operational risks, regulatory risks, and geopolitical risks impacting cross-border freight and just-in-time logistics. Effective risk management is essential to mitigate disruptions such as strikes, fuel price volatility, or geopolitical conflicts, ensuring < 103 > business continuity.

< 106 > Compliance obligations are extensive, requiring adherence to vehicle certification, safety < 101 > audits, emission controls, transport licensing, and customs procedures. International bodies like the International Civil Aviation Organization set standards for safety and trade. These < 134 > regulatory frameworks necessitate robust < 115 > internal controls and < 105 > certification processes, often verified by third-party bodies. Public-private collaboration, common in infrastructure and mobility planning, relies on clear < 126 > organizational structures and < 131 > RACI frameworks to define responsibilities and enhance accountability.

Governance also addresses environmental and sustainability challenges, with < 127 > policies to promote decarbonization and territorial cohesion. The < 124 > organizational culture shapes how these policies are implemented, fostering values of safety, reliability, and sustainability. < 116 > KPIs are used to measure service punctuality, safety compliance, and operational efficiency, ensuring governance supports long-term resilience and stakeholder trust.

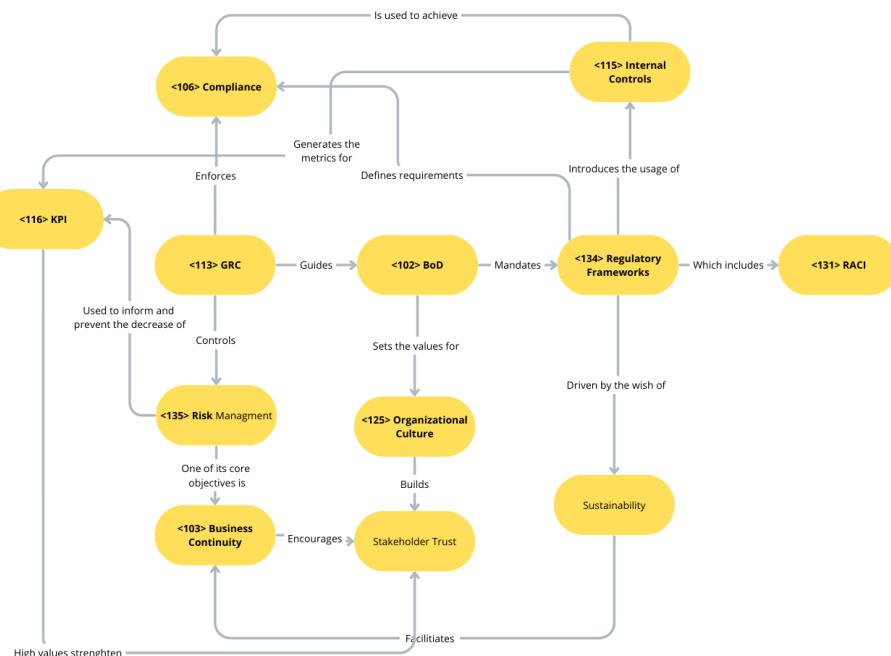


Figure 3: Concept map for Industry 4 - Organisations, Governance, and Management.

2.2 Connection of industry 4 to the Theme 2 - Governance of IT and IT Management.

The Transport and Logistics industry relies heavily on < 212 > Governance of IT to direct and control the use of information technology, ensuring alignment with organizational objectives. IT systems are critical for digital coordination, encompassing traffic and fleet management, logistics platforms, passenger information systems, and IoT for cargo tracking. These systems enhance operational efficiency, real-time routing, and inventory visibility, supporting the sector's role in supply chain resilience.

A cornerstone of IT management is the < 216 > Information Security Management System, which safeguards the < 202 > CIA triad of information. < 206 > Cybersecurity is paramount, as control systems and booking platforms are vulnerable to cybersecurity threats. < 233 > Vulnerability management and < 234 > zero trust architectures are increasingly adopted to mitigate risks, particularly in supply chain software. The industry also employs < 205 > Cybersecurity Supply Chain Risk Management to address risks from third-party vendors, ensuring secure data exchange.

Data protection is governed by < 211 > GDPR, mandating < 228 > privacy-by-design principles in system architectures, such as opt-in < 203 > consent mechanisms for passenger data processing. The EU's eFTI Regulation facilitates digital freight data exchange, requiring interoperable systems like Logistics Management Systems (LMS) and fleet telematics. These systems must comply with < 207 > data residency and < 210 > data retention < 127 > policies, ensuring < 233 > PII is processed securely by < 224 > PII controllers and < 226 > PII processors.

Interoperability challenges arise from integrating diverse systems, such as port and airport management platforms. < 217 > ITSM practices ensure these systems deliver value, while < 220 > MSSPs offer outsourced threat detection. Strategic IT management must address automation, electrification, and platform integration, aligning with the sector's decarbonization and digital transformation goals.

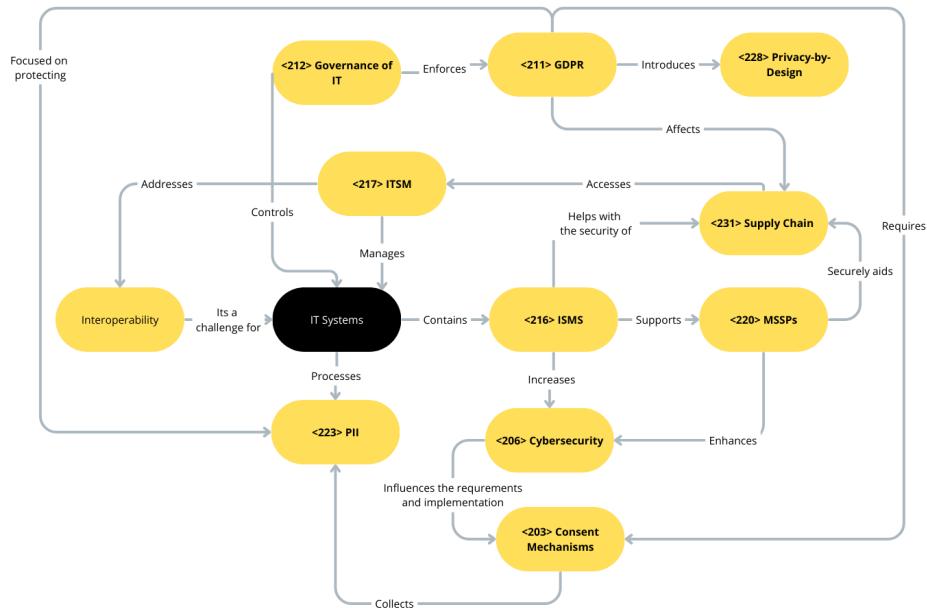


Figure 4: Concept map for Industry 4 - Governance of IT and IT Operations.

3 Industry 5 - Hospitality and Leisure

The Hospitality and Leisure industry is a diverse sector encompassing accommodation, food services, travel, entertainment, and recreation, unified by its focus on guest experience, service quality, and discretionary consumption. It is characterized by operational intensity, high employee turnover, and strong reliance on reputation. Highly sensitive to external factors like economic shifts and geopolitical events, it navigates a complex landscape of varied ownership structures, digital platform dependencies, and fragmented regulatory frameworks, requiring robust governance for managing operational, reputational, and compliance risks.

3.1 Connection of industry 5 to the Theme 1 - Organisations, Governance, and Management.

Governance in Hospitality and Leisure revolves around aligning operational agility with regulatory and ethical standards. Corporate Governance <107> is driven by the Board of Directors <102> and Top Management <136>, who establish policies <127> and procedures <128> to ensure compliance with diverse frameworks like GDPR <211> (for guest data), health and safety regulations, and sustainability certifications (e.g., Green Key). The GRC <113> framework integrates risk management <135> (e.g., operational disruptions, reputational damage) and compliance <106> obligations, supported by internal controls <115> and regular audits <101>.

The sector's organizational structure <126> must balance centralized governance with localized adaptability, reflecting organizational culture <124> and leadership <117> priorities. For example, multinational hotel chains enforce standardized management systems <120> (e.g., ISO 9001 for quality), while family-owned resorts may prioritize community engagement. Business Continuity <103> planning is critical to address seasonal demand fluctuations and crises like pandemics. Maturity <121> in governance is evidenced by adherence to regulatory frameworks <134> (e.g., labor laws, environmental codes) and alignment with ethical values <111>.

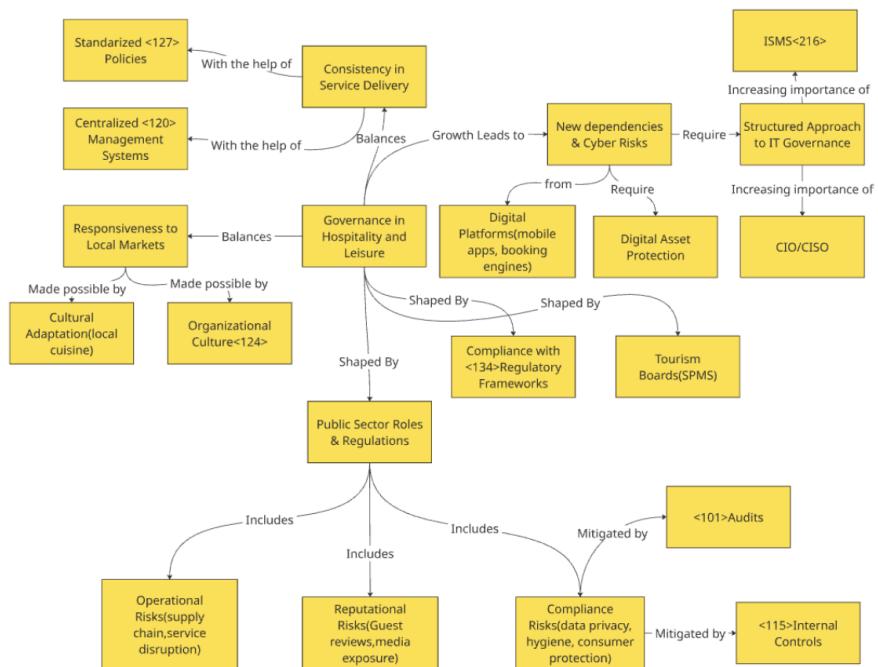


Figure 5: Concept map for Industry 4 - Organisations, Governance, and Management.

3.2 Connection of industry 5 to the Theme 1 - Organisations, Governance, and Management.

IT Management is critical in Hospitality and Leisure, balancing seamless guest experiences with robust security and compliance. The sector's reliance on digital tools such as Property Management Systems (PMS) for bookings and Online Travel Agencies (OTA) like Booking demands rigorous Governance of IT < 212 >. Implementing an ISMS < 216 > ensures compliance with GDPR < 211 > when handling PII < 223 >, such as guest payment details or loyalty program data. For example, hotels must embed Privacy-by-design < 228 > in CRM systems to manage consent (opt-in/opt-out) transparently, avoiding fines and reputational damage.

Cybersecurity < 206 > is paramount due to third-party risks. OTAs and IoT devices (e.g., smart room controls) expand attack surfaces, necessitating IAM < 214 > for role-based access and Zero Trust < 234 > models to secure hybrid environments. A compromised OTA API could leak reservation data, underscoring the need for Vendor Assessment < 232 > to ensure partners meet security standards. ITSM < 217 > ensures operational reliability like resolving ePOS outages during peak dining hours while Vulnerability Management < 233 > patches weaknesses in interconnected systems, such as outdated PMS firmware.

Hospitality's supply chain < 231 > includes vendors for IoT devices or cloud services, requiring Public Procurement < 229 > checks for cybersecurity certifications. Data Localization < 207 > rules further complicate cloud strategies for global chains storing EU guest data.

Ultimately, IT Management enables Business Continuity < 103 >, ensuring PMS and booking engines function during crises. By aligning IT governance with the sector's guest-centric culture, organizations mitigate risks while enhancing competitiveness through secure, innovative services.

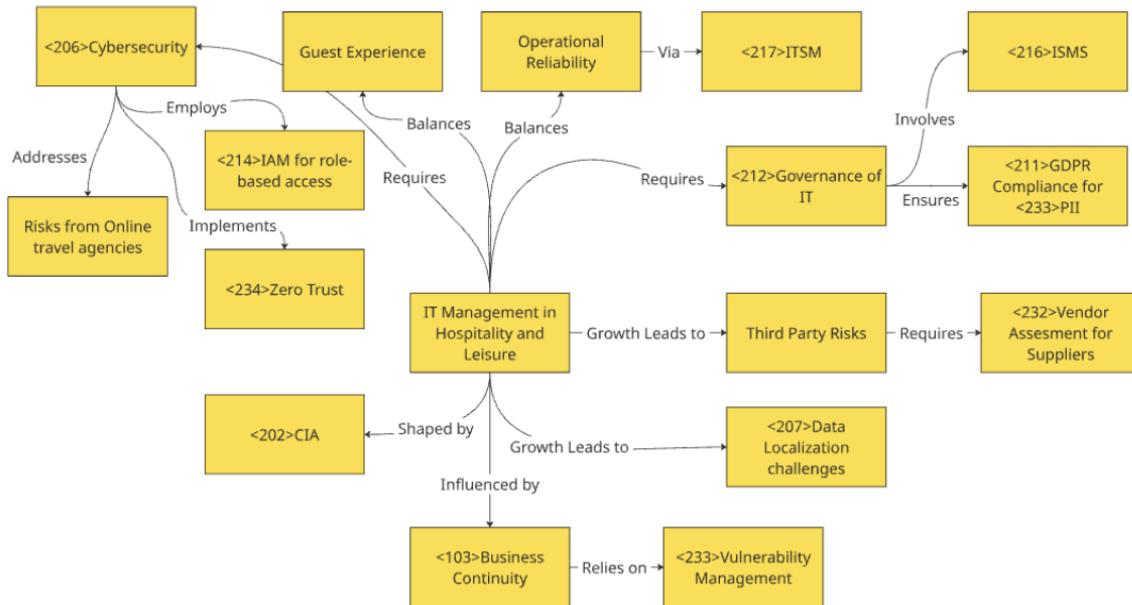


Figure 6: Concept map for Industry 4 - Governance of IT and IT Operations.

4 Comparison of the Industries

4.1 Theme 2 – Governance of IT and IT Management: Retail and Digital Commerce vs. Transport and Logistics

Retail and Digital Commerce and Transport and Logistics both rely heavily on IT systems, but their governance models, regulatory environments, and strategic orientations diverge significantly.

Retail operates in agile, rapidly evolving digital ecosystems, such as e-commerce platforms, social media, and mobile apps. IT governance in this context tends to be decentralized, often led by Chief Digital Officers (CDOs), and aims to support fast innovation cycles and customer-centric services. Tools like ERP, CRM, and ePOS must interoperate seamlessly across hybrid environments, requiring IT leaders to manage data integrity, third-party risk, and algorithmic accountability. However, this flexibility can lead to challenges such as shadow IT, weak accountability, and lower governance maturity.

In contrast, the Transport and Logistics industry adopts a centralized and compliance-oriented IT governance model, typically led by CIOs and CISOs, and structured around operational stability and cross-border interoperability. Systems such as fleet management platforms, traffic control systems, and IoT-enabled cargo tracking must function with high reliability, under strict regulatory frameworks like the eFTI Regulation and GDPR. The use of Information Security Management Systems (ISMS) and practices such as Cybersecurity Supply Chain Risk Management and Zero Trust Architectures reflects a high level of governance maturity.

While both sectors align IT with business goals, retail emphasizes adaptability and innovation, while logistics prioritizes safety, resilience, and regulatory alignment.

4.2 Theme 1 – Organisations, Governance, and Management: Retail and Digital Commerce vs. Hospitality and Leisure

Retail and Hospitality are both service-driven industries, yet their governance structures and strategic logics are distinct.

Retail governance is typically shareholder-oriented, focusing on competitive advantage through digital innovation and data-driven decision-making. Governance structures are centralized, with strong CxO leadership driving rapid responses to market trends, compliance with regulations such as the GDPR, and brand differentiation through digital channels. The integration of IT tools such as CRM, ERP, and e-commerce platforms is essential, and governance must ensure ethical marketing, vendor management, and algorithmic transparency.

Hospitality and Leisure, on the other hand, operates under a stakeholder-oriented model, balancing the interests of guests, employees, regulators, and franchisees. Governance mechanisms prioritize service consistency, health and safety compliance, and brand reputation, often supported by formal systems like ISO 9001, GDPR, and sustainability certifications (e.g., Green Key). Organizational structures are often hybrid, allowing local autonomy while maintaining central brand governance, and leadership focuses on business continuity and ethical values.

Thus, retail governance is driven by agility and innovation, while hospitality emphasizes compliance, trust, and service quality.

4.3 Theme 1 – Organisations, Governance, and Management: Transport and Logistics vs. Hospitality and Leisure

Looking into theme 1, both the industry of Hospitality and Leisure and the industry of Transport and Logistics operate complex, multi-site service operations, but differ substantially in governance logic, organisational structure, and stakeholder orientation. Hospitality typically follows a stakeholder-oriented model, balancing the interests of various stakeholders. Its governance structure is often hybrid or federated, combining central brand oversight with local operational autonomy. Governance mechanisms focus on service quality, customer satisfaction, and regulatory compliance, often supported by formal management systems like ISO 9001 or local health and safety laws. Decision-making is shared, with strong attention to reputation, service consistency, and brand alignment.

In contrast, Transport and Logistics tends to adopt a more centralised, hierarchical model, often aligned with a shareholder or public service governance logic, depending on whether the organisation is private or public. Here, operational efficiency, safety, and regulatory adherence are top priorities. Governance structures emphasise role clarity, compliance enforcement, and coordination across infrastructure and technology systems, especially in regulated domains.

While both industries require alignment between operations and strategy, hospitality aligns through guest experience and service quality, whereas transport aligns through efficiency, safety, and continuity of service. These differences illustrate how sector-specific missions and stakeholder complexity define governance structures and management approaches across service industries.

4.4 Theme 2 - Governance of IT and IT Management: Retail and Digital Commerce - Hospitality and Leisure

From the viewpoint of Theme 2 both Retail and Digital Commerce and Hospitality and Leisure use IT to enhance service delivery, but differ in governance posture, risk orientation, and digital maturity.

Retail typically adopts a decentralised, agile governance model, with roles like the Chief Digital Officer (CDO) driving customer analytics, platform integration, and fast innovation cycles. IT decisions are often business-led, enabling quick adaptation to consumer trends, which can lead to fragmented responsibilities, shadow IT, and lower governance maturity.

In contrast, Hospitality and Leisure tends toward a more structured and risk-aware governance posture, with IT supporting operational continuity, guest experience, and compliance with local regulations (e.g., safety, privacy). Governance is often shaped by federated organisational models, where central systems (e.g., booking, CRM) must interoperate with locally managed operations across venues. This requires balancing central IT strategy with local needs, often resulting in hybrid IT governance models.

While both industries aim to align IT with strategic goals, retail treats IT as a growth engine and competitive differentiator, whereas hospitality sees it as a support function for operational excellence and brand consistency.

Industry 3: Retail and Digital Commerce - Organizations, Governance, and Management - Subdomain of Direct-to-consumer (DTC) brands

Direct-to-consumer (DTC) brands sell products directly to customers, bypassing the traditional retail channels. These companies scale quickly via e-commerce platforms and social media, but with higher challenges in terms of **Governance** and with higher risks. These risks are only elevated if there is no mature governance and **vulnerability management**, including things like:

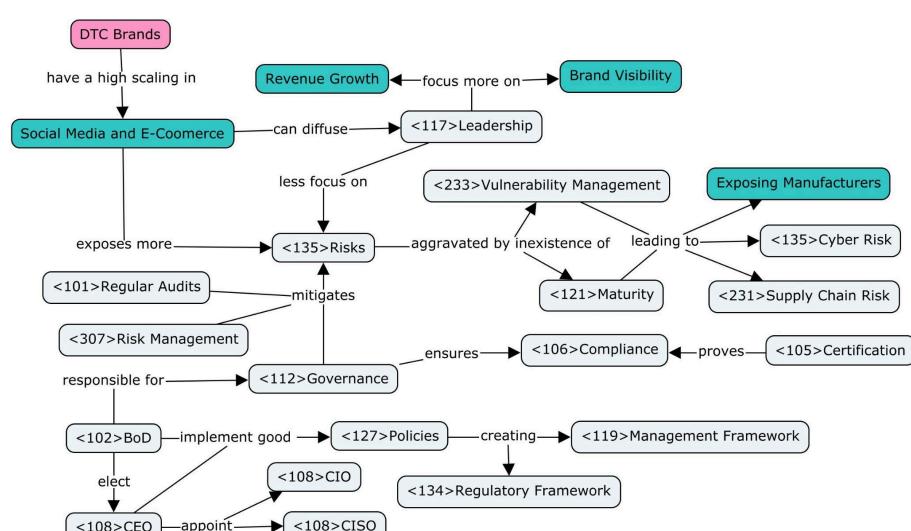
- Exposing manufacturers to consumers instead of relying on retailers that typically have the infrastructure to deal with labelling, shipping, and overall liability risks that comes with running an e-commerce store;
- Higher cyber **risk** in handling sensitive customer and financial data;
- Higher Complexity in **Supply Chain** that can be seen as possible vulnerability in terms of a possible disruption leading to the entire collapse of the company. Now, instead of having to sell to only a few retailers, it has to deliver its products to all of the customers, leading to possible risks.

DTC brands also face serious issues when rapid scaling comes into play. On this topic, **leadership (stakeholders)** accountability can be diffused: investors and executives may focus on revenue growth and visibility, sometimes neglecting all the risks that come with this. In this environment, failures in **governance** manifest as overruns in technical spending, unchecked security gaps, or even legal violations. DTC strategies can "introduce new risks that wholesale or retail partners would typically retain", *Zahi Harakeh, Manufacturing Lead, Liberty Mutual Insurance*.

These types of brands often are very young in the market leading, most of the time to problems in governance **maturity**. They may lack a clear **regulatory** or **management framework** or **risk management plans**, they tend to fail in defining roles (such as **CIO** or **CISO**), and there could be a problem with **board oversight**. Frameworks like **ISO 27001** and **COBIT**, for example, can provide some of the topics that are missing in these low **maturity** companies: formal **risk assessment**, continuous **monitoring**, and periodic **audits** are just a few of the examples. Besides that, **Organizational Structure** also matters. A flat startup might leave critical decisions in the hands of the **CEO**, that to further make the company better, might bypass reporting channels, which could lead to the board to remain passive, in all of this.

Talking a little about a real case, where it's possible to see an example of governance failure, we have a DTC eyewear brand called Warby Parker. In early 2025, the U.S. Department of Health and Human Services (HHS) fined the company \$1.5 million for multiple HIPAA (Health Insurance Portability and Accountability Act) Security Rule Violations following customer data breaches. The HHS investigation found that Warby Parker had no formal **risk analysis**, the staff never conducted any risk assessments of their data systems, and did not review their **audit logs**. The breaches that happened in 2018-2022 could have been mitigated if only a proper **management framework** was implemented. This resulted in both legal penalties as a loss of customer trust (<https://shorturl.at/Ny2IS>).

To conclude, it is important that, while these DTC brands grow, they assume a reactive posture to a formal **governance regime** that embeds IT within overall corporate strategy to take advantage of this type of digital commerce system.



Industry 3: Retail and Digital Commerce - Governance of IT and IT Management - Subdomain of Direct-to-consumer (DTC) brands

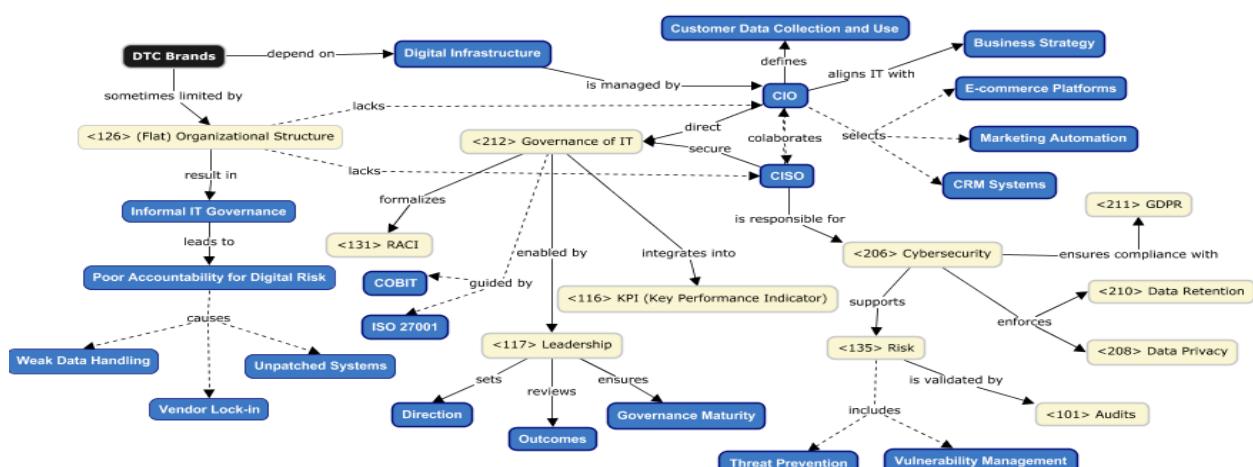
In environments like those of the Direct-to-Consumer (DTC) brands, the need for structured <212> Governance of IT becomes essential due to these companies' heavy dependency on digital infrastructure to manage everything from customer data to logistics. With this, IT is directly tied to <103> Business Continuity and growth, while also being related to the customer's experience. Considering this context, <212> Governance of IT ensures that the company's technology ecosystem aligns with business strategy, regulatory frameworks, and operational demands.

In order to oversee the digital roadmap of the company, DTC brands usually have a Chief Information Officer (CIO), that plays a critical role in selecting and integrating the e-commerce platforms used, the CRM tools, and marketing automation systems, while also defining how the customer data is going to be collected and used. Alongside the CIO, the Chief Information Security Officer (CISO) is responsible for <206> Cybersecurity and risk management. Some of this might include the enforcement of policies on <208> Data Privacy, access control, and <210> Data Retention, while trying to ensure the compliance with <211> GDPR and other international standards. Since DTC companies have a very high volume of sensitive information that needs to be processed every day, the CISO need to ensure the prevention of data breaches and resilience to cyber attacks like credential stuffing or exploit of supply chain vulnerabilities

Both roles, CIO and CISO, are essential when building a secure and scalable technology environment, however, many DTC startups operate with flat <126> Organizational structures, where formal IT roles like the CIO or CISO may not exist or may be combined under a single operational lead. In these cases, <212> Governance of IT is often considered informal or immature, which leads to an unclear, or rather difficult accountability for digital risks. This usually results in oversights such as unpatched systems, weak data handling practices, or vendor lock-in through poorly negotiated cloud contracts.

To be considered mature, DTC brands must formalize their IT governance model. This includes defining clear <131> RACI structures, integrating <116> KPI's into leadership dashboards, and conducting regular <101> Audits and risk assessments. Frameworks like COBIT and ISO 27001 offer practical guidelines for building these governance layers and ensuring that both the CIO's innovation agenda and the CISO's compliance efforts are aligned with the broader <112> Governance model.

The importance of IT Governance and the implementation of comprehensive governance practices, including regular risk assessments, data protection measures, and compliance with regulations like the



GDPR, can be illustrated by the case of ISTO, a Portuguese clothing brand, that in 2024, a misconfigured API exposed customer data, leading to an investigation by Portugal's CNPD (Comissão Nacional de Proteção de Dados). The company lacked a formal <135> Risk, <101> Audit mechanisms, and a defined <131> RACI structure for data protection. With no dedicated <212> IT Governance roles like a CIO or CISO, ISTO's flat organizational structure contributed to delayed detection and response. This is one of several cases that demonstrates how the absence of structured IT governance can expose DTC brands to compliance and security risks, particularly as they scale operations. To conclude, <117> leadership is responsible for setting direction and reviewing outcomes, and that's why as DTC brands scale, proper IT management becomes not just a support function but a competitive advantage.

Industry 4: Transport and Logistics - Organizations, Governance, and Management

- Subdomain of Freight and Distribution

Freight and distribution are core components of the transport and logistics sector, underpinning supply chains, trade flows, and economic resilience. In Portugal, the niche is anchored by critical infrastructures such as the Port of Sines, the Port of Leixões, major logistics corridors, and intermodal hubs connecting maritime, rail, and road networks. Operators span large freight companies, warehousing providers, and last-mile distributors, often functioning in public-private ecosystems.

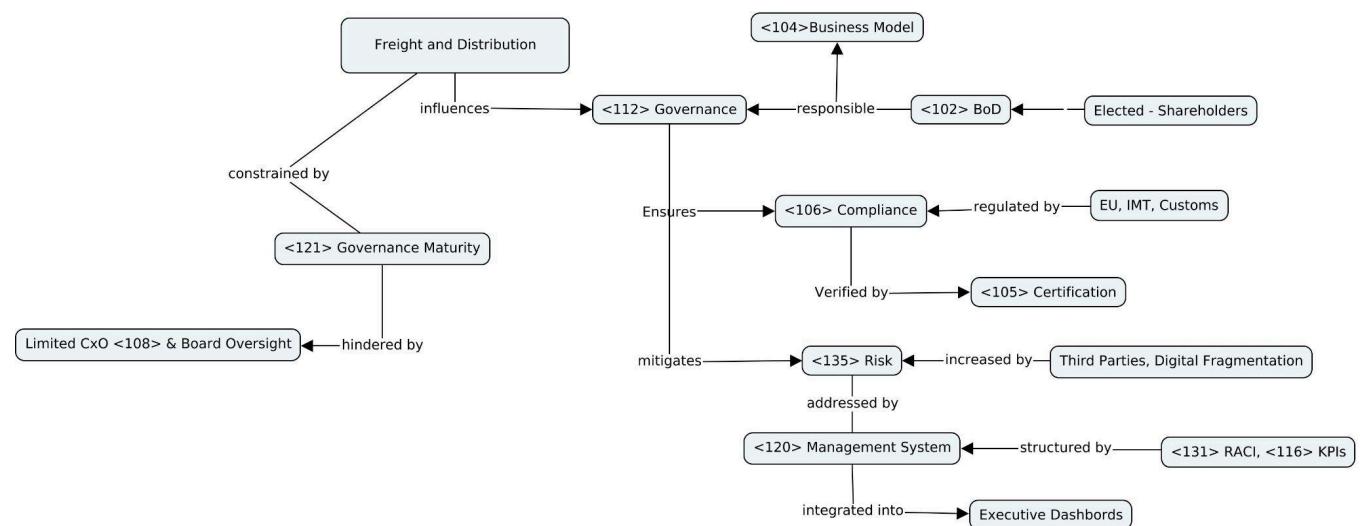
From a <112> governance standpoint, freight logistics involves coordinating physical assets, IT platforms, and partner networks across complex value chains. Key challenges include aligning operational practices with regulatory obligations, managing third-party <135> risk, and adapting to digital transformation. Organisations in this niche must ensure strategic direction (<104> Business Model), maintain regulatory <106> compliance (<105> Certification), and provide accountability across increasingly digital and fragmented operations.

Portuguese freight governance is shaped by EU regulations such as the eFTI Regulation for digital freight data exchange and GDPR for handling logistics-related personal data. At the national level, oversight is shared among IMT, customs authorities, and regional port administrations. Projects like Sines Tech – Innovation and Data Centre Hub demonstrate Portugal's strategic push to integrate freight with digital platforms, boosting international competitiveness while raising new <112> governance demands.

Many firms struggle with low governance <121> maturity, lacking clearly defined roles and <108> CxO involvement in digital logistics strategy. There is often limited integration of digital performance indicators into board-level oversight (<102> BoD), which hinders responsiveness to disruptions, cyber threats, or infrastructure delays. Additionally, fragmented <126> organizational structures across the freight chain can result in poor visibility and inconsistent accountability, especially where subcontracting is widespread.

To advance, freight organizations in Portugal need stronger <120> management systems that embed <135> risk, <106> compliance, and data governance into operational routines. Establishing clear <131> RACI structures and integrating logistics <116> KPIs into executive dashboards would improve strategic alignment. Public-sector actors can support this by incentivising <112> governance innovation through procurement criteria and national funding programs aligned with EU priorities.

In conclusion, freight and distribution governance in Portugal must evolve from fragmented compliance practices toward integrated, proactive oversight. As logistics becomes more digital, responsive, and interconnected, robust governance structures will be key to balancing efficiency, resilience, and regulatory conformity.



Industry 4: Transport and Logistics - Governance of IT and IT Management - Subdomain of Freight and Distribution

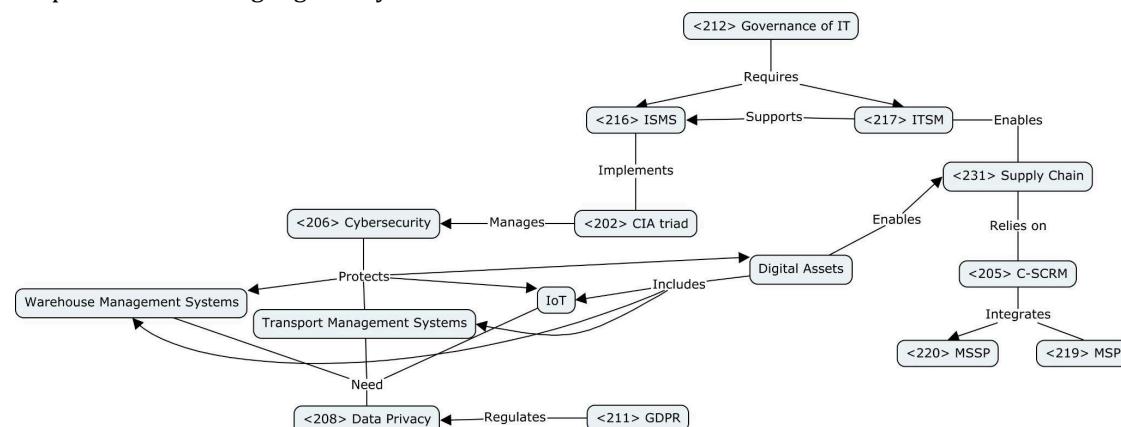
Transport and Logistics depend on end-to-end networks to get goods to customers in a timely and efficient manner. Freight and Distribution involve planning intermodal shipping, last-mile delivery, and warehousing. Good <112> Governance is required in these operations to align day-to-day activity with strategic goals. As digital technologies become ubiquitous, <212> Governance of IT and <217> IT Service Management ensure that technology improves logistics performance, <106> Compliance, and optimization.

In the freight and distribution subdomain, robust <212> Governance of IT ensures alignment of Transport Management Systems, Warehouse Management Systems, and IoT-based monitoring to business objectives, and <217> IT Service Management delivers the "how" through process-driven deployment and ongoing improvement. Organizations protect vital shipment data and live visibility networks through the implementation of a well-defined risk position, embodying the <202> CIA triad of confidentiality, integrity, and availability, and implementing <206> Cybersecurity controls. This is recorded in an <216> ISMS, codifying policy and responsibility, and regularly certified under ISO 27001 norms to prove compliance.

To manage digital <231> Supply chains, freight operators follow intensive <232> Vendor Assessment of <219> MSPs and <220> MSSPs, including <205> Cybersecurity Supply Chain Risk Management for minimizing third-party risks. At the same time, <208> Data Privacy regulations through the <211> GDPR (or other regulators) encourage transparent management of customer tracking and delivery status, using <221> Opt-in and <222> Opt-out controls for respecting individual rights. An overall stakeholder management approach, including carriers, shippers, 3PLs, and regulators, is driven by shared performance measures that are continually applied to drive intermodal coordination, last touch effectiveness, and warehouse efficiency, transforming the governance role from control into a catalyst for operational excellence.

At the top of the governance structure, a board-level CIO or CTO manages IT strategy, translating business goals into technology roadmaps that prioritize investments in TMS, WMS, and real-time IoT tracking. The CIO oversees budgeting, vendor selection, and alignment of digital initiatives with customer-service and cost-efficiency targets. Reporting separately to the CEO or a board-level risk committee, the CISO leads all information-security and compliance efforts. The CISO's responsibilities include developing and enforcing <206> Cybersecurity policies, conducting regular <135> Risk assessments, and ensuring adherence to industry regulations. In particular, the CISO maintains controls that manage <208> Data Privacy and <210> Data Retention in compliance with the <211> GDPR (or other regulators), and serves as the escalation point for any security incidents or <101> Audit findings.

In addition to the above-mentioned regulations, freight operators must follow transport-specific requirements, bill of lading electronic standards, cross-border data-transfer rules, and regional privacy laws. For this purpose, the <216> ISMS integrates programmed checks on compliance: effectiveness of control, <323> SLA compliance, and incident-response metrics are tracked in real-time dashboards. Quarterly governance meetings review these metrics along with vendor performance under <205> C-SCRM, ensuring that <219> MSPs and <220> MSSPs are providing contractual security obligations. This continuous integration of <106> Compliance not only ensures operational integrity but also enables agile adaptation to evolving regulatory and market demands.



Industry 7: Agriculture and Farming - Organizations, Governance, and Management - Subdomain of Crop Farming

In the Agriculture Industry, specifically the Crop Farming subdomain, there are several factors that affect the <113> Governance, Risk and Compliance. These influence how workers prepare the land, select the seeds, irrigate the land, grow crops, harvest, handle post-harvest, and integrate technology into the process.

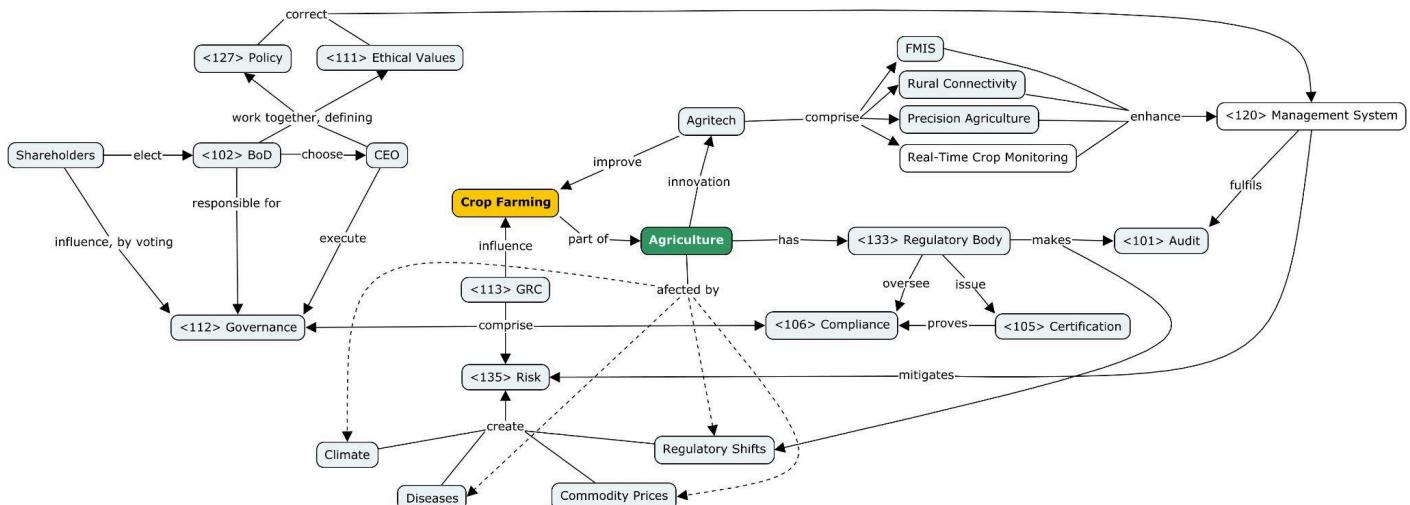
In terms of <112> Governance, although the decisions differ from other Industries, the hierarchy is very similar. CEO, CFO and COO roles are standard. The <102> Board of Directors is present, where there are independent directors for oversight. These independent directors, formally elected by Shareholders during annual general meetings (AGMs), work with the CEO to develop <127> Policies and <111> Ethical Values to be followed by <120> Management Systems.

In terms of <135> Risk, there are several external factors that affect the Industry, making it a necessity to take them into consideration upon decision making. Climate changes such as temperature shifts, water scarcity and extreme weather events influence production levels and growing seasons, making them earlier/later than expected, or even disrupt harvesting completely. Diseases such as fungal/bacterial or pests of insects can also disrupt harvesting, making crops unsafe for consumption. Commodity Prices also have a high power, as the shortage of fertilizers or shipping delays can influence sales and prices of crops. Lastly, Regulatory Shifts are crucial as trade policies can make companies lose key customers due to high tariffs or export bans.

In terms of <106> Compliance, the Industry has <133> Regulatory Bodies that differ from country to country (as well as continent). These entities are responsible for <101> Auditing and providing <105> Certification, when <120> Management Systems show that requirements and policies are being fulfilled.

In order to fulfil policies and implement ethical values, <120> Management Systems use Agri-Tech Risk Management Systems and Smart Farming Compliance Tools. Farm Management Information Systems (FMIS) centralize data management, helping in identifying possible pest outbreaks and weather impacts using historical and real-time data for predictions. Rural Connectivity conditions how these systems work, as availability and access to reliable internet can differ in each location. Precision Agriculture optimizes the use of commodities (water, fertilizers, pesticides) through sensors and counters, being also able to detect early signs of stress, disease, or nutrient deficiencies, preventing yield loss. Lastly, Real-Time Crop Monitoring identifies issues before they spread through the usage of machine learning image analysis.

These allow <120> Management Systems to better control and mitigate <135> Risks in an automated and ethical manner.

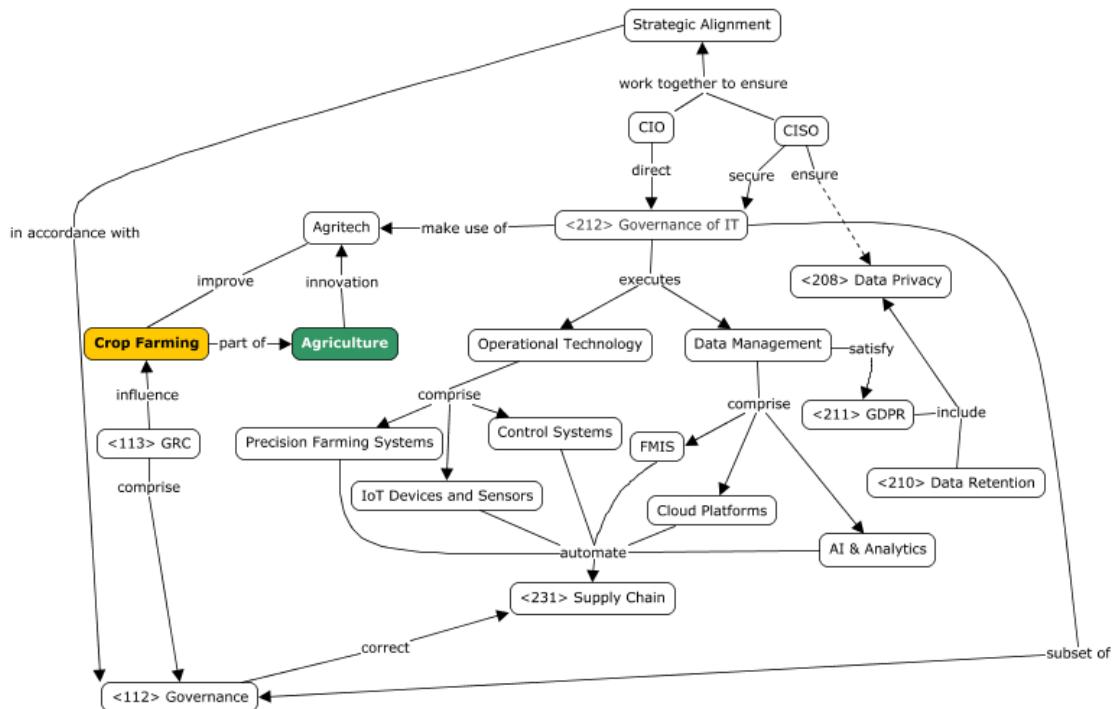


Industry 7: Agriculture and Farming - Governance of IT and IT Management - Subdomain of Crop Farming

Within most industries that have a strong integration of IT, it is possible to find a subset of <112> Governance called <212> Governance of IT that ensures IT supports and extends the organisation's goals, while managing associated risks and complying with external obligations. This subset involves multiple stakeholders across the organization. The most noticeable ones are the Chief Information Officer (CIO), responsible for leading IT strategy, operations and digital transformation, and the Chief Information Security Officer (CISO) which is responsible for overseeing <206> Cybersecurity, Risk Management and <106> Compliance.

Within the Crop Farming subdomain of the Agriculture Industry, the CIO directs <212> Governance of IT by making key decisions about Operational Technology and Data Management. Decisions like implementing Precision Farming Systems that directly integrate and manage IoT Devices, sensors and drones, or the usage of Cloud Platforms to gather telemetry and formulate predictions using AI and Analytics are of the responsibility of the CIO. Technologies working correctly, the company having <303> Cyber Resilience, and systems being in accordance with compliance, are all responsibilities of the CISO. The CISO is a key part in securing Operational Technology, and ensuring that Data Management is in accordance with the <211> GDPR (in Europe, in other continents, these might differ, such as CCPA in California and PIPL in China). Properties such as <208> Data Privacy and <210> Data Retention are all part of the <211> GDPR, created in 2018 by the European Parliament and The Council of the European Union.

In a few words, the CIO drives innovation, while CISO ensures <228> Privacy-by-design. As such, these work together in order to formulate decisions concerning <212> Governance of IT that are in accordance with the mission established by <112> Governance. With the automation in place, and with an outside view of the <231> Supply Chain, <117> Leadership corrects the decisions that were put in practice.



First Comparison - “4 Transport and Logistics” and “3 Retail and Digital Commerce” on “Organizations, Governance, and Management”

Even though there are some concerns about the maturity of companies related to Transport and Logistics, in the subdomain of Freight and Distribution, the level of maturity in Retail and Digital Commerce, especially in the domain of DTC brands, is much lower. Several important <108> CxO roles (e.g., CISO and CIO) might be missing, the <102> board level oversight may be minimal as well, in contrast to the one needed in Transport and Logistics. There needs to be a much higher <126> Organizational Structure from the start compared to the DTC brands.

Rapid Scaling DTC firms often lack a formal <120> management system leading to several security gaps and ad hoc processes. As the <121> maturity in these companies rises, they also lean into adopting frameworks like the <119> ISO 27001 or COBIT. In freight, analogous systems (e.g., FMIS, logistic ERPs) and compliance tools are mandatory under EU regulations and other agencies like the IMT. Yet many smaller logistics providers could still be missing <131> RACI frameworks or clear <116> KPIs in executive dashboards.

DTC brands tend to outsource a lot of their logistics to a third party heightening <231> Supply Chain risk. Similarly, freight operators manage contractors, carriers, and IT vendors making mature <113> GRC practices woven into daily operations. In contrast, for DTC companies, embedding <113> GRC remains a nascent discipline, often trailing behind their digital ambitions.

Both industries benefit from aligning IT initiatives with <104> business models. DTC firms that acknowledge the importance of <116> KPIs see way fewer incident reports. In the freight industry, projects like Sines Tech demonstrate how governance can drive competitiveness. Ultimately, robust governance with clear roles, formal systems, <135> risk control, and <106> compliance controls is essential whether you are selling products of your DTC brand or managing the container flows through Portugal's ports.

Second Comparison - “4 Transport and Logistics” and “3 Retail and Digital Commerce” on theme “Governance of IT and IT Management”

While both the Transport and Logistics and Retail and Digital Commerce industries rely heavily on digital infrastructure, the maturity and formalization of IT Management practices differ significantly, especially when talking about Direct-to-Consumer (DTC) brands and Freight and Distribution.

In the domain of IT Management, Transport and Logistics, especially in Freight and Distribution, companies tend to have a more established structure for <212> Governance of IT, since they often operate with formalized CIO and CISO roles, where the CIO leads digital transformation initiatives, such as the integration of logistics ERP systems, fleet tracking technologies, and predictive maintenance tools and the CISO ensures <206> cybersecurity across the operational network, especially in protecting IoT-enabled devices used for shipment tracking and warehouse automation.

By contrast, in Retail and Digital Commerce, especially in DTC brands, the situation is frequently less mature, especially among early-stage or fast-scaling companies where it's common for formal roles like CIO or CISO to be missing or merged under a single operational executive. As a result, <126> organizational structures are flat, <131> RACI models are unclear, and IT decisions may lack strategic coordination. This creates environments where IT is treated more as a tool for marketing and customer interaction than as a foundation for <103> Business Continuity, risk mitigation, or regulatory adherence.

Both industries handle sensitive data, but their treatment diverges significantly. Freight companies adhere to stringent <208> data privacy mandates (e.g., <211> GDPR), applying <221> opt-in and <222> opt-out mechanisms with auditable trails. On the other hand, DTC brands, while equally data-intensive, may skip structured controls, leading to preventable failures, where the absence of <135> risk analysis and formal <101> audits, compounded by a non-existent <131> RACI structure, can contribute to regulatory action.

In conclusion, while both industries rely on IT for growth and efficiency, Transport and Logistics firms often lead in IT Management maturity, with formal roles, regulatory compliance, and risk planning baked into operations. DTC brands, despite being digitally native, frequently lag in formal IT governance, making them more vulnerable as they scale, unless they proactively mature their IT management practices.

Third Comparison - “4 Transport and Logistics” and “7 Agriculture and Farming” on “Organizations, Governance, and Management”

While both Transport and Logistics and Agriculture and Farming depend on strong governance structures to manage risk, ensure compliance, and coordinate operations, their contexts and challenges differ significantly.

In Transport and Logistics, particularly in the Freight and Distribution subdomain, **<112>** governance must address complex ecosystems involving public-private partnerships, international regulations, and IT-integrated infrastructures. Oversight is typically shared between national authorities like IMT, infrastructure managers, and EU frameworks such as eFTI. Governance **<121>** maturity is often uneven, with many firms lacking formal **<108>** CxO roles and clear **<102>** board-level oversight, especially around digital strategy and cyber risks.

Conversely, in Agriculture, especially in Crop Farming, governance is traditionally more hierarchical and driven by regulatory and environmental uncertainty. Boards and executives define **<111>** ethical values and implement **<127>** policies through structured **<120>** management systems. However, this sector is more exposed to external risk factors such as climate change, disease, and commodity volatility, requiring governance to be more adaptive and aligned with **<135>** risk-based **<106>** compliance.

Both industries share the challenge of digital integration, but agriculture often suffers from weaker connectivity and infrastructure, affecting governance automation and responsiveness. In contrast, logistics faces risks linked to digital fragmentation across actors and platforms.

In sum, governance in transport emphasizes regulatory alignment and operational efficiency, while in agriculture it prioritizes adaptability, ethical compliance, and resilience to external shocks.

Fourth Comparison - “4 - Transport and Logistics” and “7 - Agriculture and Farming” on theme “Governance of IT and IT Management”

IT Management is critical but context-dependent for the transport and logistics and agriculture, and farming industries. The two industries are undergoing digital transformation, but the degree of maturity and IT strategic integration is significantly different.

In Transport and Logistics, IT Management is the center of operational effectiveness. IoT solutions for real-time monitoring and performance measurement in business-process-integrated core systems, such as Transport Management Systems and Warehouse Management Systems, are complemented in most instances. Here, **<217>** IT Service Management frameworks ensure organized service delivery, and **<212>** Governance of IT enables strategic alignment, risk management, and compliance. **<206>** Cybersecurity controls manage weaknesses in logistics chains, with the **<202>** CIA triad applied to protect information's integrity, availability, and confidentiality. It is usually formalized as an **<216>** Information Security Management System, and then further developed by engaging with **<219>** Managed Service Providers and **<220>** Managed Security Service Providers, under **<205>** Cyber Supply Chain Risk Management.

On the other hand, the Farming and Agriculture sector opens a more mixed IT landscape. While large-scale agribusinesses may adopt Farm Management Information Systems and IoT services using sensors more and data increasingly, smaller farms might lack defined IT structures or architectures. But the application of **<217>** IT Service Management principles is becoming visible, especially where precision farming and monitoring equipment demand system uptime, data handling, and remote diagnostics. **<206>** Cybersecurity and governance problems are increasing in parallel, with digital assets such as crop data and environmental readings requiring protection and adherence to compliance requirements (e.g., **<211>** GDPR for data privacy). However, **<219>** Managed Service Providers and **<220>** Managed Security Service Providers usage and **<216>** Information Security Management System implementation in a proper sense are less frequent than in the logistics situation.

In conclusion, even though both sectors benefit from IT Management, Transport and Logistics possess a more mature and governed philosophy, whereas Agriculture and Farming are still developing towards systematic digital customs.

SGSI Project part 1

Industries:

- 3: Retail and Digital Commerce
- 5: Hospitality and Leisure
- 6: Banking and Financial Services

Authors:

- Henrik Niskanen - 115383
- Sara Echary- 115340
- Laura Staszko - 112985
- Natan Gloeh - 112475

Theme 1 – Business Governance & Management

Industry: Retail & Digital Commerce

Niche: Subscription models in the food & beverage segment

Subscription-based F&B platforms exemplify **<112> governance challenges** arising from managing scalability, customer data, and stringent **<134> regulatory frameworks** such as **<211> GDPR** and food safety regulations enforced by **<133> regulatory bodies**.

1. Governance, compliance, and organizational structure

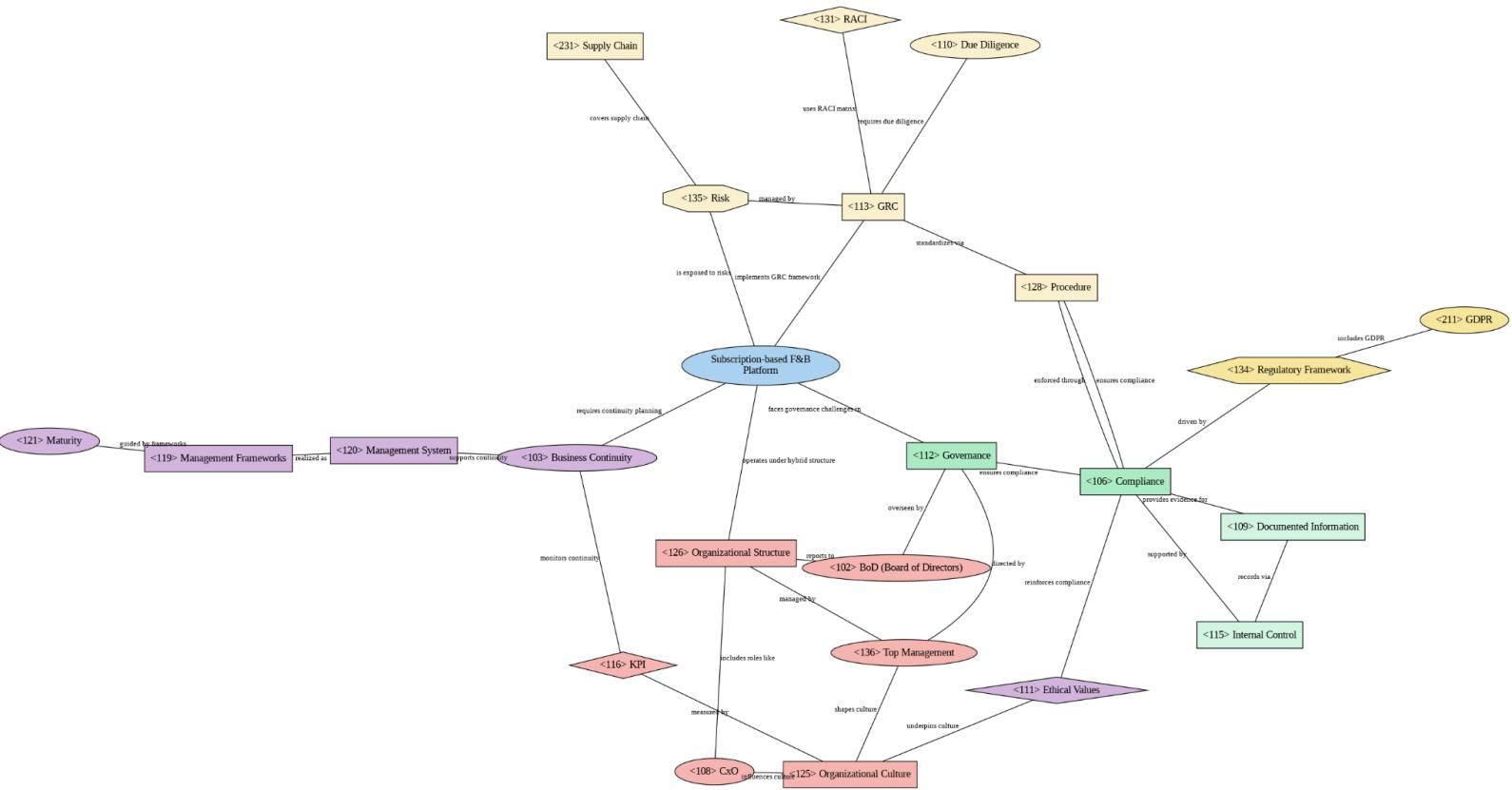
Effective **<112> governance** ensures robust adherence to **<106> compliance mandates** across diverse jurisdictions, particularly in handling sensitive consumer information and food safety standards. Subscription models typically deploy a hybrid **<126> organizational structure**, blending centralized strategic teams with regional operational units, to balance scalability with localized compliance demands. The **<136> top management** (**<108> CxOs**) emphasizes agility, fostering a customer-centric **<125> organizational culture** crucial for maintaining subscription growth and customer loyalty. This culture is continuously assessed through **<116> KPIs** like churn rates, customer lifetime value (CLV), and overall satisfaction, ensuring alignment with strategic goals such as **<103> business continuity**.

2. Risk and policy frameworks

The **<135> risk profile** for subscription F&B services prominently includes data breaches, regulatory non-compliance, and **<231> supply chain disruptions**. To mitigate these risks, platforms integrate comprehensive **<113> GRC** frameworks that emphasize meticulous **<110> due diligence** processes in vendor management and customer data handling. Clear accountability is structured through **<131> RACI matrices**, particularly in sensitive operations such as data privacy and dispute resolution. Standardized **<128> procedures**, notably in customer service and logistics, enhance operational consistency and help maintain high standards of service **<130> quality**.

3. Organizational maturity and culture

Subscription F&B organizations typically demonstrate moderate to high **<121> maturity**, characterized by structured and documented processes aligned with established **<119> management frameworks**. Mature organizations exhibit robust **<120> management systems** ensuring efficient and consistent service delivery. The platforms emphasize strong **<111> ethical values**, notably transparency in consumer interactions, data privacy, and sustainability practices, vital for maintaining consumer trust and competitive advantage in the digital marketplace.



Theme 2 – Governance of IT and IT Management

Industry: Retail & Digital Commerce

Niche: Subscription models in the food & beverage segment

Strategic Alignment & Compliance

The core of IT governance (<212> Governance of IT) is ensuring that subscription-F&B initiatives map to business goals - subscriber growth, churn reduction, LTV - and comply with external mandates. An Information Security Management System ([216] ISMS) guided by ISO/IEC underpins this alignment, embedding COBIT processes for strategic planning and performance measurement. Regulatory frameworks like GDPR (<211>) dictate [C-Data Retention] policies (<210>) and breach-reporting obligations to the <133> Regulatory Body, ensuring subscriber PII (<223>) is handled lawfully.

Privacy & Data Protection

Subscription services collect granular consumption and preference data - classified as <223> PII so a robust <227> PIMS (Privacy Information Management System) with <228> Privacy-by-Design principles is mandatory. The PIMS mandates data minimization, purpose-limitation, and automated retention/deletion workflows. It must integrate with billing and CRM systems to enforce consent records and support data-subject requests.

Cybersecurity Operations

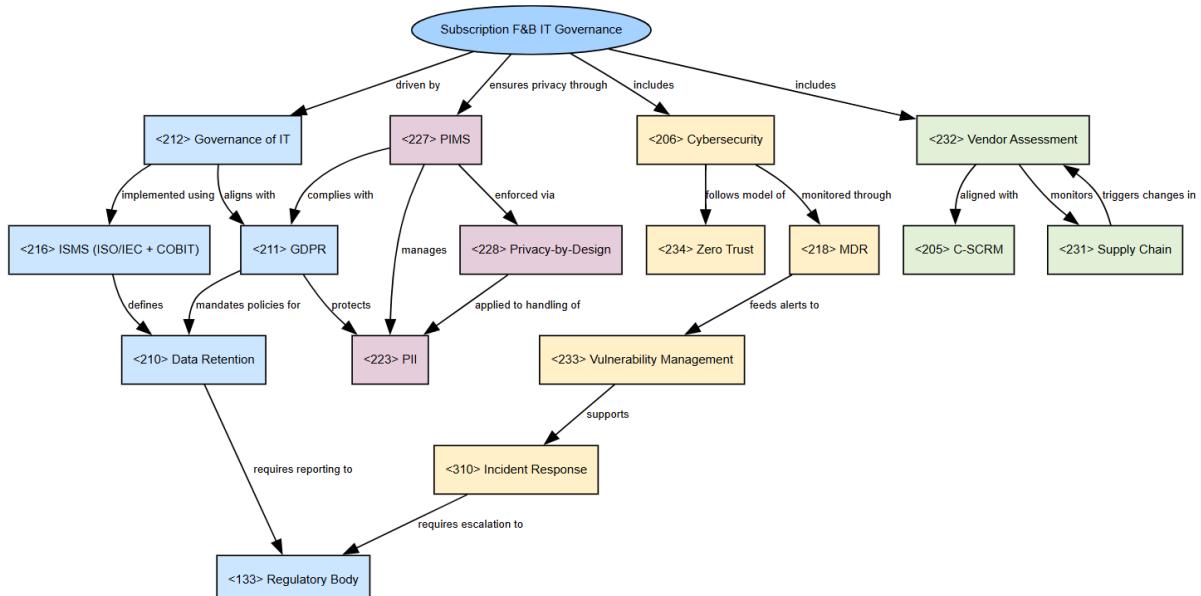
Operational resilience against threats depends on layered controls:

- <206> Cybersecurity governed by the ISMS and enforced through <234> Zero Trust (strict identity-and-access controls)
- 24/7 monitoring by <218> MDR (Managed Detection & Response)
- Proactive <233> Vulnerability Management feeding into quarterly penetration tests
- Formal <310> Incident Response (breach plans) executed under the ISMS and reported to regulators.

These processes protect the billing engine, subscription-lifecycle workflows (onboarding - recurring payments - renewal), and subscriber portals.

Supply-Chain & Vendor Risk

Subscription-box fulfilment and digital-platform integrations rely on third-party logistics, payment gateways, and content-recommendation APIs. A <232> Vendor Assessment program, aligned with <205> C-SCRM (Cyber Supply-Chain Risk Management), identifies risks across the supplier ecosystem. Ongoing monitoring under <231> Supply Chain governance ensures that new menu-item rollouts or packaging changes don't introduce vulnerabilities.



Theme 1 – Business Governance & Management

Industry: Hospitality and Leisure

Niche: Short-term rental platforms

Short-term rental platforms (STRPs) like Airbnb face multifaceted **<112> Governance** challenges due to their global scale, decentralized operations, and **<134> Regulatory Frameworks** (e.g., housing laws, tax codes, **<211> GDPR**) across jurisdictions.

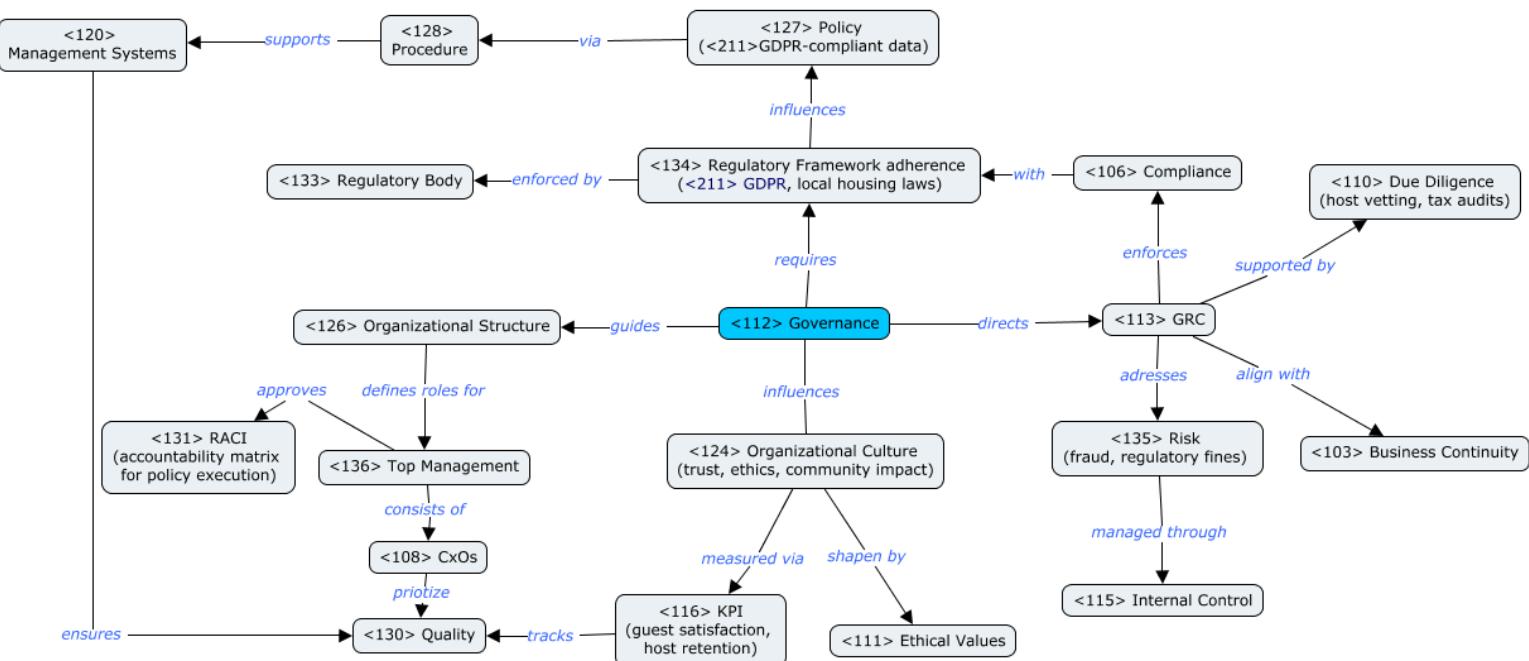
1. Governance, compliance and organizational structure

<112> Governance is central to balancing scalability with localized compliance (**<106>**). STRPs must navigate diverse **<134> Regulatory frameworks** (EU's **<211> GDPR** for **<223> PII**, zoning laws) enforced by **<133> Regulatory bodies**. **<113> GRC** (Governance, Risk, and Compliance) frameworks integrate **<135> Risk mitigation** (as fraudulent listings, safety incidents) and **<110> Due Diligence** (host verification, tax reporting).

STRPs adopt a hybrid **<126> Organizational Structure**, combining centralized tech teams with regional compliance units. **<136> Top Management** (**<108> CxOs**) ensures **<103> Business Continuity** during crises like pandemics. **<124> Organizational Culture** prioritizes trust but faces tensions between profit motives and community impact (housing shortages). This culture is measured via **<116> KPIs** like guest satisfaction and host retention.

2. Risk and policy frameworks

<135> Risk profiles include regulatory fines (**<106> Compliance failures**) and reputational damage from unethical practices. **<127> Policy** (**<211> GDPR-compliant data**) **<134> Regulatory Framework adherence** (**<211> GDPR, local housing laws**) **<106> Compliance** **<110> Due Diligence** (host vetting, tax audits) **<113> GRC** (**<112> Governance**, **<128> Procedure**, **<120> Management Systems**) **<126> Organizational Structure** (**<131> RACI** (accountability matrix for policy execution), **<136> Top Management** (**<108> CxOs**)) **<124> Organizational Culture** (trust, ethics, community impact) **<116> KPI** (guest satisfaction, host retention) **<111> Ethical Values** **<115> Internal Control** **<103> Business Continuity** **<135> Risk** (fraud, regulatory fines) **<115> Internal Control** **<103> Business Continuity**



Theme 2 – Governance of IT and IT Management

Industry: Hospitality and Leisure

Niche: Short-term rental platforms

Short-term rental platforms (STRPs) like Airbnb rely heavily on IT infrastructure to manage decentralized operations, process sensitive data, and deliver seamless user experiences.

1. IT Governance and compliance

<212> Governance of IT ensures alignment between technology investments (like PMS, booking engines) and business goals. STRPs must comply with <211> GDPR for handling <223> PII (guest/host data) and enforce <228> Privacy-by-design principles. <216> ISMS (Information Security Management System) frameworks (ISO 27001) address <206> Cybersecurity risks like data breaches or ransomware attacks. <231> Supply Chain risks (third-party integrations for payments) require <232> Vendor Assessment and <205> C-SCRM.

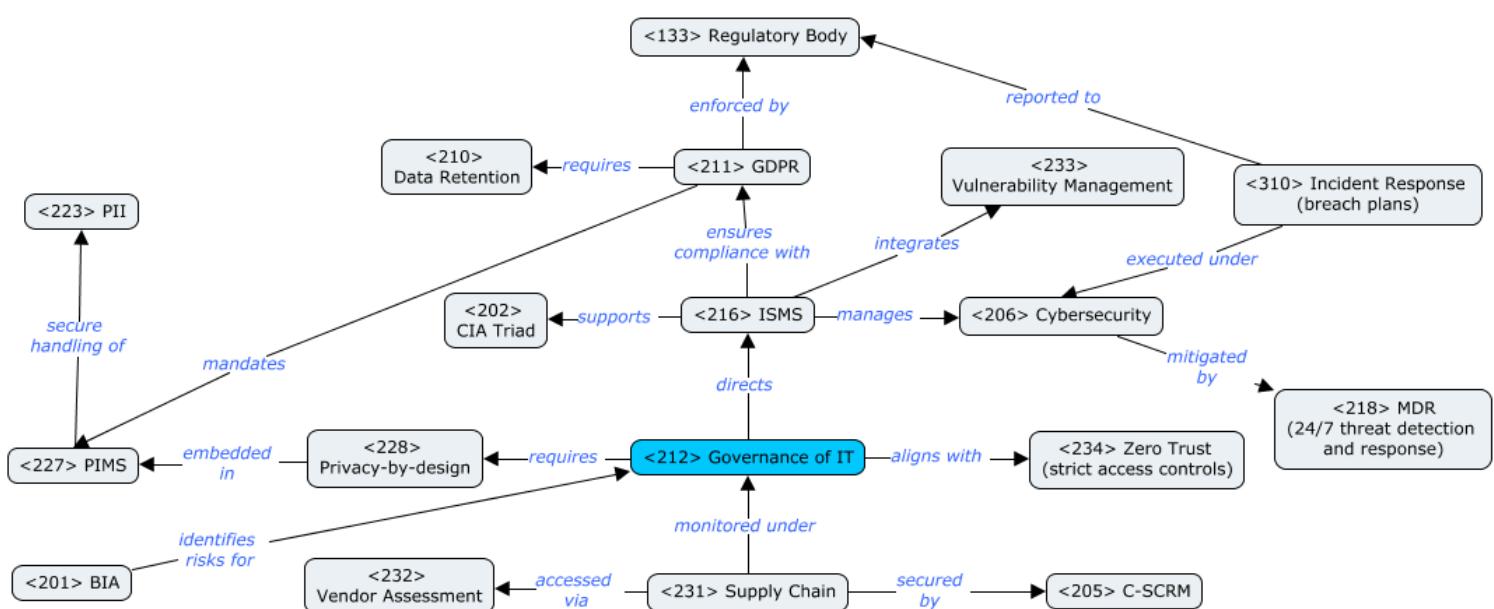
2. Data privacy and access control

<234> Zero Trust architectures validate every user/device interaction, critical for platforms with decentralized hosts and guests. <227> PIMS (Personal Information Management System) ensures GDPR compliance via <210> Data Retention policies.

3. Cybersecurity, incident management and risk mitigation

<206> Cybersecurity strategies include <233> Vulnerability Management (patching flaws in booking APIs) and <218> MDR (Managed Detection and Response) for threat monitoring. <310> Incident Response plans address breaches (like stolen payment data), requiring coordination with <133> Regulatory Body.

<201> BIA identifies critical IT systems (PMS downtime risks). <202> CIA Triad (Confidentiality, Integrity, Availability) is critical for information security.



Theme 1 – Business Governance & Management

Industry: Banking and financial services

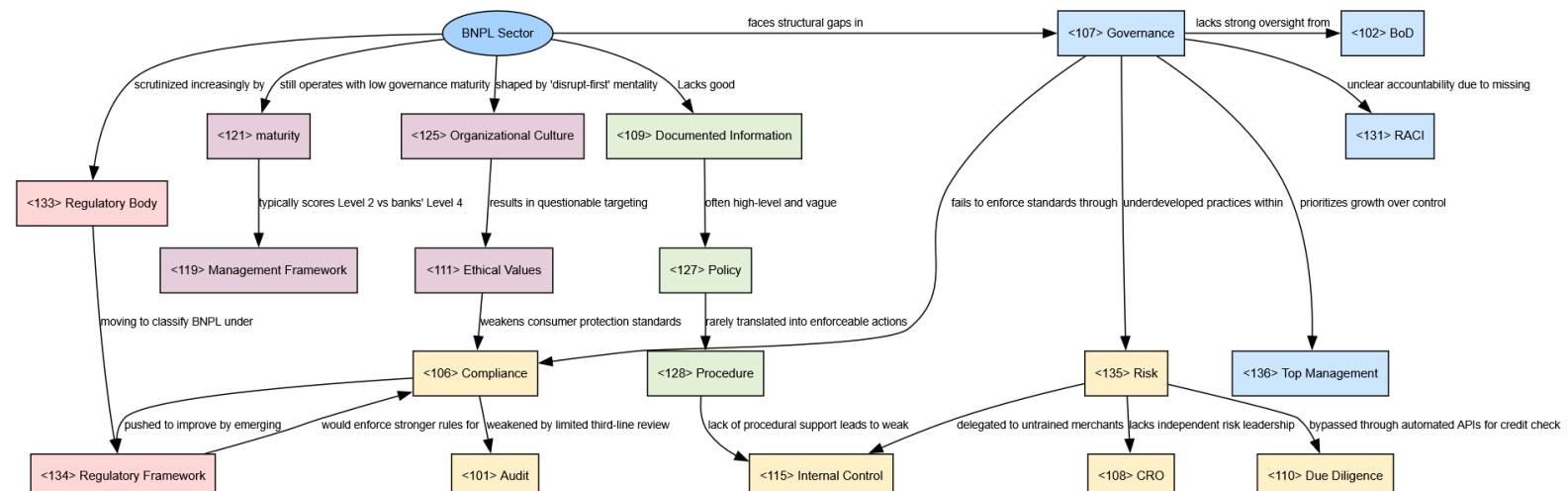
Niche: Buy now, Pay Later (BNPL)

The Buy Now, Pay Later (BNPL) sector exemplifies the governance (<112>) tensions that arise when financial innovation outpaces existing regulatory frameworks (<134>). As a nascent industry, BNPL firms often lack the robust corporate governance (<107>) structures typical of traditional banks—particularly in Board of Directors (BoD) (<102>) oversight and top management (<136>) accountability. Many fintechs prioritize rapid growth over risk control, often bypassing formal certification (<105>) standards such as ISO 27001. This leads to notable compliance (<106>) deficiencies; for instance, recent FCA data reports that 40% of BNPL users miss payments, highlighting weak affordability checks and consumer protections.

BNPL providers' GRC (<113>) capabilities remain underdeveloped relative to industry norms. Risk (<135>) management is fragmented across the Three Lines of Defense: first-line internal controls (<115>) are often delegated to under-trained merchants; second-line reliance on external scoring APIs limits effective due diligence (<110>); and third-line audit (<101>) mechanisms are minimal. Compounding these gaps are weaknesses in documented information (<109>), with generic policies (<127>) and poorly defined procedures (<128>), especially in areas like dispute resolution and fraud handling.

A lack of stakeholder alignment further complicates governance. Fintech firms like Afterpay prioritize scale over formal Chief Risk Officer (CRO) (<108>) oversight, while traditional banks lobby for regulatory parity in capital requirements. Meanwhile, regulatory bodies (<133>) like the CFPB face pressure to balance innovation with oversight, increasingly moving to classify BNPL under traditional credit regimes. Accountability is blurred, especially in cases of merchant fraud, where the absence of a clear RACI (<131>) structure obscures responsibility.

These structural issues reflect deeper cultural misalignments. BNPL's "move fast" ethos clashes with the risk-averse norms of finance, eroding shared organizational culture (<125>) and fostering questionable ethical values (<111>), e.g., targeting younger consumers with low financial literacy. In terms of maturity (<121>), most BNPL providers operate at Level 2 (ad-hoc) when benchmarked against established management frameworks (<119>) like ISO 31000, seen in traditional banks.



Theme 2 – Governance of IT and IT Management

Industry: Banking and financial services

Niche: Buy now, Pay Later (BNPL)

1. Strategic Alignment & Compliance

BNPL IT governance (<212> Governance of IT) is enforced by an ISMS (<216> ISO/IEC 27001 + COBIT) that aligns approval-rate and default-rate initiatives with business KPIs. Controls tie each project to PSD2 (<211> Open Banking) and GDPR (<211>), ensuring data-subject rights, breach notification, and automated compliance. Major incidents and exceptions are reported to the <133> Regulatory Body (e.g., FCA, SEC) for full auditability.

2. Privacy & Data Protection

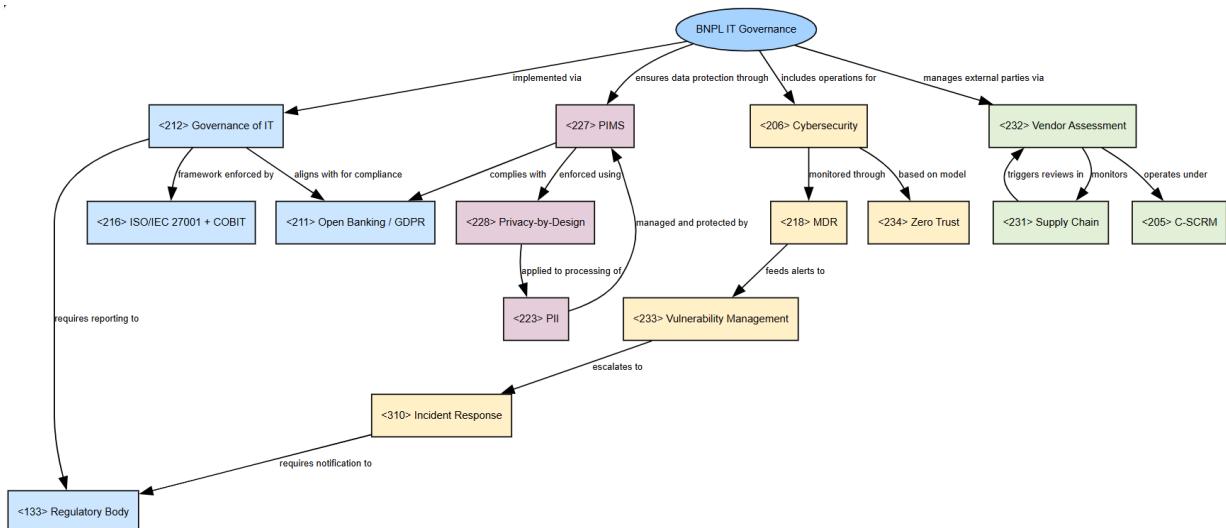
Consumer credit-score and PII data (<223>) power BNPL underwriting and personalized reminders—so a robust Privacy Information Management System (<227> PIMS) is mandatory. Leveraging <228> Privacy-by-Design, it enforces consent capture, strict minimization, and automated retention/deletion. Tight integration with CRM and underwriting platforms logs all subject-access and rectification requests.

3. Cybersecurity Operations

Under the ISMS, <206> Cybersecurity employs a Zero Trust model (<234>) requiring continuous authentication and least-privilege access. A 24/7 Managed Detection & Response service (<218> MDR) feeds into <233> Vulnerability Management for CVE scanning and patching. On detecting a breach or fraud event, a formal <310> Incident Response plan triggers escalation, forensic logging, and post-mortem audit.

4. Third-Party & Payment-Network Risk

BNPL relies on merchant integrations, card-network tokenization, and credit-bureau APIs. A structured <232> Vendor Assessment program under <205> C-SCRM rates each provider on security posture and SLA compliance. Ongoing monitoring via the <231> Supply Chain layer triggers contract reviews or technical mitigations whenever a vendor's risk profile shifts.



Comparing theme Business Governance & Management

in BNPL (Banking) and Short-term Rentals (Hospitality)

BNPL and short-term rental platforms both disrupt traditional industries but face distinct governance challenges.

Structural Governance: BNPL lacks mature corporate governance (107), with weak BoD (102) oversight and top management (136) accountability. Short-term rentals employ hybrid organizational structures (126), balancing centralized tech with local compliance teams.

Regulation & Compliance: BNPL struggles with regulatory frameworks (134), avoiding credit classification, leading to compliance (106) gaps (e.g. missed payments). Short-term rentals actively navigate zoning laws and GDPR (211), implementing automated due diligence (110) for hosts.

Risk Management: BNPL's risk (135) controls are fragmented, relying on unvetted APIs and lacking internal controls (115). Short-term rentals use standardized procedures (128) for safety checks and fraud prevention.

Culture & Ethics: BNPL's organizational culture (125) prioritizes growth over consumer protection, raising ethical (111) concerns (e.g., targeting vulnerable users). Short-term rentals focus on trust, measured via KPIs (116) like guest satisfaction, though face criticism over housing shortages.

Accountability: BNPL lacks clear RACI (131) accountability, especially for fraud. Short-term rentals define roles in policy frameworks (127) for disputes.

Maturity: BNPL operates at Level 2 (ad-hoc), while short-term rentals reach Level 3 (defined processes), showing better adaptation to regulatory demands.

in subscription models in the F&B (Retail) and Short-term Rentals (Hospitality)

Governance Structures: Subscription F&B platforms leverage their organizational culture (125) to embed compliance within operations, using KPIs (116) like customer lifetime value as governance tools. Their hybrid organizational structure (126) tightly couples centralized strategy with regional food safety teams. Short-term rentals employ a different hybrid model, balancing tech scalability with hyperlocal compliance units for zoning laws, reflecting more complex regulatory frameworks (134).

Compliance Challenges: Where F&B contends with dual GDPR (211) and food safety regimes, rentals navigate a triple burden adding property/tax rules. Both deploy GRC frameworks (113), but F&B's due diligence (110) focuses on supply chain (231) risks, while rentals prioritize host verification and tax reporting through automated controls (115).

Risk & Operational Maturity: F&B demonstrates higher maturity (121) in standardizing procedures (128) for perishable logistics, while rentals excel in scaling management systems (120). Their risk profiles (135) diverge: F&B worries about ingredient sourcing, rentals about fraudulent listings. Both use RACI matrices (131) but apply them differently—F&B for recall protocols, rentals for dispute resolution.

Cultural Alignment: The sectors manifest ethical values (111) differently: F&B through sustainability pledges measured by product quality (130) metrics, rentals via trust-building KPIs like host retention. This reflects their core challenges, F&B's subscription model demands consistent experience, while rentals' peer-to-peer nature requires community balance.

Business Resilience: Both maintain robust business continuity (103) plans, though F&B's center on supply chain redundancy and rentals on crisis response (e.g., pandemic refund policies). Their top management (136) prioritizes different resilience aspects, F&B on delivery reliability, rentals on platform stability.

Comparing theme IT Governance and Management in BNPL (Banking) and Short-term Rentals (Hospitality)

Strategic Alignment & Compliance: In BNPL sector, **Governance** of IT ensures compliance with financial regulations like PSD2 (Open Banking) and GDPR, using frameworks such as ISMS to automate risk assessments and fraud detection. STRPs, by contrast, focus on GDPR to protect guest data, relying on ISMS to secure booking systems against cyber threats like ransomware.

Privacy & Data Protection: BNPL services implement PIMS to manage sensitive credit scores with Privacy-by-Design to enforce strict consent mechanisms (Opt-in). STRPs, use PIMS to safeguard guest identities and payment details, via Zero Trust to validate host-guest interactions. BNPL emphasizes financial vetting, when STRPs enforce decentralized access controls.

Cybersecurity Operations: BNPL platforms combat financial fraud through MDR services and the CIA Triad. STRPs prioritize PMS uptime, using Vulnerability Management to patch API flaws and prevent downtime. Both sectors face cyber risks, but BNPL targets transaction integrity, whereas STRPs mitigate disruptions to guest experiences.

Third-Party & Supply Chain Risk: BNPL relies on C-SCRM to secure credit bureaus, requiring SBOM for payment software transparency. STRPs employ C-SCRM to assess property services, conducting BIA to prioritize PMS recovery.

Incident Response: BNPL's Incident Response ensures transaction logging and regulatory reporting. STRPs focus on notifying GDPR authorities and restoring bookings. Both sectors emphasize accountability, but BNPL safeguards financial workflows, while STRPs protect user-facing platforms

in subscription models in the F&B (Retail) and BNPL (Banking)

Strategic Alignment & Compliance: Subscription F&B platforms use an ISMS (ISO/IEC 27001 + COBIT) to link fulfillment SLAs and churn KPIs to GDPR and food-safety rules, with exceptions reported to the Regulatory Body, while BNPL embeds approval-rate and default-rate metrics into PSD2 and GDPR workflows, routing all breaches to financial regulators (e.g., FCA, SEC).

Privacy & Data Protection: Subscription F&B leverages a PIMS with Privacy-by-Design to govern PII in CRM and billing, logging every data-subject request, whereas BNPL secures credit scores and transaction histories via its PIMS plus explicit Opt-in flows and encrypted vaults in underwriting systems.

Cybersecurity Operations: Both sectors apply Zero Trust under their ISMS with 24/7 MDR and Vulnerability Management, but Subscription F&B focuses on supply-chain API resilience and order-management services, while BNPL prioritizes payment-gateway telemetry and fraud-response drills in its Incident Response playbook.

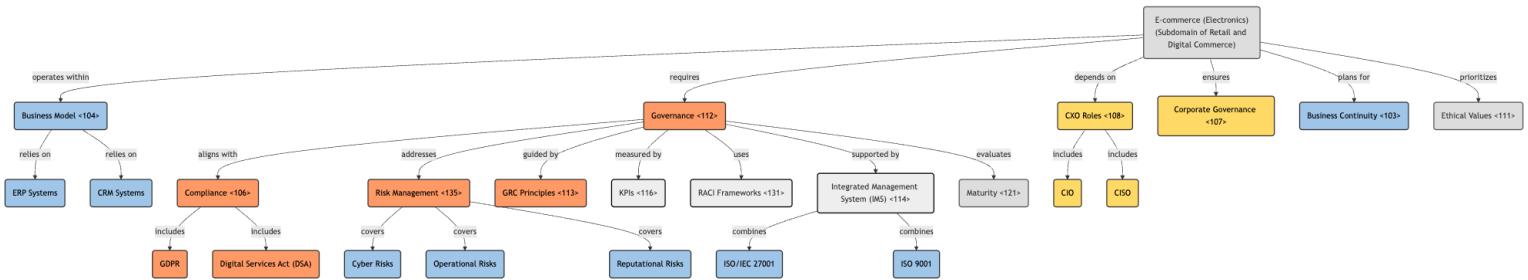
Third-Party & Supply-Chain Risk: Subscription F&B rates kitchens, couriers, and suppliers via Vendor Assessment under C-SCRM with Supply Chain triggering contract reviews, and BNPL similarly evaluates merchants, card networks, and bureaus—adding SBOM transparency and API-gateway isolation for high-risk partners.

E-commerce (Electronics) in the Context of Organizations, Governance and Management

The **e-commerce (electronics)** niche operates within the broader **retail and digital commerce** sector, characterized by a **<104> business model** centered on online sales of electronic goods. This niche relies heavily on **digital platforms**, such as **Enterprise Resource Planning (ERP)** and **Customer Relationship Management (CRM)** systems, to manage inventory, logistics, and customer interactions. The **<112> governance** of these platforms must align with **<106> compliance** requirements like the **GDPR** and **Digital Services Act (DSA)**, ensuring data protection and transparency in customer transactions.

<135> Risk management is critical, addressing **cyber risks** (e.g., payment fraud), **operational risks** (e.g., supply chain disruptions), and **reputational risks** (e.g., product quality issues). An **<114> Integrated Management System (IMS)** can harmonize these efforts, combining **ISO/IEC 27001** for information security and **ISO 9001** for quality management. The **<121> maturity** of governance structures is evident in the adoption of **<116> KPIs** to monitor performance and **<131> RACI frameworks** to clarify roles in incident response.

<108> CXO roles, such as the **CIO** and **CISO**, play pivotal roles in aligning **IT governance** with strategic goals, while **<107> corporate governance** ensures accountability to stakeholders. The niche's **<103> business continuity** plans must address disruptions, reflecting **<113> GRC principles**. Culturally, **<111> ethical values** like transparency in pricing and sustainability claims are increasingly prioritized to build consumer trust.



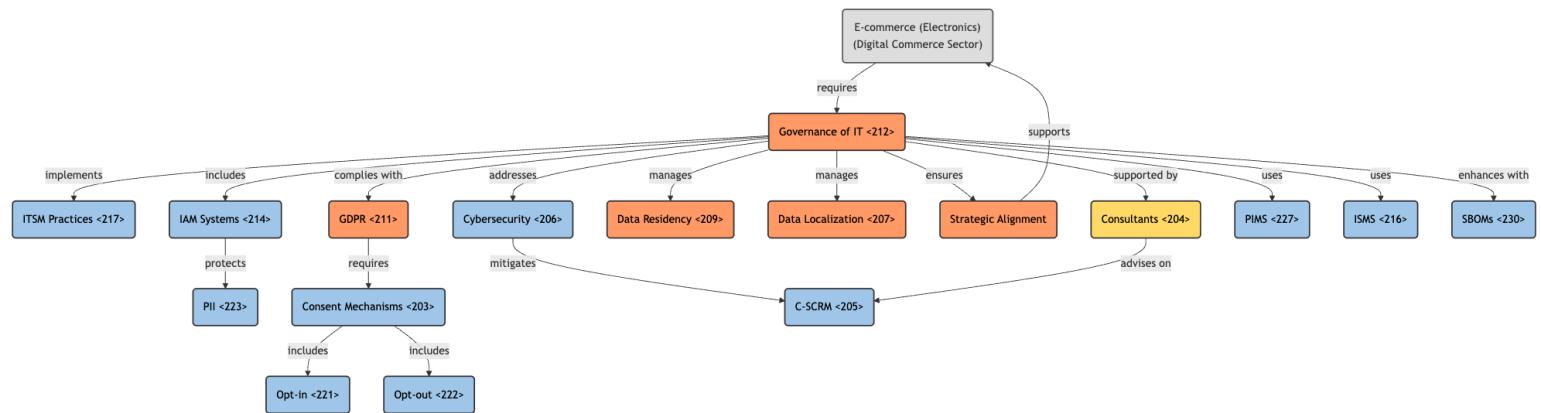
E-commerce (Electronics) in the Context of Governance of IT and IT Management

The e-commerce sector, particularly in electronics, operates within a highly dynamic and competitive digital environment, necessitating robust **Governance of IT** to align technology with strategic business goals. This niche relies heavily on digital platforms, requiring seamless integration of **ITSM** practices to ensure operational efficiency and customer satisfaction. Key components such as **IAM systems** are critical for securing customer data and managing access across omnichannel touchpoints, while **Cybersecurity measures** protect against threats like payment fraud and data breaches.

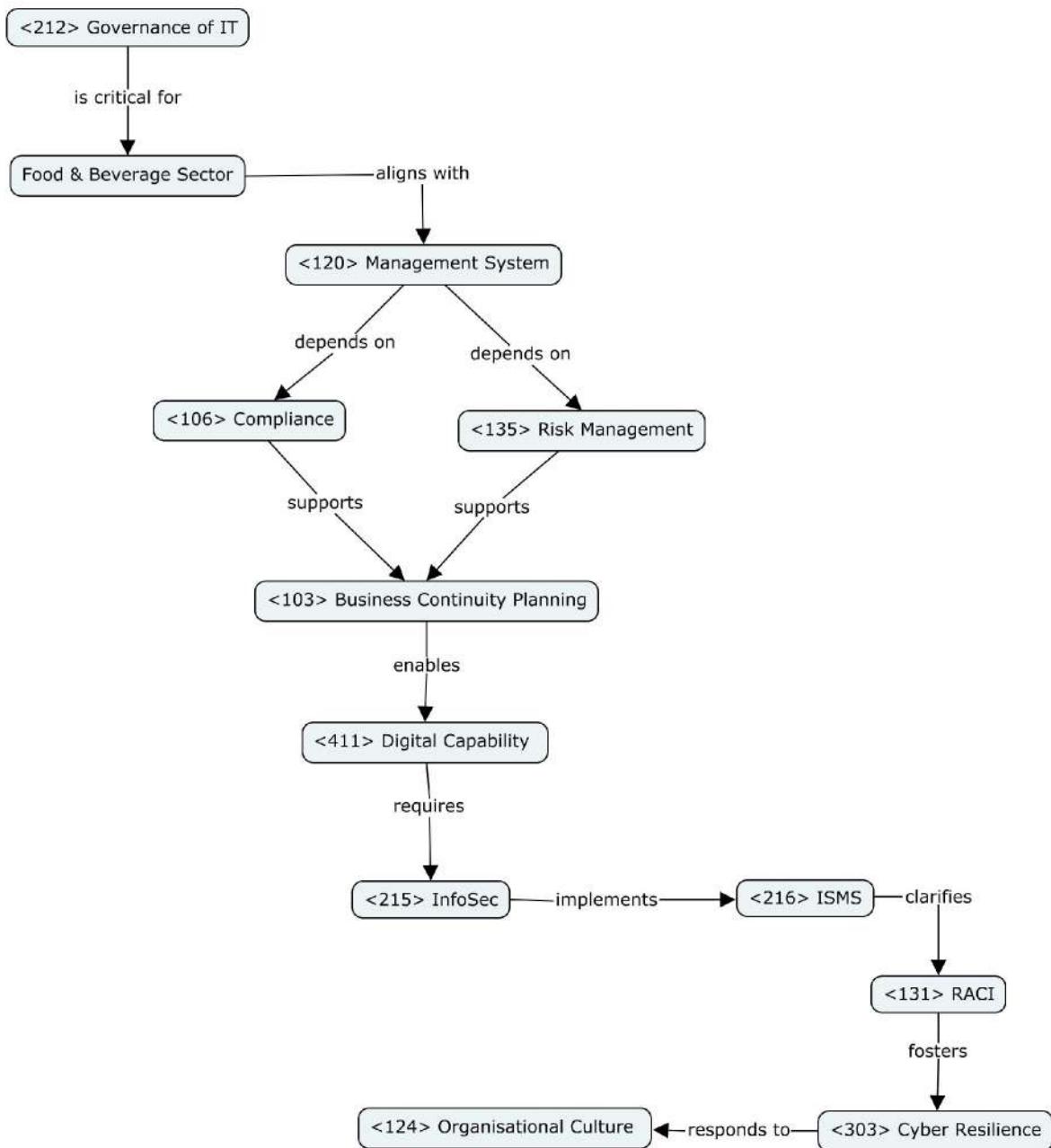
Compliance with **GDPR** and other data protection regulations is paramount, given the handling of sensitive **PII**. Effective **Consent mechanisms**, including **Opt-in** and **Opt-out** options, ensure transparency and build consumer trust. The sector also faces challenges related to **Data Residency** and **Data Localization**, as cross-border sales necessitate adherence to varying regional laws.

Strategic alignment is achieved through frameworks like **Governance of IT**, ensuring that IT investments support business objectives such as personalized marketing and inventory optimization. The role of **Consultants** is often pivotal in auditing processes and advising on **C-SCRM** to mitigate risks in the supply chain. Additionally, **PIMS** and **ISMS** frameworks help maintain data integrity and security, while **SBOMs** enhance transparency in software dependencies.

In summary, the e-commerce (electronics) niche exemplifies the interplay between **Governance of IT** and operational agility, where compliance, security, and strategic alignment are critical to sustaining competitive advantage and customer trust.



Concept Map: Governance of IT in the Hospitality & Leisure Industry



This concept map shows how **<212> Governance of IT** enables secure and efficient digital transformation in the Food & Beverage (F&B) sector, where service speed, hygiene standards, and guest experience are vital to competitiveness.

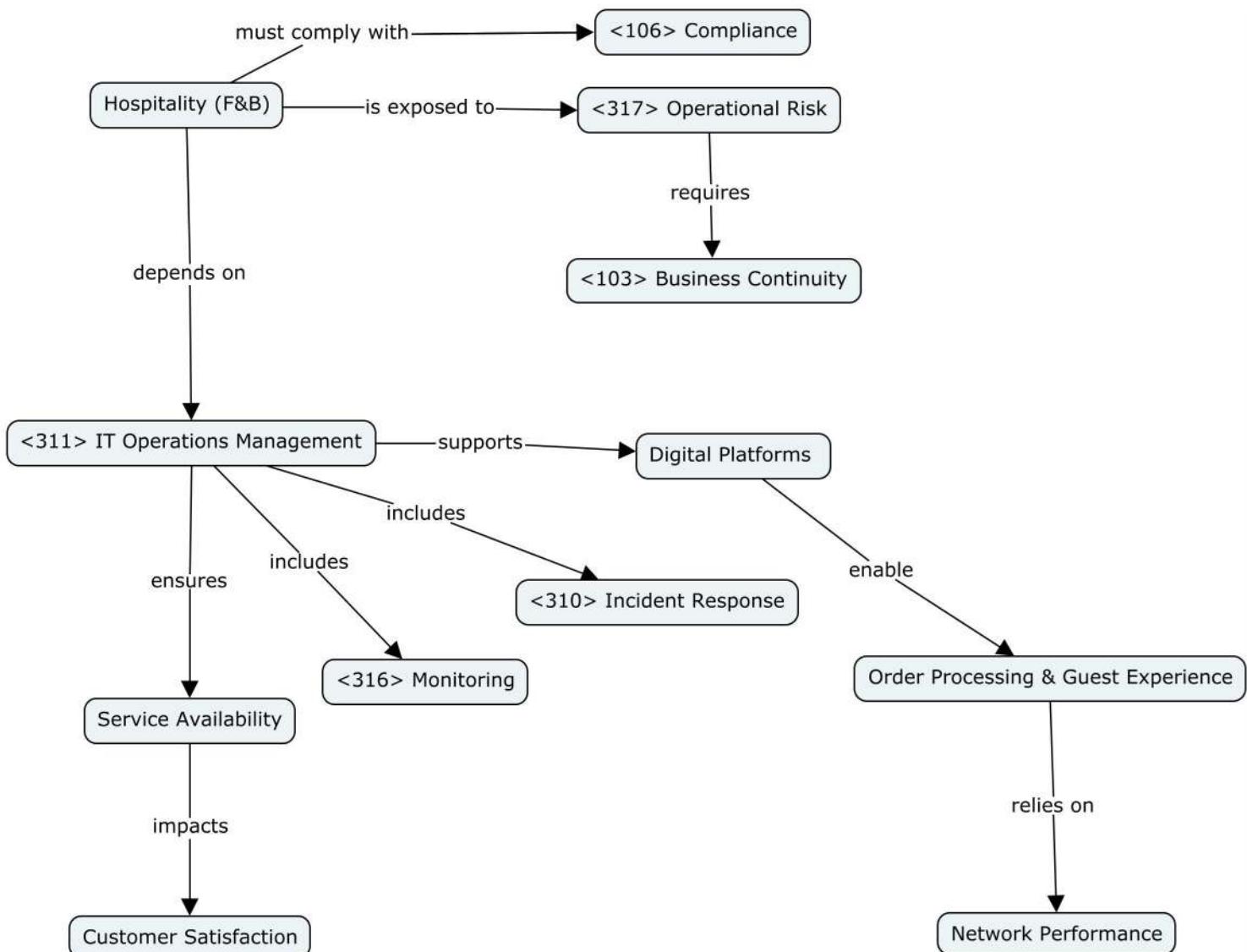
The sector's growing use of digital tools—such as POS systems, mobile ordering, and loyalty apps—requires a structured **<120> Management System** to ensure consistency and performance across branches or franchises. To meet regulatory demands (e.g., food safety, GDPR), strong **<106> Compliance** and **<135> Risk Management** practices are necessary.

<103> Business Continuity Planning becomes essential in maintaining service delivery during system outages or crises, particularly in high-turnover, time-sensitive environments like restaurants and catering services.

<411> Digital Capability supports innovation and operational agility but must be built upon solid **<215> Information Security** practices. This includes protecting payment and customer data through formal **<216> ISMS** controls. Clear **<131> RACI** structures help define roles in multi-shift, high-volume settings.

Strong **<124> Organisational Culture** aligned with IT processes helps foster **<303> Cyber Resilience**—ensuring the ability to sustain service and brand reputation in the face of digital threats.

Concept Map: IT Management and Hospitality and Leisure (Food and Beverage) Industry



This concept map focuses on the role of **<311> IT Operations Management** in supporting digital reliability within the Food & Beverage (F&B) sector, a core component of the hospitality industry. The F&B sector includes businesses such as restaurants, cafes, bars, quick-service outlets, catering firms, and digital food delivery platforms. These operations are often fast-paced, labour-intensive, and regulated environments where efficiency, compliance, and customer experience are tightly linked to IT systems.

In this context, **<311> IT Operations Management** ensures the provisioning, capacity, performance, and availability of essential systems—such as POS platforms, loyalty apps, digital ordering tools, and property management systems. The effectiveness of these operations is fundamental to maintaining real-time service availability and smooth **<310> Incident Response**, particularly during busy periods or unexpected disruptions.

Given the sector's vulnerability to **<317> Operational Risk**—ranging from supply chain failures and equipment breakdowns to surges in seasonal demand—a well-developed **<103> Business Continuity** plan is necessary to safeguard uninterrupted service.

Further, **<106> Compliance** is critical in the F&B space, covering food safety standards, labour laws, and increasingly, data privacy regulations like the GDPR. These compliance demands must be addressed through secure and stable IT operations.

Digital Platforms supported by IT operations play a central role in enabling Order Processing & Guest Experience, both of which are reliant on robust **<316> Monitoring** and stable **<Network Performance>**. The consistent execution of these tasks ensures high **<Service Availability>**, which directly affects **<Customer Satisfaction>**—a decisive factor in customer loyalty and business success.

By linking operational resilience with digital tools and compliance frameworks, this map underscores how **<311> IT Operations Management** underpins service excellence in the fast-moving, digitally mediated F&B industry.

Agriculture and Farming

The **Agriculture and Farming** industry encompasses the cultivation of crops, raising of livestock, and management of natural resources to produce food, fiber, and raw materials. It is characterized by its dual nature, combining traditional practices with industrialized operations. The sector integrates diverse subdomains such as crop farming, animal husbandry, agroforestry, agricultural finance, and agri-food processing and distribution, the latter focusing on transforming raw agricultural outputs into consumable products and ensuring their efficient delivery to markets. Governance, climate resilience, technological adoption, and compliance with food safety and trade standards are central to its operations. Definitions vary across contexts due to the industry's heterogeneity, requiring tailored explanations to reflect specific subdomains and strategic priorities.

Organizations, Governance and Management in Agri-Food Processing and Distribution

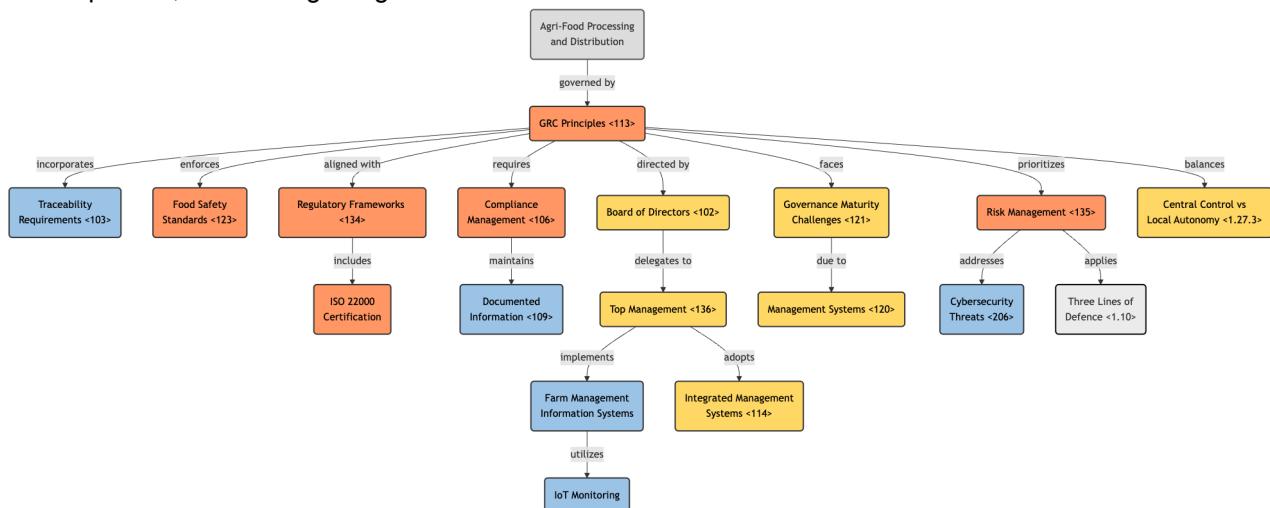
Agriculture and Farming, particularly within the Agri-Food Processing and Distribution subdomain, presents a unique governance landscape when analyzed. This sector operates at the intersection of traditional agricultural practices and modern supply chain dynamics, requiring governance frameworks that balance regulatory compliance, risk management, and operational efficiency.

Governance in Agri-Food Processing and Distribution is heavily influenced by traceability and food safety requirements (<103>, <123>), aligning with Governance, Risk, and Compliance (GRC) principles (<113>). The sector adheres to stringent regulatory frameworks (<134>) such as ISO 22000, ensuring products meet established criteria from farm to table. This mirrors the emphasis on compliance (<106>) and documented information (<109>), where systematic processes are critical for accountability.

The Board of Directors (BoD) (<102>) and top management (<136>) play pivotal roles in setting strategic direction, particularly integrating technologies like Farm Management Information Systems (FMIS) and IoT for real-time monitoring. The sector faces governance maturity challenges (<121>), as smaller producers may lack resources for formalized management systems (<120>), while larger agribusinesses leverage Integrated Management Systems (IMS) (<114>) to align quality, safety, and environmental standards.

Risk management (<135>) is critical, with exposure to supply chain disruptions, regulatory shifts, and cybersecurity threats (<206>). The Three Lines of Defence model applies here: operational teams (first line) ensure daily compliance, risk managers (second line) monitor threats, and internal audits (third line) validate controls. The sector highlights tension between central control and local autonomy, as global supply chains require standardized governance while accommodating regional regulations.

Agri-Food Processing and Distribution exemplifies how governance structures must adapt to sector-specific demands, blending traditional oversight with modern GRC principles for resilience, compliance, and strategic alignment.



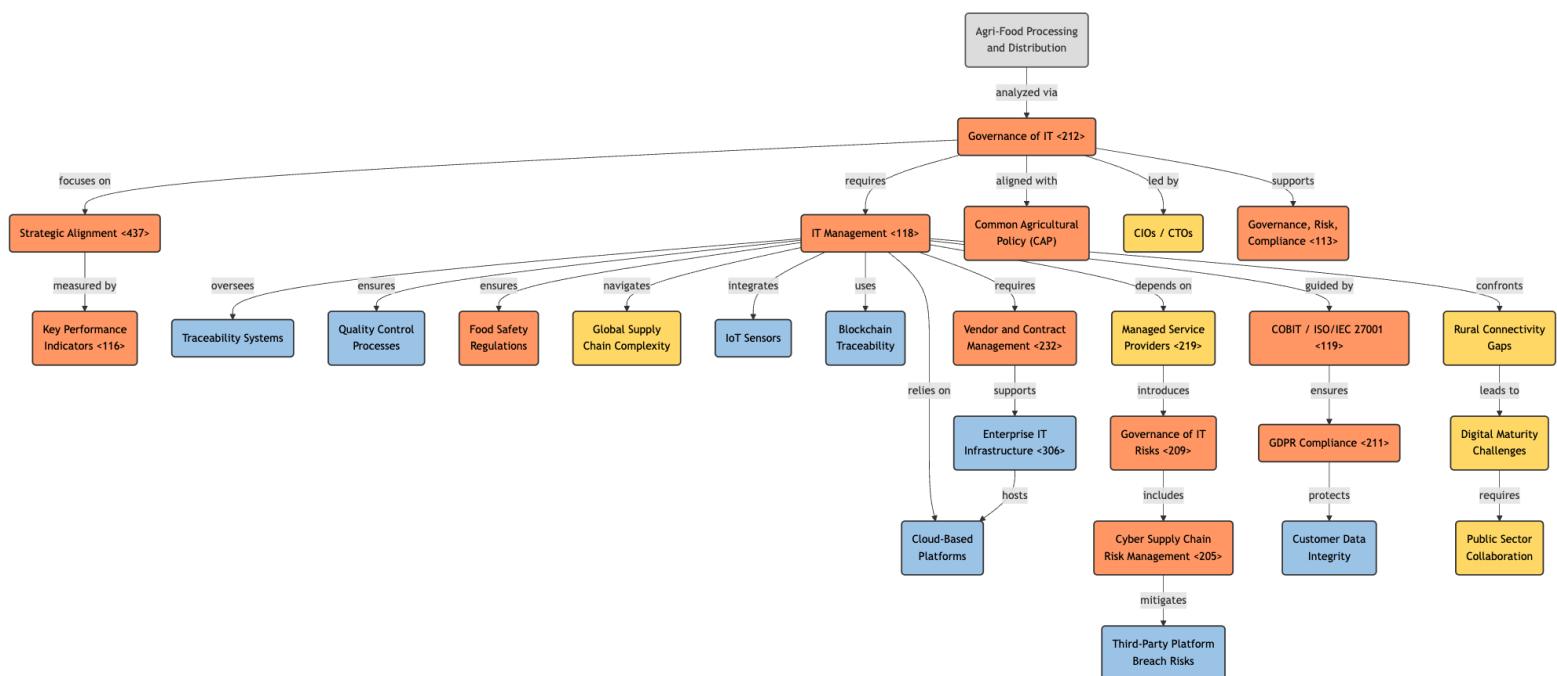
IT Management in Agri-Food Processing and Distribution

Agriculture and Farming, particularly within the Agri-Food Processing and Distribution subdomain, presents a unique intersection of traditional practices and modern IT Management challenges. This sector relies heavily on information systems to ensure traceability, quality control, and compliance with stringent food safety regulations while navigating global supply chain complexities. From a governance of IT (<212>) perspective, the focus is on aligning systems with business goals like optimizing cold chain logistics or meeting regulatory requirements such as the EU's Common Agricultural Policy (CAP). Strategic alignment (<437>) is critical, as IT investments must support operational efficiency and risk mitigation, including managing supply chain disruptions and ensuring data integrity for audits.

IT Management (<118>) in Agri-Food Processing and Distribution oversees systems tracking products from farm to table, integrating IoT sensors, blockchain for traceability, and cloud-based platforms for real-time data sharing. These technologies require robust vendor and contract management (<232>) within enterprise IT infrastructure (<306>) to ensure seamless integration and compliance. Reliance on Managed Service Providers (MSPs) (<219>) introduces risks like vendor dependency and cybersecurity vulnerabilities, necessitating strong governance of IT risks (<209>). Third-party logistics platform breaches could compromise data or disrupt operations, highlighting the need for Cyber Supply Chain Risk Management (C-SCRM) (<205>).

CIOs and CTOs must balance innovation with operational stability, working within frameworks like COBIT or ISO/IEC 27001 (<119>) to ensure systems meet business and compliance needs, including GDPR (<211>) requirements for customer data. Key Performance Indicators (KPIs) (<116>) such as system uptime during harvest seasons and traceability record accuracy measure effectiveness. Challenges like rural connectivity gaps and uneven digital maturity among smaller producers require adaptive strategies and public sector collaboration.

This subdomain exemplifies how IT Management in Agriculture and Farming must bridge legacy practices with cutting-edge technologies while maintaining focus on governance, risk, and compliance (<113>). Success hinges on leveraging IT as a strategic enabler of resilience, transparency, and value creation across the supply chain.



Industry Comparison: Organizations, Governance and Management in Retail and Digital Commerce and in Agriculture and Farming

The domains of Pure Play E-Commerce and Agri-Food Processing and Distribution differ significantly in <112> governance and <118> management.

The <126> organizational structure within e-commerce varies considerably but tends to be decentralized, with a digital-first <439> strategy and <112> governance prioritizing customer experience and scalability. <134> Regulatory frameworks and <106> compliance concerns centre on <208> data privacy, pricing and advertisement, while <134> risk management must focus on <206> cyber security, disruptions to the <231> supply chain and reputational issues.

<126> Organizational structure in Agri-Food Processing and Distribution is even more varied in size and ownership model. <112> Governance contrasts the previous industry by focusing on <106> compliance with food safety and environmental <134> regulations, and on <134> risks associated with natural external factors and common digital gaps in the sector.

Broadly speaking, e-commerce emphasizes speed and innovation, while agri-food prioritizes traceability and regulatory compliance.

Industry Comparison: Governance and Management of IT in Retail and Digital Commerce and in Hospitality and Leisure

IT Governance and management in Pure Play E-Commerce and Food & Beverage reflect the differences between the two sectors' operational models.

In the context of e-commerce, <212> governance of IT is centred around guaranteeing security and scalability in omnichannel platforms that handle large volumes of data and <223> personally identifiable information. <214> IAM and <205> C-SCRM systems are used to ensure <206> cyber security amidst complex <206> supply chains, while <203> consent mechanisms and handling of <305> data protection in general help gain consumer trust and <106> compliance with standards such as <211> GDPR.

On the other hand, the priority of <212> IT Governance within Food & Beverage is operational reliability, which is sought out, for example, by means of inventory systems. While not as data intensive as the e-commerce industry, concerns of <305> data protection and <106> compliance with <211> GDPR still surface from the use of <223> PII in increasingly prominent digital platforms.

Industry Comparison: Organizations, Governance, and Management in Hospitality and Leisure vs. Agriculture and Farming

The Hospitality and Leisure industry typically operates under structured and formalized **<126> Organizational Structures**. Large hotel and tourism chains adopt a centralized decision-making model at the corporate level while delegating daily operations to local managers.

In contrast, the Agriculture and Farming industry relies on decentralized and informal **<112> Governance** structures, especially among family-run farms and agricultural cooperatives. Many agricultural operations are small to medium-sized, while others are part of large agribusiness conglomerates with integrated supply chains and global market exposure, which means governance frameworks need to accommodate both traditional and industrial farming models.

Regarding **<135> Risk <118> Management**, Hospitality and Leisure needs to be aware of operational, reputational and **<106> Compliance** risks. These include service disruptions, negative reviews and adherence to food safety, labor and protection regulations. Agriculture and Farming, on the other hand, must manage risks tied to weather events, disease outbreaks, commodity price fluctuations, and regulatory shifts related to pesticides, land use, or water rights.

Industry Comparison: Governance of IT and IT Management in Hospitality and Leisure vs. Agriculture and Farming

In the Hospitality and Leisure industry, IT systems revolve around Property Management Systems (PMS), Online Travel Agencies (OTA), and Customer Relationship Management (CRM) tools. The integration of guest-facing apps and loyalty platforms generates significant data processing, making GDPR **<106> Compliance** essential for protecting personal information.

In contrast, Agriculture and Farming shows uneven IT adoption, creating digital asymmetries. While large firms use advanced systems like Farm Management Information Systems (FMIS), many smaller producers still depend on legacy tools or informal practices, limiting digital integration and data-driven decision-making.

Project Report
Industries Analysis:
Retail and Digital Commerce,
Hospitality and Leisure
Healthcare

Segurança e Gestão de Sistemas de Informação
Group: 358

2º Semestre
Ano Lectivo: 2024/2025
Professor: Luís Borbinha
Curso: METI/MEIC

Alunos:
Diogo Marques, nº102760
Afonso Pires, nº102803
António Dias da Silva, nº102879
Tiago Basílio, nº103326

Índice

<i>Retail and Digital Commerce – Governance</i>	4
<i>Retail and Digital Commerce – IT Management</i>	5
<i>Hospitality and Leisure – Governance</i>	6
<i>Hospitality and Leisure – IT Management</i>	7
<i>Healthcare – Governance</i>	8
<i>Healthcare – IT Management</i>	9
<i>Industry Comparisons</i>	10

Retail and Digital Commerce – Governance

The Retail and Digital Commerce industry refers to the complex ecosystem in which goods and services are offered to consumers through both physical and digital channels. This industry encompasses traditional retail stores, e-commerce platforms, omnichannel operations, and marketplace-based models.

In this context, governance plays a critical role in ensuring accountability, integrity, and strategic alignment in a highly competitive and data-driven environment. As companies adopt platform-based and omnichannel models, their governance frameworks must extend beyond traditional retail oversight to include digital infrastructure, customer data handling, and third-party dependencies. Boards of Directors <102> and CxOs <108> are required to integrate Governance, Risk, and Compliance (GRC) <113> practices to manage risks ranging from supply chain disruptions and unethical advertising to cybersecurity breaches involving ePOS systems.

Effective governance demands formalized policies <127>, internal controls <115>, and structured management systems <120> to ensure compliance <106> with regulatory standards such as the GDPR and the Digital Services Act (DSA). Ethical values <111> are central, particularly in data usage and algorithmic decision-making. Due diligence <110> must cover vendor assessment, environmental claims, and algorithmic transparency. Sound governance underpins business continuity <103>, strengthens consumer trust, and supports the adaptive capacity of business models <104> in a fast-changing legal and technological landscape.

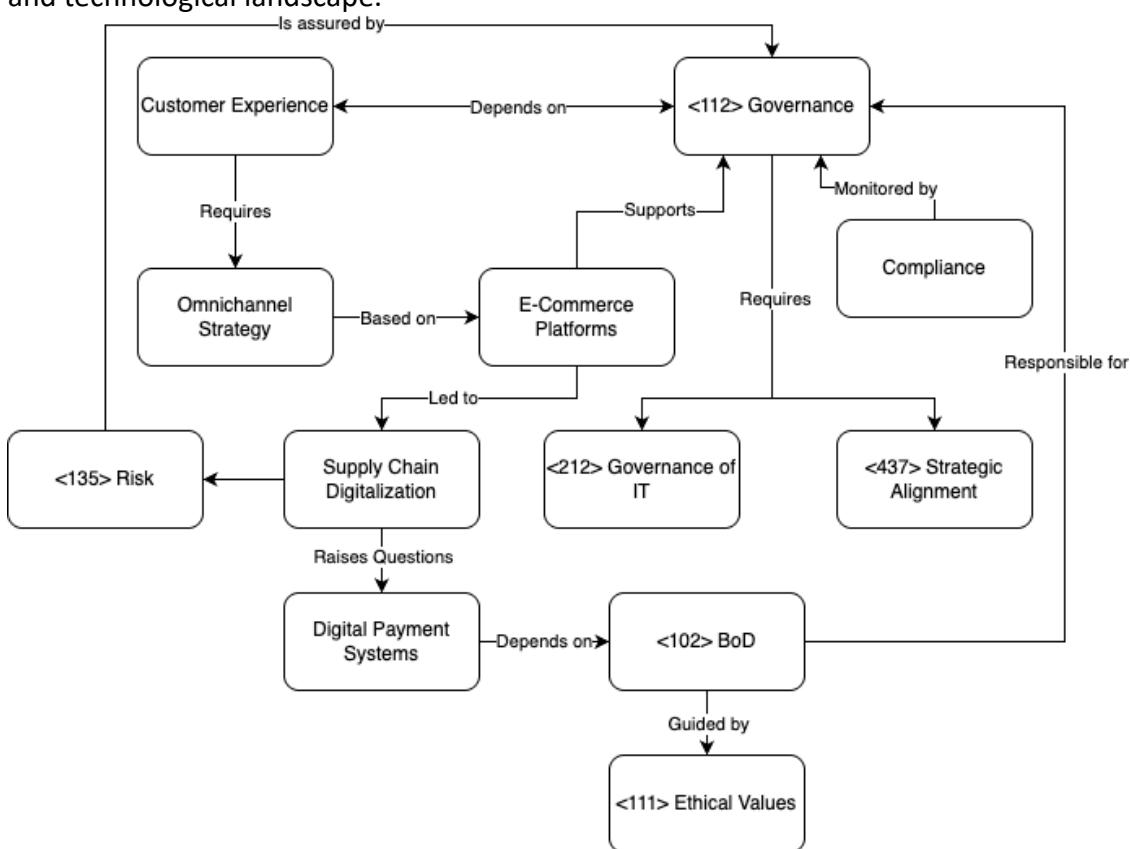


Figure 1 – Concept Map of Governance in Retail and Digital Commerce

Retail and Digital Commerce – IT Management

The retail and digital commerce sector has evolved into a highly digitized, data-driven environment that demands robust and adaptive IT management. As omnichannel models blur the boundaries between physical stores and online platforms, organisations must ensure seamless integration of POS/ePOS systems, ERP, CRM, and analytics tools. This complexity necessitates strong IT Service Management (ITSM) <217>, where the delivery and support of IT services must align with fast-paced retail operations. Equally, Governance of IT <212> becomes essential to ensure that retail technologies support business goals while mitigating cyber risks <206> and maintaining compliance.

With increasing reliance on third-party platforms and cloud infrastructures, vulnerabilities and supply chain risks intensify, calling for Cybersecurity Supply Chain Risk Management (C-SCRM) <205> and Vendor Assessment <232> as routine components of IT oversight. Sensitive customer data processed across these platforms also raises Data Privacy <208> and GDPR <211> concerns. Effective implementation of Consent Mechanisms <203>, especially opt-in <221> processes, is crucial for trust and legal compliance. Moreover, digital commerce's global reach confronts IT leaders with data residency <209> and localization <207> issues, requiring strategic decisions aligned with data sovereignty and risk exposure.

Ultimately, retail CIOs must manage IT not only as a support function but as a driver of innovation, operational continuity, and reputational resilience—aligning governance principles with technical execution to sustain competitive advantage in an increasingly regulated and platform-dependent industry.

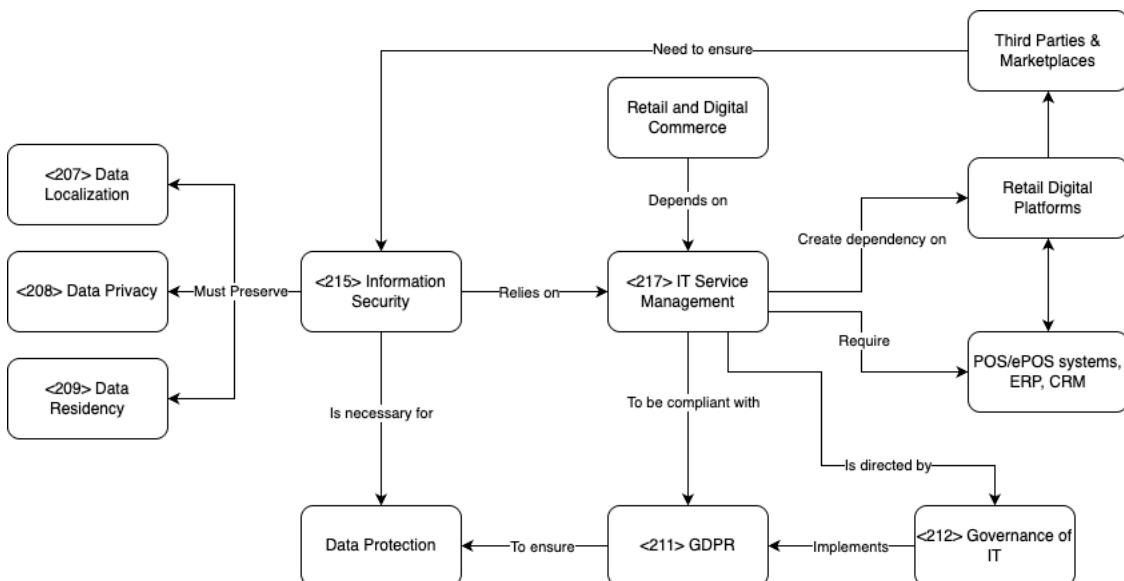


Figure 2 – Concept Map of IT Management in Retail and Digital Commerce

Hospitality and Leisure – Governance

IT Management focuses on delivering consistent and personalized experiences to guests while optimizing back-office processes. The sector faces unique challenges such as high service variability, seasonality, and integration of online and on-site experiences.

The Hospitality and Leisure industry comprises businesses that offer services aimed at relaxation, entertainment, and travel. This includes hotels, resorts, restaurants, casinos, theme parks, and tour operators. We define the industry as service-oriented establishments that prioritize customer experience and depend heavily on physical locations, complemented increasingly by digital channels.

In this industry, governance <112> is essential for balancing service consistency with local market responsiveness, a challenge heightened by its diverse subdomains such as accommodation, food and beverage, and event management. Boards of Directors <102> and CxOs <108> steer brand management, partner selection, and technology adoption, embedding governance, risk, and compliance <113> (GRC) to address operational risks like service disruptions during peak seasons or reputational damage from negative guest reviews or data breaches. Internal controls <115> and documented policies <127> enforce compliance <106> with stringent health, safety, and data protection laws (e.g., GDPR <211>), particularly in regions with frequent regulatory updates. Ethical values <111> shape practices around guest data usage and sustainability commitments, with due diligence <110> playing a key role in vetting vendors and preparing for crises like natural disasters or pandemics, which have historically disrupted operations. The industry's reliance on public-private partnerships and franchising models requires robust management systems <120> to ensure accountability and business continuity <103>, especially as global chains pursue certifications like ISO 9001 while smaller firms lean on informal governance, highlighting a maturity gap that demands tailored frameworks to align strategies with stakeholder expectations and enhance resilience.

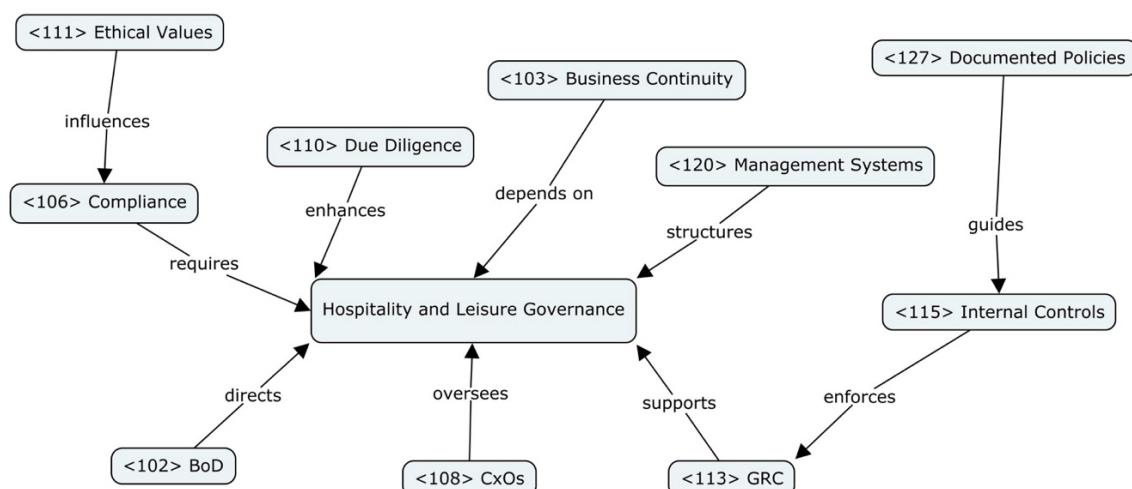


Figure 3 – Concept Map of Governance in Hospitality and Leisure

Hospitality and Leisure – IT Management

The Hospitality and Leisure industry depends on IT management to drive digital transformation and sustain operational excellence amid high guest expectations. Governance of IT <212> aligns property management systems (PMS), online travel agencies (OTA), and loyalty platforms with business objectives, while tackling cyber risks <206> that escalate with interconnected digital ecosystems. IT Service Management (ITSM) <217> underpins seamless guest experiences through booking engines and mobile check-ins, requiring meticulous IT operations management to maintain uptime during peak travel periods. The sector's reliance on third-party providers heightens cybersecurity supply chain risk management (C-SCRM) <205> and vendor assessment <232> priorities, especially given GDPR <211> mandates for protecting guest data across borders. Data privacy <208> and consent mechanisms <203> (e.g., opt-in <221>) build trust, while data residency <209> issues complicate compliance in multi-jurisdictional operations, such as managing EU and APAC data separately. CIOs or CISO-equivalents lead innovation with cloud-based solutions and ensure regulatory adherence, positioning IT as a strategic asset in a competitive landscape where downtime or breaches can erode customer loyalty and brand reputation.

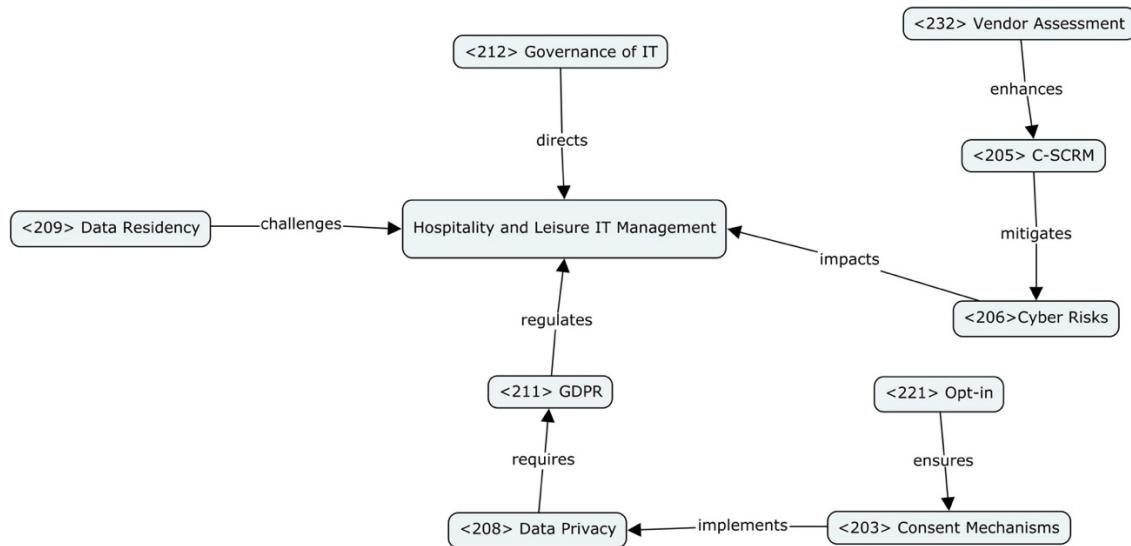


Figure 4 – Concept Map of IT Management in Hospitality and Leisure

Healthcare – Governance

The Healthcare industry encompasses providers and institutions that deliver medical, diagnostic, and preventive care. This includes hospitals, clinics, research labs, and public health authorities.

Governance integrates clinical accountability, financial oversight, and regulatory compliance <106> to balance service quality with systemic resilience. The Serviço Nacional de Saúde (SNS)—a Beveridge-style system—exemplifies public-sector governance, prioritizing universal access while managing risks like workforce shortages and aging populations. Clinical governance structures enforce standards for patient safety, supported by documented policies <127> (e.g., treatment protocols) and internal controls <115> to audit outcomes.

The European Health Data Space (EHDS) amplifies governance demands, requiring interoperability of EHRs across EU borders and strict data privacy <208> safeguards under GDPR <211>. Portugal's SPMS aligns with these mandates, managing national EHRs and e-prescriptions while enabling secondary use of data for research. Risk management <118> extends to systemic threats: pandemics demand cross-institutional coordination, while cyberattacks on hospitals necessitate business continuity <103> plans.

Ethical challenges—such as AI diagnostics or genomic data use—require governance frameworks to embed ethical values <111>, ensuring transparency and patient consent. Hybrid systems like Portugal's, blending public universality with private-sector partnerships, face corporate governance <113> tensions between financial sustainability and equitable access. Finally, regulatory compliance <106> intersects with data residency <209> rules, as cross-border data flows under EHDS demand harmonized cybersecurity protocols and vendor assessments <232> for third-party tools.

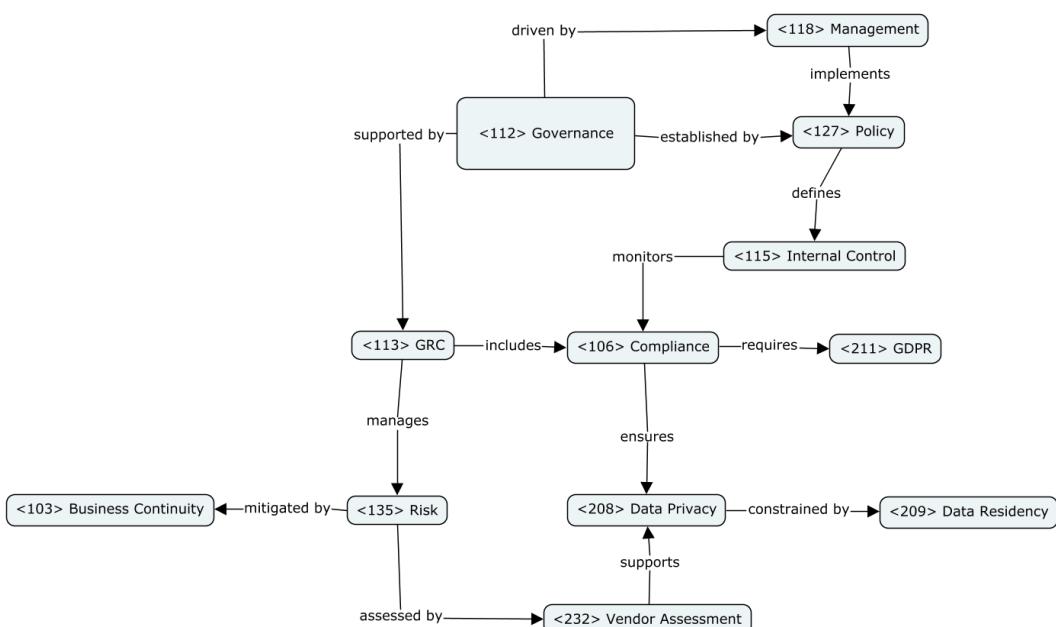


Figure 5 - Concept Map of Governance in Healthcare

Healthcare – IT Management

Healthcare's digital transformation relies on IT management strategies that merge innovation with compliance. Electronic Health Records (EHRs), managed nationally by Portugal's SPMS, are foundational but require interoperability to fulfill the EHDS vision of cross-border care continuity. IT Service Management (ITSM) <217> ensures uptime for critical systems like telehealth platforms and IoT-enabled medical devices, which are vulnerable to cybersecurity <206> threats (e.g., ransomware targeting hospitals).

The EHDS mandates secondary use of health data for research, driving demand for data analysis <109> tools and AI algorithms. However, these technologies require explainability and data diligence <112> to avoid biases and ensure GDPR <211> compliance. Cloud infrastructure adoption, while enhancing scalability, introduces supply chain risks, necessitating rigorous vendor assessments <232> and data sovereignty <207> strategies to comply with EU regulations.

eHealth initiatives, such as teleconsultations, depend on consent mechanisms <203> to align with ethical and legal standards. For instance, Portugal's e-prescription system integrates patient consent workflows while adhering to data residency <209> rules. Business continuity <103> plans are critical to mitigate disruptions from cyberattacks or natural disasters, ensuring IT systems like real-time patient monitoring remain operational.

Ultimately, healthcare IT must balance innovation with governance principles, ensuring technologies like AI and EHRs enhance care without compromising ethical values <111> or regulatory compliance <106>. The SPMS exemplifies this balance, harmonizing national digital infrastructures with European frameworks like the EHDS and GDPR.

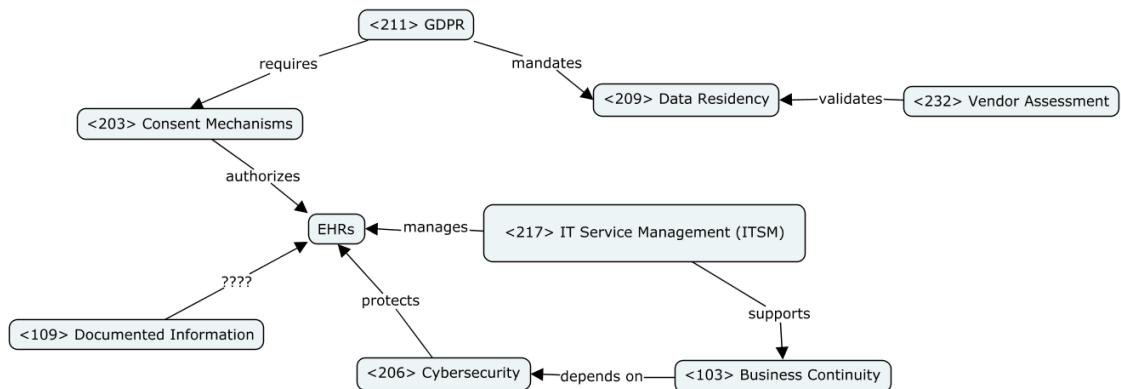


Figure 6 - Concept Map of IT Management in Healthcare

Industry Comparisons

Comparing with Theme 1: Organizations, Governance, and Management

Retail & Digital Commerce vs Hospitality & Leisure

Retail governance is driven by brand-and-data alignment across online and physical channels: steering committees oversee omnichannel KPIs, digital-marketing ethics, and GDPR-compliant loyalty programs. Boards meet quarterly to review supply-chain dashboards and vendor risk registers, emphasizing rapid pivoting in response to consumer trends.

Hospitality governance, by contrast, fuses brand-standards with local autonomy: global chains enforce ISO 9001 quality schemes yet empower regional General Managers to tailor guest-experience protocols. Governance forums rotate between operations, F&B, and sustainability leads to balance service consistency with seasonal market dynamics.

Retail & Digital Commerce vs Healthcare

In Retail, executive teams formalize risk through a digital GRC approach that brings together data-privacy safeguards, platform compliance (GDPR, DSA) and uninterrupted operation of ePOS systems. Their management systems emphasize brand-reputation metrics and clear decision rights between marketing and IT.

In Healthcare, boards work under tight public mandates. Patient-safety councils establish clinical-governance frameworks, set policies for EHR interoperability and run regular pandemic-response exercises. Management reviews bring clinical leads together with the CIO and CISO to ensure quality-of-care audits and resilience planning stay fully aligned.

Hospitality & Leisure vs Healthcare

Hospitality's governance combines service charters (guest satisfaction, F&B safety) with franchise-compliance councils, where risk committees include urban-planning and events teams to manage peak-season pressures. Management systems hinge on rapid feedback loops from PMS and OTA partners.

Healthcare governance is prescriptive: clinical governance boards, ethics committees, and cross-institutional audit teams co-chair policy on EHR access, telehealth credentials, and vendor-certification (ISO 27799). Management blends CMO, CIO, and administration to uphold both clinical outcomes and operational resilience.

Retail & Digital Commerce vs Hospitality & Leisure

From an organizational-culture lens, Retail firms structure around value-stream squads (product, UX, analytics) enabling fast-cycle governance sprints, while Hospitality embeds cross-functional “guest-journey” councils (front-desk, F&B, ops) that meet daily during peak weeks. Although both deploy tiered escalation paths for service failures, Retail relies on digital-service-level dashboards, whereas Hospitality leans on in-person incident-response protocols.

Comparing with Theme 2: Governance of IT and IT Management

Retail & Digital Commerce vs Hospitality & Leisure

Retail's IT governance is centered on omnichannel integration: an IT steering committee (CIO, CISO, Head of e-Commerce) vets new microservices, enforces C-SCRM for cloud vendors, and thresholds change requests through DevOps pipelines. Data-residency rules (GDPR) and PCI-DSS compliance are codified in IT-policy artefacts.

Hospitality's IT governance pivots on PMS–OTA linkages: a digital-services board balances guest-privacy opt-in flows with POS-security, mandating quarterly penetration tests and “consent-by-design” workflows in booking engines. IT-management cycles sync with peak travel seasons to ensure system uptime.

Retail & Digital Commerce vs Healthcare

Retail IT teams manage CI/CD release trains for mobile apps, blending real-time analytics with ePOS stability; risk reviews focus on third party-API SLAs. Governance docs include change-enablement playbooks and incident-response runbooks.

Healthcare IT governance demands EHR and medical-device interoperability under HL7/FHIR standards; a clinical-IT board (CMIO, CIO, CISO) oversees vendor-certification, AI-algorithm explainability, and GDPR-aligned patient-consent management. Business-continuity drills simulate ransomware scenarios in hybrid-cloud setups.

Hospitality & Leisure vs Healthcare

Hospitality IT management deploys CloudOps for seasonal scaling, guided by FinOps policies to control OTA-driven cost volatility. Governance rituals include monthly “resilience sprints” between IT, operations, and marketing.

Healthcare's IT governance is more formal: an ITGRC council enforces ISO 27017/27018 in multi-tenant clouds, governs telehealth platforms, and integrates incident-reporting with clinical-risk committees. IT roadmaps tie directly to patient-safety and regulatory-audit milestones.

Retail & Digital Commerce vs Healthcare

Looking at agile maturity, Retail IT has decentralized “product-tech squads” with embedded governance via guardrails (e.g., security champions), while Healthcare IT retains centralized change advisory boards to vet every EHR update. Both share a need for rapid change but differ in risk appetite: Retail tolerates nightly deployments, Healthcare restricts to “maintenance windows” post-clinical approval.

Industry: Retail and Digital Commerce | Niche: D2C food brands

Theme: Organizations, Governance, and Management

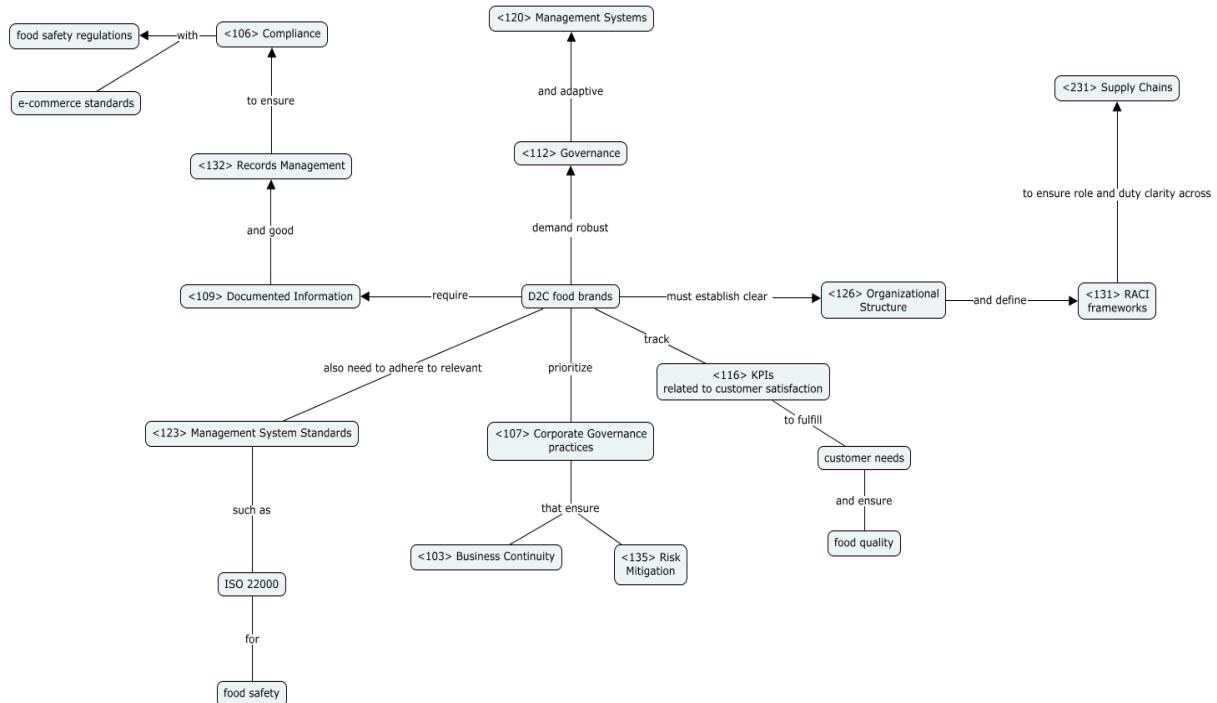
The Direct-to-Consumer food brand sector of Retail and Digital Commerce has rapidly evolved in the past few years, which demands robust **<112> governance** and adaptive **<120> management systems**. As these brands bypass traditional intermediaries, they must establish clear **<126> organizational structures** and define **<131> RACI (Responsible, Accountable, Consulted, Informed)** frameworks to ensure role and duty clarity across employees and digital **<231> supply chains**.

In this sector, **<112> governance** is driven by the need for **<106> compliance** with food safety regulations and e-commerce standards, which require **<109> documented information** and good **<132> records management**. They also need to adhere to relevant **<123> Management System Standards (MSS)**, such as ISO 22000 to control food safety.

<136> Top management in this niche prioritize **<107> corporate governance** practices that ensure **<103> business continuity** and **<135> risk mitigation**, especially in a business field so vulnerable to **<231> supply chain** disruptions and **<206> cybersecurity** threats.

Effective **<113> governance, risk, and compliance (GRC)** frameworks support **<110> due diligence** processes when integrating new technologies or suppliers. **<101> Audit** mechanisms and **<115> internal controls** are essential to validate **<106> compliance**, and tracking **<116> Key Performance Indicators (KPIs)** related to customer satisfaction are key to fulfilling customer needs and ensuring food quality.

The following concept map reinforces the description given about the Direct-to-Consumer food brands niche of the Retail and Digital Commerce industry.



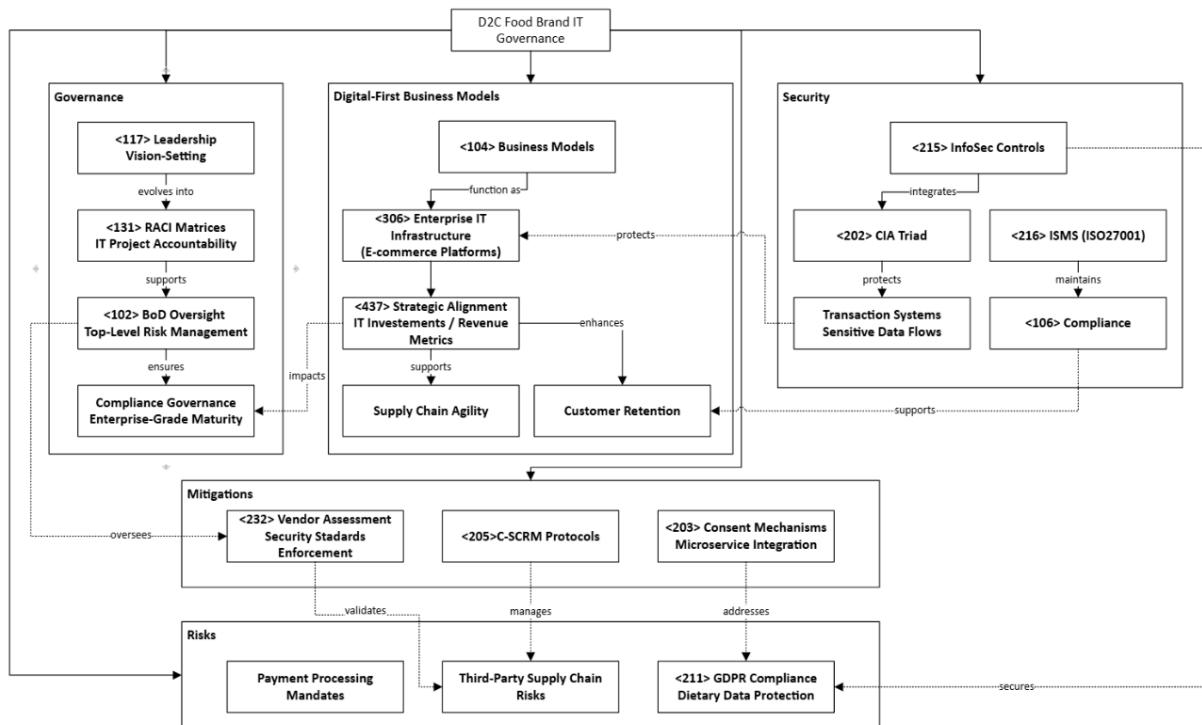
Theme: IT Governance and Management

D2C food brands operate on digital-first **<104> Business Models**, where e-commerce platforms function as **<306> Enterprise IT Infrastructure**, requiring **<437> Strategic Alignment** between IT investments and revenue metrics. This alignment ensures that technical decisions, such as adopting cloud-native inventory systems, directly support business objectives like supply chain agility and customer retention.

Governance in these organizations evolved through structured frameworks, transitioning from **<117> Leadership** (executive vision-setting and stakeholder coordination) to formalized **<131> RACI** matrices for clarifying accountability in IT projects and **<102> BoD** oversight to deal with top-level risks and ensure compliance governance, reflecting enterprise-grade maturity, as companies begin to steer away from outdated ad hoc or founder-centric approaches.

Operational risks include **<211> GDPR** compliance for sensitive customer dietary data, payment processing mandates, and third-party dependencies. These are generally addressed by enterprises through **<216> ISMS** controls aligned with ISO 27001, **<203> Consent Mechanisms** embedded in microservice architectures, and **<205> C-SCRM** protocols alongside with **<232> Vendor Assessment** processes that allow enterprises to properly manage multi-tier supply chain risks and ensure that third-party partners meet the industry security standards.

Security architecture integrates **<215> InfoSec** controls with **<202> CIA** triad prioritization to protect transaction systems handling sensitive customer/enterprise data. Through these measures, enterprises maintain **<106> Compliance** with the necessary requirements in an environment where technical decisions increasingly have a direct impact in inventory reliability and revenue streams.



Industry: Banking and Financial Services | Niche: Fintech for Small Businesses

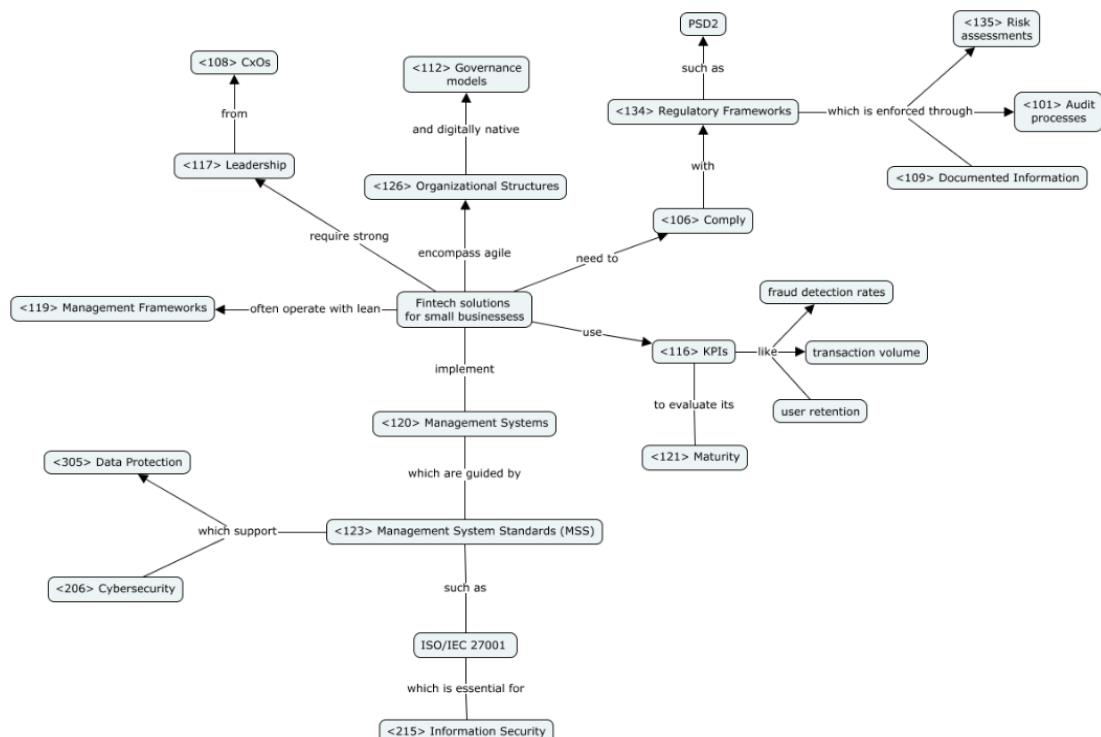
Theme: Organizations, Governance, and Management

In recent years, there has been a rise of Fintech solutions for Small Businesses in the Banking and Financial services industry, which calls for agile **<126> organizational structures** and digitally native **<112> governance** models. These organizations often operate with lean **<119> management frameworks**, requiring strong **<117> leadership** from **<108> CxOs** to maintain alignment with customer-centric service models. Given the sensitivity of financial data, **<106> compliance** with **<134> regulatory frameworks**, such as PSD2 in the EU, is non-negotiable, and enforced through rigorous **<101> audit processes**, **<135> risk assessments**, and **<109> documented information**.

In these firms, **<120> management systems** are guided by **<123> management system standards (MSS)**, such as ISO/IEC 27001 for example, which specifies the requirements for an **<216> Information Security Management System (ISMS)**, which is essential for **<215> information security**. These standards support **<305> data protection** and **<206> cybersecurity**, which are critical quality benchmarks in this niche.

<113> Governance, risk, and compliance (GRC) programs are integral to the operational backbone, enabling **<110> due diligence** during technology integration and service expansion. **<116> Key Performance Indicators (KPIs)**, such as transaction volume, fraud detection rates, and user retention, are tracked to evaluate the **<121> maturity** and effectiveness of processes. **<131> Responsible, accountable, consulted, informed (RACI)** models are key to ensuring that roles and responsibilities are clear among teams where decision-making must be quick and accountable.

In these organizations, it is essential to maintain an ethical and transparent **<125> organizational culture** supported by comprehensive **<127> policies** and robust **<132> records management**. This allows to satisfy not only **<133> regulatory bodies** but also build trust with small businesses.



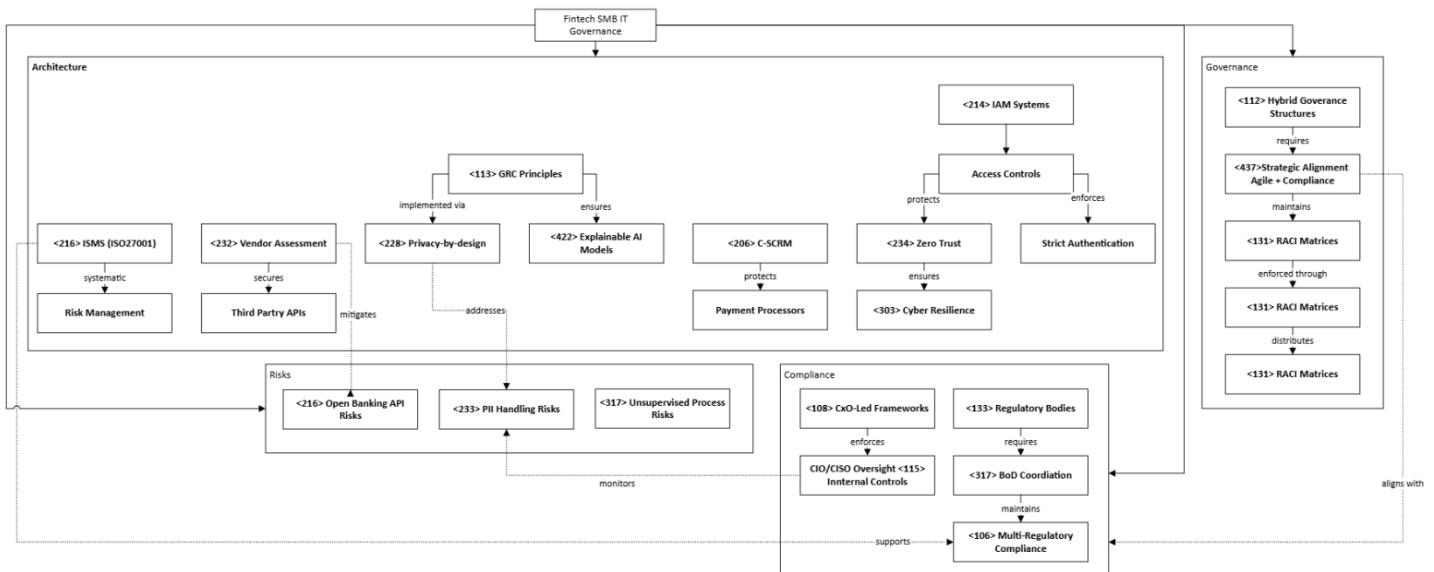
Theme: IT Governance and Management

Fintech solutions for SMBs mostly rely on hybrid **<112> Governance** structures, where **<437> Strategic Alignment** integrates agile development methodologies with compliance requirements to ensure that IT initiatives are aligned with the organizational objectives. In turn, this alignment is enforced through the use of **<131> RACI** matrices, which clarify accountability by distributing **<117> Leadership** responsibilities across technical, risk, and compliance teams.

Investor priorities and different **<133> Regulatory** bodies require the **<102> BoD** to be involved in the coordination of different departments, to allow proper business innovation while maintaining **<106> Compliance** with the many requirements. This is particularly important in **<108> CxO-led** frameworks that enforce CIO or CISO oversight over **<115> Internal Control** systems for financial monitoring and fraud detection.

Operational risks in Fintech for SMBs mostly come from **<223> PII** handling vulnerabilities, **<231> Supply Chain** weaknesses in open banking APIs, and **<317> Operational Risk** that originates from unsupervised tools or processes. These risks can be mitigated through the implementation and further use of **<216> ISMS** frameworks aligned with ISO 27001 for systematic risk management, **<232> Vendor Assessment** protocols to evaluate third-party API providers, and **<205> C-SCRM** practices to secure dependencies on payment processors.

Technical architectures reflect **<113> GRC** principles through the **<228> Privacy-by-design** approach in customer-facing applications to meet GDPR requirements and **<422> Explainability** in lending models to ensure auditability and stakeholder trust. **<214> IAM** systems accommodate SMB client hierarchies with multi-tier access controls, while **<234> Zero Trust** principles enforce strict authentication for distributed access to financial data ensuring the necessary **<303> Cyber Resilience** for the continuity of core financial operations (e.g., payment processing) during disruptions.



Industry: Agriculture and Farming | Niche: Smart Farming (AgTech)

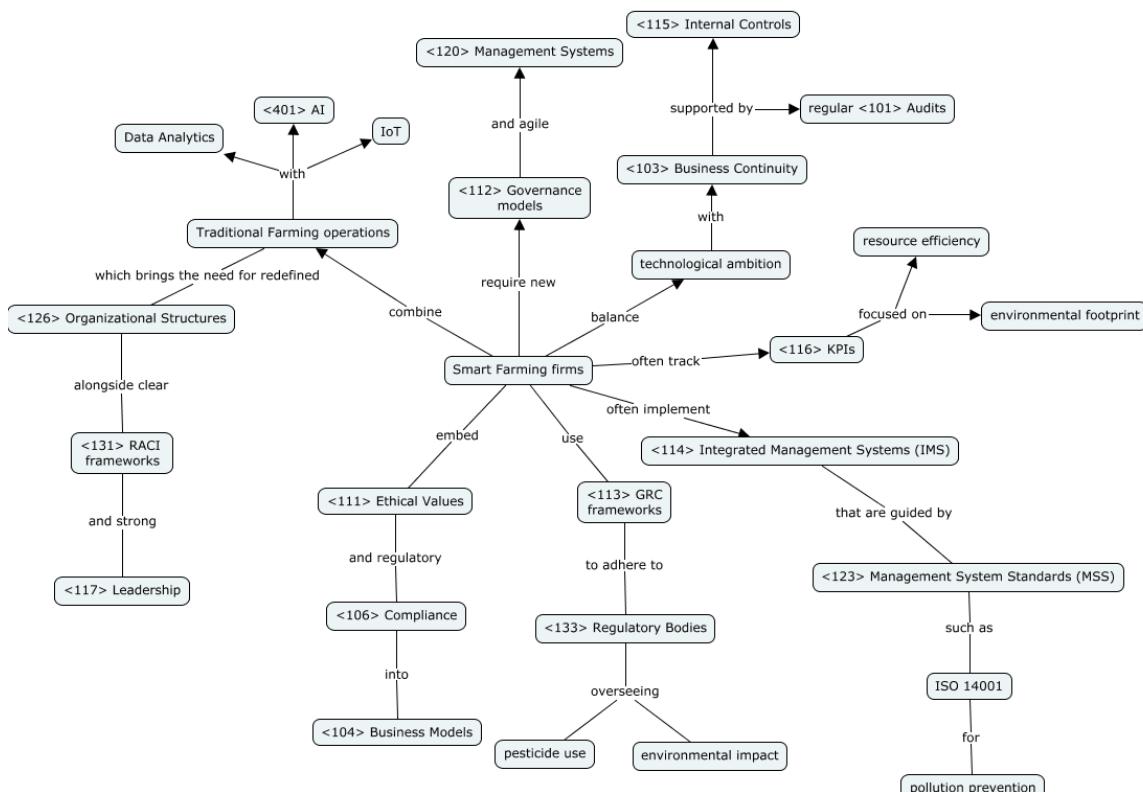
Theme: Organizations, Governance, and Management

Smart farming, or AgTech, has revolutionized the industry of Agriculture and Farming in recent years, through the integration of digital technologies in its operations, which demands new **<112> governance** models and agile **<120> management systems**. Organizations in this niche combine traditional farming operations with sophisticated technologies like IoT (Internet of Things), **<401> AI (Artificial Intelligence)**, and data analytics. This brings the need for redefined **<126> organizational structures** among these organizations, alongside clear **<131> RACI** frameworks for a good role and responsibility understanding across employees, and strong cross-functional **<117> leadership** to align innovation with sustainability and productivity.

<136> Top management in AgTech firms are tasked with embedding **<111> ethical values** and regulatory **<106> compliance** into **<104> business models** that often involve sensitive environmental and land-use data. **<113> Governance, risk, and compliance (GRC)** frameworks are critical to ensure these organizations adhere to **<133> regulatory bodies** overseeing pesticide use and environmental impact, for example. These organizations must balance technological ambition with **<103> business continuity**, supported by **<115> internal controls** and regular **<101> audits**.

AgTech firms often track **<116> Key Performance Indicators (KPIs)** focused on resource efficiency and environmental footprint. These organizations regularly implement **<114> integrated management systems (IMS)** that need to follow **<123> management system standards (MSS)**, such as ISO 14001, for example, which focuses on pollution prevention.

Ultimately, all of these measures, alongside others not referenced above, are essential for a sustainable transformation in modern agriculture.



Theme: IT Governance and Management

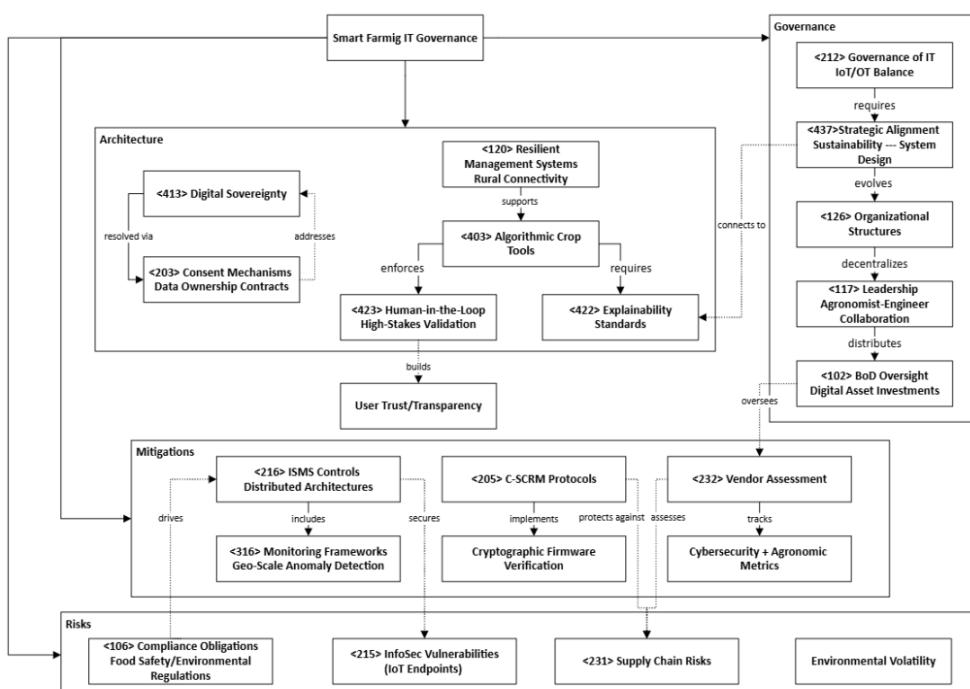
Smart farming relies on **<212> Governance of IT** to balance IoT networks with **<318> Operational Technology**, which requires **<437> Strategic Alignment** that connects agronomic objectives such as sustainability targets to IT system design priorities. Foundational **<126> Organizational Structures** evolve as **<117> Leadership** responsibilities decentralize between agronomists and engineers, with **<102> BoD** oversight escalating proportionally to capital investments in digital assets like autonomous harvesting systems.

The risk profile mainly consists in environmental volatility, **<215> InfoSec vulnerabilities** in endpoint IoT devices, and **<106> Compliance** obligations related to food safety audits and environmental regulations like pesticide application limits. Mitigation strategies generally involve the deployment of **<216> ISMS** controls adapted for distributed architectures, that include **<316> Monitoring** frameworks capable of detecting anomalies in real-time across vast geographies.

Technical architecture prioritizes **<120> Management Systems** engineered for resilience against rural connectivity constraints. Because these systems operate in challenging environments, **<403> Algorithmic** crop management tools demand robust **<422> Explainability** standards and **<423> Human-in-the-loop** safeguards that require manual validation for high-stakes decisions which in turn, builds trust and transparency with users while supporting operational decision making.

<231> Supply Chain risks are particularly relevant for this industry, which drives the adoption of **<205> C-SCRM** protocols like cryptographic verification of firmware updates and **<232> Vendor Assessment** processes that track agricultural performance metrics and cybersecurity criteria such as vulnerability disclosure policies for IoT component suppliers.

<413> Digital Sovereignty tensions arise over farm data ownership between agricultural cooperatives and equipment manufacturers, requiring contractual **<203> Consent Mechanisms** with data usage permissions.



Theme: Organizations, Governance, and Management

D2C Food Brands vs Fintech for Small Businesses

Both D2C food brands and Fintech startups reflect new organizational models within traditionally structured industries. <112> **Governance** in both niches has evolved, but for different reasons: D2C food brands require governance aligned with <106> **compliance** for food safety and digital <231> **supply chains**, while Fintechs must comply with financial regulations and <305> **data protection** rules. The <120> **management systems** also diverge: D2C brands lean on ISO 22000 to ensure product safety and supplier reliability, while Fintechs implement ISO/IEC 27001 to ensure <206> **cybersecurity** and <215> **information security**.

<126> **Organizational structure** in both sectors incorporate <131> **RACI** frameworks, but Fintech firms favor lean, agile structures with high decision velocity, supported by <117> **leadership** from <108> **CxOs**. In contrast, D2C companies often scale fast but must formalize roles as operations expand. Both use <113> **GRC** frameworks for <110> **due diligence** and track <116> **KPIs**, but Fintechs emphasize fraud prevention and transaction performance, whereas D2C brands focus on food quality and customer satisfaction. The core contrast lies in the <121> **maturity** of digital governance: Fintechs are born digital, while D2C firms must retroactively layer governance onto fast-growing commercial ecosystems.

D2C Food Brands vs Smart Farming (AgTech)

Though operating in different domains, D2C food brands and AgTech firms share the challenge of integrating digital infrastructure with physical product and operational processes. Both rely on adaptive <120> **management systems** to coordinate <231> **supply chains** and integrate emerging technologies, but while D2C brands focus on logistics and vendor control, AgTech's systems often link <401> AI, IoT, and environmental <316> **monitoring** with ISO 14001-compliant <114> **integrated management systems**.

Their <112> **governance** structures reflect this distinction: D2C food brands center <106> **compliance** around consumer protection and food regulation, while AgTech governance must address broader <111> **ethical values** and environmental compliance. AgTech organization faces more complex coordination challenges, requiring cross-functional <117> **leadership** to align innovation with sustainability, whereas D2C firms manage internal growth dynamics through tighter <131> **RACI** alignment and <132> **records management**.

While both use <113> **GRC** frameworks and track <116> **KPIs**, the content differs: D2C KPIs often relate to satisfaction and delivery, AgTech KPIs emphasize resource efficiency and environmental footprint. Ultimately, D2C food brands are optimizing commercial delivery and operational compliance, while AgTech firms are navigating a deeper transformation of agricultural governance toward sustainable innovation.

Theme: IT Governance and Management

D2C Food Brands vs. Fintech for Small Businesses

D2C Food Brands have evolved from founder-centric IT **<118> Management** to formalized **<131> RACI** matrices, which distribute technology accountability across teams. Their IT management prioritizes **<437> Strategic Alignment** between technology investments and revenue metrics, with **<102> BoD** oversight ensuring that IT supports their digital-first **<104> Business Models**. This structure grants IT management some autonomy when customer-facing systems perform well.

Fintech for SMBs operates under a more constrained IT **<118> Management** model where the compliance requirements heavily influence decision-making. Their **<131> RACI** matrices must include external stakeholders in accountability frameworks. IT managers must also implement **<115> Internal Control** systems satisfying both the innovation needs and the regulatory requirements, with **<108> CxO-led** frameworks that create a formal separation between initiative approval and risk assessment.

The key differences are that D2C brands can optimize primarily for customer experience and efficiency, while Fintech IT managers must balance innovation with regulatory constraints, requiring more extensive documentation and approval processes for new technologies to be developed.

Smart Farming (AgTech) vs. D2C Food Brands

Smart Farming IT **<118> Management** allocates resources across distributed physical environments, balancing investments between **<318> Operational Technology** and modern analytics. Their practices require expertise in maintaining availability despite rural connectivity limitations. Resource decisions must account for seasonal and environmental factors, with **<316> Monitoring** frameworks detecting anomalies across vast areas, which leads to more complex systems. IT managers maintain **<120> Management Systems** engineered for physical resilience while implementing **<423> Human-in-the-loop** safeguards for manual overrides.

D2C Food Brands focuses IT **<118> Management** resources on scalable **<306> Enterprise IT Infrastructure** supporting e-commerce. Prioritizing customer-facing systems and inventory management, with resilience efforts protecting transactions and **<215> InfoSec** controls. IT management also leverages standardized cloud services by directing resources toward business differentiation rather than infrastructure maintenance. System resilience is measured through digital metrics rather than adaptation to physical-world variability.

The key differences are that Smart Farming IT managers maintain complex hybrid physical-digital systems in challenging environments, while D2C brand IT managers optimize standardized digital platforms by shaping resource strategies, skills, and performance metrics.

Healthcare - Organisations, Governance, and Management

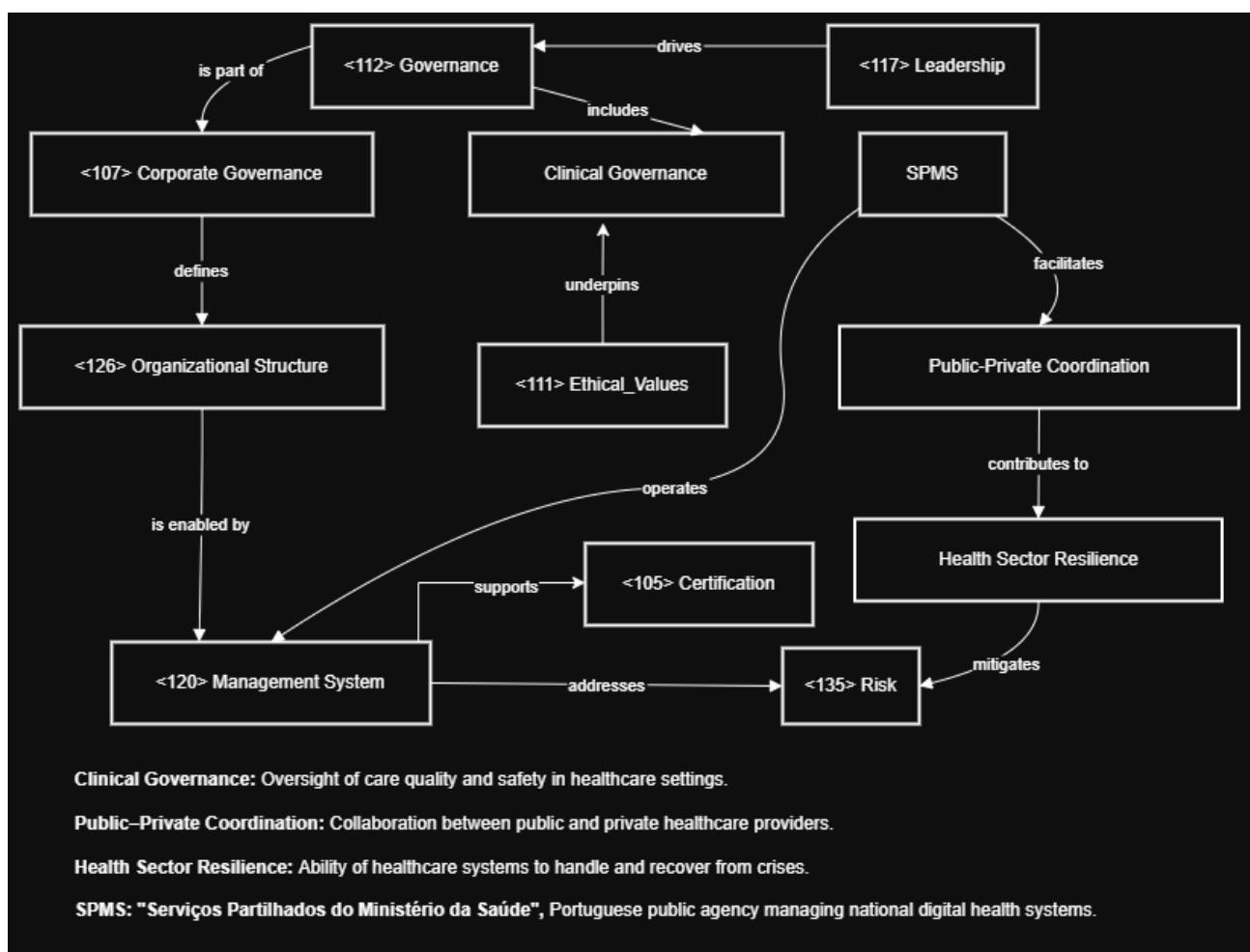
The healthcare sector operates at the intersection of public interest, professional ethics, and systemic complexity. In Portugal, <112> Governance is centred around the **Serviço Nacional de Saúde (SNS)** — a Beveridge-style system funded through taxation and providing universal coverage. This is complemented by a growing private sector that delivers elective and diagnostic services, forming a hybrid model that demands effective <126> Organizational Structure and strategic coordination across entities.

Organisational governance in this context is multidimensional. It involves both <107> Corporate Governance — such as oversight by the Ministry of Health and coordination by **SPMS** — and **Clinical Governance**, which ensures care quality and safety. This dual structure requires a mature <120> Management System to integrate operations, alongside clearly defined leadership responsibilities and alignment with <111> Ethical Values.

At a regulatory level, both national and European <134> Regulatory Frameworks shape expectations concerning equity, access, and quality. Within this environment, <117> Leadership must align policy with system-wide priorities, public trust, and digital innovation goals. In practice, this means not only coordinating across fragmented care providers, but also stewarding system-wide digital transformation via SPMS and similar agencies.

Indicators of governance maturity include sector-specific <105> Certification, mechanisms for <115> Internal Control, and consistent engagement in <135> Risk management, especially in areas tied to patient safety, data privacy, and service continuity. Public–Private Coordination is a critical governance capability that supports sustainability and strengthens **Health Sector Resilience** against future shocks, such as pandemics or cyberattacks.

Ultimately, <112> Governance in healthcare is not merely a matter of <106> Compliance, but one of stewardship — ensuring that public resources are managed ethically, transparently, and in service of collective wellbeing.



Healthcare - Governance of IT and IT Management

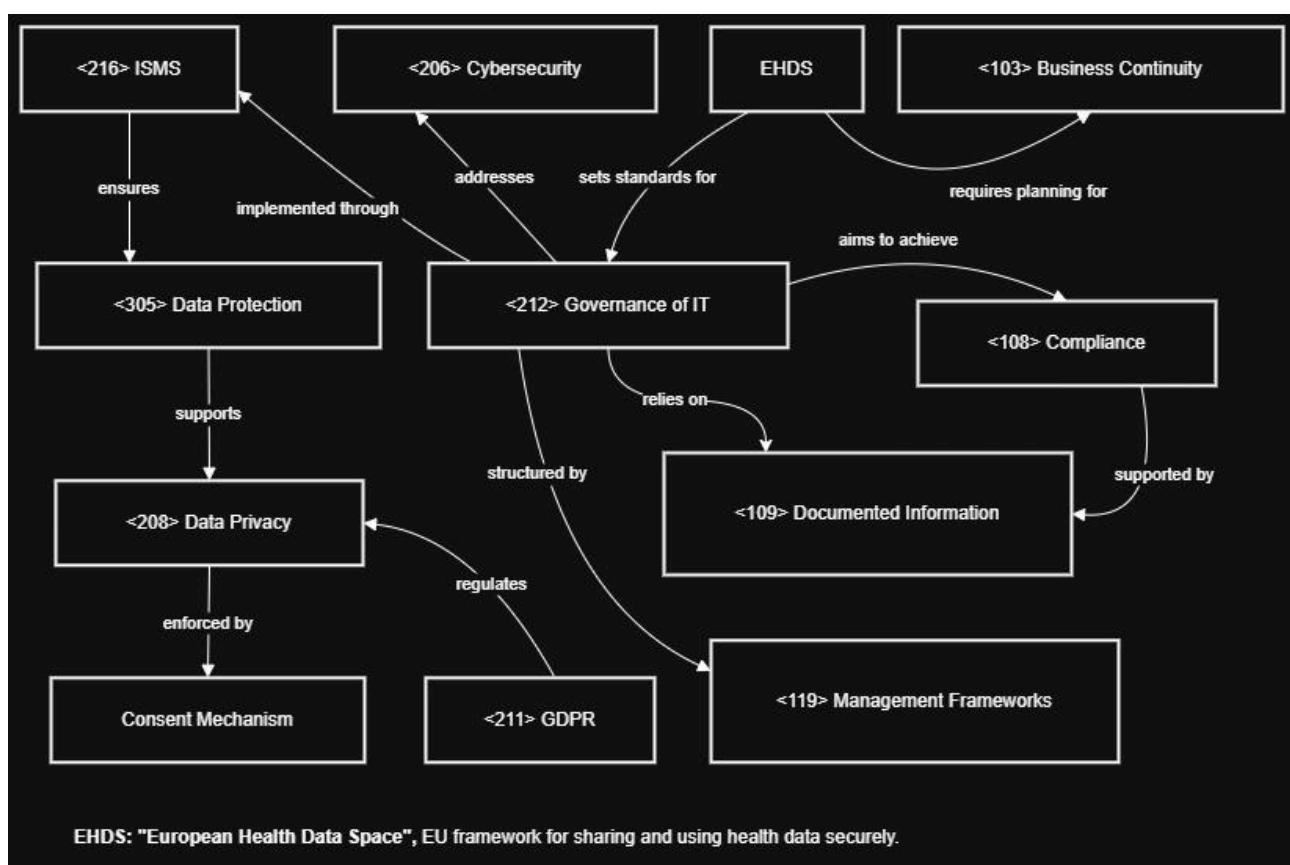
The governance of IT in the healthcare sector demands precision, resilience, and accountability due to the sensitivity of data, the criticality of systems, and the heterogeneity of actors involved. Central to this is the <212> Governance of IT, which must integrate clinical, operational, and digital priorities into a unified strategic direction.

Portugal's national agency, SPMS, exemplifies sector-wide <118> Management of digital infrastructures — such as Electronic Health Records (EHR), e-prescriptions, and citizen health portals — within a coordinated framework aligned with European initiatives. This calls for a robust <216> ISMS (Information Security Management System) to safeguard patient data, ensure service availability, and meet evolving compliance requirements under the <211> GDPR.

The upcoming **European Health Data Space (EHDS)** reinforces the need for <305> Data Protection and interoperability across systems and borders. These imperatives highlight the role of <208> Data Privacy and technical <203> Consent Mechanisms in shaping responsible data access and secondary usage. SPMS and hospital IT teams must therefore balance innovation with rigorous <106> Compliance and <206> Cybersecurity standards.

<136> Top Management in healthcare organisations must engage actively with IT governance — not only through budgetary oversight or risk tolerance, but by embedding <437> Strategic Alignment between clinical priorities and digital transformation efforts. This includes anticipating infrastructure needs, defining policies for access and retention, and enabling continuity strategies through <103> Business Continuity planning and IT incident response.

As the healthcare sector increasingly adopts cloud services, AI diagnostics, and cross-border data exchanges, its digital maturity hinges on continuous investment in IT capabilities, formalised governance structures, and accountability mechanisms. Without clear ownership, <109> Documented Information, and sector-adapted <119> Management Frameworks, healthcare systems risk fragmentation, inefficiency, and cyber vulnerabilities.



Retail and Digital Commerce – Organisations, Governance, and Management

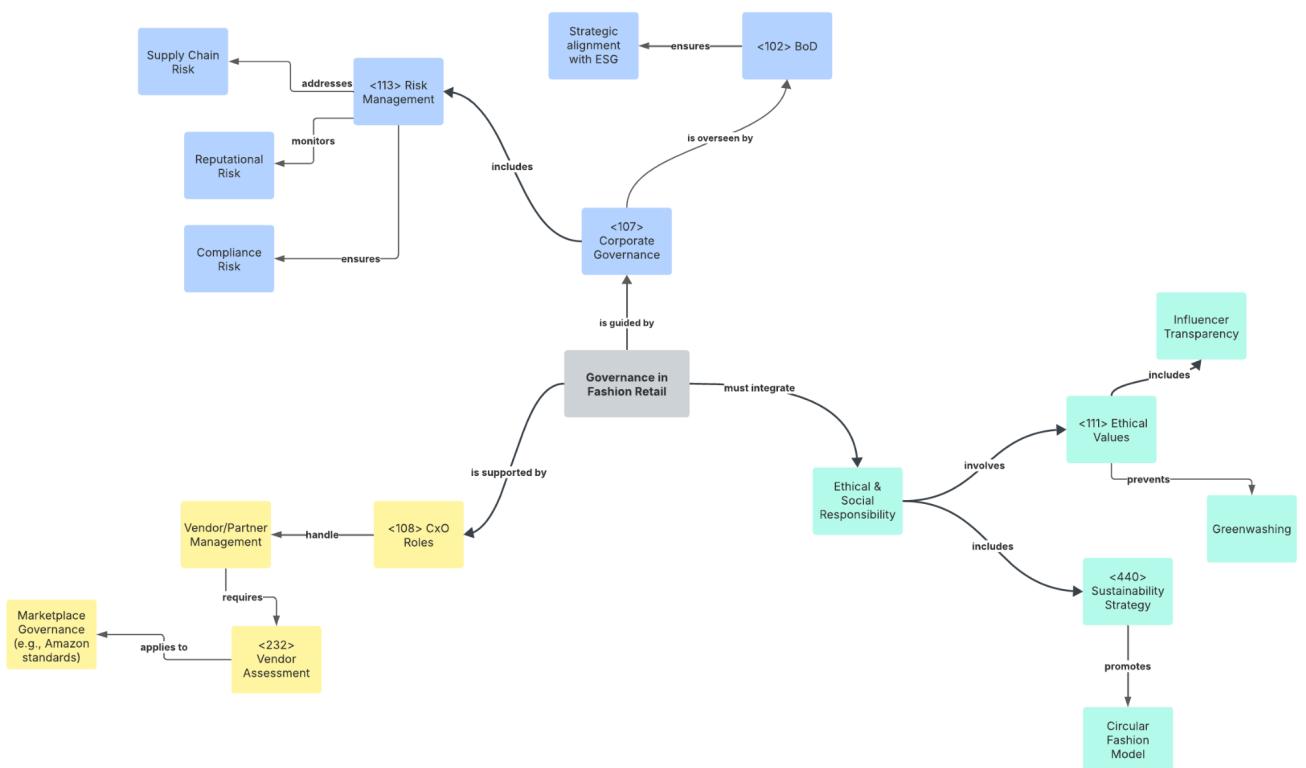
The retail and digital commerce sector combines high operational dynamism with complex governance needs. It spans multichannel operations, intense competition, and rapidly evolving consumer expectations. In omnichannel fashion retail, **<112> Governance** is exercised through hybrid corporate structures, integrating both digital-native and traditional brick-and-mortar entities.

Core to this governance is **<107> Corporate Governance**, which sets strategic direction across sales channels, supplier networks, and platform partnerships. **<102> Boards of Directors** oversee compliance with **<134> Regulatory Frameworks**, such as the EU's Digital Services Act (DSA) and the Consumer Rights Directive, especially relevant when interacting with large marketplaces (e.g., Zalando, Amazon).

Operational **<135> Risk** is managed through robust supply chain planning, returns processing, and fraud detection. However, reputational risks, especially linked to **<111> Ethical Values** like inclusivity or environmental claims are increasing. This is particularly true in influencer marketing or sustainability positioning, where missteps can rapidly go viral and damage consumer trust.

The integration of **<113> GRC** capabilities allows firms to maintain agility while ensuring **<106> Compliance**. Fashion retailers often face audit and regulatory checks across marketing, logistics, and data handling. Franchises and platform sellers must also manage **<232> Vendor Assessment** processes to ensure alignment with ethical sourcing and labor standards.

Executive roles such as CIOs and CISOs are becoming increasingly central to governance, reflecting the strategic importance of digital transformation. These **<108> CxO** actors also lead **<110> Due Diligence** efforts in new technology adoption, helping to align innovation with legal and reputational safeguards. Ultimately, retail governance requires alignment between speed and stewardship, combining rapid response to trends with long-term brand integrity.



Retail and Digital Commerce – Governance of IT and IT Management

Omnichannel fashion retailers operate on top of sophisticated digital infrastructures that power their ERP, CRM, ePOS, and recommendation engines. Effective **<212> Governance of IT** in this sector requires integrating these systems to deliver seamless customer experiences while safeguarding data integrity and system resilience.

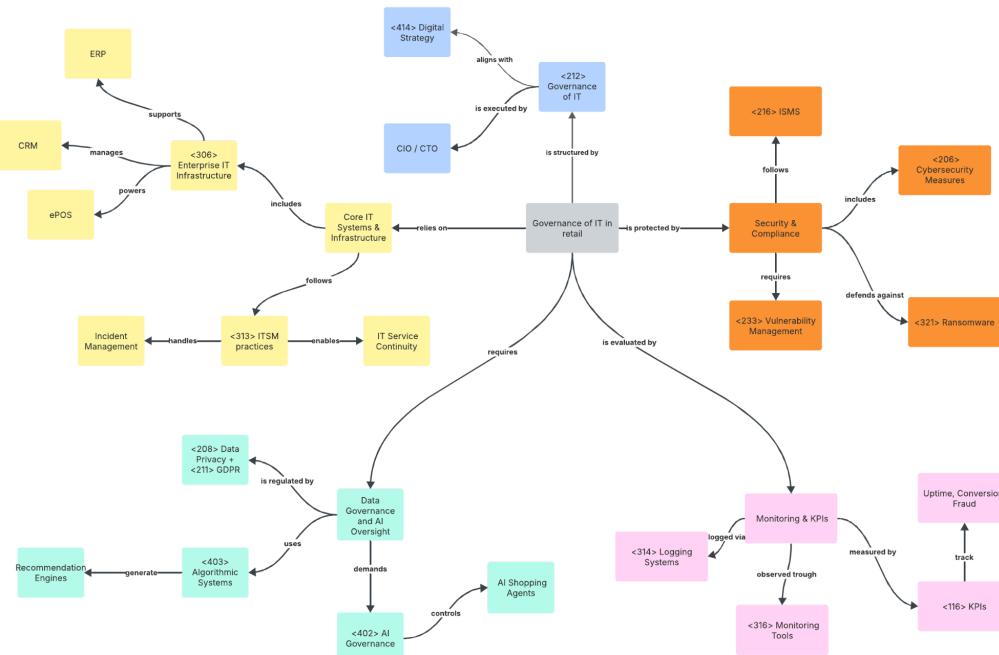
<118> Management of IT assets includes omnichannel systems for real-time inventory visibility, loyalty programs, and cross-border logistics coordination. As platforms like Shopify and Meta increasingly act as intermediaries, digital retailers must navigate data-sharing complexities and maintain control over their infrastructure. The emergence of AI shopping agents, as discussed in The Wall Street Journal, highlights how **<403> algorithmic systems** are shifting decision-making and necessitating clear **<402> AI governance** protocols.

Security remains a dominant concern. The integration of **<216> ISMS** and **<206> Cybersecurity** policies ensures resilience against fraud, credential theft, or **<321> ransomware**. IT teams must also manage **<315> Maintenance Windows** and incident response to guarantee continuity during flash sales, peak seasons, or influencer campaigns.

Compliance with **<211> GDPR** and the DSA introduces constraints around **<208> Data Privacy** and profiling practices. Retailers must implement strong **<203> Consent Mechanisms** to ensure transparency in tracking and personalization. The handling of **<223> PII** across analytics engines and recommendation systems introduces additional regulatory scrutiny, especially with cross-border data flows.

<136> Top Management plays a central role in aligning **<414> Digital Strategy** with business priorities. CIOs and CTOs lead platform selection, while CISOs oversee **<233> Vulnerability Management** and resilience audits. **<116> KPIs** such as uptime, basket conversion rate, and fraud incidence are actively monitored, often automated through **<316> Monitoring** dashboards and system **<314> Logging**.

As digital maturity increases, governance frameworks like COBIT and ITIL help standardize IT decision-making. With new technologies such as headless commerce and AI agents, retailers must evolve their IT governance to remain compliant, ethical, and competitive.



Farming and Agriculture - Organisations, Governance, and Management

Agricultural governance represents a complex landscape where **<112> Governance** interfaces with multifaceted organizational structures ranging from family-owned farms to large agribusiness conglomerates. **<107> Corporate Governance** in this sector must navigate intricate challenges including environmental regulations, market volatility, and technological transformation.

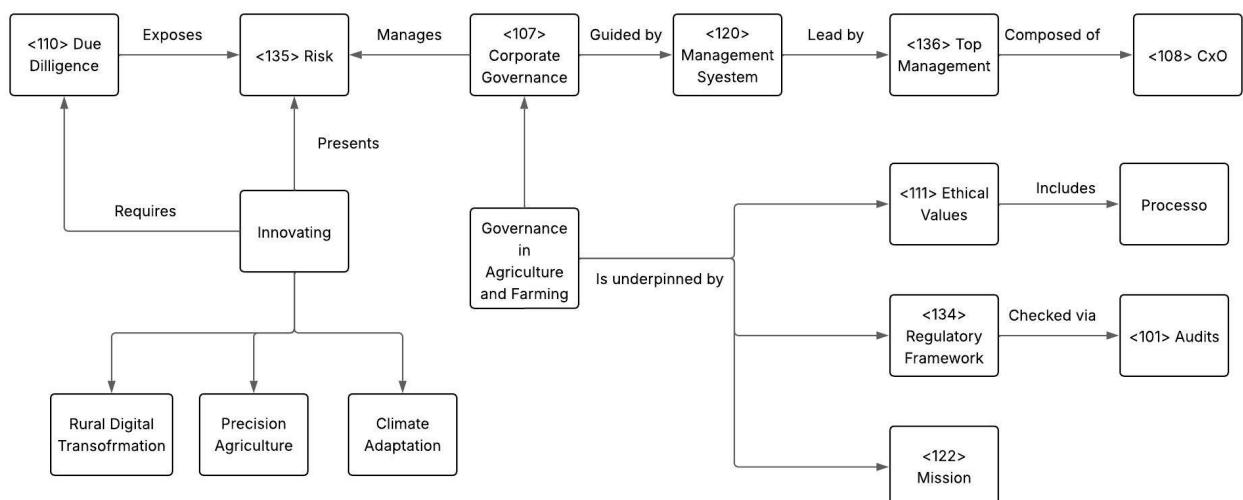
<135> Risk management emerges as a critical governance dimension, encompassing diverse challenges like weather unpredictability, disease outbreaks, commodity price fluctuations, and regulatory shifts. These risks demand sophisticated **<120> Management Systems** that can adapt to rapidly changing conditions while maintaining operational stability.

<111> Ethical Values play a fundamental role, particularly in addressing sustainability, land stewardship, and food safety standards. Agricultural governance increasingly emphasizes transparency in land use, environmental impact, and supply chain practices. **<117> Leadership** must demonstrate agility in balancing technological innovation with traditional farming practices.

Regulatory frameworks significantly shape governance, with **<134> Regulatory Frameworks** influencing everything from pesticide usage to land rights and environmental conservation. Public policy mechanisms, such as the EU's Common Agricultural Policy, create additional layers of compliance and strategic planning.

The sector's governance is further complicated by its diverse subdomains – crop farming, animal husbandry, agroforestry, and agri-food processing – each requiring nuanced governance approaches. **<126> Organizational Structures** must be flexible enough to accommodate these varied operational models while maintaining coherent strategic direction.

Emerging trends like precision agriculture, climate adaptation, and digital transformation are pushing governance models to become more integrated, data-driven, and responsive to global challenges.



Farming and Agriculture - Governance of IT and IT Management

<212> Governance of IT in agriculture represents a dynamic and evolving landscape characterized by significant technological diversity and infrastructural challenges. The sector's digital ecosystem spans sophisticated technologies like satellite monitoring, IoT sensors, precision agriculture tools, and complex <231> supply chain management systems.

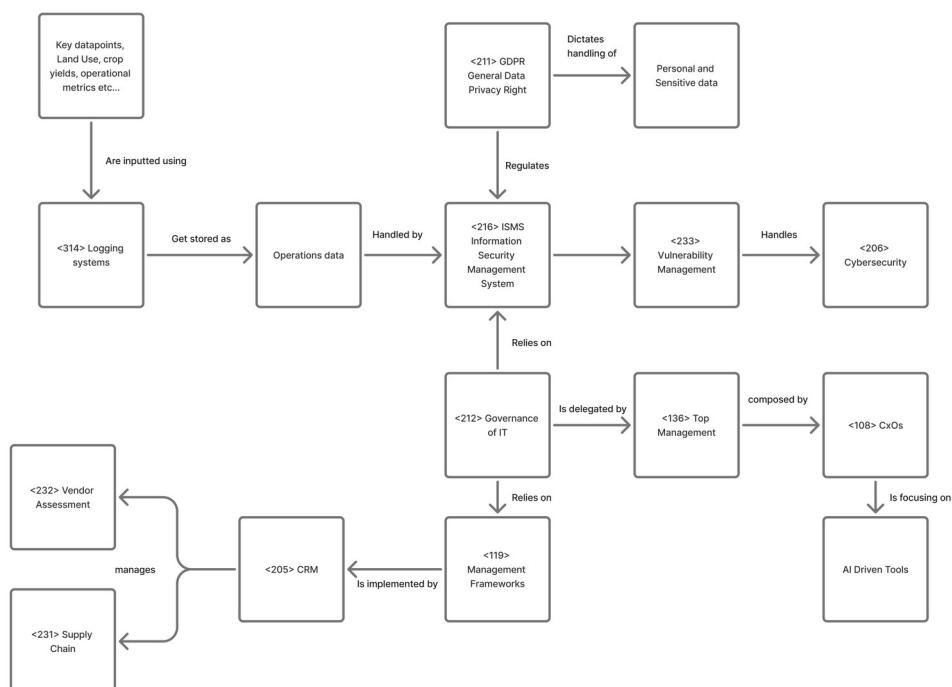
<118> Management of digital infrastructures must address substantial technological asymmetries. While large agribusinesses deploy advanced <205> CRM and yield forecasting and logistics optimization systems, many smaller producers still rely on legacy or informal tools. <232> Vendor assessment becomes crucial in selecting appropriate technological solutions. This digital divide necessitates adaptive IT governance strategies.

<216> Information Security Management Systems (ISMS) are crucial, protecting sensitive data about land use, crop yields, financial information, and operational metrics that are gathered and inputted into <314> Logging Systems. <206> Cybersecurity becomes particularly important in distributed, often low-infrastructure agricultural environments where digital vulnerabilities can have significant economic consequences.

Data governance in agriculture presents unique challenges at the intersection of technological innovation and regulatory compliance. The <211> GDPR provides a comprehensive framework for managing personal and sensitive data, such as client data. It is also a challenge to store securely proprietary data, regarding financial and operations data.

Technological subdomains like crop farming, animal husbandry, and agri-food processing each require specialized IT management approaches. Systems must support diverse functions including soil monitoring, animal health tracking, traceability, and regulatory compliance.

The role of <136> Top Management in driving IT strategy is evolving, with <108> CxOs (CIOs and CTOs) increasingly needed to integrate advanced technologies like AI-driven advisory tools, drone monitoring, and predictive analytics into agricultural operations.



Governance in Healthcare vs. Retail and Digital Commerce

In Healthcare, governance frameworks are built on a foundation of **<106> Compliance** and **<111> Ethical Values**, with a strong emphasis on **<115> Internal Control** and rigorous oversight from **<133> Regulatory Bodies**. The sector operates within tightly defined **<134> Regulatory Frameworks**, such as HIPAA or regional equivalents, and is driven by principles such as patient autonomy, privacy, and clinical accountability. Governance here is not just about formal structures, but also about reinforcing **<124> Organisational Culture** through **<109> Documented Information**, standard **<128> Procedures**, and **<127> Policies** that align with legal and moral obligations. **<136> Top Management** and **<108> CxOs** are directly accountable for governance failures, making **<110> Due Diligence** a key ongoing activity, particularly in digital health transformation initiatives.

In contrast, Retail and Digital Commerce governance tends to be more agile and market-driven. While **<107> Corporate Governance** exists to ensure investor and board alignment, much of the governance activity is shaped by **<208> Data Privacy**, consumer trust, and responsiveness to digital risks. Governance practices often incorporate **<113> GRC (Governance, Risk and Compliance)** frameworks to maintain control over decentralized digital environments, third-party logistics, and e-commerce platforms. The rapid innovation cycle in this industry demands a flexible yet robust governance model, particularly as **<206> Cybersecurity threats**, **<223> PII protection**, and global **<209> Data Residency laws** continue to evolve. Governance here enables strategic scaling while protecting the **<445> Value Proposition** that defines consumer loyalty and brand reputation.

Governance in Agriculture and Farming vs. Healthcare

While healthcare governance is defined by strong vertical structures, Agriculture and Farming presents a more decentralized, often under-governed picture, especially in traditional or smallholder-dominated regions. Governance in agriculture primarily focuses on compliance with environmental policies, land use laws, and **<440> Sustainability Strategy**. Formal **<120> Management Systems** and **<121> Maturity levels** vary significantly across regions, and **<127> Policy adherence** is often enforced more through incentive (e.g., subsidies) than obligation. As agriculture integrates **<411> Digital Capabilities** such as IoT-based soil monitoring or AI-driven yield optimization, governance frameworks are struggling to catch up. There is growing demand for improved data governance, particularly around **<210> Data Retention** and proprietary farming techniques.

By comparison, healthcare operates under well-established **<105> Certification regimes** and **<123> MSS (Management System Standards)** that codify clinical processes. Where agriculture might see inconsistent **<132> Records Management**, healthcare treats it as foundational. However, both sectors face a shared challenge in governing the **<231> Supply Chain**, healthcare from a pharmaceutical and equipment angle, and agriculture from seed to shelf. For both, enhanced **<212> Governance of IT** and better **<437> Strategic Alignment** between policy and operations are critical for next-phase digital evolution.

IT Management in Retail and Digital Commerce vs. Agriculture and Farming

In Retail and Digital Commerce, IT Management is tightly woven into core operations, supporting <414> Digital Strategy, customer analytics, logistics, and omnichannel engagement. IT teams leverage <313> ITSM (IT Service Management) frameworks to ensure agility, resilience, and high service quality across fast-changing customer-facing systems. Technologies like <409> CIAM (Customer Identity and Access Management) and <326> XaaS (Everything as a Service) allow rapid scaling and personalization, all supported by real-time <316> Monitoring and <310> Incident Response. Retail IT leaders use metrics like <116> KPI (Key Performance Indicators) and maintain governance via <323> Service Level Agreements (SLAs) to manage third-party platforms.

In contrast, Agriculture and Farming often lack the <306> Enterprise IT Infrastructure needed for full-scale digital transformation. While innovations such as precision farming and sensor-based monitoring are on the rise, <311> IT Operations Management (ITOM) is often fragmented or underdeveloped. Many farms operate without a formal <426> IT Strategy, making long-term planning difficult. The emerging use of <405> Cloud Foundations and <406> Capability-Based Planning is promising, but significant barriers remain: digital literacy, infrastructure costs, and lack of <204> Consultants to guide strategic deployments. <325> Technical Debt accumulates quickly in this context, slowing modernization unless supported by government or co-op intervention.

IT Management in Healthcare vs. Retail and Digital Commerce

Both Healthcare and Retail and Digital Commerce heavily depend on IT, but their approaches to IT Management diverge sharply due to different priorities and constraints.

Healthcare IT Management is deeply intertwined with <216> ISMS (Information Security Management Systems) and risk protocols like <307> ERM (Enterprise Risk Management). Systems such as EHRs and PACS must operate securely under high availability, strict <305> Data Protection, and <223> PII compliance standards. Due to <115> Internal Control needs, even simple updates are subject to layered approvals. Innovations like <402> AI Governance and <423> Human-in-the-loop decision tools must pass through rigorous ethical review and <441> Technology Due Diligence, slowing deployment but ensuring safety.

Retail, however, emphasizes speed, customer experience, and modular scalability. IT departments focus on integrating multiple platforms and apps to support sales, marketing, and logistics. Here, IT management leans heavily on <424> Hyperautomation and <412> Digital Maturity to reduce manual tasks and respond to customer behavior in real time. Where healthcare emphasizes system stability, retail champions experimentation, often using pilot projects and <435> Roadmaps to guide IT innovation. Both sectors manage high data volumes, but the risk appetite and regulatory burdens diverge significantly.

Group 456 - 111187 and 110971

Transport and Logistics

The transport and logistics sector encompasses the systems, infrastructure, and services that facilitate the movement of goods and people across regional and international networks. Comprising public and private stakeholders involved in freight logistics, passenger mobility and intermodal coordination, it spans road, rail, maritime and air modes. For the purposes of this analysis, the sector is defined as a hybrid ecosystem that integrates physical assets, such as terminals and fleets, with digital systems, such as eFTI, SCADA and telematics. It operates under a complex regulatory framework that is shaped by safety standards, cross-border dependencies and digital transformation.

Organizational Structures and Governance

The governance structures of this sector are shaped by the coexistence of public and private actors, particularly with regard to infrastructure ownership and service delivery. Institutions must coordinate multimodal operations in accordance with international frameworks such as TEN-T, eFTI and the Single European Sky. Governance mechanisms operate at multiple levels, combining regulatory mandates, asset lifecycle management, and contract-based oversight. While operators prioritise efficiency and service quality, infrastructure governance emphasises long-term planning and compliance.

Risk, Regulation, and Management Culture

The scope of risk management includes operational disruptions, cyber threats to digital logistics systems, regulatory changes and geopolitical tensions. Organisations must comply with a variety of legal regimes, including those relating to emissions controls, labour laws and data protection (e.g. the GDPR). Management culture varies by subdomain: for example, freight prioritises safety, urban mobility prioritises responsiveness, and postal services prioritise innovation. The Three Lines of Defence model is becoming increasingly popular, particularly among larger companies that use GRC systems and ISO standards for safety, environmental protection, and asset management.

Governance of IT and Digital Integration

Digital systems are essential for operational visibility, coordination and asset tracking. As platforms such as eFTI, telematics and smart infrastructure become more widespread, IT governance plays a central role in ensuring strategic alignment and regulatory compliance. Frameworks such as COBIT and ISO/IEC 38500 are being adopted in order to manage IT complexity and ensure that investments are aligned with operational goals. The prominence of board-level CIOs and IT steering committees is growing, particularly in terms of aligning digital strategies with EU initiatives such as the Digital Transport and Logistics Forum (DTLF).

IT Management, Risk, and Operational Resilience

The sector is exposed to a number of significant cyber-physical risks, including ransomware attacks, GPS spoofing and SCADA vulnerabilities. IT governance must therefore encompass not only cybersecurity, but also business continuity and third-party oversight. CISOs are becoming increasingly accountable to independent risk committees. The Three Lines of Defence model promotes clear separation of roles across IT delivery, oversight, and audit. Mature organisations implement integrated governance models that combine IT architecture, risk control and regulatory alignment. This enables innovation while safeguarding the resilience of digitally enabled mobility networks.

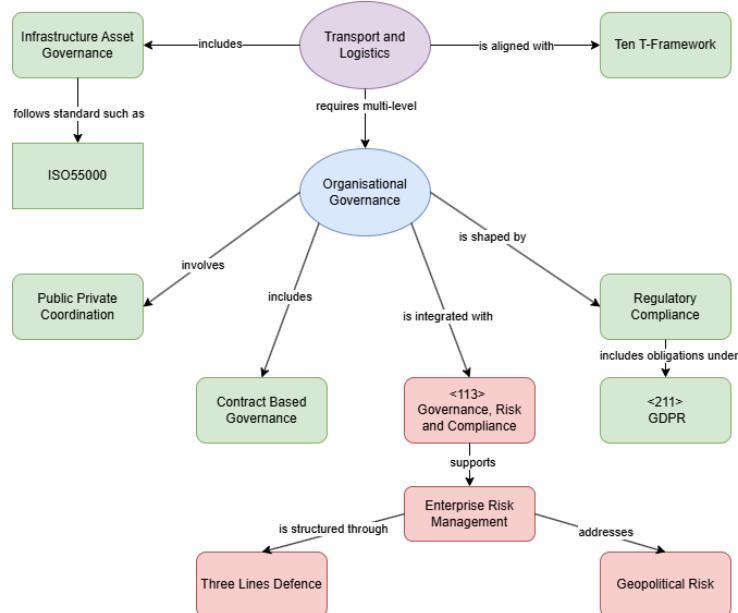


Figure 1: Transports and Logistics CMAP according to Theme 1.

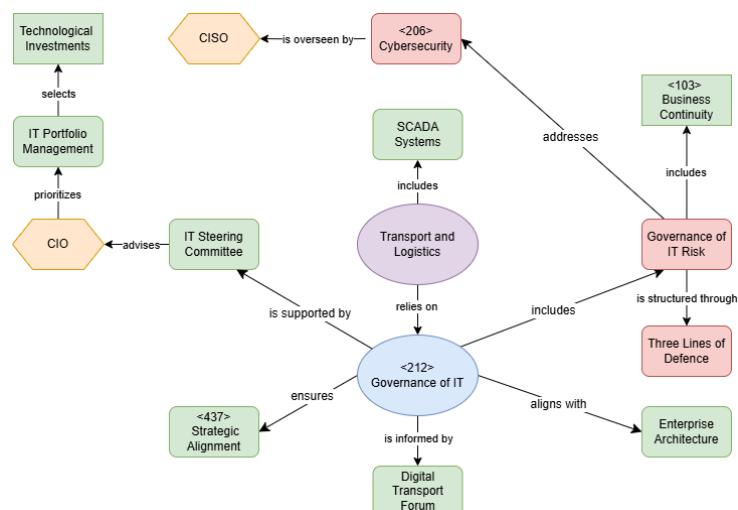


Figure 2: Transports and Logistics CMAP according to Theme 2.

Hospitality and Leisure

The hospitality and leisure sector encompasses a wide variety of service industries, including accommodation, food and drink, recreation and travel. Examples include hotel chains, independent accommodation providers, restaurants, theme parks, resorts, and cultural or entertainment venues. It is characterised by high levels of customer interaction, significant seasonal variability and an increasing reliance on digital platforms for booking, managing experiences and monitoring reputation. For the purposes of this analysis, we define the sector as a multi-tiered ecosystem integrating corporate governance structures with local operational practices and operating within a regulatory context focused on customer safety, data protection and environmental sustainability.

Organizational Structures and Governance

The hospitality and leisure sector comprises a variety of organisational structures, ranging from centralised hotel chains to decentralised franchises. Many operations combine corporate control with local autonomy, resulting in dual governance needs. Priorities for governance include reputation, service quality and customer trust, and these are supported by standards such as GDPR, ISO 14001 and integrated management systems. However, franchise models present oversight challenges, necessitating clear contractual governance and regular compliance audits to maintain brand integrity.

Maturity, Risk, and Management Culture

Organisations in this sector typically have hybrid governance structures, blending formal systems with service-driven cultures. While frontline autonomy improves the guest experience, risk management protocols must be in place to address guest safety, cyber threats and financial fraud. The Three Lines of Defence model is becoming increasingly prevalent. Larger firms typically exhibit higher governance maturity and have more structured IT roles (e.g. CIO and CDO), whereas smaller operators may rely on ad hoc practices. Digital platforms such as CRM and PMS further increase the need for strategic IT alignment.

Governance of IT and Strategic Integration

In the hospitality and leisure sector, digital services such as booking systems, property management software (PMS) and customer relationship management (CRM) platforms are integral to daily operations and the guest experience. Therefore, IT governance must be embedded in strategic planning to ensure that digital initiatives align with service quality, brand standards and regulatory expectations. Frameworks such as COBIT and ISO/IEC 38500 help to define clear lines of accountability between corporate leadership and digital units, thereby preventing IT from becoming isolated or reactive.

IT Management, Risk, and Operational Continuity

Day-to-day IT management in the hospitality industry is often decentralised, yet critically interdependent. While CIOs or CDOs oversee infrastructure and platforms across chains, property-level managers depend on IT systems for front-desk operations, bookings, and service delivery. Governance mechanisms must therefore account for cybersecurity, data privacy, especially under GDPR, and system resilience. As many venues operate 24/7, ensuring IT continuity and enabling rapid incident response are vital. The Three Lines of Defence model supports risk distribution, with oversight extending from the board to IT steering committees, the internal audit function, and the CISO. Integrating IT governance into enterprise risk management enhances regulatory compliance and digital trust.

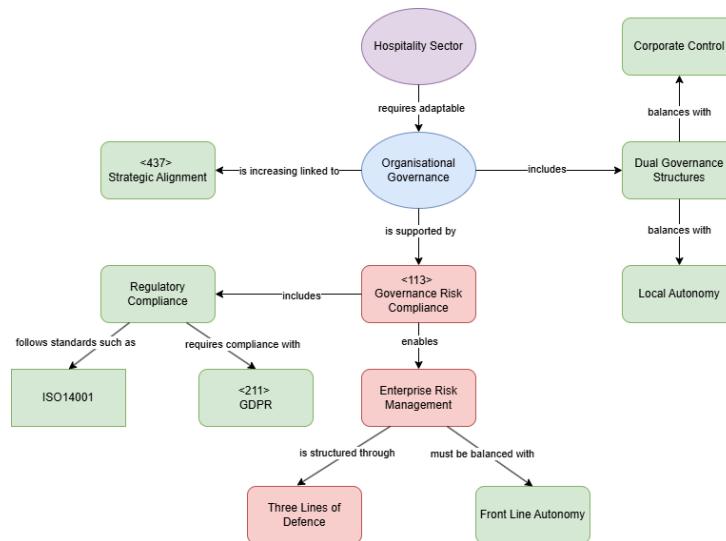


Figure 3: Hospitality and Leisure CMAP according to Theme 1.

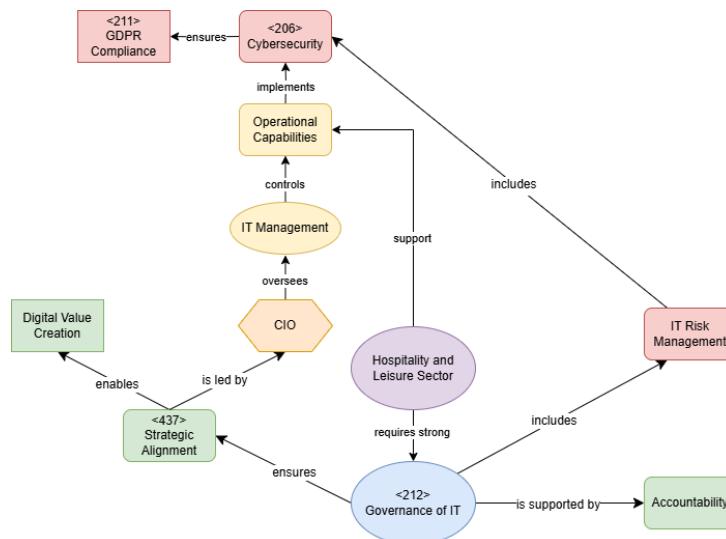


Figure 4: Hospitality and Leisure CMAP according to Theme 2.

Banking and Financial Services

The banking and financial services sector comprises institutions involved in the provision, management, and regulation of monetary assets, credit, and investment products. This includes retail banks, commercial banks, insurance providers, asset managers, and fintech firms. The sector is characterised by its systemic importance, high regulatory oversight, and critical reliance on digital infrastructure for core operations such as payments, compliance, credit assessment, and financial reporting. For the purpose of this analysis, the sector is understood as a tightly regulated ecosystem where governance structures, risk management frameworks, and IT systems are central to institutional trust, operational continuity, and market stability.

Organizational Structures and Governance

The banking and financial services sector is built around highly formalised organisational structures and layered governance systems. Retail banks, insurers and investment firms, for example, operate under board-led hierarchies, which are supported by specialised audit, compliance and risk committees. Regulatory bodies, including the ECB, the EBA and national supervisors, impose stringent governance standards concerning capital adequacy, internal control, board accountability and operational resilience. The maturity of a company's governance is reflected in its use of integrated compliance systems, third-party audits, and alignment with international frameworks such as Basel III and DORA.

Risk, Regulation, and Management Culture

Risk governance is deeply embedded in strategic and operational decision-making processes, covering areas such as credit, market, liquidity and cyber risk. Financial institutions apply the Three Lines of Defence model, which involves strong roles for internal auditors, compliance officers and C-suite executives (e.g. CROs and CISOs). The sector's high exposure to systemic risk and public scrutiny fosters a culture of procedural control, regulatory responsiveness and ethical accountability. Digital transformation, cloud outsourcing and fintech integration are increasing the need for adaptive governance and board-level digital literacy, thereby reinforcing the interdependence between risk, compliance and IT management.

Governance of IT and Strategic Oversight

In the banking sector, digital infrastructure is mission-critical, supporting payments, credit, risk assessment and regulatory reporting. Consequently, IT governance is deeply integrated into enterprise oversight structures, frequently via board-level CIOs, IT steering committees, and dedicated digital risk units. Frameworks such as COBIT and ISO/IEC 38500 are widely used to ensure that IT investments align with regulatory compliance, service continuity and innovation mandates. Regulatory developments such as DORA and GDPR have further elevated IT governance to a board-level concern, making accountability and cross-functional coordination essential.

IT Management, Resilience, and Risk Control

In financial institutions, IT management encompasses complex systems such as core banking, cybersecurity, cloud infrastructure and third-party services. CIOs and CISOs are responsible for overseeing IT operations, risk management, and incident response, while portfolio and architecture management ensure controlled innovation. The Three Lines of Defence model is standard practice, involving a clear separation between IT delivery, oversight, and audit. Due to high regulatory exposure and system interdependence, cybersecurity governance is treated as a strategic priority. Institutions must strike a balance between digital transformation and resilience, employing risk-based frameworks and integrated controls to mitigate systemic threats and preserve public trust.

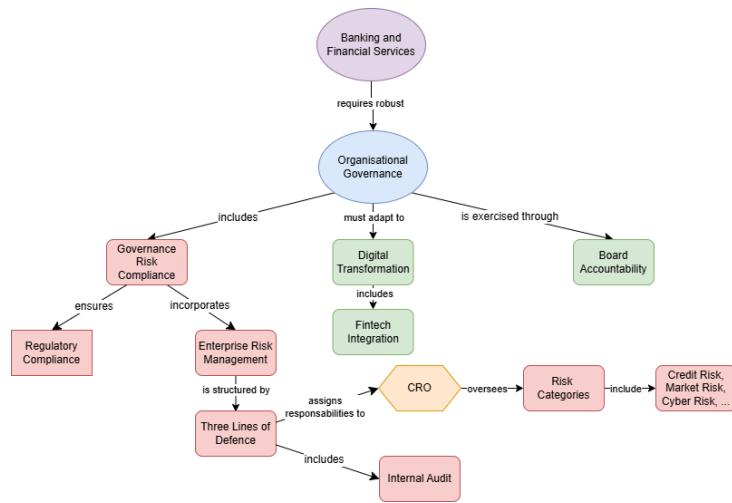


Figure 5: Banking and Financial Services CMAP according to Theme 1.

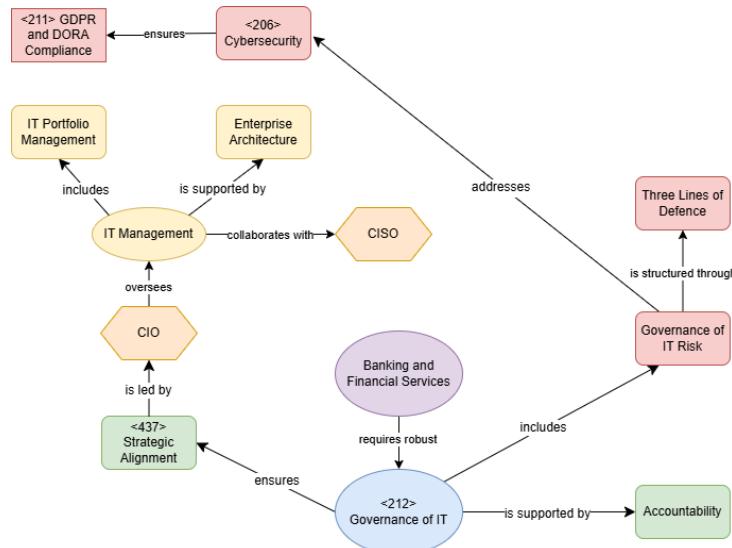


Figure 6: Banking and Financial Services CMAP according to Theme 2.

Banking and Financial Services vs Transport and Logistics

Organizations, Governance, and Management

Organisational structures in banking and financial services are highly formalised, featuring board-led oversight, audit and risk committees, and executive roles such as Chief Risk Officer (CRO) and Chief Compliance Officer (CCO). Regulatory frameworks such as Basel III, the General Data Protection Regulation (GDPR) and the Digital Operational Resilience Act (DORA) embed accountability and compliance into strategic and operational decision-making processes. Integrated GRC systems and structured models such as the Three Lines of Defence reinforce governance maturity.

By contrast, transport and logistics operate through more heterogeneous and multi-actor governance models. These models involve public authorities, private operators and infrastructure managers, who often coordinate across borders. Governance mechanisms combine public–private coordination, long-term asset management, and contract-based oversight, particularly in the rail, aviation, and maritime sectors. Frameworks such as TEN-T and eFTI guide infrastructure planning and interoperability, although the level of governance maturity varies among different stakeholders.

Although both sectors are subject to complex regulatory demands and operational risks, the banking sector has a centralised, compliance-driven governance culture that is shaped by systemic financial risk. In contrast, transport governance is more distributed and operationally adaptive, with an increasing emphasis on risk-based practices and digital integration. As banking becomes more decentralised through fintech and transport becomes more digitised, the two sectors are converging towards governance models that are more flexible, resilient and transparent.

Governance of IT and IT Management

In banking, IT governance is deeply embedded within enterprise control systems. Institutions operate under strict mandates, such as DORA and GDPR, which require CIO-led governance, IT steering committees and independent risk oversight. Frameworks such as COBIT and ISO/IEC 38500 promote strategic alignment, and cybersecurity and IT risk are managed via integrated GRC platforms and the Three Lines of Defence model. Core systems and digital infrastructures are centrally managed, with resilience and compliance being prioritised.

The transport and logistics sector has a more fragmented IT governance landscape due to its physical-digital hybrid structure and reliance on multi-actor coordination. Although IT supports critical operations such as SCADA, telematics and eFTI, governance practices are often decentralised and dependent on vendor platforms or data-sharing partnerships. Although cybersecurity is evolving, particularly in relation to critical infrastructure and OT systems, it is typically less mature than in banking.

Despite their different levels of formalisation, the two sectors are becoming increasingly aligned on key IT governance issues, such as managing digital risk, third-party exposure and regulatory accountability. While banking offers a benchmark for structured governance under regulatory pressure, transport highlights the challenges of coordinating digital ecosystems across diverse operational domains.

Banking and Financial Services vs Hospitality and Leisure

Organizations, Governance, and Management

The banking and financial services sector relies on formalised, hierarchical organisational structures, reinforced by board-level governance, audit and risk committees, and executive functions such as the Chief Risk Officer (CRO) and Chief Compliance Officer (CCO). Regulatory frameworks such as Basel III, GDPR and DORA demand a high degree of internal control, accountability and structured risk management. The maturity of governance is demonstrated through integrated GRC systems and standardised models such as the Three Lines of Defence. By contrast, the hospitality and leisure sector exhibits more decentralised and hybrid structures. This sector encompasses corporate chains, franchises and independent operators, which can have varying degrees of formal governance. Service delivery often blends central standards with local autonomy, particularly within franchised models. Although practices differ significantly in formality and consistency across organisations, governance focuses on customer trust, brand protection, and regulatory compliance (e.g. GDPR, health and safety).

Although both sectors manage compliance and reputational risk, the banking sector has a more centralised, regulation-driven governance culture. In contrast, hospitality governance is more service-oriented and adaptive, often relying on informal controls, particularly in smaller firms. As the banking sector evolves with fintech and the hospitality sector expands its digital platforms and global brands, both sectors are increasingly requiring hybrid governance models that balance control with agility.

Governance of IT and IT Management

In banking, IT governance is institutionalised and aligned with enterprise strategy. Regulatory mandates such as DORA and GDPR enforce the adoption of formal structures, such as IT steering committees and CIO-led decision-making processes. Frameworks such as COBIT and ISO/IEC 38500 are widely adopted to support the alignment of IT, risk and compliance. Cybersecurity and IT risk are tightly controlled through integrated governance, risk and compliance (GRC) tools and formalised reporting structures.

The hospitality and leisure industries present a more varied IT governance landscape. Digital platforms such as CRM systems, booking engines and property management systems (PMS) are central to the customer experience, yet IT oversight is often decentralised, particularly among franchised or smaller operators. While larger groups are adopting CIO roles and compliance standards (e.g. ISO 27001), the level of governance maturity across the sector is uneven. Cybersecurity and data protection are growing concerns, particularly given the reliance on third-party digital platforms and customer-facing technologies.

Both sectors face growing demands for IT governance, albeit from different drivers: banking due to regulatory scrutiny and systemic risk, and hospitality due to service expectations and digital exposure. While banking provides a reference for structured IT governance, hospitality illustrates the challenges of aligning technology with brand, privacy and decentralised control.

Group 467

Ana Sá ist nº112111, Daniela Camarinha nº112265, Joana Matias ist nº112438,
Rita Martins nº112505, Sofia Du nº104195

Industry: Transport and Logistics **Theme 1:** Organizations, Governance, and Management

1. Conceptual Map

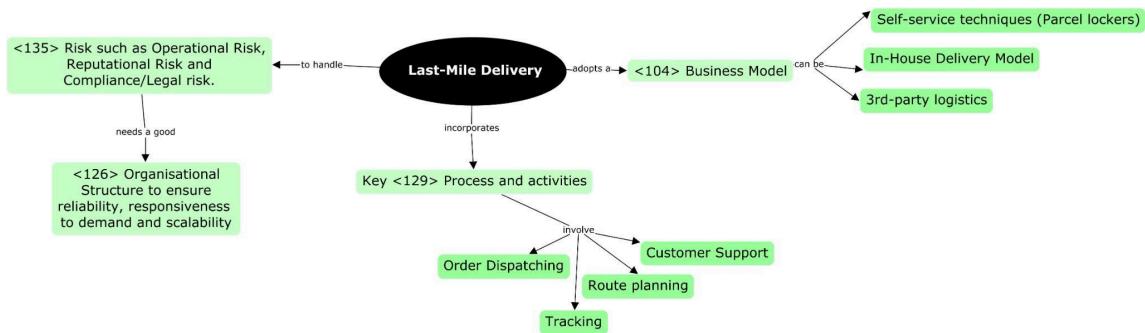


Image 1. Conceptual Map for Transport and Logistics niche: Last-Mile Delivery focused on Theme 1

2. Textual Analysis

This industry is defined by being the final step of transporting goods to the end customer. The principal risks in this industry are operational, such as dispatch failures, reputational, for example, service delays, and compliance/legal (e.g., labor and safety violations).

Embedding a **<113> GRC** framework to promote accountability and alignment of activities is key since Last-Mile Delivery is an aggregation of several departments that work together in order to deliver a package to a client. Another key aspect of this industry is **<116> KPIs**, which enable performance monitoring, risk control, and alignment with customer expectations. This industry would not be the same without KPI tracking, since even drivers have a certain number of packages they need to deliver daily. Everything is tracked from missing delivery to the time it takes to get to the customer's house. Key KPIs in this industry are mainly: On-time-delivery rate, Average delivery rate, delivery accuracy, and cost per delivery.

This industry is also characterized by having several possible **<104> business models**, such as click and collect (self-service), in-house delivery model, and 3rd party logistics. Depending on the business model being used, there are different **<135> risks** associated. For example, if using 3rd party logistics, you need to have strong **<323> SLAs** and performance tracking.

In conclusion, last-mile delivery, as the final and most visible step of transporting goods to the end customer, is defined by rising operational costs, increasing sustainability demands, and the need for seamless cross-departmental collaboration. Meeting these challenges requires high levels of coordination, supported by effective corporate governance and strong **<117> leadership** by CxOs, who play a vital role in managing critical risks.

Industry: Transport and Logistics **Theme 2:** Governance of IT and IT Management

1. Conceptual Map

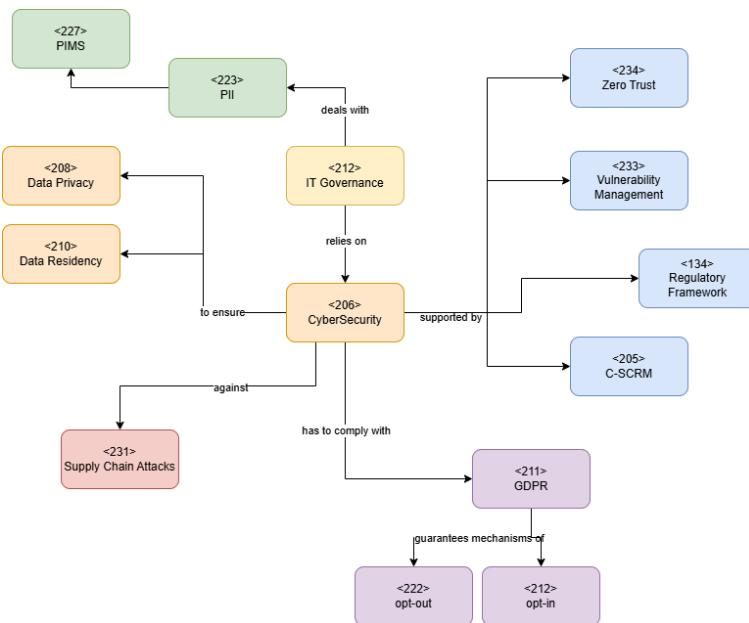


Image 2. Conceptual Map for Transport and Logistics niche: Last-Mile Delivery focused on Theme 2

2. Textual Analysis

Last mile delivery faces strong **<212> IT Governance and Management** concerns, as it is immensely dependent on technology to perform core business tasks, such as retrieving and storing package information, tracking geolocation of operators and goods, storing and consulting clients' personal information, such as name and address, these are **<223> PII** that are sensitive and should have a **<227>PIMS** to guarantee the **<208>Data Privacy** of both end-clients and other members of the **<231> Supply Chain**.

Bounding themselves to **<134> Regulatory Frameworks**, like the **<211> GDPR**, clients of last-mile delivery have the right to **<221> opt-in** and **<222> opt-out** of the system and delete their data when they please, fostering information security and self-sovereignty.

International expansion brings the question of how companies can maintain flexibility while not infringing international laws. Following regulatory laws such as the CCPA (California) PDPA (Singapore). That's where maintaining an IT Framework that adopts **<210>Data Residency** strategies like COBIT and ISO/IE 38500 comes in huge importance.

Due to dealing with sensitive data, they are prone to being targets of **<206> CyberSecurity** attacks, mostly **<231> Supply Chain** attacks, where they are the connection at the edge of the chain. To counter this, companies need to maintain a **<205> C-SCRM**, **<233> Vulnerability Management** system, and **<234> Zero Trust** procedures.

Industry: Banking and Financial Services **Theme 1:** Organizations, Governance, and Management

1. Conceptual Map

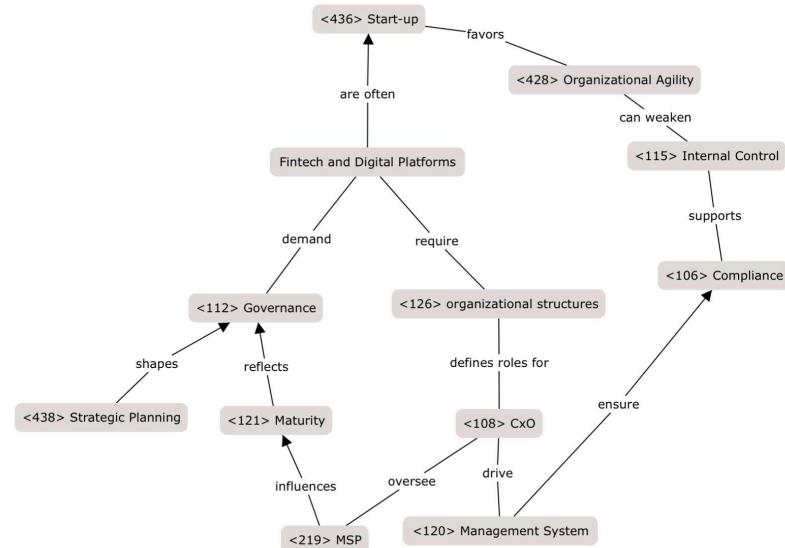


Image 3. Conceptual Map for Banking and Financial Services niche: Fintech and Digital Platforms

2. Textual Analysis

Fintech firms often operate as an intersection between financial services and digital innovation, demanding strong **<112> Governance** and adaptive **<126> Organizational Structures**. Unlike traditional banks, many fintechs are **<436> Start-ups** and have flat hierarchies, informal processes and agile teams that still must comply with intense regulatory expectations due to their systemic impact on payments, lending, and capital flows.

This creates a tension between **<428> Organisational Agility** and **<115> Internal Control**, without clear **<108> CxO** roles and a mature **<120> Management System**, rapid scaling can introduce risks to **<106> Compliance**, especially under frameworks like AML/KYC or PSD2.

Moreover, many fintech partners rely on **<219> MSPs**, which demand contractual clarity, role accountability, and oversight, which in traditional financial governance usually falls under the **<102> Board of Directors** and internal audits. However, many startups have not formalized these oversight processes, which in most cases lead to weak **<121> Maturity levels**.

Examples like algorithmic lending or peer-to-peer finance raise additional concerns on **<111> Ethical Values**, especially when these decisions impact vulnerable consumers, making it crucial for Institutions to integrate ethics into **<438> Strategic Planning** and **<127> Policy** development.

The drive for innovation must not overtake the implementation of good management frameworks. Fintech firms benefit from investing early in governance structures such as **<131> RACI** matrices, internal controls, and **<109> Documented Information systems** to ensure both operational stability and trustworthiness.

Industry: Banking and Financial Services Theme 2: Governance of IT and IT Management

1. Conceptual Map

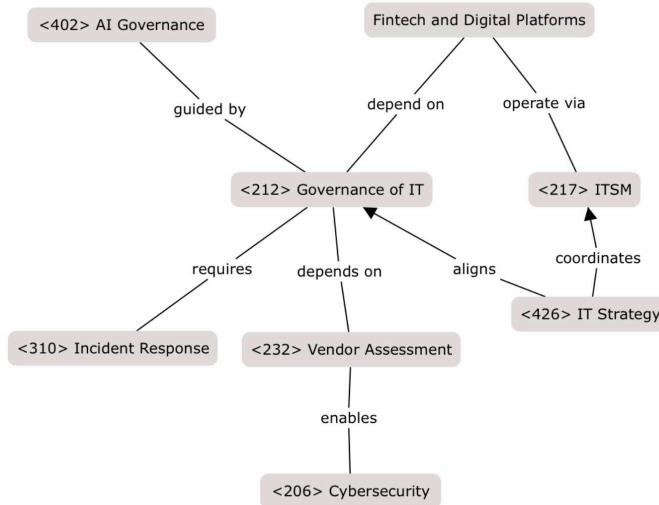


Image 4. Conceptual Map for Banking and Financial Services niche: Fintechs and Digital Platforms

2. Textual Analysis

Fintechs depend fundamentally on digital infrastructures, and their success hinges on robust **<212> Governance of IT**, embedded **<217> ITSM**, and responsive **<310> Incident Response** mechanisms.

Unlike incumbent banks that built IT around physical branches, fintechs are often “cloud-native” and use a stack of third-party services (e.g., identity verification, payment gateways, crypto custody), making it require advanced **<232> Vendor Assessment** and **<206> Cybersecurity** coordination across supply chains. Fintech firms that fail to manage these relationships can risk having problems such as cascading outages and much more.

As their data footprint grows, these firms must also ensure compliance with **<208> Data Privacy** and **<305> Data Protection**, particularly under frameworks like **<211> GDPR**, since that firms with weak **<216> ISMS** or improvised **<319> Patch Management** are vulnerable to breach, regulatory fines and reputational damage.

Fintechs deploying AI in credit or fraud scoring need strong **<402> AI Governance** and **<422> Explainability**, making sure model outputs are interpretable and fair, these governance responsibilities must be incorporated in both technical and executive layers of the organization.

Moreover, many fintechs rely on **<326> XaaS** services for scalability, but this also introduces **<317> Operational Risk** if failovers or **<322> Redundancy** are not robust and so having a mature **<311> IT Operations Management** layer is essential for resilience.

Finally, incorporating these governance elements under a clear **<426> IT Strategy** that aligns with the fintech's mission and regulatory footprint is a major foundational differentiator in a highly competitive and scrutinized environment.

Industry: Agriculture and Farming Theme 1: Organizations, Governance, and Management

1. Conceptual Map

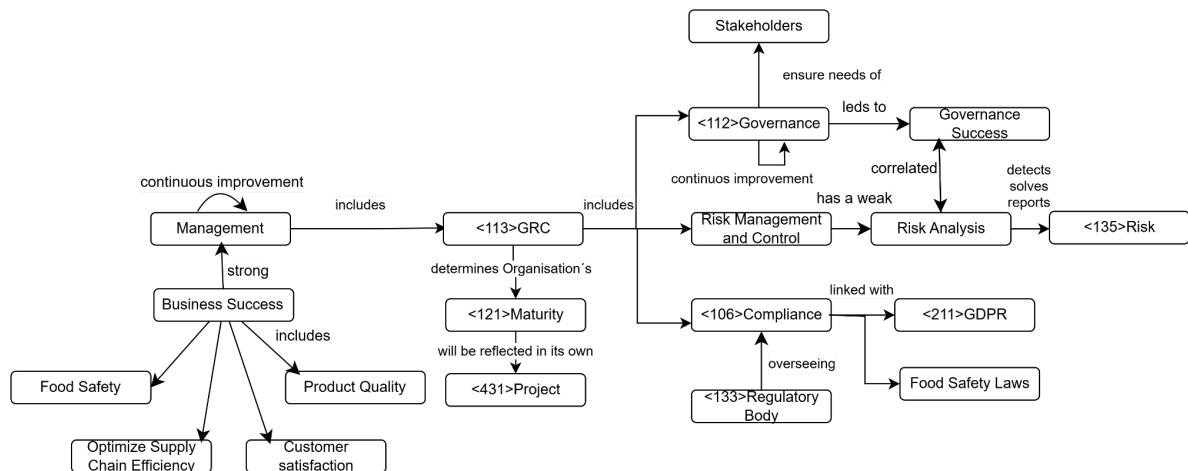


Image 5. Conceptual Map for Agriculture and Farming niche: The Role of Management and Risk Control in Agri-Food Processing and Distribution, focused on Theme 1

2. Textual Analysis

Agri-food processing and distribution play a vital role in linking agricultural production with consumer markets. It is a sector deeply influenced by regulations, logistics, and consumer expectations for **<130>quality**, safety, and transparency. Companies must implement strong **<118> management** and **<135>risk** control frameworks to ensure reliable operations and meet business goals.

Effective **<118>management** in this subdomain involves coordinating production processes, **<130>quality control**, and delivery logistics, often across multiple countries and supply chain actors. It requires aligning business objectives with operational capabilities, balancing efficiency, cost control, and customer satisfaction.

<135>Risk management and Compliance are essential due to the sector's exposure to diverse threats such as supply chain disruptions, temperature failures in cold storage (cold chain), and compliance violations. Poor risk control can lead to recalls, reputational damage, or regulatory penalties.

Maintaining **<106>compliance** with food safety standards is non-negotiable. These systems also contribute to continuous improvement, helping businesses meet customer and legal expectations while improving performance.

In conclusion, integrating **<118>management** and **<135>risk** control in agri-food processing and distribution not only protects against disruptions but also drives **<130>quality**, efficiency, and long-term success.

Industry: Agriculture and Farming Theme 2: Governance of IT and IT Management

1. Conceptual Map

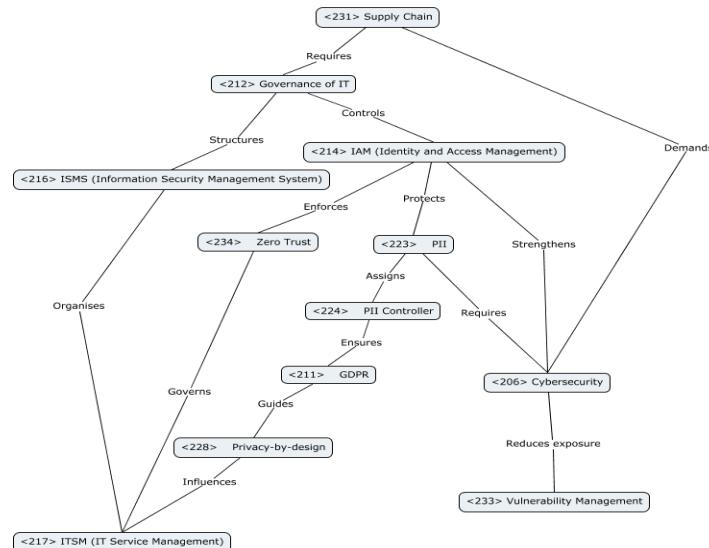


Image 6. Conceptual Map for Agriculture and Farming niche: Agri-food processing and Distribution

2. Textual Analysis

Agri-food processing and distribution is characterized by transforming raw agricultural products (like meat, dairy, or grains) into **consumable goods and delivering them through refrigerated logistics and retail**. It is defined by strict food safety rules, high traceability demands, and a strong reliance on IT systems to ensure quality, compliance, and trust across production and delivery stages.

Agri-food processing is based on coupled **IT systems** that ensure traceability, quality, and regulatory compliance. Effective <212> **Governance of IT** is crucial to manage systems dealing with sensitive information, logistics, and compliance.

A robust <216> **ISMS** coordinates the security policies of the organisation, which are executed through <217> **ITSM** to ensure consistency in services. The systems must be protected by robust <206> **Cybersecurity** frameworks that include proactive <233> **Vulnerability Management** to detect and neutralise threats. With <214> **IAM** and <234> **Zero Trust**, only permitted users and systems can talk to **sensitive platforms**, essential for preventing **unauthorized access** and food supply **data protection**.

Due to the food traceability regulation, handling of <223> **PII** is also correctly ensured by organisations. Data protection lies with the <224> **PII Controller** and must comply with <211> **GDPR** to ensure legal processing of transaction and user information. This is supplemented by <228> **Privacy-by-design**, which includes conformity from the beginning of any system implementation.

Finally, the complexity of the <231> **Supply Chain** requires that IT managers provide system integrity and oversight of numerous external partners, highlighting once again the role of governance, data control, and access restrictions along the agri-food value chain.

Comparisons of Industries

1. Transport and Logistics vs Agriculture and Farming in Theme 1: Organizations, Governance, and Management

A key distinction between Transport and Logistics and Agriculture and Farming lies in their **<104>Business Models**. Transport operates on a service-based model focused on efficiency, time, and route optimization. Agriculture, by contrast, is production-based, generating value through natural resource cultivation, and is subject to environmental variability. **<107>Corporate Governance** in transport involves structured oversight by **<102>BoD** and **<108>CxO**, aligned with global compliance, safety, and emissions controls. Agriculture governance is typically local, shaped by **<133>regulatory bodies** overseeing food safety, land use, and environmental impact.

The scope of **<112>Governance** is broader in transport due to cross-border operations and regulatory complexity. **<135>Risk** profiles diverge significantly. Transport faces operational, financial, and geopolitical risks; agriculture is more exposed to environmental and biological risks. **<106>Compliance** in logistics centers on trade and transport safety, while agriculture emphasizes chemical usage, land regulations, and sustainability. **<118>Management systems** also differ. Logistics relies on formal, tech-driven **<120>Management Systems** (e.g., ERP, TMS) and strong **<115>Internal Controls**, supported by performance-focused **<116>KPIs**. Agriculture is less centralized but evolving, integrating data tools in precision farming with the growing use of indicators like yield and input efficiency.

Finally, **<101>Audit** practices in logistics are standardized and frequent, linked to ISO and international norms. In agriculture, **<101>audits** are often tied to sustainability certifications or subsidy requirements, with oversight varying significantly by farm size and structure.

2. Transport and Logistics vs Banking and Financial Services in Theme 2: Governance of IT and IT Management

Both the Banking and Financial Services and Transport and Logistics sectors rely on digital infrastructures, but their governance priorities and IT management structures are slightly different due to different operational pressures and risk scenarios. Fintechs, inherently cloud-native, require sophisticated **<212> Governance of IT** practices in order to manage their heavy reliance on third-party platforms (**<326> XaaS**) and outsourced services, this makes mature **<232> Vendor Assessment** and robust **<206> Cybersecurity** policies a requirement, specially because failures may compromise financial flows.

Where fintechs are regulated by financial-specific rules, logistics must navigate a medley of international **<134> Regulatory Frameworks** and balance **<210> Data Residency** in cross-border contexts, nevertheless both sectors demand proactive **<216> ISMS** and **<233> Vulnerability Management** systems, yet the strategic posture can differ as fintechs embed governance into innovation scaling and regulatory alignment, while logistics firms embed it in service continuity and global compliance.

3. Banking and Financial Services vs Agriculture and Farming Theme 1: Organizations, Governance, and Management

Banking and Financial Services are extremely formal and regulated environments. They are supported by effective <107> **Corporate Governance**, which is commonly enforced by an unequivocally set <102> **Board of Directors** and supported by effective <119> **Management** Frameworks. Sectoral Governance has a direct impact upon the regulatory needs, with requirements for strict <106> **Compliance**, internal <101> **Audit**, and constant monitoring by <115> **Internal Control** measures. Leadership is centralized with well-defined roles for <108> **CxO** executives, and operations are directed by formalized <127> **Policies**, <128> **Procedures**, and written-down <129> **Processes**.

On the other hand, Agriculture and Farming will prefer less formalized and centralized <126> **Organizational Structures**. Formalized <120> **Management Systems** can be employed by agri-businesses operating on a large scale, but smaller-scale or local producers will employ tacit knowledge and experience-based management. Their <125> **Organizational Culture** will therefore be based on local values and informal leadership rather than formal structures. Documentation, <132> **Records Management**, and <110> **Due Diligence** procedures may differ according to the level of digital maturity and resources available.

Despite these differences, both domains are concerned with long-term sustainability, and <112> **Governance** is responsible for bridging the <122> **Mission** and operational and ethical requirements. The financial world is concerned with formal control and auditability, but the world of agriculture is concerned with flexibility, resilience, and contextual decision-making.

4. Agriculture and Farming Theme vs Banking and Financial Services in Theme 2: Governance of IT and IT Management

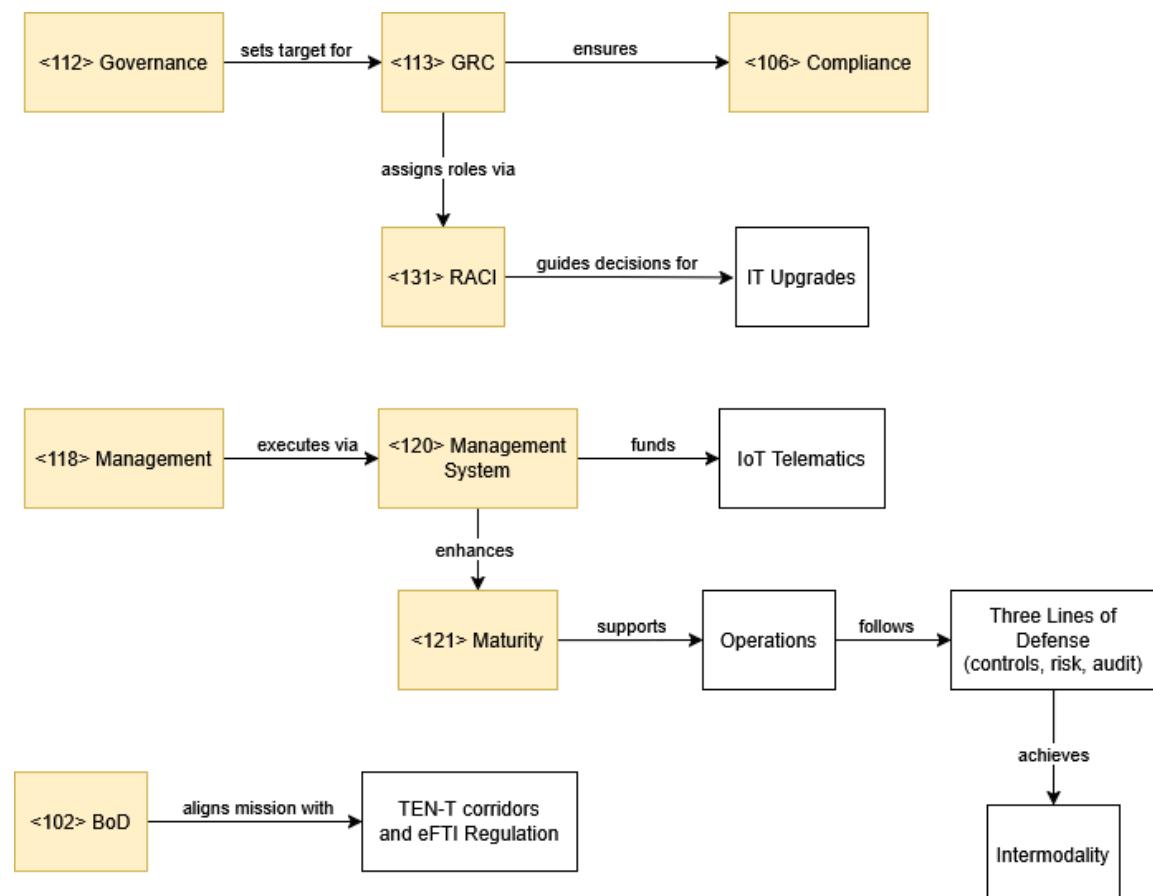
On one hand, in the **Banking and Financial Services** sector <212> **Governance of IT** is deeply integrated into regulatory compliance and <228>**privacy-by-design** principles, especially under <211>**GDPR**. Institutions must manage <209>**Data Residency** and <210>**Data Retention** to ensure lawful processing of <223>**PII** within a defined <227>**PIMS**. Cybersecurity risks are imminent, with <234>**Zero Trust** architectures, strong <214>**IAM**, and <215>**InfoSec** policies under a mature <216>**ISMS**. Banks use <217>**ITSM** frameworks to deliver resilient IT services and often rely on <219>**MSPs** and <220>**MSSPs** for infrastructure and threat monitoring. Compliance-driven <233>**Vulnerability Management**, <232>**Vendor Assessment**, and secure <231>**Supply Chain** practices, including <230>**SBOMs**, help mitigate third-party risks. On the other hand, the **Agriculture and Farming** sector, while evolving, has less stringent IT governance. IT focuses more on operational efficiency, with selective adoption of <217>**ITSM**, basic <214>**IAM**, and light <216>**ISMS**. <229>**Public Procurement** policies may mandate data protections, but <221>**Opt-in**/<><222>**Opt-out** and <223>**PII** handling are often less formalized.

Theme 1 - Industry 4 - Transport and Logistics

The intermodal logistics coordination industry focuses on integrating multiple transportation modes (road, rail, maritime, and air) to optimise the movement of goods across global supply chains. This sector is characterised by its reliance on interconnected infrastructure (e.g., ports, rail terminals, warehouses), digital systems for real-time tracking (e.g., IoT telematics, freight management platforms), and adherence to cross-border regulatory frameworks (e.g., EU's eFTI Regulation for digital freight data). Its primary goal is to ensure seamless, cost-effective, and sustainable cargo transfers between transport modes while meeting compliance, safety, and environmental standards.

The <102> Board of Directors in this industry sets strategic priorities such as carbon reduction targets and infrastructure interoperability, aligning with transnational initiatives like the EU's TEN-T corridors. <113> GRC (Governance, Risk, Compliance) frameworks address risks like cyber threats to logistics platforms, regulatory penalties for emission non-compliance, and supply chain disruptions. Role clarity is ensured through <131> RACI matrices, defining accountability for decisions like fleet electrification or terminal expansions.

<118> Management translates strategy into action via integrated <120> Management Systems, deploying technologies (e.g., AI-driven routing algorithms) and standardising cross-modal processes. Frontline operations rely on real-time data from warehouse management systems and telematics, while the Three Lines of Defence model ensures risk controls (e.g., cybersecurity protocols) are monitored and audited.



Theme 1 - Industry 6 - Banking and Financial Services

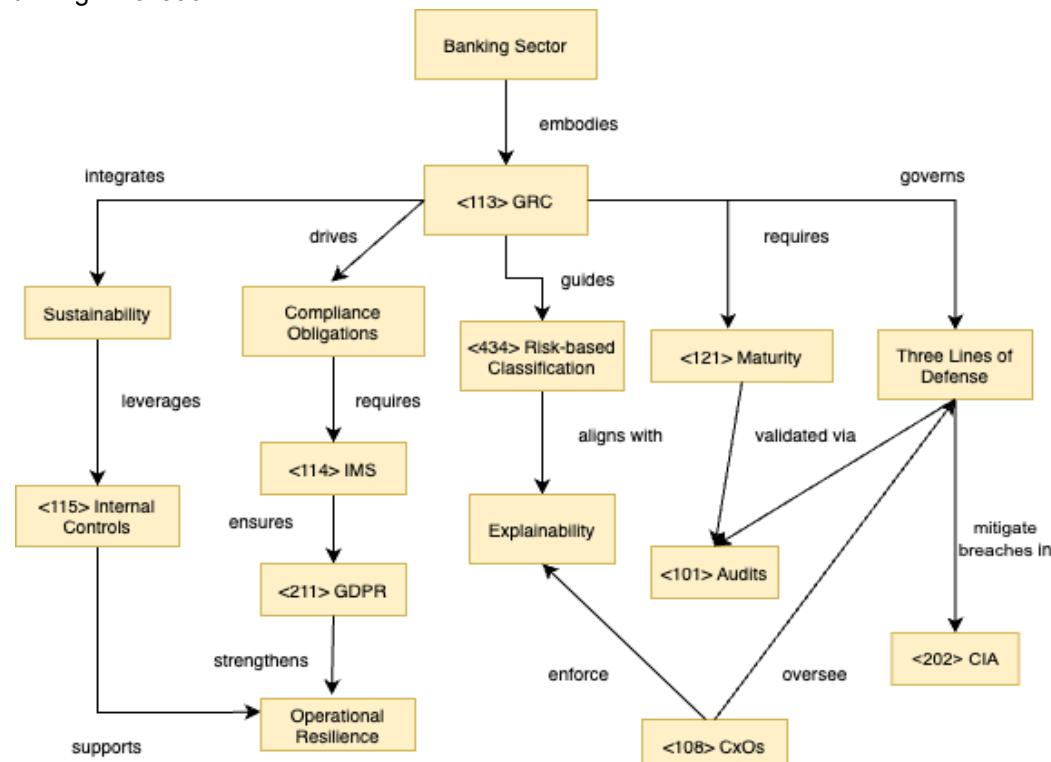
The Banking and Financial Services sector embodies the governance, risk, and management principles central to Theme 1, operating within a framework defined by rigorous oversight, <113> GRC, and <121> maturity in organisational practices.

Governance structures in this sector mirror Theme 1's emphasis on accountability, with boards and <108> CxO roles such as Chief Risk Officers (CROs) and CISOs ensuring alignment between strategic objectives and operational execution. External supervision by entities like the ECB or Basel Committee aligns with the Three Lines of Defence model, where frontline operations (1st line), risk/compliance teams (2nd line), and independent audits (3rd line) collaborate to mitigate risks like cybersecurity breaches (<202> CIA Triad: Confidentiality, Integrity, Availability) and operational disruptions.

<106> Compliance obligations, such as Basel III capital adequacy rules and DORA, reflect Theme 1's focus on regulatory alignment. Financial institutions rely on integrated management systems (<114> IMS) to harmonise IT governance, data protection (like <211> GDPR), and business continuity, ensuring adherence to global standards while fostering operational resilience.

Strategic challenges like fintech innovation and AI-driven decision-making intersect with Theme 1's adaptive governance principles. Banks must balance agility with <434> risk-based classification for emerging technologies, ensuring explainability in algorithmic systems to uphold ethical standards. Meanwhile, sustainability strategies and ESG disclosures highlight how governance extends to modern imperatives like climate risk and social accountability.

By leveraging <101> audits, certifications, and <115> internal controls, the sector demonstrates maturity in governance practices, ensuring stakeholder trust amid digital disruption. Ultimately, Banking and Financial Services operationalise Theme 1's core tenets (structured governance, risk-aware decision-making, and compliance-driven accountability) to navigate complexity while driving innovation.



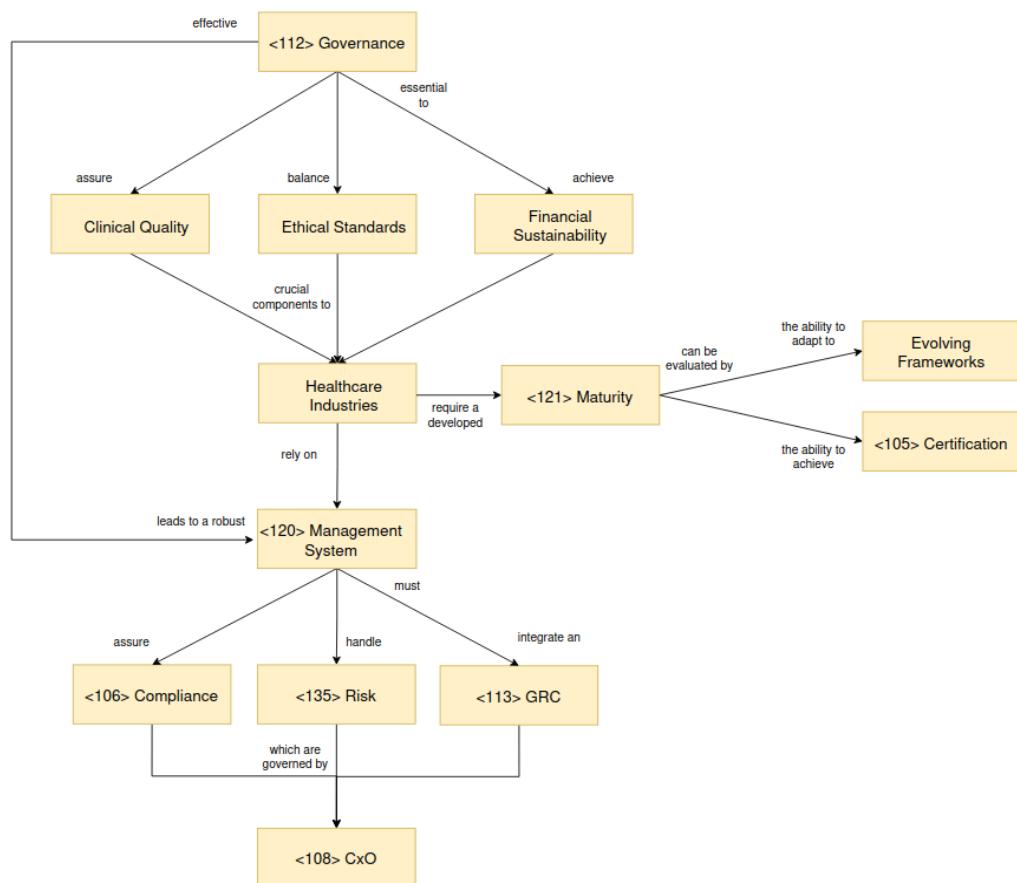
Theme 1 - Industry 8 - Healthcare

The healthcare industry combines service delivery, science, and public interest under strict regulation, encompassing hospitals, clinics, labs, pharmaceutical supply chains, insurers, and public health authorities. Systems typically follow Beveridge (public), Bismarck (social insurance), or market-based models (often blended in Europe) to deliver universal coverage alongside private services. Across all structures, healthcare must guarantee equitable access, patient safety, regulatory compliance, and resilience to systemic risks like pandemics or cyberattacks.

In the healthcare sector, effective <112> Governance ensures alignment between clinical quality, ethical obligations, and financial goals. Systems like Portugal's SNS operate within strict regulations, coordinating diverse stakeholders to meet legal and societal expectations. This is supported by a robust <120> Management System that integrates clinical workflows, digital platforms, and supply chains, reinforced by continuous monitoring and feedback mechanisms.

Given the sensitive nature of health data, institutions must adopt an integrated <113> GRC approach that unifies risk identification, <135> Risk treatment, and <106> Compliance with regulations like GDPR. This integration is often governed by specialised <108> CxO roles, such as the CIO, who aligns IT strategy with care delivery, and the CISO, who oversees cybersecurity and privacy controls.

Healthcare organisations' <121> Maturity can be evaluated by their ability to adapt to evolving frameworks like the European Health Data Space, embed proactive risk management, and achieve <105> Certification against standards (e.g., ISO/IEC 27001 for information security). High-maturity entities demonstrate cohesive policies, data-driven decision-making, and resilient operations, whereas low-maturity counterparts may struggle with fragmented systems and reactive compliance. In an industry where lives depend on reliability and trust, the seamless interplay of governance, management, and assurance underpins both patient safety and organisational resilience.

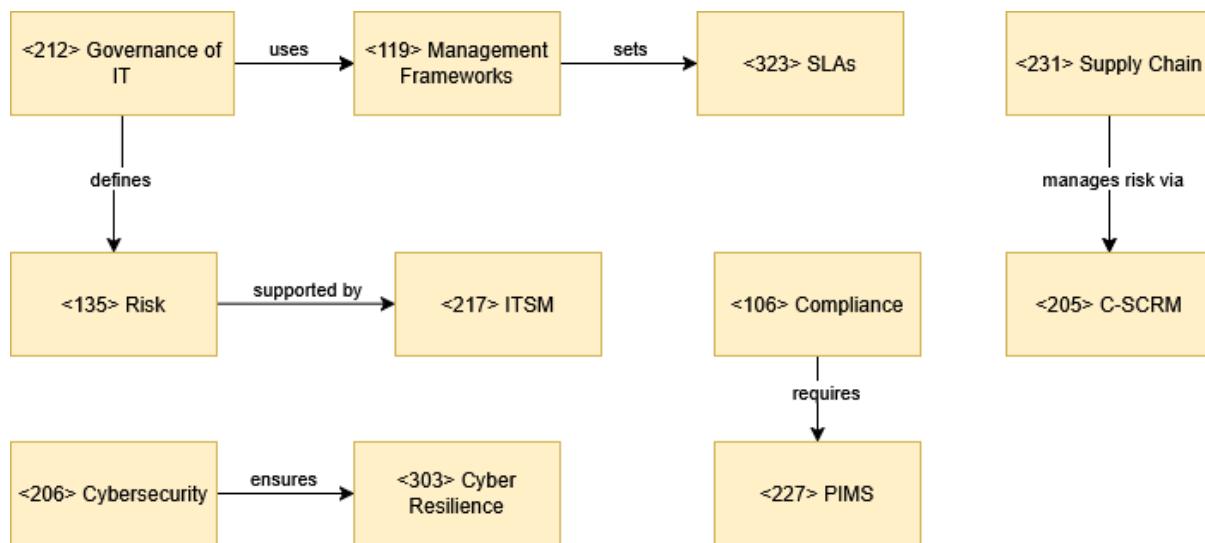


Theme 2 - Industry 4 - Transport and Logistics

In the transport and logistics sector, effective <212> Governance of IT ensures that digital investments, such as <318> Operational Technology (OT) for fleet telematics and IoT-enabled cargo tracking, align with strategic objectives like route optimisation and compliance with frameworks like eFTI. <119> Management Frameworks such as COBIT establish accountability, guiding organisations to prioritise projects that enhance <323> Service Level Agreements (SLAs) for real-time monitoring systems. The CISO plays a critical role in mitigating <206> Cybersecurity risks, particularly for safety-critical infrastructure, while collaborating with the CIO to balance innovation with <303> Cyber Resilience across multimodal networks.

Operational IT Management focuses on lifecycle oversight of systems like <313> IT Service Management (ITSM) platforms for passenger information and <311> IT Operations Management (ITOM) for fleet performance analytics. Metrics such as system availability <116> (KPI) and <310> Incident Response times ensure alignment with organisational <135> Risk appetite, addressing vulnerabilities in interconnected supply chains through <216> ISMS implementations. Compliance with <211> GDPR for passenger data and <305> Data Protection in e-commerce logistics underscores the need for <227> PIMS to embed privacy-by-design principles.

The sector's reliance on <231> Supply Chain interoperability demands robust <205> C-SCRM practices, particularly for digital dependencies in port management and freight exchanges. Mature organisations adopt <232> Vendor Assessment protocols to ensure third-party platforms meet <134> Regulatory frameworks like TEN-T. By institutionalising <131> RACI matrices for decision rights and aligning IT portfolios with <437> Strategic Alignment goals, transport entities transform IT into an enabler of sustainability and agility, navigating <446> VUCA challenges inherent in global logistics networks. This governance-maturity nexus ensures resilience while advancing cross-border digital integration.



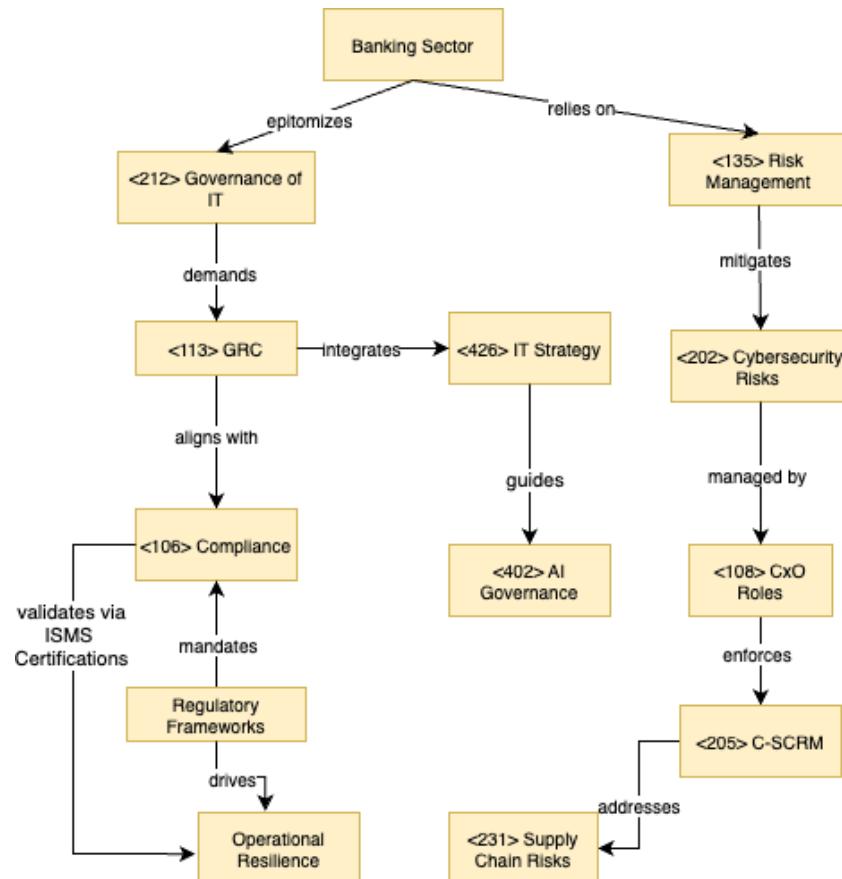
Theme 2 - Industry 6 - Banking and Financial Services

The banking and financial services sector epitomises the critical interplay between <212> governance of IT and <135> risk management, as highlighted in Theme 2. Financial institutions operate under stringent regulatory frameworks (e.g., DORA, Basel III) that demand robust alignment of IT systems with strategic objectives like operational resilience and <106> compliance. For example, <108> CxO roles, such as CISOs and CIOs, are pivotal in governing cybersecurity risks (like <202> CIA triad) and ensuring third-party cloud providers meet <323> SLA obligations under <205> C-SCRM principles.

The sector's reliance on digital transformation introduces governance challenges like <324> shadow IT and algorithmic accountability, necessitating frameworks such as <113> GRC to integrate <426> IT strategy with ethical standards (e.g., <402> AI governance). Supervisory authorities (e.g., ECB, EBA) enforce risk-based classification of IT dependencies, mandating ISMS certifications (ISO/IEC 27001) and <417> DPIA for fintech innovations.

Theme 2's emphasis on strategic alignment resonates in practices like <425> IT investment portfolios prioritising Basel III capital requirements or sustainable finance ESG disclosures. Meanwhile, <232> vendor assessments and <230> SBOM adoption reflect governance maturity in managing <231> supply chain risks, critical under DORA's digital resilience mandates.

Ultimately, banking's governance ecosystem, bridging <102> BoD oversight, regulatory compliance, and IT operational agility, exemplifies Theme 2's core thesis: effective IT governance is not a constraint but an enabler of trust, innovation, and systemic stability in highly regulated industries.



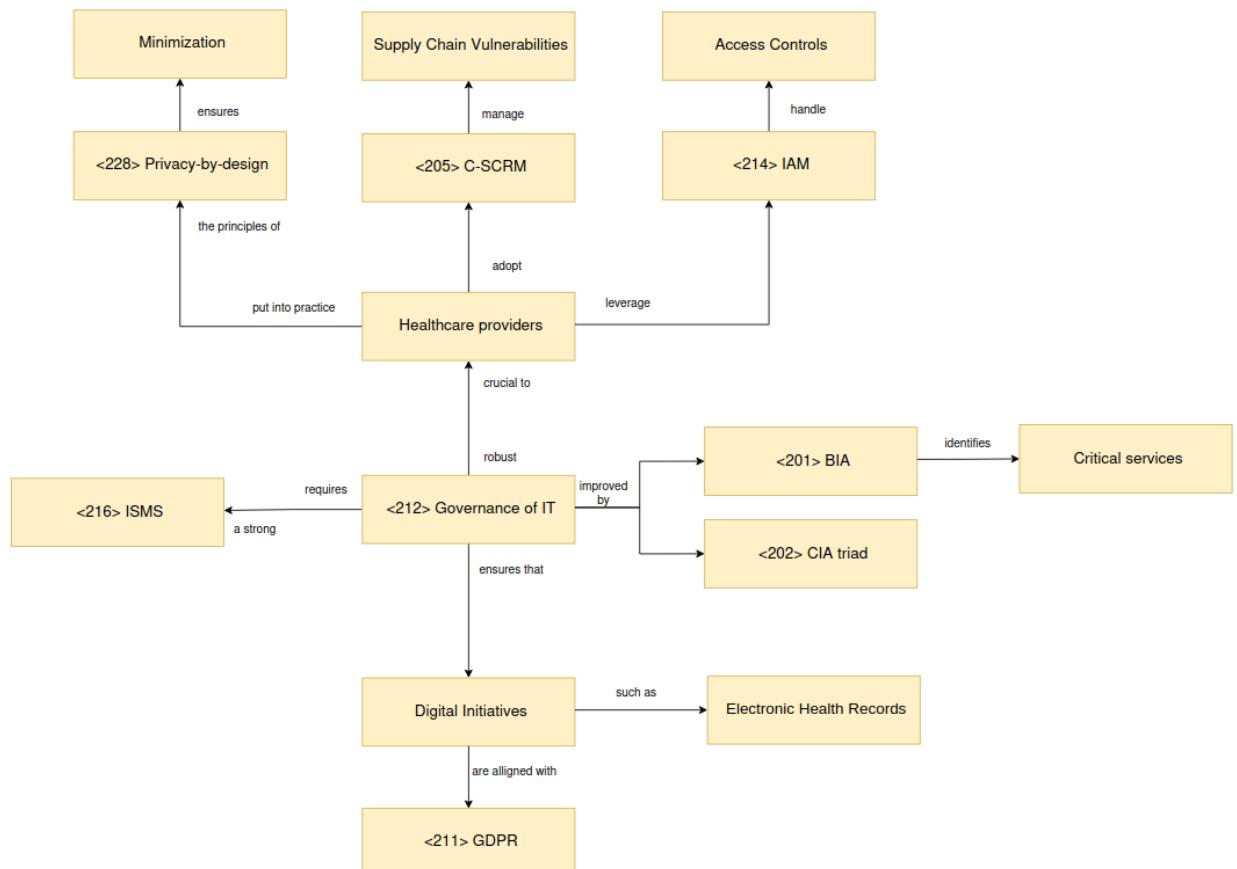
Theme 2 - Industry 8 - Healthcare

In the healthcare sector, effective <212> Governance of IT ensures that digital initiatives (such as electronic health records, telemedicine platforms, and inventory systems) are aligned with clinical priorities, patient safety, and regulatory mandates like <211> GDPR. Central to this governance is a mature <216> ISMS, which translates high-level directives into operational controls, incident-response procedures, and audit mechanisms.

A thorough <201> BIA informs both governance and management by identifying critical services (e.g., ICU monitoring, pharmacy dispensing) and defining recovery time objectives. Simultaneously, the <202> CIA triad underpins all security decisions: confidentiality guards patient privacy, integrity upholds clinical accuracy, and availability guarantees access to lifesaving information.

To manage supply-chain vulnerabilities, healthcare providers adopt <205> C-SCRM practices (screening medical device vendors and ensuring firmware updates) while leveraging <214> IAM solutions to enforce least-privilege access across diverse user groups. Embedding <228> Privacy-by-design principles in system development further ensures that consent flows and data-minimisation measures are integral from inception.

Together, these interlocking mechanisms form a cohesive framework: governance defines policy and accountability; the ISMS operationalises security; and specialised processes (BIA, C-SCRM, IAM, Privacy-by-design) deliver resilient, compliant, and patient-centric IT services.



Theme 1 - Banking and Financial Services vs Healthcare

In Banking and Financial Services, organisations operate as tightly-integrated systems of people, processes, and technology, underpinned by formal <112> Governance and <107> Corporate Governance structures. A hierarchical <126> Organisational Structure separates business lines, compliance and risk functions, and internal audit, following a clear <131> RACI to assign responsibilities across the <102> BoD, executive team, and three lines of defence. Their <120> Management System typically merges an ISO-based <216> ISMS with financial-quality frameworks, yielding high <121> Maturity: policies and <128> Procedures are codified, controls are automated, and <101> Audit cycles validate adherence to Basel, AML/KYC, and other <134> Regulatory Frameworks. A unified <113> GRC platform captures risk metrics (<135>), compliance findings (<106>), and key performance indicators (<116>), enabling the <108> CxO suite to steer strategic decisions with precision.

By contrast, Healthcare providers (whether public, private or not-for-profit) are mission-driven systems focused on patient outcomes and safety. Their <120> Management System blends clinical quality (often ISO 9001-certified <105>) with health-sector standards (HIPAA, FDA), yet governance maturity varies widely across hospitals and clinics. Multidisciplinary matrix teams share accountability through local ethics committees and an executive <102> BoD or health-authority board, often without the same level of process automation seen in banks. Risk and <115> Internal Control are managed via specialised clinical risk and safety offices, supported by <201> BIA and <103> Business Continuity plans focused on critical care systems. While both sectors leverage <113> GRC, healthcare relies more on manual workflows and peer reviews, reflecting a culture (<125>) that balances regulatory compliance (<106>) with fluid, patient-centric decision-making.

Theme 1 - Banking and Financial Services vs Healthcare

In Transport and Logistics, organisations are networked assemblages of carriers, warehouses, and third-party providers, governed through a federated <126> Organisational Structure that emphasises operational resilience and supply-chain integrity. Governance (<112>) roles are distributed across safety, procurement, and IT, with <131> RACI matrices guiding escalation to senior leadership and external regulators. Their <120> Management System often takes the form of an <114> IMS (integrating ISO 9001, ISO 14001, ISO 45001) to harmonise quality (<130>), environmental, and safety objectives. A modular <113> GRC approach stitches together vendor assessment (<232>), <205> C-SCRM, and continuous <233> Vulnerability Management, while <115> Internal Control functions conduct regular <101> Audit of carriers and terminals. Maturity (<121>) is driven by standardised <128> Procedures, digital track-and-trace platforms, and KPI-based dashboards that monitor on-time delivery, fuel efficiency, and incident rates, all feeding into <103> Business Continuity planning.

By comparison, Banking and Financial Services firms are centralised, process-centric organisations with a unified <420> Enterprise Architecture that aligns business operations, risk, and compliance under a single <120> Management System. Governance is anchored by a strong <102> BoD and three-lines-of-defence model, with a dedicated risk committee overseeing market, credit, and operational <135> Risks. Their <113> GRC suites enforce end-to-end <106> Compliance with financial regulations, embedding policies (<127>), controls, and automated <116> KPIs directly into trading, payments, and lending workflows. Through rigorous <110> Due Diligence and use of <230> SBOMs, banks govern third-party fintechs alongside in-house development, maintaining high governance maturity, even as digital transformations introduce new imperatives like Zero Trust and privacy-by-design.

Theme 2 - Transport and Logistics vs Banking and Financial Services

Transport and Logistics organisations often confront complex dependencies across multiple tiers of suppliers and carriers, making <205> C-SCRM indispensable for mapping and mitigating cybersecurity exposures throughout their networks. In this industry, ensuring uninterrupted operations demands rigorous <201> BIA processes to quantify how delays or system failures propagate over time, while continuous <233> Vulnerability Management identifies and prioritises flaws in fleet telematics or warehouse control systems.

By contrast, Banking and Financial Services firms emphasise the preservation of the <202> CIA triad within their digital platforms, relying on mature <216> ISMS frameworks to monitor transactional integrity and customer privacy. Both sectors share a need for robust identity controls, but whereas transport providers may outsource much of their perimeter defence to an <219> MSP or a specialised <220> MSSP, financial institutions frequently augment these services with in-house <214> IAM deployments that enforce stringent multi-factor authentication and session governance. Data residency and <207> Data Localization considerations impact both industries, logistics operators often store tracking and routing data in regional hubs for latency reasons, while banks must comply with the <211> GDPR for cross-border customer records.

Finally, as both sectors embrace digital transformation, they are converging on a <234> Zero Trust ethos, embedding <228> Privacy-by-design principles into system architectures so that resilience, compliance, and customer trust advance in parallel.

Theme 2 - Banking and Financial Services vs Healthcare

In the Banking and Financial Services sector, rigorous <212> Governance of IT frameworks orchestrate every technology initiative to satisfy complex regulatory demands. A certified <216> ISMS under ISO/IEC standards enshrines the <202> CIA triad across all digital channels (from real-time payment rails to mobile banking apps) while mature <217> ITSM processes ensure resilient service delivery and rapid incident resolution. Banks couple sophisticated <214> IAM deployments with strategic partnerships with <220> MSSPs to maintain continuous <233> Vulnerability Management across sprawling software estates. They leverage <230> SBOMs to trace third-party components and adhere to strict <207> Data Localization and <209> Data Residency rules, partitioning customer records among regional data centers to remain compliant with <211> GDPR. Underpinning these measures is a migration toward <234> Zero Trust architectures and embedding <228> Privacy-by-design principles to reinforce customer confidence and meet evolving threat landscapes.

By contrast, Healthcare organisations must safeguard deeply personal <223> PII in electronic medical records while ensuring that critical medical devices maintain uptime and integrity. They conduct thorough <201> BIA exercises to understand how system downtimes affect patient outcomes and extend <233> Vulnerability Management to cover both IT infrastructure and embedded device firmware. Through comprehensive <205> C-SCRM programs, hospitals vet suppliers of life-support and diagnostic equipment, using <230> SBOMs to identify vulnerable components ahead of deployment. Patient data sharing relies on robust <203> consent mechanisms (predominantly <221> opt-in processes) while integrated <216> ISMS and <217> ITSM functions support both regulatory compliance and clinical exigencies. Healthcare providers are adopting <234> Zero Trust models and <228> Privacy-by-design, tailoring them to high-pressure environments where rapid access to life-critical information must coexist with uncompromising data protection.

Transport & Logistics - Freight & Distribution

Business governance and business management

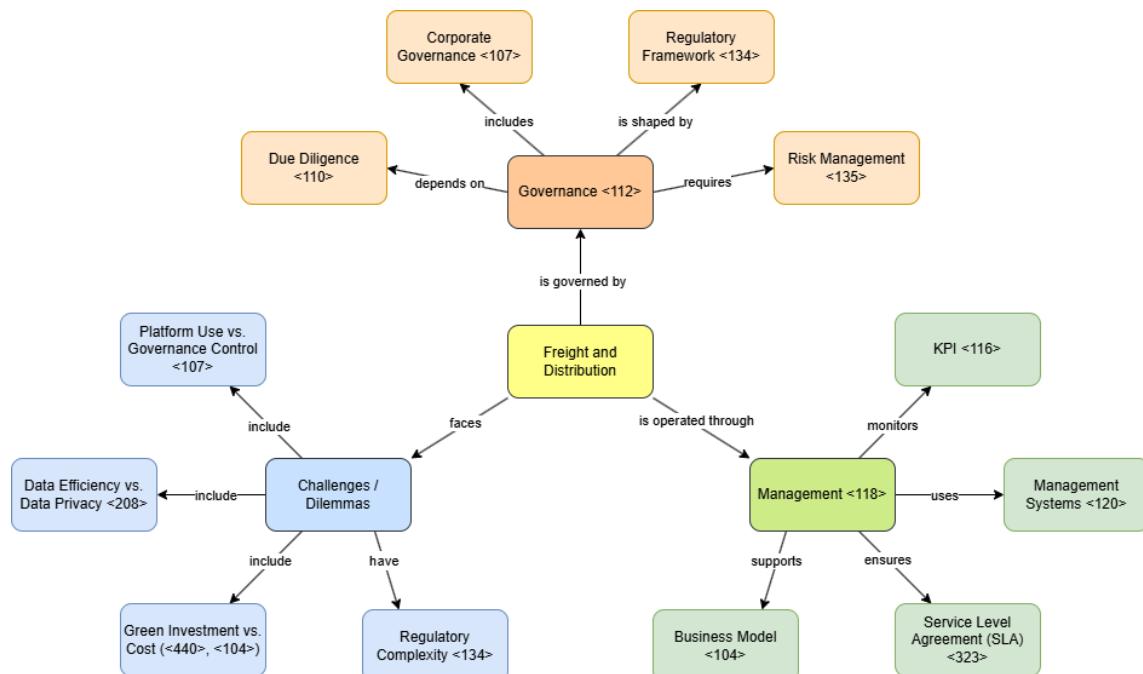
The Freight and Distribution sector is integral to the transportation and logistics industry, focusing on the movement of goods across various modes of transport, including road, rail, air, and sea. It involves the systematic planning, execution, and control of freight movement within supply chains, ensuring that goods flow seamlessly from manufacturers to retailers or end consumers.

This sector relies on effective Governance <112> and Management <118> to navigate complex logistics networks. Growing digitalisation, regulatory demands, and sustainability goals make these roles increasingly interconnected. Operators face strict Regulatory frameworks <134> such as customs laws, emissions standards, and digital freight data regulations like eFTI. Risk <135> oversight is essential and includes Operational Risk <317> such as delays, Cybersecurity <206> threats to digital platforms, and geopolitical instability that can disrupt supply chains. Sustainability targets must be integrated into the Sustainability Strategy<440> while aligning with Corporate Governance <107> principles and ensuring compliance <106> with environmental regulations and privacy standards.

Daily operations depend heavily on digital Management Systems <120> such as Learning Management Systems (LMS), which support routing, warehouse optimisation, and service tracking. To maintain reliability and competitiveness, companies must monitor KPIs <116> and comply with Service Level Agreements (SLAs <323>).

However, this landscape brings several strategic dilemmas. The use of real-time tracking enhances visibility but may conflict with Data Privacy <208> compliance. Environmental upgrades that support sustainability can also increase costs, creating tension with the Business Model <104>. Dependence on digital logistics platforms may undermine Corporate Governance <107> oversight, while efforts to harmonise rules across the EU must contend with the global diversity of Regulatory frameworks <134>.

Ultimately, governance and management in freight must work in tandem to balance operational efficiency, regulatory compliance, and long-term sustainability. This alignment is critical for ensuring business resilience and ongoing success in an increasingly complex environment.



Agriculture & Farming - Agri-Food Processing & Distribution

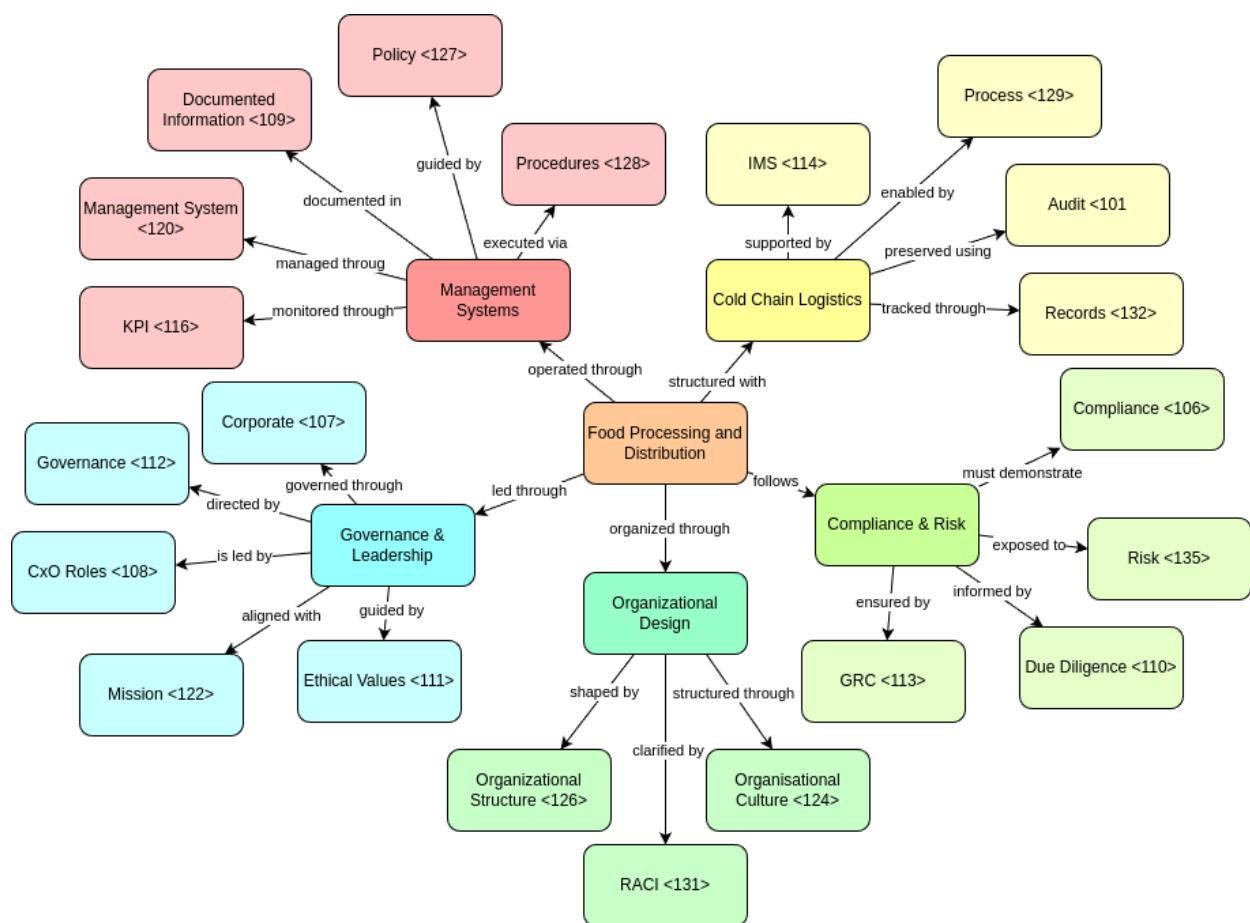
Business governance and business management

The Agri-Food Processing and Distribution industry is defined as the sector responsible for the transformation, packaging and movement of agricultural products from their primary sources, encompassing food manufacturing and the distribution of goods to consumers.

According to workforce development data from the Cambridgeshire & Peterborough region*, the sector increasingly relies on skilled labor to meet consumer and regulatory expectations. These operations are guided by Management Systems <120> that ensure Compliance <106> with food safety, traceability, and quality regulations, supported by attentive Documented Information <109> and Records Management <132>.

Technologies supporting cold chain logistics are critical in maintaining these products. These are integrated through Integrated Management Systems <114> that streamline Processes <129> under defined Policies <127> and Procedures <128>. The reliability of such systems enables effective Audits <101> and continuous monitoring via KPIs <116> to meet both operational and regulatory goals.

Oversight is managed through Governance <112> structures and Corporate Governance <107> principles, where CxO <108> roles lead strategic efforts. These leaders ensure alignment with the organization's Mission <122>, uphold Ethical Values <111>, and exercise Due Diligence <110> across supply chains. A clear Organizational Structure <126> and defined roles using frameworks like RACI <131> enhance coordination and accountability.



* - Cambridgeshire & Peterborough

<https://www.growthworkswitskills.com/lmi-hub/spotlight/local-industries/agriculture-food-processing/>

Healthcare - Pharmaceuticals & Devices

Business governance and business management

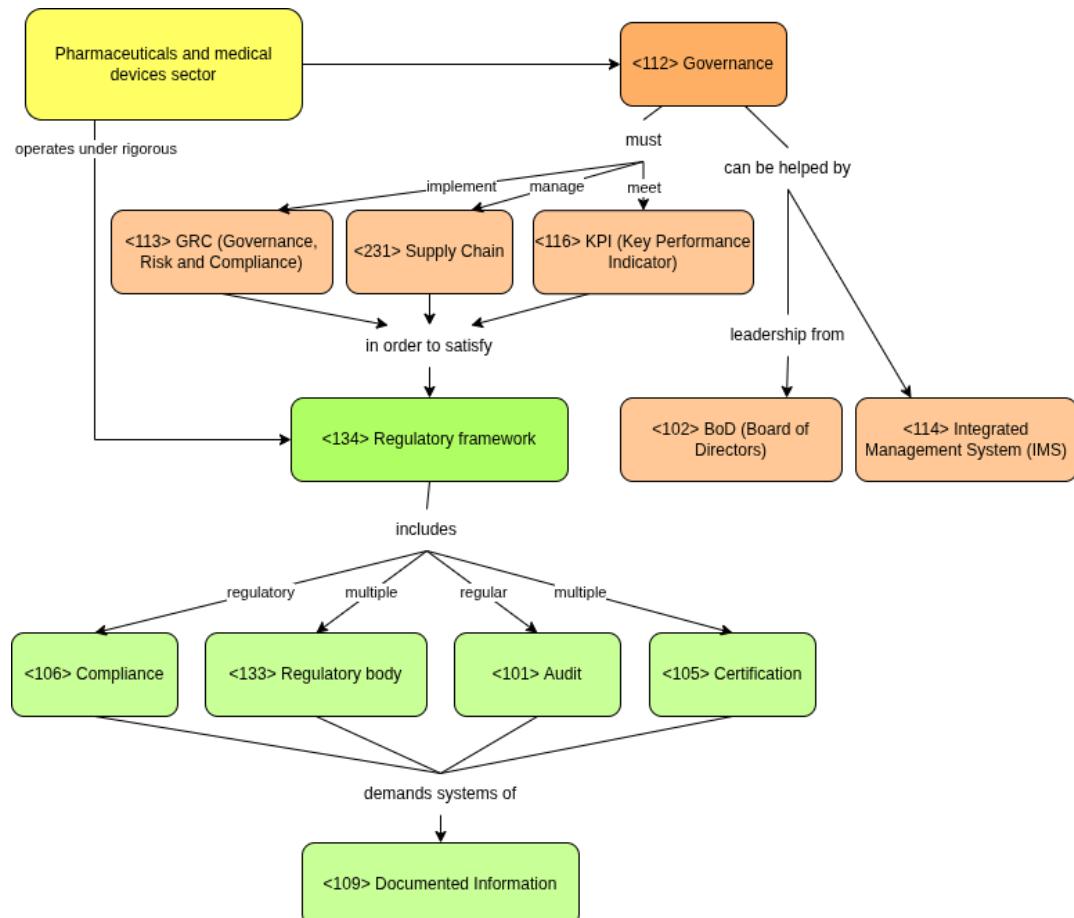
The pharmaceuticals and medical devices sector is a critical component of the healthcare industry. It is characterized by its essential role in delivering therapeutic and diagnostic innovations that support both individual and public health.

Consequently, the sector operates under some of the most rigorous regulatory frameworks <134>, where effective governance <112> must balance patient safety with Governance, Risk, and Compliance (GRC) (<113>) demands to effectively manage complex supply chains <231> and meet stringent quality standards.

Regulatory compliance <106> forms the foundation, with organizations needing to satisfy multiple regulatory bodies <133> including the FDA, EMA, and MDR. This demands comprehensive documented information <109> systems to ensure full product traceability from development through distribution. Regular audits <101> and certifications <105> like ISO 13485 validate these quality management systems.

Strategic governance requires alignment between innovation and compliance. Integrated Management Systems (IMS) <114> can harmonize these priorities, while leadership from the Board (BoD) <102> ensures proper oversight. Key metrics <116> should track both compliance performance and operational resilience.

In conclusion, a successful governance in this sector must create a system that is compliant and also adaptable. Embedding GRC <113> principles across all operations enables organizations to ensure patient safety while fostering a culture of innovation and adaptability.



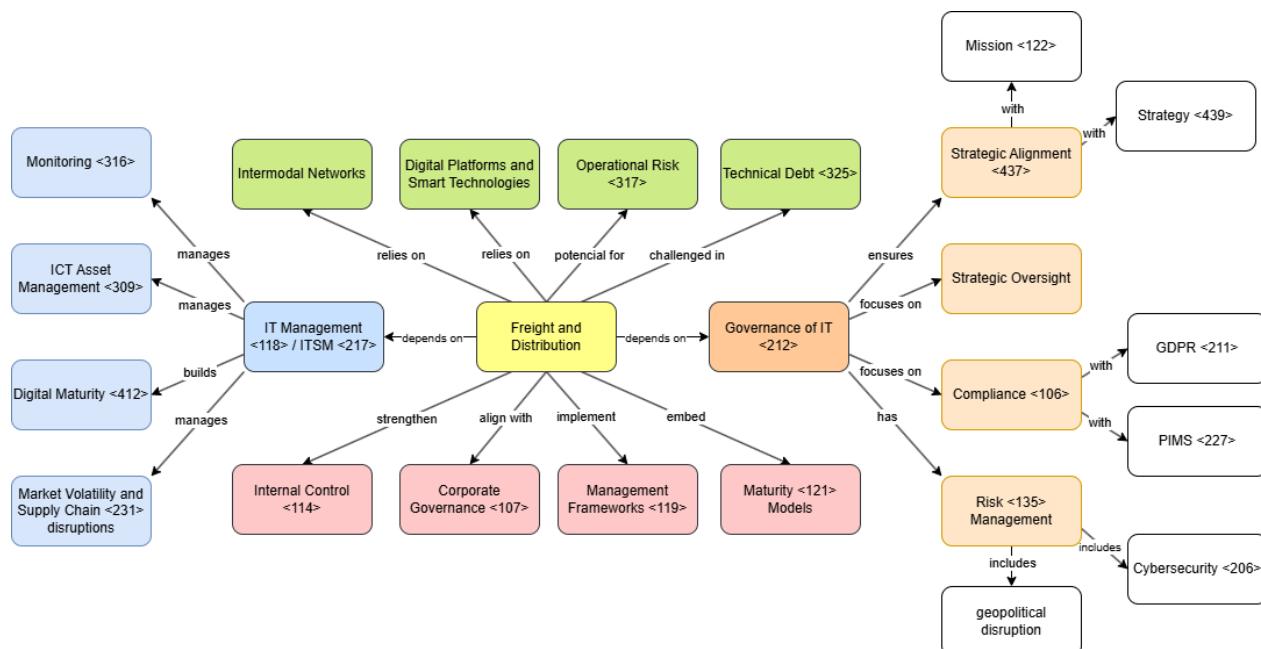
Transport & Logistics - Freight & Distribution

Governance of IT and IT Management

Freight and distribution, a core subdomain of the transport and logistics industry, increasingly relies on digital platforms and smart technologies. Managing the movement of goods across intermodal networks demands advanced IT coordination, presenting both opportunities and challenges for Governance of IT <212> and Management <118>. Ensuring alignment between Governance of IT <212>, which emphasizes strategic oversight, Compliance <106>, and value delivery, and ITSM (IT Service Management) <217>, focused on operations and performance, is critical.

These operations depend on Logistics Management Systems <120> and ICT Asset Management <309> tools, including Operational Technology (OT) <318> and telematics, for functions like inventory tracking and route optimisation. However, issues such as technical debt <325>, fragmented infrastructure, and disjointed data flows hinder effective coordination. Governance <112> must respond to increasing Compliance <106> requirements through frameworks like GDPR <211> and PIMS <227>, manage Cybersecurity <206> risks, and maintain Strategic Alignment <437> with the overall Mission <122> and Strategy <439> of logistics organisations.

Simultaneously, ITSM <217> must oversee hybrid infrastructures, ensure proper Monitoring <316> and Incident Response <310>, and build Digital Maturity <412> to stay resilient amid market volatility and Supply Chain <231> shocks. Advancing in this landscape requires Management Frameworks <119> that unify Management <118> and Corporate Governance <107> priorities, foster Maturity <121>, and reinforce Internal Control <114>—without which digitalisation may become a source of Operational Risk <317> rather than a driver of resilience.



Agriculture & Farming - Agri-Food Processing & Distribution

Governance of IT and IT Management

The Agri-Food Processing and Distribution industry encompasses processing, packaging and distribution of food and agricultural products. It includes activities such as food manufacturing, processing, logistics and distribution, bridging the gap between primary producers and end consumers.

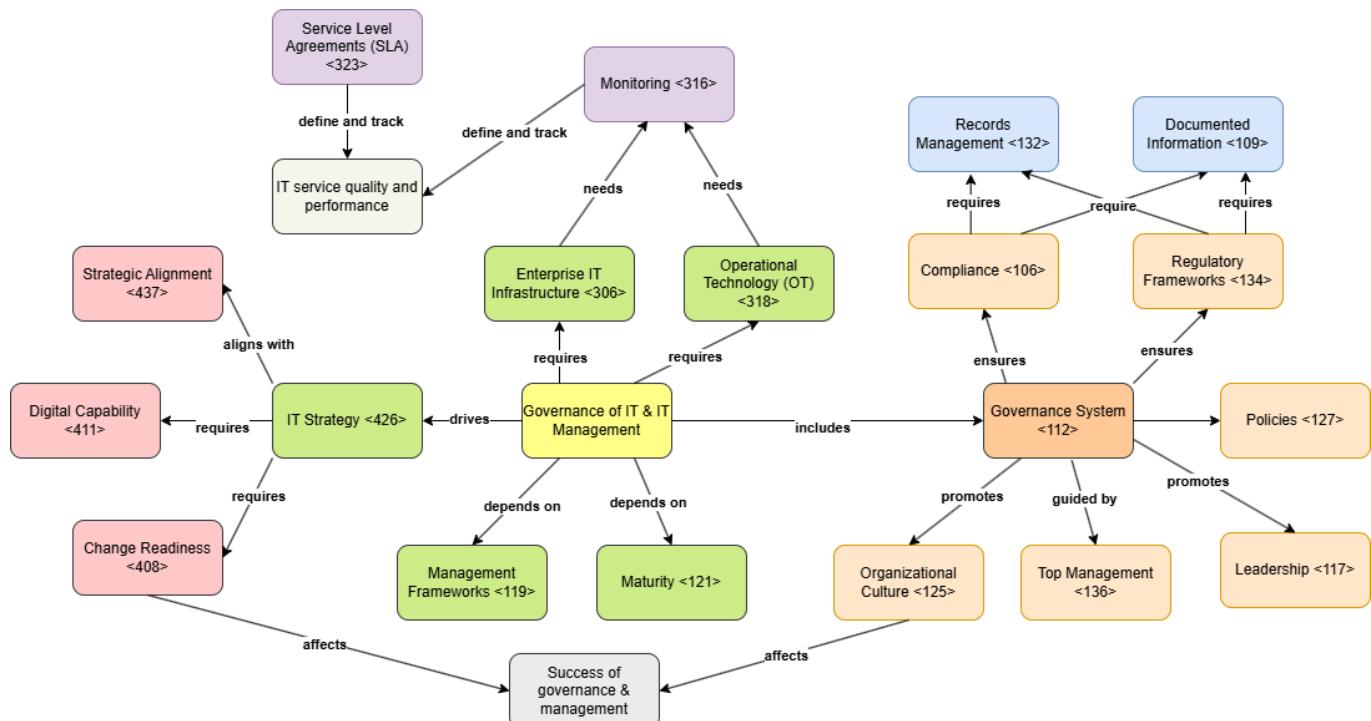
In this sector, Governance of IT and IT Management are critical to ensuring traceability and effective cold chain logistics. However, the sector often faces data fragmentation, where different actors operate isolated systems, hindering real-time coordination and complicating compliance [<106>](#) with sector regulations and broader regulatory frameworks [<134>](#).

A well-structured governance system [<112>](#) helps align IT investments with business objectives, supported by top management [<136>](#) and guided by a clear IT strategy [<426>](#). Yet in practice, many organizations—especially SMEs—lack the maturity [<121>](#) and management frameworks [<119>](#) needed for effective oversight and strategic alignment [<437>](#) between IT and business.

Cold chain logistics depend on Operational Technology (OT) [<318>](#) integrated with Enterprise IT Infrastructure [<306>](#), often monitored using IoT devices. This integration introduces complexity and regulatory exposure, and, to handle this, organizations benefit from solid documented information [<109>](#) and records management [<132>](#) practices.

Clearly defined policies [<127>](#) and procedures [<128>](#) reinforce governance by fostering accountability, consistency, and preparedness for audit [<101>](#). However, efforts to evolve these practices are often challenged by underdeveloped organizational culture [<125>](#) and low change readiness [<408>](#).

Innovation and agility in the sector require more than technology—it takes clear leadership [<117>](#), shared objectives, and the ability to coordinate IT and operations effectively. Strengthening this collaboration—frequently structured through service level agreements (SLAs) [<323>](#) and continuous monitoring [<316>](#)—is essential to delivering reliable and compliant services at scale.



Healthcare - Pharmaceuticals & Medical Devices

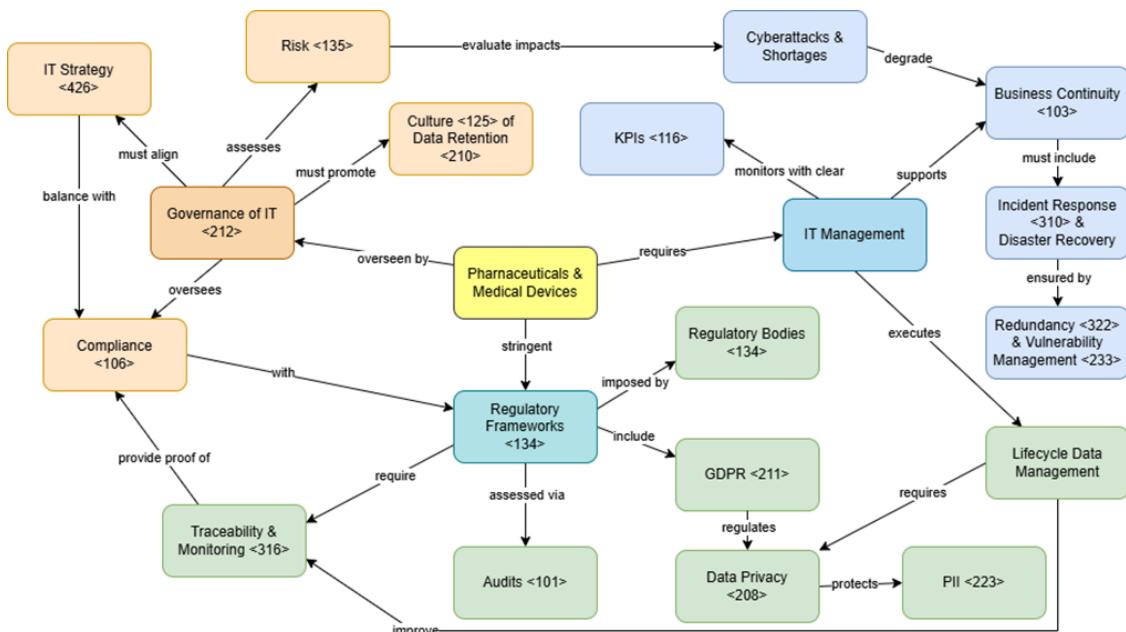
Governance of IT and IT Management

The pharmaceuticals and medical devices subdomain of healthcare is characterized by the research, development and manufacturing of drugs and medical technologies, followed by their supply to authorized distributors and retailers. It produces life-critical products intended to diagnose, treat or prevent diseases. The industry operates under stringent regulatory frameworks [<134>](#), and ITGM (Governance of IT [<212>](#) and IT Management) play a significant role in ensuring patient safety and quality assurance.

Pharmaceuticals and medical devices must comply with regulatory frameworks [<134>](#) set by bodies [<133>](#) like the FDA¹, in the US, and EMA² or MDR³, in the EU. Ensuring data integrity across the entire product lifecycle, from R&D⁴ to manufacturing and post-market, is essential to maintain traceability [<316>](#) for audits [<101>](#) and proof of compliance [<106>](#). Data privacy [<208>](#) is another critical concern, enforced by GDPR [<211>](#) in the EU, requiring secure handling of sensitive patient data (PII [<223>](#)). These can be achieved through strong data management, zero trust [<234>](#) security and vulnerability management [<233>](#), alongside fostering an organizational culture [<125>](#) of data retention [<210>](#) awareness.

Business continuity [<103>](#) is a high priority, requiring risk assessments of potential disruptions caused by cyberattacks like medicine shortages or medical device malfunctions. Organizations must implement disaster recovery plans that include redundancy [<322>](#) backups and alternative power sources, to ensure continuous availability, especially for life-saving treatments.

IT investments [<426>](#) must align with business goals, such as accelerating drug development with AI [<401>](#) and improving device interoperability, while ensuring compliance [<106>](#). Clear KPIs [<116>](#), including system uptime, compliance metrics and cybersecurity [<206>](#) posture, are key to achieve high digital health maturity [<412>](#).



1 - US Food & Drug Administration <https://www.fda.gov/>

2 - European Medicines Agency <https://www.ema.europa.eu/>

3 - Medical Device Regulation <https://www.medical-device-regulation.eu/>

BGM comparison - Transport & Logistics vs Agriculture & Farming

Freight and Distribution and Agri-Food Processing and Distribution both rely on structured governance, but their priorities diverge. Freight operations emphasize efficiency, punctuality, and regulatory compliance, governed by formal Corporate Governance [<107>](#) and led by senior CxO [<108>](#) roles. Risks focus on logistics delays and regulatory issues, managed through GRC [<113>](#) frameworks and role clarity using RACI [<131>](#).

Agri-Food, in contrast, must address food safety, perishability, and ethical concerns. Its governance integrates Ethical Values [<111>](#) and Governance [<112>](#) principles to maintain traceability and uphold Quality [<130>](#). Cold chain logistics and Audits [<101>](#) play a central role, and Documented Information [<109>](#) ensures compliance.

While both sectors use Management Systems [<120>](#), Freight focuses on route and warehouse optimization, whereas Agri-Food emphasizes quality control and traceability. Organizationally, Freight tends toward hierarchical Organizational Structures [<126>](#), while Agri-Food often coordinates across diverse partners. Each one reflects its main objective, efficiency in Freight (Mission [<122>](#)) and safety and sustainability in Agri-Food.

BGM comparison - Agriculture & Farming vs Healthcare

The Agri-Food Processing and Distribution and Pharmaceuticals and Medical Devices sectors share key priorities such as traceability and quality control [<130>](#), but diverge significantly in their business governance [<112>](#) structures and management [<118>](#) models.

In pharmaceuticals, governance [<112>](#) is centralized and tightly regulated. Agencies such as the EMA and FDA enforce strict compliance [<106>](#) regimes, requiring full product lifecycle traceability and certified quality systems (e.g., ISO 13485, a form of certification [<105>](#)). Business governance is formalized, typically supported by boards of directors (BoD) [<102>](#) and compliance [<106>](#) units. Management [<118>](#) practices are process-driven [<129>](#), focused on strategic alignment [<437>](#), risk management [<135>](#), regulatory assurance and controlled innovation.

In agri-food, governance [<112>](#) is more decentralized, reflecting the diversity of stakeholders, including smallholders, cooperatives, and large agribusinesses. Regulatory oversight focuses on food safety, environmental compliance, and supply chain [<231>](#) standards, but is often mediated by public agencies and sectoral organizations. Management [<118>](#) practices vary widely: while some firms implement integrated systems [<114>](#), many actors rely on informal or cooperative mechanisms, influenced by scale, infrastructure, and local policy frameworks.

In summary, pharmaceuticals rely on hierarchical, compliance-based governance [<106, 112>](#) and formal organizational structures [<126>](#), while the agri-food sector operates under flexible, multi-actor governance with heterogeneous management practices. Both depend on effective traceability, regulatory credibility, and certification [<105>](#) systems to succeed in complex and risk-sensitive [<135>](#) markets.

ITGM comparison - Transport & Logistics vs Agriculture & Farming

Both *Agri-Food Processing and Distribution* and *Freight and Distribution* rely heavily on efficient and reliable information systems to manage complexity and ensure service quality. However, their approaches to Governance of IT <212> and IT Management reflect sector-specific priorities and challenges.

In Agri-Food, the emphasis lies in traceability, cold chain logistics, and compliance with safety and quality standards. Here, governance mechanisms must ensure that IT and Operational Technology (OT) integrate to support real-time monitoring (e.g., temperature, humidity), often using IoT. This calls for clear IT strategy, top management support <136>, and structured records management <132> to meet regulatory demands. Still, many agri-food SMEs struggle with low maturity <121> and fragmented systems, making strategic alignment <437> between IT and business difficult.

By contrast, Freight and Distribution is driven by efficiency, scalability, and interoperability across intermodal systems. Governance here focuses on performance optimisation, with an emphasis on SLAs <323>, real-time tracking, and warehouse automation. IT Management must ensure system availability, data integration, and continuous monitoring <316> across a vast network of actors. While large logistics providers often have mature governance models, smaller players may lack consistent IT policy frameworks <127>/<128>, affecting service reliability.

Both sectors face change resistance <408> and require strong leadership <117> to align evolving technologies with operational realities. Yet while Agri-Food governance often stems from regulatory pressure, Freight IT governance is usually performance-driven, aiming to reduce delivery times and costs.

ITGM comparison - Transport & Logistics vs Healthcare

The niche of pharmaceuticals and medical devices prioritizes governance of IT <212> and IT management to ensure regulatory compliance <106> and patient safety, while freight and distribution emphasizes operational resilience and cost efficiency. Despite differing priorities, both manage complex IT systems <306>.

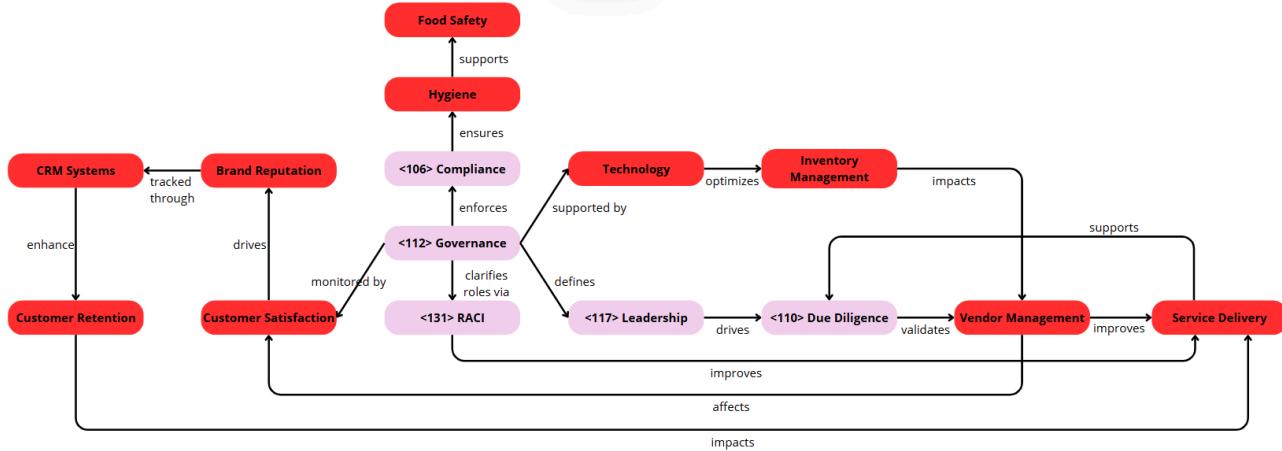
In pharmaceuticals and medical devices, ITSM <217> must be aligned to support secure drug development, EHRs integrity and medical device interoperability, all while adhering to strict regulatory frameworks <134>. This importance of compliance <106> requires focus on cybersecurity <206>, and as result CISOs <108> typically maintain high autonomy to mitigate data privacy <208> risks affecting patient safety or intellectual property.

In contrast, freight and distribution IT strategy <426> target route optimization, warehouse automation and real-time monitoring, aiming to reduce delays and costs. Unlike healthcare, CISO <108> often have less board <102> visibility unless major incidents occur, highlighting differences in cyber governance maturity <121>.

Cyber threats in both sectors have serious consequences. Pharmaceuticals and medical devices involve life-critical stakes needing fast incident response <310> and failover systems <308>. In freight and distribution, disruptions in supply chains <231>, especially for pharma, can lead to shortages and widespread societal impacts. Both sectors share a need for high digital maturity <412> to ensure business continuity <103> and adapt to disruptions <303>, such as re-routing shipments.

Additionally, traceability and monitoring <316> is crucial in both industries. Pharmaceutical and medical device organizations require documented proofs <109> to comply with stringent regulations <133>, while freight and distribution leverage real-time tracking to enhance logistics operations.

Industry 5 (Food and Beverage) - Theme 1



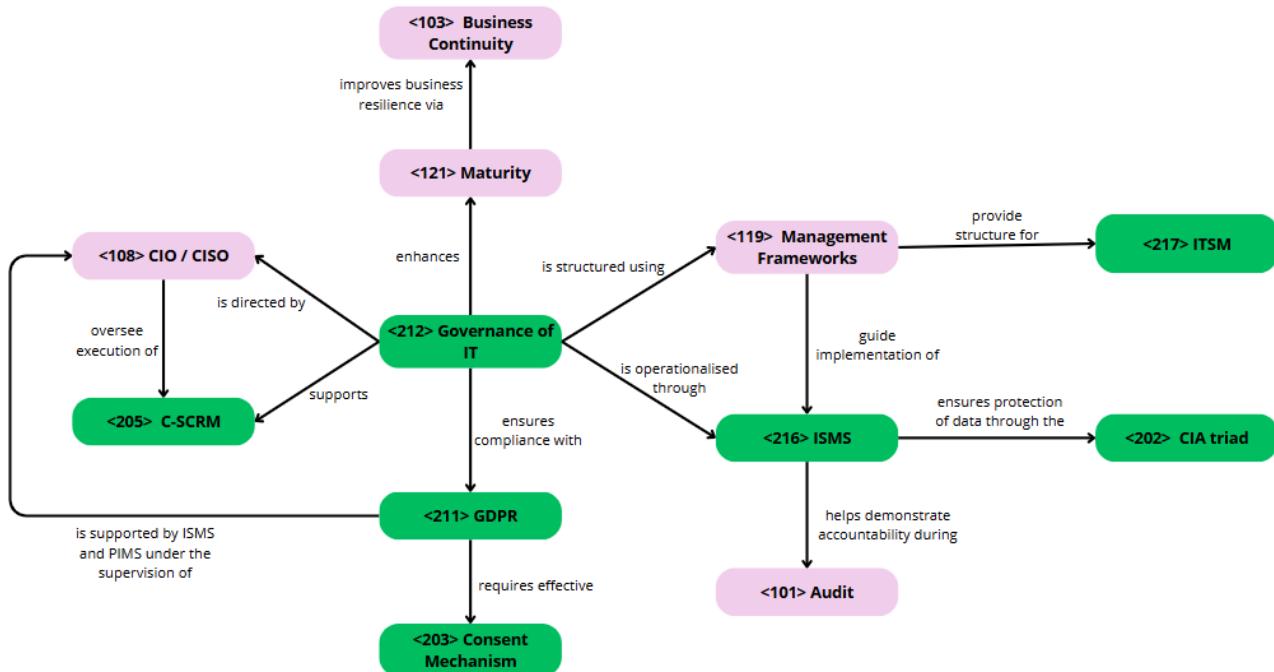
The **Food & Beverage (F&B) industry** encompasses all businesses involved in the preparation, processing, packaging, distribution and service of food and beverages. It includes a wide range of organizations, from farms and food manufacturers to restaurants, retailers and service providers. This industry is characterized by strict regulatory oversight, high consumer expectations and a constant need for innovation and efficiency in both operations and customer engagement.

In this context, **<117> Leadership** plays a central role by defining the strategic direction and ensuring alignment between operations and organizational goals. Strong **<112> Governance** is essential, as it enforces **<106> Compliance** with food safety regulations and operational standards. Governance efforts are supported by **<110> Due Diligence**, which ensures that supplier practices meet required standards through effective Vendor Management. This enhances traceability and quality assurance across the supply chain.

Moreover, to reduce **<131> RACI** Ambiguity in Service Delivery, it is vital to clearly assign roles and responsibilities, which improves execution and directly impacts Customer Satisfaction. In the F&B sector, Customer Satisfaction is a key driver of Brand Reputation. This reputation is increasingly managed through digital platforms such as CRM Systems, which help foster Customer Retention by personalizing communication, managing feedback and optimizing loyalty programs through the use of technology.

On the operational side, technology plays a critical role in areas like Inventory Management, where real-time tracking systems and ERP tools help reduce waste and maintain product availability. Additionally, strict Hygiene standards underpin Food Safety by ensuring that sanitation protocols are consistently applied and monitored, an essential requirement in every segment of the F&B industry.

Industry 5 (Food and Beverage) - Theme 2

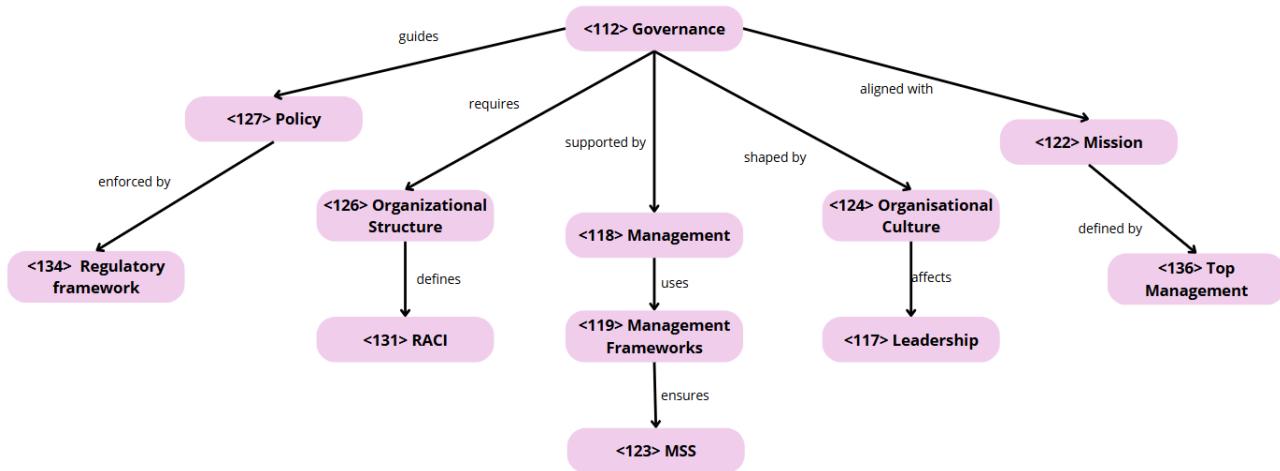


The Food & Beverage (F&B) industry increasingly depends on digital systems for operations and customer interaction, making the **<212> Governance of IT** essential. In F&B organisations, executives such as the **<108> CIO** or **CISO** are responsible for aligning IT with strategy, supported by **<119> management frameworks** like COBIT and ITIL. These frameworks guide decisions and ensure accountability across distributed environments.

To operationalise **<112> Governance**, F&B firms adopt **<216> ISMS**, and particularly **<227> PIMS**, to manage security and privacy risks, particularly under **<211> GDPR**. These systems, often part of an **<114> Integrated Management System**, help ensure **<106> Compliance** with **<305> data protection** rules and service reliability. IT operations are managed using **<217> ITSM** practices, covering platforms such as POS, CRM and loyalty systems.

Furthermore, the industry faces critical **<135> risks**, including **<206> cybersecurity** threats and data misuse. **<203> Consent mechanisms** like **<221> opt-in** approaches are essential for legal data processing, while **<215> InfoSec** practices, such as **<202> CIA triad**, ensure confidentiality, integrity and availability. With increasing third-party dependencies, **<205> C-SCRM** is also adopted to assess supplier risks.

Industry 6 (Investment Banking) - Theme 1



Commercial and Investment Banking refers to the financial services that provide corporate lending, capital markets operation, and advisory services. These institutions are core to the global economy, facilitating large-scale financial transactions and investment activities. Due to their systemic importance and exposure to cyber and operational risks, they operate under strict regulatory oversight and require robust IT governance frameworks.

Governance is crucial in commercial and investment banking to guarantee control, adherence to regulations and alignment with corporate strategy. **<112> Governance**, which outlines decision-making roles and procedures, is at the core. Clear **<127> policies** that are influenced by stringent **<134> regulatory frameworks**, such as Basel III and AML/KYC laws, are used to implement it.

A strong **<126> Organizational Structure** is crucial in such high-risk environments. **<131> RACI** models are used by banks to define roles and guarantee accountability in intricate operations such as trading or compliance.

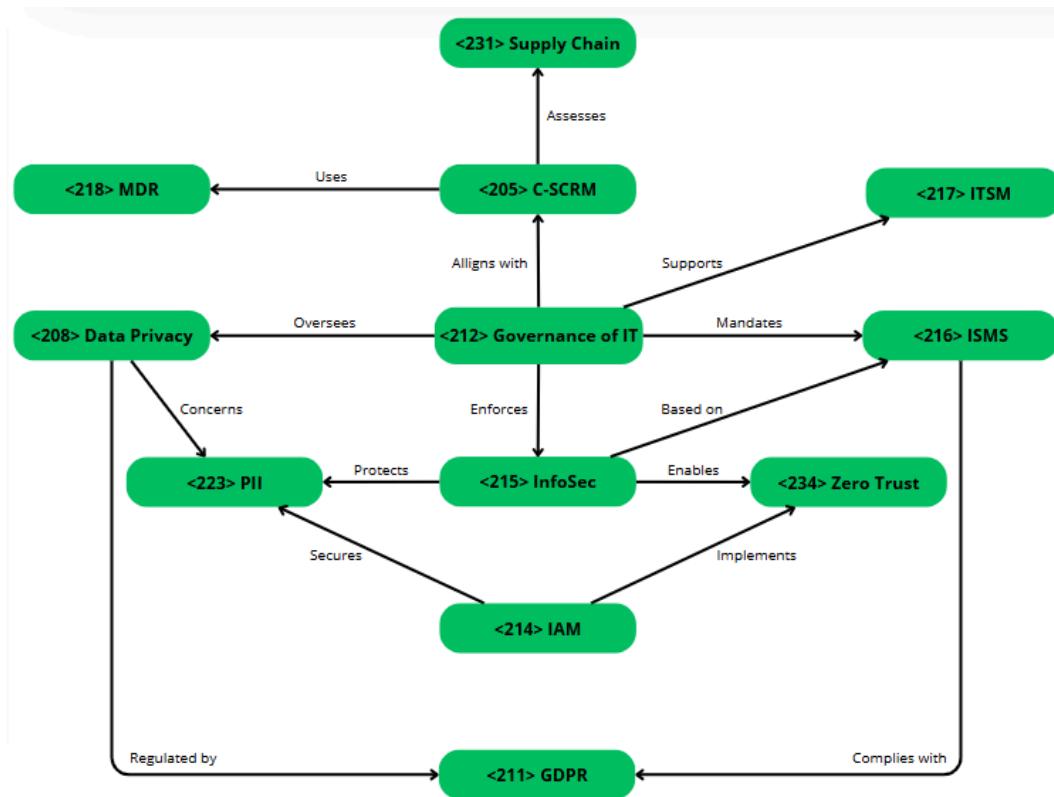
<118> Management operationalizes governance by structuring service delivery and risk control using **<119> Management Frameworks** (e.g., COBIT, ITIL). **<123> Management System Standards**, such as ISO/IEC 27001, frequently support these frameworks, particularly when it comes to information security.

Beyond structure, organizational culture has an impact on governance, affecting how regulations are adhered to and risks are managed. To reinforce accountability and set an example of moral behavior, strong **<117> leadership** is required.

Every governance mechanism is linked to the bank's **<122> Mission**, which is established by **<136> Top Management** and includes goals like stability and sustainable growth. This alignment guarantees that governance choices support long-range strategic objectives.

Governance in this sector is more than just control; it's about making sure that leadership, culture, regulations and strategic intent all work together in a highly regulated, high-stakes sector.

Industry 6 (Investment Banking) - Theme 2



In **Commercial and Investment Banking**, **<212> Governance of IT** is vital for maintaining operational continuity, regulatory compliance and digital resilience. Given the critical and regulated nature of these institutions, governance integrates IT with risk management and compliance frameworks.

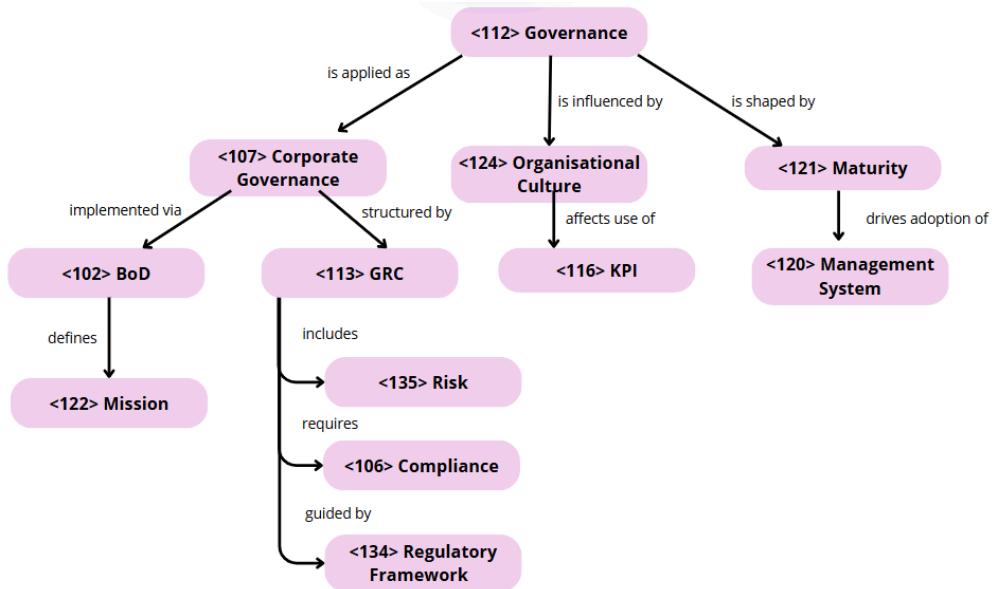
A key enabler is **<217> ITSM**, which ensures IT services align with business and legal expectations. **<215> InfoSec** provides the security foundation, supported by **<216> ISMS**, which defines controls and ensures compliance with standards like **<211> GDPR**, which governs how this data is stored and shared, helping protect both legal standing and customer trust.

Managing **<208> Data Privacy** is essential, due to the volume of sensitive **<223> PII**. Access is secured via **<214> IAM**, enforcing least-privilege principles and enabling **<234> Zero Trust**, which verifies every access request. This is critical for mitigating insider threats and credential misuse.

Externally, **<205> C-SCRM** helps manage third-party risks across the **<231> Supply Chain**, especially as functions are outsourced to cloud and fintech partners. This is enhanced by **<218> MDR**, offering real-time threat detection and response.

Together, these practices create a mature IT governance framework, essential for safeguarding investment banks in a high-risk high-regulation digital landscape.

Industry 7 (Dairy farming) - Theme 1



Dairy farming refers to the agricultural activity focused on the production of milk and its derivatives. It includes both small family-run farms and large-scale cooperatives, making it a structurally diverse sector. While some operations follow traditional, informal practices, others are governed through formal frameworks, particularly when integrated into broader supply chains.

In cooperative settings, **<107> Corporate Governance** is typically exercised through a **<102> Board of Directors (BoD)**, which defines the organisation's **<122> Mission** and ensures alignment with ethical standards and performance goals.

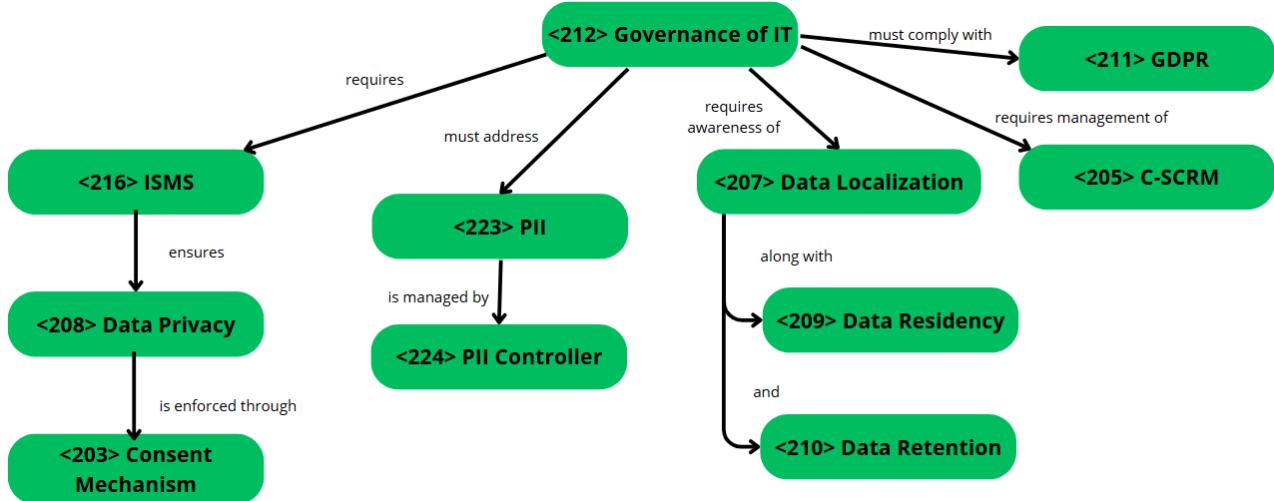
A strong **<113> GRC framework** is required to manage key **<135> Risks**, such as disease outbreaks, climate volatility, and price fluctuations. **<106> Compliance** with **<134> Regulatory Frameworks**, especially those related to food safety and animal welfare under EU law, is enforced through **<101> Audits** and **<105> Certifications**, supported by **<115> Internal Control** mechanisms.

<124> Organisational Culture varies greatly across the sector. Traditional farms may resist formalisation, while professional cooperatives promote **<109> Documented Information** and enforce **<127> Policies** to standardise operations.

<116> KPIs, such as milk yield, hygiene performance, or antibiotic use, are increasingly used to monitor outcomes. However, governance **<121> Maturity** remains uneven. While some actors adopt **<120> Management Systems** based on **<123> MSS**, many small producers still operate with informal structures.

This disparity often results from unequal access to resources, training, and the influence of **<133> Regulatory Bodies**. Strengthening governance capabilities across all farm types is essential to ensure resilience, accountability, and long-term sustainability in the dairy sector.

Industry 7 (Dairy farming) - Theme 2



Although increasingly digitised, dairy farming remains a sector where formal **<212> Governance of IT** is weak or absent. Digital tools such as automated milking systems, herd health sensors and farm management platforms are now common, but their adoption is often fragmented and poorly coordinated. Most farms show low **<121> Maturity**, with IT decisions frequently outsourced to vendors or handled informally by non-specialised staff.

This digital expansion brings growing responsibility. Many farms collect **<223> Personally Identifiable Information (PII)**, including worker records, animal treatment logs, geolocation data, and production outputs. Yet awareness of **<208> Data Privacy** and compliance with **<211> GDPR** remains limited. **<203> Consent Mechanisms** are rarely established, even when data is processed by third-party software used in cooperatives or public programmes.

In more structured environments, such as national cooperatives, **<224> PII Controllers** may be appointed, but this is uncommon at the level of small or independent producers. The absence of **<216> Information Security Management Systems (ISMS)** leads to inconsistent practices in data protection, access control, and breach response.

Smart farming technologies depend heavily on cloud platforms and connected devices. However, **<205> Cybersecurity Supply Chain Risk Management (C-SCRM)** is virtually nonexistent, despite increasing reliance on external service providers for data storage, equipment maintenance, and software updates.

Furthermore, few actors actively manage **<207> Data Localization**, **<209> Data Residency**, or **<210> Data Retention**, especially when using international software. Weak or nonexistent **<214> Identity and Access Management (IAM)** means systems are often accessed by multiple users without role-based control, increasing vulnerability.

To ensure ethical, resilient and compliant digital operations in dairy farming, IT governance must evolve, integrating security standards, clarifying responsibilities, and building digital awareness throughout the production chain.

Comparison Industries 5 and 7 (Theme 1)

The Food & Beverage (F&B) industry is a highly regulated sector that includes companies involved in the production, processing, packaging, distribution, and service of food and beverages. Its complex and interconnected value chain requires robust digital oversight, especially due to strict food safety regulations and increasing consumer expectations.

In this sector, IT **<112> Governance** is formalized and supported by structured **<119> management frameworks** such as COBIT and ITIL. These are implemented under the leadership of **<108> CxO-level roles** (e.g., CIO, CISO), enabling strong **<106> Compliance** through frequent **<101> Audits**, comprehensive **<115> Internal Controls**, and clearly documented **<127> Policies**. As a result, the F&B sector demonstrates a high **<121> Maturity** level in managing digital systems and risks.

In contrast, the Dairy Farming industry is characterized by decentralized and less formal IT governance. Technology-related decisions are typically made at the operational level, often by farm managers or technicians, without the oversight of specialized **<108> CxOs**. While the sector has begun to adopt precision agriculture technologies, it lacks standardized **<119> frameworks** and formal **<101> Audit** practices. This results in a comparatively lower **<121> Maturity** level, with compliance efforts focusing more on operational safety and food hygiene than digital or data governance.

Both industries face increasing **<135> Risks** from digitalization, such as cyber threats and data breaches. However, the F&B sector's structured approach, through integrated **<120> Management Systems**, offers a stronger defense in terms of cybersecurity and regulatory adaptation. As digital transformation progresses, the Dairy sector may benefit from adopting elements of the F&B model to enhance its governance and risk management capabilities.

-----//-----

Comparison Industries 5 and 7 (Theme 2)

<212> Governance of IT in the Food & Beverage (F&B) industry is typically formalised through **<119> management frameworks** (e.g., COBIT, ITIL) and led by **<108> CxO** roles such as CIOs or CISOs. These organisations implement **<216> ISMS**, like **<227> PIMS**, to manage **<215> InfoSec** and comply with **<211> GDPR**, especially in platforms handling customer data. IT operations are structured via **<217> ITSM** practices, ensuring alignment with business strategy and clear accountability.

In contrast, the Dairy Farming sector shows lower **<121> maturity** in **<212> Governance of IT**. Although it uses digital tools for automation and traceability, it lacks formal frameworks or dedicated leadership. **<216> ISMS** adoption is rare and IT decisions are often decentralised or vendor-driven. **<101> Audits** and **<105> certifications** are uncommon and **<135> risk** management is generally reactive, focused on operational continuity rather than **<206> cybersecurity**. There is limited awareness or implementation of **<205> C-SCRM**, despite increasing dependence on connected equipment and external service providers.

Overall, F&B demonstrates a more integrated and proactive governance model, with structured risk mitigation and compliance mechanisms, while Dairy Farming remains functional and informal, reflecting lower regulatory demands and the more peripheral role of IT in its core operations. Nonetheless, both industries recognise the importance of IT in sustaining operations and reducing uncertainty. As digital systems become more embedded, both sectors are increasingly aware of data integrity, system availability and **<106> compliance** obligations, even if their approaches differ significantly in structure and **<121> maturity**.

Comparison Industries 6 and 7 (Theme 1)

Because of their size, level of regulation, and strategic maturity, investment banking and dairy farming offer two radically different governance environments. In the highly regulated and globalized world of investment banking, governance is formally defined and closely linked to strategic oversight. To clearly assign accountability in high-risk operations, banks use **<126> Organizational Structures** that are enforced by **<131> RACI** models. These structures are reinforced by **<119> Management Frameworks** and **<123> Management System Standards** (e.g., ISO/IEC 27001), and they are supported by **<127> Policies** that adhere to intricate **<134> Regulatory Frameworks** like Basel III and AML/KYC.

On the other hand, community-based and informal governance is common in dairy farming, especially among small or independent producers. Many farms lack formal **<115> Internal Controls** and **<101> Audits**, even though some cooperatives define a **<122> Mission** of sustainability and practice **<107> Corporate Governance** through a **<102> Board of Directors**. Traditional **<124> organizational culture** and operational procedures are more important to governance than formalized frameworks. The primary focus of risk management and **<106> compliance** is on environmental standards, animal welfare, and hygiene, which are regulated by **<134> regulatory frameworks** (such as EU food safety).

There are also notable differences in leadership. In banking, mission-driven governance is guided by **<117> Leadership**, which is professionalized and linked to **<136> Top Management**. Leadership in dairy farming is more decentralized and influenced by cooperative norms or family dynamics. In conclusion, dairy farming is more dispersed and informal, whereas investment banking exhibits high **<121> maturity** and integrated governance.

-----//-----

Comparison Industries 6 and 5 (Theme 2)

Food and Beverage and Investment Banking represent two highly distinct environments in their approach to IT Governance and Management. While both rely on digital systems, their governance priorities and maturity levels differ significantly. In **Investment Banking**, governance is a structured, top-down function integrated into risk and compliance strategy. Regulatory oversight demands frameworks such as **<216> ISMS**, ensuring cybersecurity and data integrity. Protection of sensitive data like **<223> PII** is enforced through **<211> GDPR**, supported by access controls like **<214> IAM**. Third-party risk is managed via **<205> C-SCRM**, which evaluates the digital supply chain and enforces vendor accountability. IT plays a strategic role and is core to institutional trust and regulatory compliance.

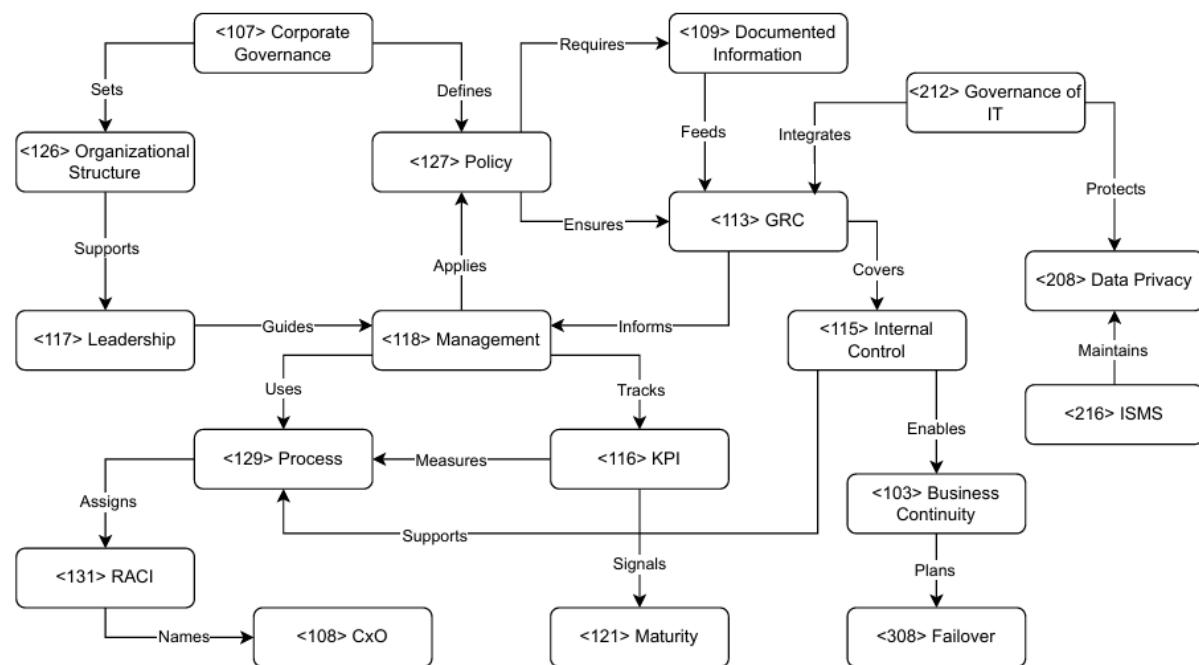
In contrast, **Food and Beverage** takes a more decentralized, operational approach. Digital tools support payments, reservations and loyalty systems, but governance varies widely. Larger chains may apply structured strategies, while smaller operators rely on **<204> Consultants** or informal decision-making. Though **<211> GDPR** compliance exists, **<208> Data Privacy** is often addressed reactively. With less regulatory pressure, governance focuses more on customer service and business continuity than on formal risk controls.

Overall, **<212> Governance of IT** in Investment Banking is proactive and deeply institutionalized, while in Food and Beverage it is service-driven, flexible, and often less formalized.

Group 568 , Students numbers: 103095, 103603, 104147, 104156

5 Hospitality and Leisure (Theme: Governance)

Chosen Niche: Accommodation



In accommodation services, the board and top leaders set clear rules about how the business should run and grow. This **<107>** corporate governance decides the main **<126>** organizational structure, making sure everyone from **<108>** chief officers to front-line managers knows their role. Good **<117>** leadership creates a friendly work culture where staff feel valued and work to provide great guest experiences.

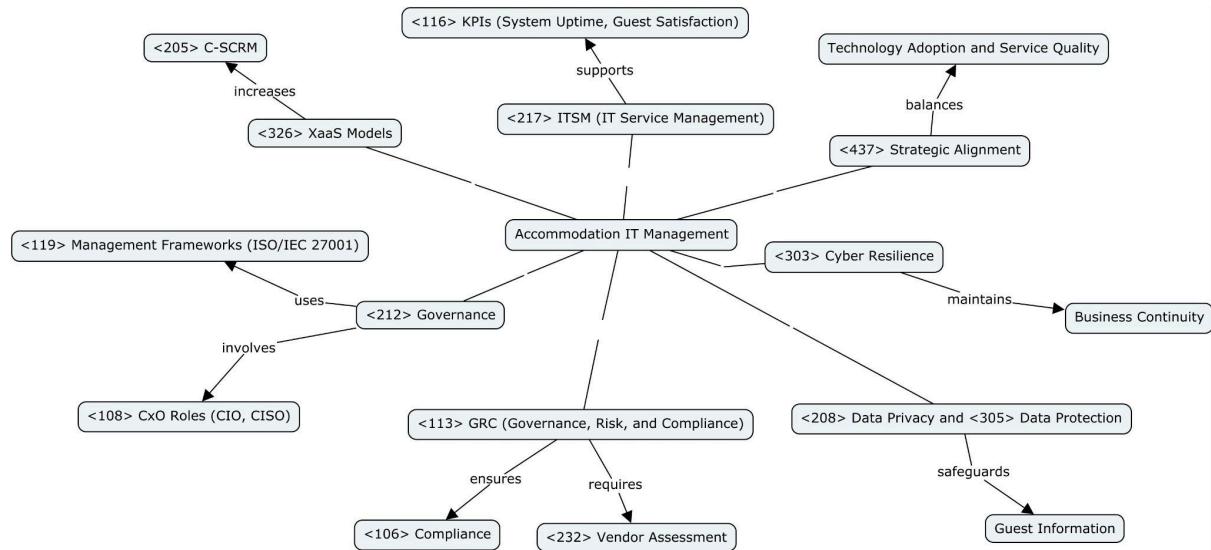
Day-to-day **<118>** management turns these rules into real actions by writing **<127>** policies for things like safety checks, cleaning standards, and handling guest data. These policies ensure the company follows laws and standards, such as health inspections and privacy rules. A combined system for **<112>** governance, **<135>** risk, and **<106>** compliance helps spot and handle dangers—from fires to unhappy guests—before they become big problems.

Behind the scenes, **<115>** internal control and proven **<119>** management frameworks support a plan to keep the business running (**<103>**) even during crises, like storms or power failures. Every important step—from booking a room to a guest’s checkout—is mapped out as a **<129>** process and stored in clear **<109>** documents. A **<131>** RACI chart shows who is responsible, accountable, consulted, or informed for each task, so no one is ever confused about their duties.

Managers also watch **<116>** key performance indicators like occupancy rates and guest feedback scores. These figures feed into regular **<101>** audits that check how **<121>** mature and reliable the company’s systems are. Finally, as hotels rely more on online bookings and smart devices, **<212>** IT governance works with the overall **<426>** IT strategy to keep systems safe and up to date. An **<216>** information security management system makes sure guest data stays private (**<208>**) and that the network is protected against cyber threats.

5 Hospitality and Leisure (Theme: IT Management)

Chosen Niche: Accommodation



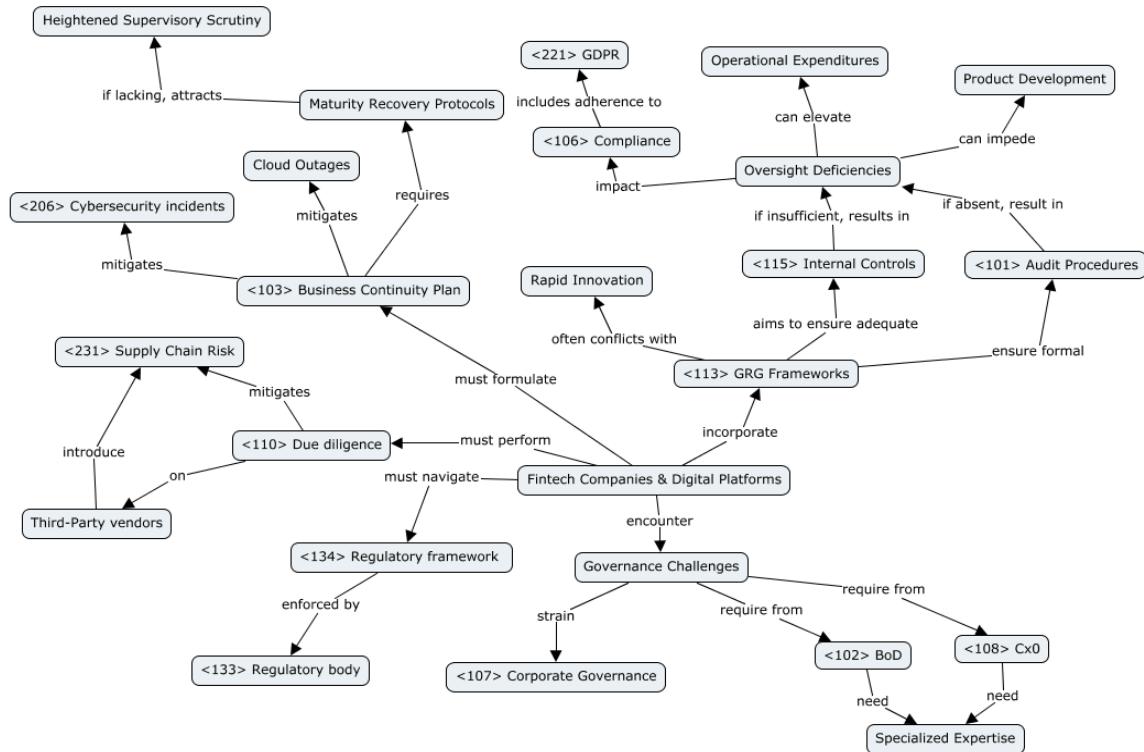
The accommodation niche within the (<112>) Hospitality and Leisure industry faces unique <113> GRC (Governance, Risk, and Compliance) challenges as digital platforms become central to operations. Modern hotels and short-term rentals rely on <323> SLAs (Service Level Agreements) with technology vendors for property management and guest services, demanding robust <232> Vendor Assessment and <205> C-SCRM (Cybersecurity Supply Chain Risk Management) to ensure <106> Compliance with regulations such as <211> GDPR. The growing use of <326> XaaS (Everything as a Service) models increases operational agility but also introduces new risks around data privacy, service continuity, and vendor dependency.

Effective <212> Governance of IT in accommodation requires clear <108> CxO roles (especially the CIO and CISO) to align digital strategy with business objectives and regulatory obligations. Adoption of <119> Management Frameworks like <123> ISO/IEC 27001 for information security and <217> ITSM (IT Service Management) ensures structured processes for incident response, risk management, and quality assurance. <116> KPIs (Key Performance Indicators) such as system uptime, guest satisfaction, and data breach incidents are critical for monitoring performance and supporting continuous improvement.

As digital transformation accelerates, accommodation providers must balance <437> Strategic Alignment between technology adoption and service quality. <303> Cyber Resilience is essential to maintain <103> Business Continuity amid cyber threats, while <208> Data Privacy and <305> Data Protection are vital for safeguarding guest information. Ultimately, the maturity of IT management in this niche depends on integrating sector-specific standards, proactive risk assessment, and adaptive governance to meet evolving guest expectations and regulatory landscapes.

6 Banking and Financial Services (Theme: Governance)

Chosen Niche: Fintech and Digital Platforms



Fintech companies and digital platforms encounter considerable governance challenges arising from stringent regulatory requirements and multilayered supervision. Boards of Directors <102> and chief officers <108> must demonstrate proficiency in advanced technologies, including artificial intelligence driven credit scoring and decentralized finance, alongside comprehensive knowledge of evolving regulatory standards. The attraction and retention of such specialized expertise represents a substantial governance concern.

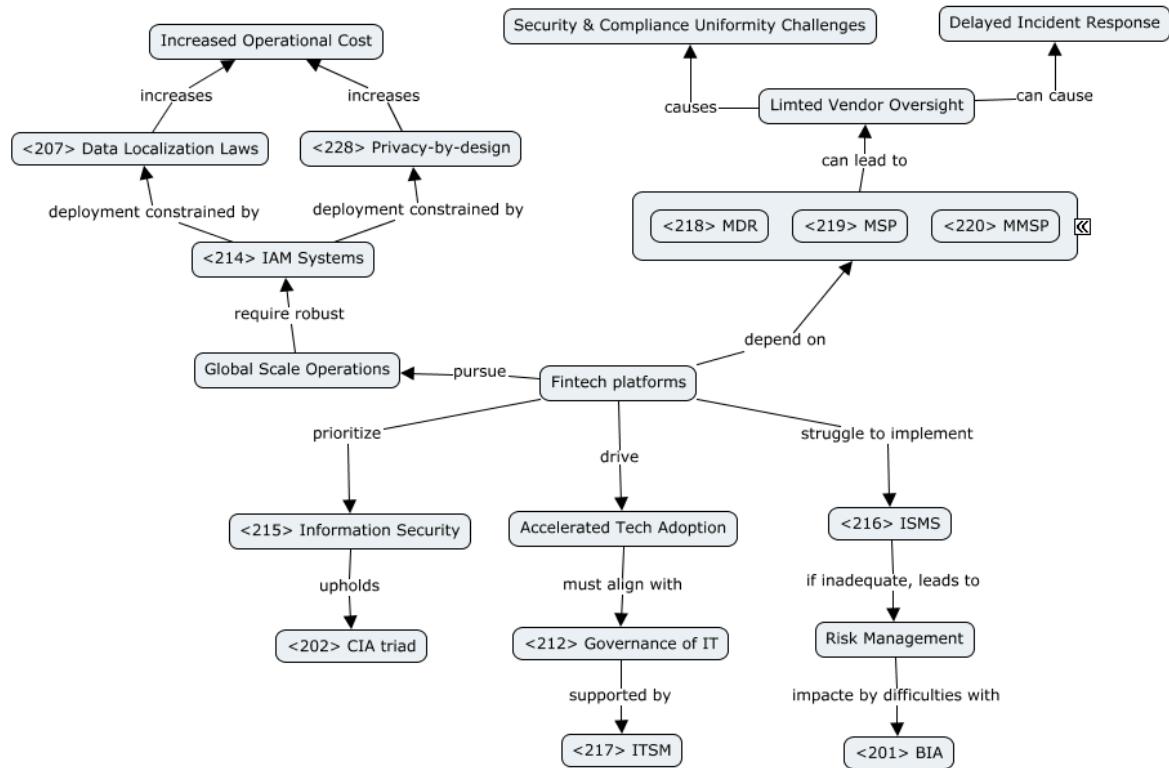
The incorporation of GRC (Governance, Risk and Compliance) <113> frameworks frequently conflicts with the imperative of rapid innovation characteristic of fintech enterprises. Insufficient internal controls <115> and the absence of formal audit <101> procedures result in oversight deficiencies regarding algorithmic decision making, data protection, and compliance with anti-money laundering and know Your Customer regulations. The retrospective establishment of these frameworks may impede product development and elevate operational expenditures.

Reliance on due diligence <110> for third party vendors introduces significant supply chain risks. Ongoing monitoring to ensure vendor adherence to regulations such as the General Data Protection Regulation and the Revised Payment Services Directive imposes substantial resource demands. Inadequate vendor oversight exposes the organization to enforcement sanctions and reputational damage.

Moreover, digital native firms must formulate comprehensive business continuity <103> plans to mitigate the impact of cloud outages, cybersecurity incidents, and abrupt regulatory interventions. Unlike established banking institutions, emerging fintech platforms often lack mature recovery protocols, thereby attracting heightened supervisory scrutiny.

6 Banking and Financial Service (Theme: IT Management)

Chosen Niche: Fintech and Digital Platforms



Fintech platforms must harmonize accelerated technological adoption with the principles of governance of IT <212> to ensure that IT resources advance organizational objectives. The integration of IT service management (ITSM) <217> practices within continuous integration and deployment workflows necessitates rigorous change control and incident management protocols.

Information security <215> demands meticulous adherence to the principles of confidentiality, integrity, and availability <202>. Early stage fintech firms frequently encounter difficulties in implementing a comprehensive information security management system <216>, thereby impairing effective risk identification. Conducting a detailed business impact analysis <201> within dynamic microservices architectures further complicates recovery planning.

Dependence on external managed detection and response providers <218>, managed security service providers <220>, and managed service providers <219> poses challenges in maintaining uniform security standards and regulatory compliance. Divergent priorities and limited oversight over vendor processes may delay incident response and resolution.

Finally, the deployment of robust identity and access management <214> systems on a global scale is constrained by disparate data localization laws and privacy by design mandates. The requirement to establish parallel systems to satisfy jurisdictional variations significantly increases architectural complexity and operational costs.

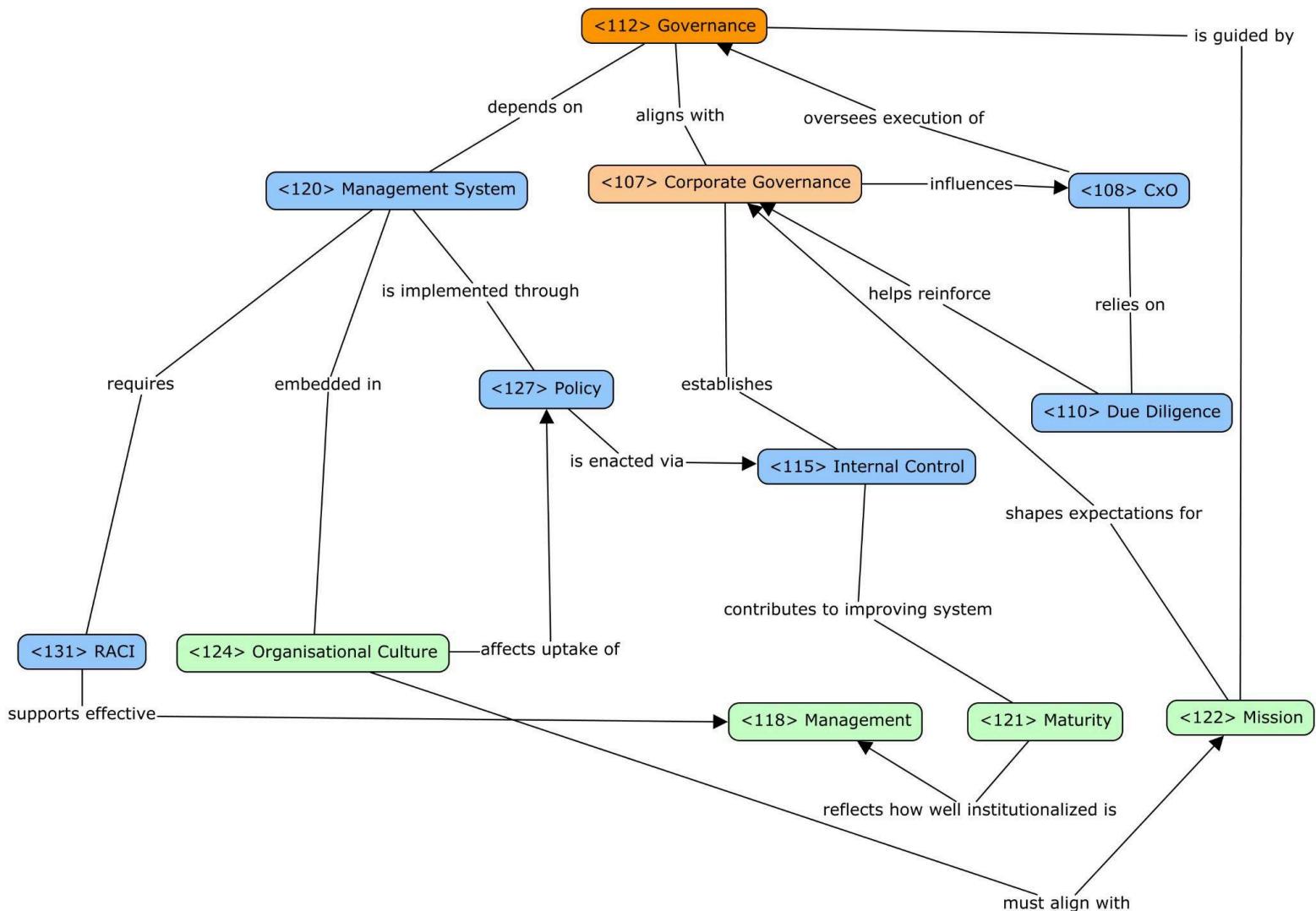
8 Healthcare (Theme: Governance)

Chosen Niche: Acute and Hospital Care

In acute and hospital care, **<112> Governance** must coordinate decisions across clinical, IT, and administrative functions to support patient-critical operations. Effective **<107> Corporate Governance** aligns **<108> CxO** roles with frontline needs, ensuring decisions are ethical, accountable, and timely. Clear **<131> RACI** structures are essential in high-pressure environments where role confusion can delay care.

A robust **<120> Management System**, underpinned by sector-specific **<127> Policies**, enables integration of workflows, risk oversight, and compliance. Strong **<115> Internal Control** helps detect failures early—essential when dealing with sensitive patient data and real-time monitoring systems. These controls must be part of the **<124> Organisational Culture**, where shared norms reinforce consistent, ethical behavior.

Governance maturity (**<121> Maturity**) varies across hospitals, affecting their ability to handle crises, maintain quality, and uphold the **<122> Mission** of safe and equitable care. In this context, well-designed governance is not just structural—it must be embedded, adaptive, and responsive to constant clinical and systemic demands.



8 Healthcare (Theme: IT Management)

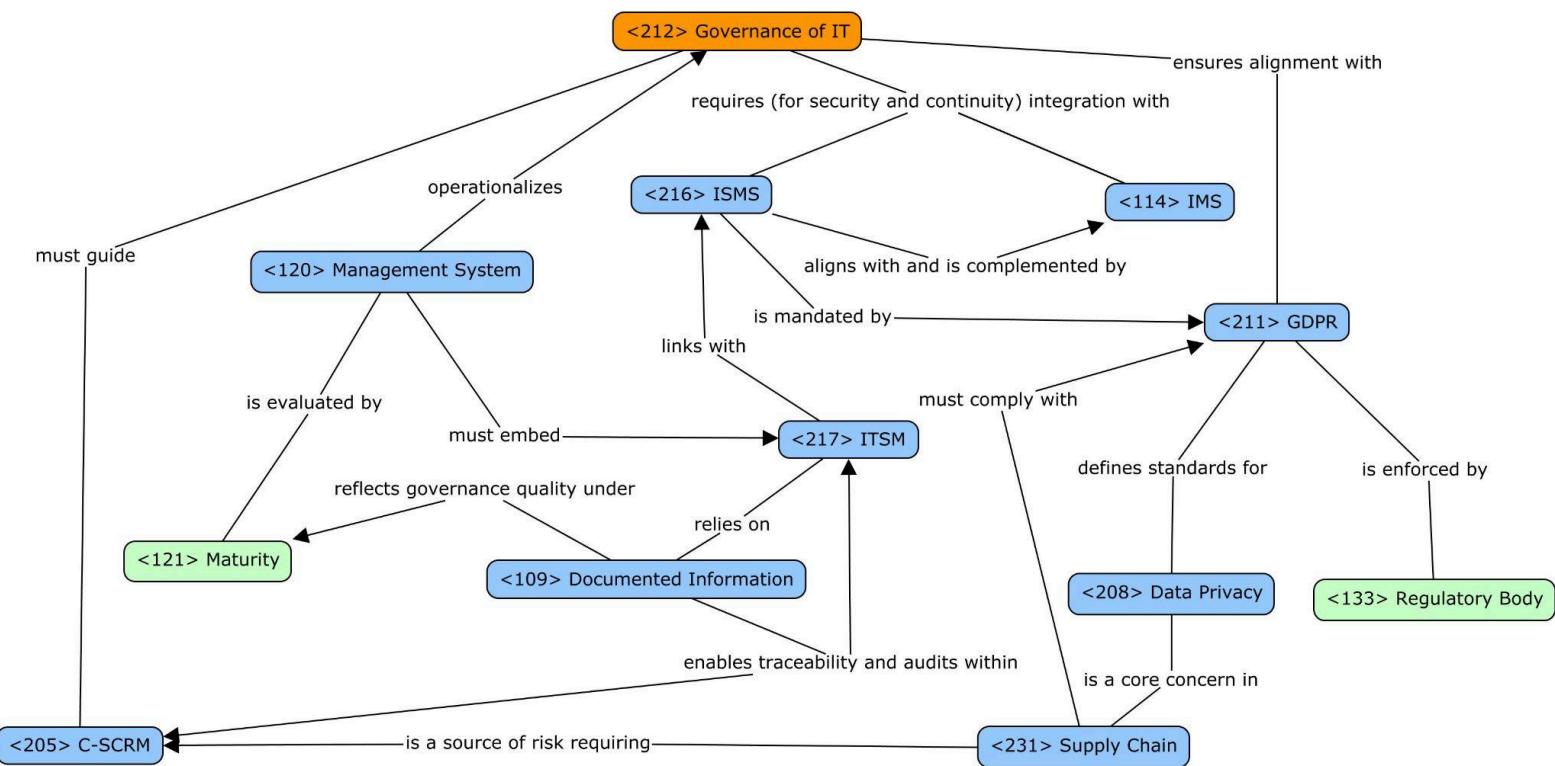
Chosen Niche: Acute and Hospital Care

In acute and hospital care, <212> Governance of IT must ensure that digital systems support real-time clinical decision-making, continuous monitoring, and operational resilience.

High-stakes environments rely on <216> ISMS to protect <208> Data Privacy across electronic health records, imaging systems, and patient portals. <120> Management System maturity, combined with strong <217> ITSM practices, is essential to maintain service continuity in intensive care or emergency units.

These systems must comply with <211> GDPR and anticipate future requirements like the EHDS, where data security and patient rights are critical. <205> C-SCRM plays a growing role as cloud-based diagnostics and AI solutions are adopted, exposing hospitals to third-party vulnerabilities. Maintaining accurate <109> Documented Information, supported by sector-aligned <114> IMS, ensures traceability, auditability, and regulatory compliance.

<121> Maturity of IT governance varies across hospitals but directly impacts their ability to respond to disruptions. <133> Regulatory Bodies enforce baseline standards, yet consistent implementation across the digital <231> Supply Chain is what enables hospitals to balance innovation with clinical safety and compliance.



Industry Comparison 1: Healthcare (Acute and Hospital Care) vs. Hospitality and Leisure (Accommodation)

Theme: <Theme 1> Organizations, Governance, and Management

In Acute and Hospital Care, **<112> Governance** must align ethical obligations, clinical oversight, and service resilience, while in Accommodation, it focuses on brand consistency, guest experience, and operational clarity. Both sectors require structured **<107> Corporate Governance**, but in healthcare, it must also reconcile public mandates with professional autonomy, unlike the typically centralized control of hotel chains. The use of **<131> RACI models** is critical in both, but more so in hospitals, where role clarity affects life-critical care. Accommodation services apply **<131>** to manage service delivery and guest satisfaction, while hospitals need it for clinical safety and emergency coordination. Both sectors rely on **<127> Policies** and **<115> Internal Control**, but healthcare emphasizes regulatory compliance and patient protection, whereas accommodation balances safety, hygiene, and customer service. **<118> Management** in hotels tends to emphasize process efficiency and **<116> KPI tracking** (e.g., occupancy), while hospital management prioritizes treatment outcomes and staff coordination. **<120> Management Systems** in hospitals are deeply embedded in care delivery and must support **<103> Business Continuity** in high-risk contexts like pandemics. Hospitality uses similar frameworks for continuity, but typically to handle logistical disruptions (e.g., storms, IT outages).

Finally, both industries need **<124> Organisational Culture** that aligns with their mission—patient-centered in hospitals and guest-centered in hotels—but healthcare faces greater stress, legal pressure, and public accountability.

Industry Comparison 2: Hospitality and Leisure (Accommodation) vs. Banking and Financial Services (Fintech and Digital Platforms)

Theme: <Theme 1> Organizations, Governance, and Management

<112> Governance in accommodation relies on a clear **<127> Policy** set by the brand's **<102> BoD** but gives local managers room to adjust to guest needs. Day-to-day **<118> Management** tracks simple **<116> KPI** such as occupancy rate and guest ratings, often set in their **<323> SLA** with the brand. To handle unexpected events like a sudden drop in bookings or a health scare, teams use **<103> Business Continuity** plans and basic **<115> Internal Control** checklists (for hygiene, safety, etc.). As online booking and guest apps grow, hotels add **<217> ITSM** and **<216> ISMS** steps to protect data under **<211> GDPR**, with a dedicated officer watching for **<206> Cybersecurity** risks.

<113> GRC in fintech platforms is far tighter. A single **<133> Regulatory body** lays out the **<134> Regulatory Framework** covering capital rules, **<106> Compliance checks** and digital-risk tests. Boards and **<101> Audit committees** enforce the rules and review every new service. Day-to-day **<118> Management** uses real-time monitoring and regular **<115> Internal Control** reviews to guard against fraud or system failures. When they build a new payment app or AI credit score, they follow strict **<402> AI governance** steps, ensuring each algorithm is explainable, human-reviewed, and that they can recover quickly if something breaks.

While both niches push digital tools and must protect customers, accommodation balances a brand's big rules with local flexibility and simple recovery plans, whereas fintech must obey tightly defined rules and run heavy-duty controls to keep money safe and regulators happy.

Industry Comparison 3: Healthcare (Acute and Hospital Care) vs Banking and Financial Services (Fintech and Digital Platforms)

Theme: <Theme 2> IT Management

Healthcare (Acute/Hospital Care) and Banking/Financial Services (Fintech) diverge significantly in IT Management priorities. Healthcare's <212> Governance of IT and <217> ITSM are driven by unwavering patient safety and system reliability, ensuring <215> Information security (especially <208> Data Privacy for patient records under <211> GDPR) directly supports life-critical clinical workflows. The cost and complexity stem from ensuring validated, high-availability systems and secure <205> C-SCRM for medical technologies.

In contrast, Fintech IT Management prioritizes rapid innovation and market agility. While also adhering to <211> GDPR, their <215> Information security and <216> ISMS focus intensely on protecting financial assets and transaction integrity, with <217> ITSM supporting fast CI/CD. Key complexities and costs for Fintech arise from managing a dynamic tech stack, often involving external providers (<218>MDR, <219>MSP, <220>MSSP), and navigating complex global regulations like <207> Data Localization for <214> IAM systems and ensuring <228> Privacy-by-design across diverse jurisdictions.

IT Management in Acute/Hospital Care centers on patient safety and data integrity, requiring secure, high-reliability systems and rigorous C-SCRM. In contrast, Fintech emphasizes agile innovation and asset protection, managing dynamic tech stacks and global compliance through partnerships with external providers and adherence to data localization laws.

Industry Comparison 4: Hospitality and Leisure (Accommodation) vs. Healthcare (Acute and Hospital Care)

Theme: <Theme 2> IT Management

When comparing IT Management (<212> Governance of IT) in Hospitality and Leisure (Accommodation) versus Healthcare (Acute and Hospital Care), key differences arise from sectoral priorities and regulatory pressures. Accommodation providers focus IT management on guest experience, operational efficiency, and digital service integration—leveraging <217> ITSM frameworks and <119> Management Frameworks like ISO 9001 or ISO/IEC 27001 to ensure service reliability, data protection, and compliance with standards such as <211> GDPR. Their IT maturity is often demonstrated through structured vendor management, <323> SLA oversight, and performance metrics like system uptime and guest satisfaction, with flexibility to adapt to local market needs.

In contrast, healthcare's IT management is driven by the critical need for patient safety, clinical data integrity, and regulatory compliance. Acute and hospital care environments require robust <216> ISMS, sector-specific standards (e.g., HL7, EHDS), and advanced <217> ITSM to guarantee business continuity and protect sensitive health data. IT management is deeply integrated into clinical workflows and subject to rigorous audit, with <215> Information Security and <208> Data Privacy as non-negotiable priorities. The stakes for failure are higher in healthcare, leading to more formalised governance structures, cross-functional CxO roles, and mandatory adherence to national and European regulations.

Agriculture

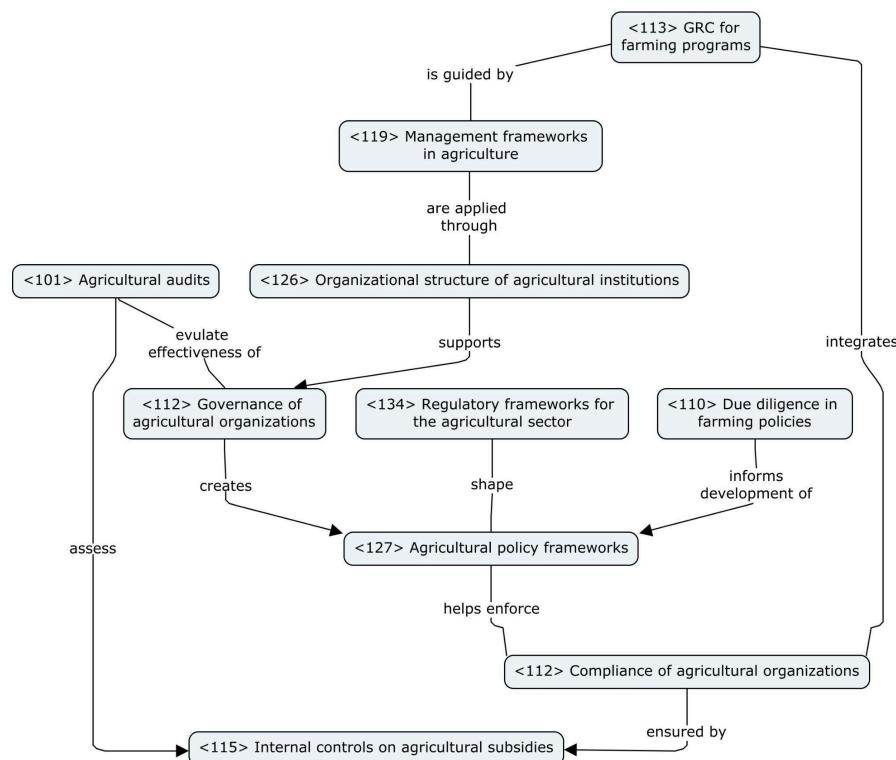
Agriculture is one of humanity's oldest industries, encompassing the cultivation of crops, animal husbandry, and related activities within a complex network of food production, environmental stewardship, and global trade. It is marked by diverse operational scales, from small family farms to large agribusinesses. The sector is increasingly influenced by digital tools such as precision agriculture, traceability systems, and farm management software.

Agriculture: Governance

Governance in agriculture is best understood through the lens of **<112> Governance**, which provides the system by which an entire organization is directed, controlled, and held accountable to achieve its long-term objectives. In the agricultural sector, this includes the development of **<127> Policy**, the enforcement of **<106> Compliance** with environmental and land-use regulations, and the oversight of institutional roles and responsibilities defined by **<126> Organizational Structure**.

At the core of effective governance lies **<107> Corporate Governance**, which ensures accountability, integrity, and transparency. High-level decisions made by **<102> BoD (Board of Directors)** and **<108> CxO** figures must align with **<111> Ethical Values** and integrate input from all stakeholders. This participatory approach is critical in overcoming fragmented **<134> Regulatory Frameworks** and limited access to decision-making platforms.

The integration of **<113> GRC (Governance, Risk and Compliance)** is becoming increasingly relevant, helping align policies across different levels and minimizing duplication of oversight functions. This is further reinforced by structured **<110> Due Diligence** in policy execution and the monitoring of **<115> Internal Control** mechanisms to ensure proper resource allocation.



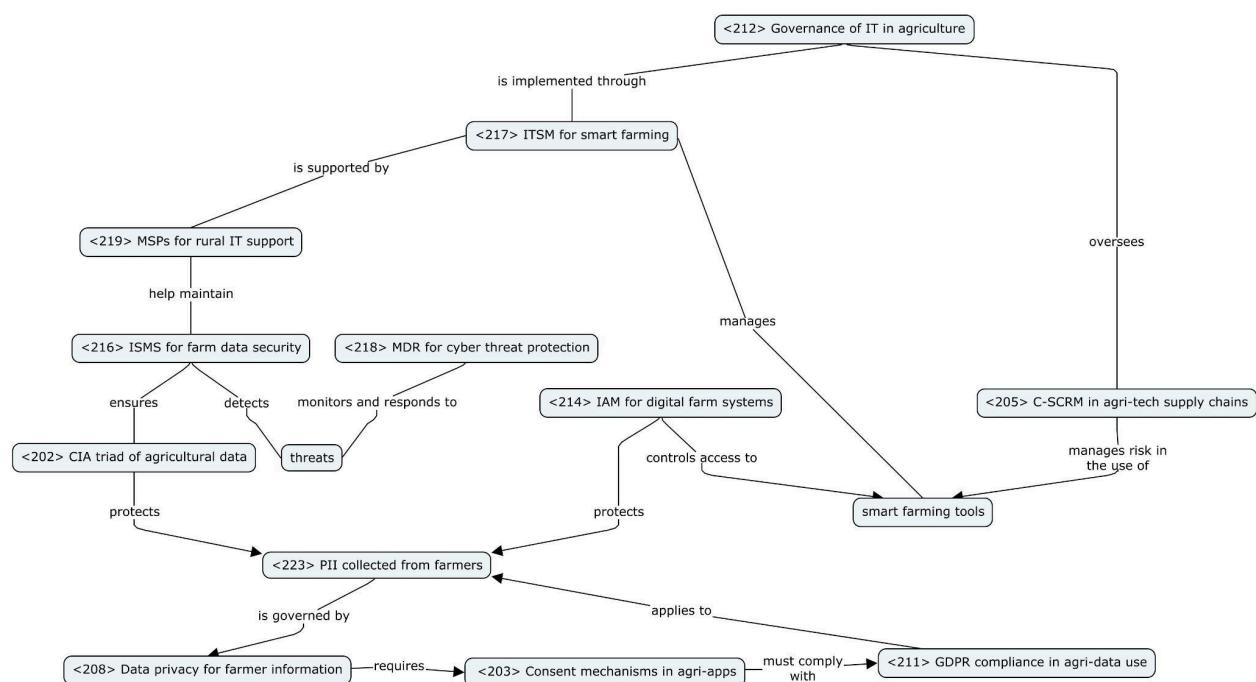
Agriculture: IT Management

Effective **IT management** in agriculture hinges on the principles of **<212> Governance of IT**, aligning digital systems with farming goals to enhance productivity, resource efficiency, and decision-making. This includes adopting secure IT frameworks like **<216> ISMS (Information Security Management System)** to mitigate risks to vital farming data, such as crop health and market trends. These systems help uphold the **<202> CIA triad**—confidentiality, integrity, and availability—of agricultural information.

Support from external **<219> MSPs (Managed Service Providers)** is essential, especially in regions with limited internal IT capacity. These providers help maintain stable operations and integrate cybersecurity tools like **<218> MDR (Managed Detection and Response)** for continuous monitoring and rapid threat response.

As digital farming platforms grow, managing personal and operational data becomes critical. Strong **<208> Data Privacy** practices and **<203> Consent mechanisms** ensure individuals' data rights are protected, aligning with regulations like **<211> GDPR**, particularly when processing **<223> PII (Personally Identifiable Information)**.

To secure the broader ecosystem, **<205> C-SCRM (Cybersecurity Supply Chain Risk Management)** helps manage risks from third-party tech partners, while **<214> IAM (Identity and Access Management)** ensures only authorized users can access sensitive systems. Altogether, coordinated **<217> ITSM** practices and privacy-focused system designs enable agricultural stakeholders to embrace digital transformation while safeguarding operational resilience and data integrity.



Healthcare

Healthcare is a critical and tightly regulated sector that combines clinical service delivery with public health and scientific research. It includes hospitals, clinics, pharmaceutical systems, and insurance bodies, operating under stringent compliance frameworks like GDPR and the European Health Data Space. Governance addresses patient safety, ethical standards, and digital integration across varied national models. Digital systems—such as electronic health records and telehealth platforms—play a vital role in improving efficiency and continuity of care, with strategic challenges spanning ageing populations, cybersecurity, and innovation.

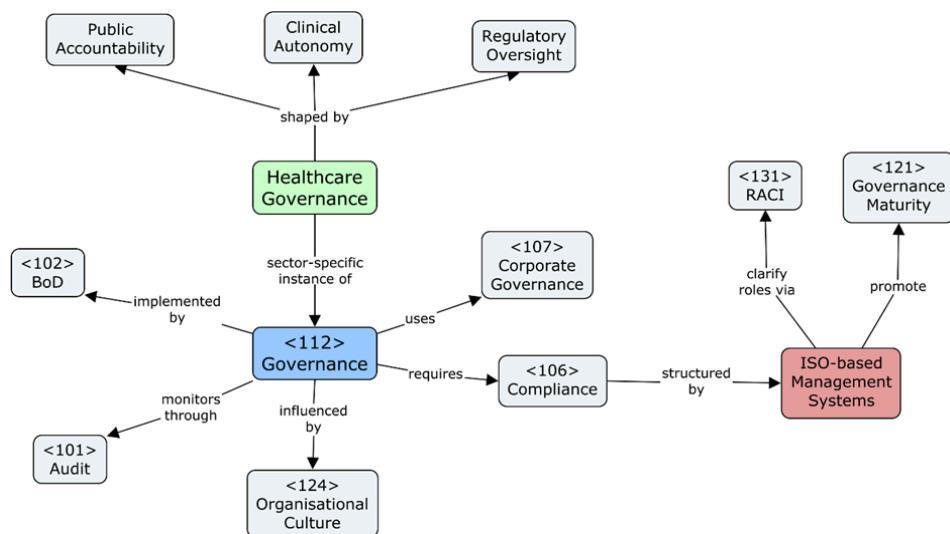
Healthcare: Governance

Governance in healthcare must balance public accountability, clinical autonomy, and financial sustainability. Unlike many industries, healthcare operates under a dual logic: medical professionalism and bureaucratic accountability. This duality requires nuanced governance frameworks that accommodate ethical considerations, evidence-based practice, and regulatory compliance. Healthcare governance typically involves multiple actors: public authorities, **institutional boards** <102>, clinical leadership, and private investors or non-profit entities. In many countries, national health systems are major players, making public governance mechanisms like oversight bodies, performance targets, and **audit systems** <101> relevant.

Key components of governance in healthcare include **quality assurance** <130>, **risk management** <135>, and **compliance** <106> with legal and ethical standards. Many institutions adopt ISO-based **management systems** <120> for quality, risk, and health informatics.

Governance maturity <121> is reflected in the adoption of structured **management frameworks** <119>, external **certifications** <105>, and role clarity through frameworks like RACI <131>. Challenges often include fragmentation between clinical and administrative leadership, accountability in hybrid setups, and tensions between innovation and regulatory conservatism.

Culturally, the healthcare sector values professionalism and **ethics** <111>, which makes **organisational culture** <124> a critical factor because without a culture of transparency and continuous improvement, even the best formal governance structures may fail in practice.

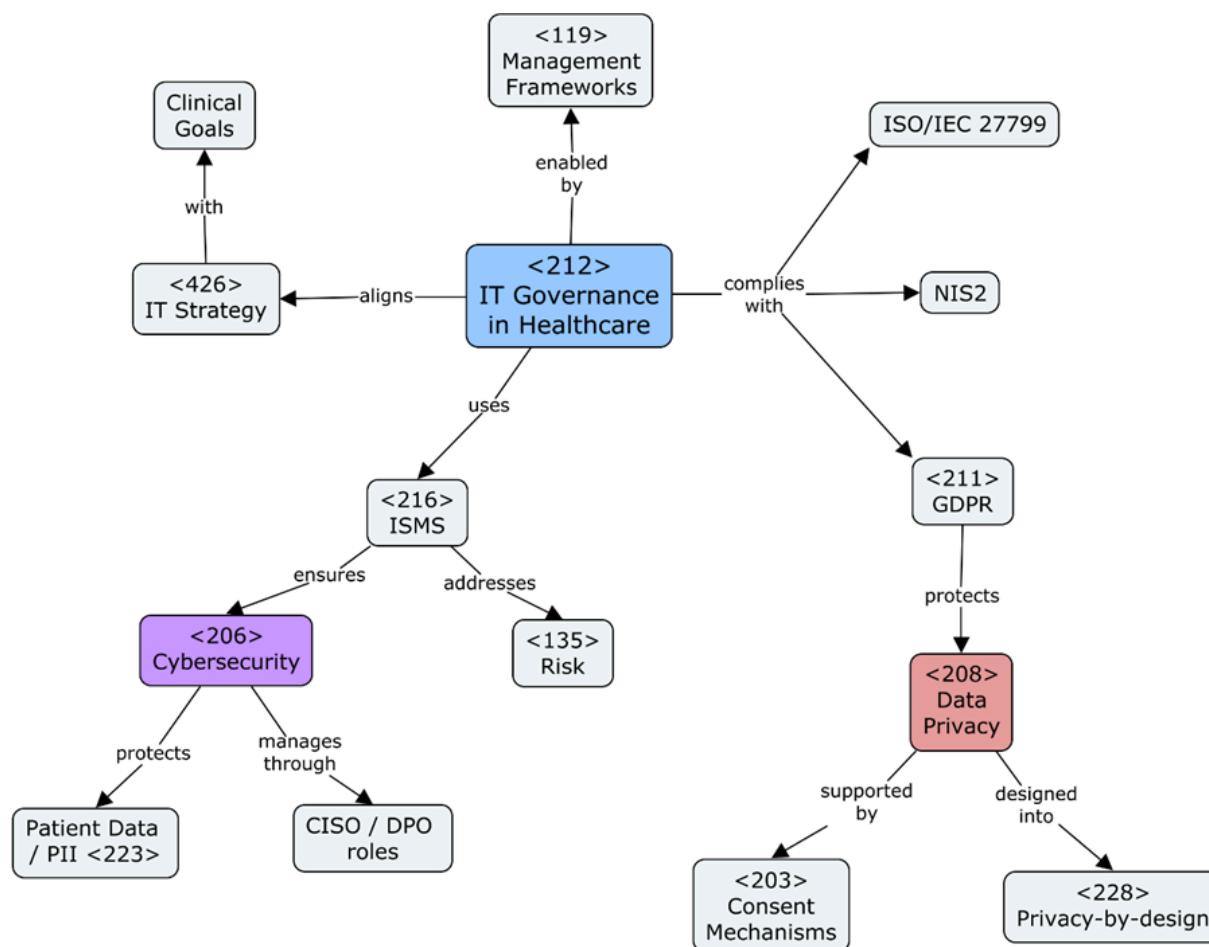


Healthcare: IT Management

Healthcare's relationship with IT is shaped by its high dependency on **data-intensive**, safety-critical, and privacy-sensitive systems. Effective **governance of IT** <212> must align IT strategy <426> with clinical and institutional goals while ensuring compliance with regulations such as the **GDPR** <211>, **NIS2**, and sector-specific standards like **ISO/IEC 27799**.

Decision-making authority is often split across IT departments, clinical units, and **regulatory bodies** <133>, requiring clear **accountability structures** such as **RACI** <131> and cross-functional coordination. A significant IT governance concern is **information security** <215> and **patient data privacy** <208>. Healthcare is one of the most targeted sectors for cyberattacks, making **cybersecurity** <206> **governance** a top priority. Boards must engage with strategic IT risk <135> management, backed by robust **ISMS** <216>.

Strategic IT management in healthcare must balance **resilience**, **cost**, and **ethical use of technology**, often under public scrutiny. Data lifecycle practices like **records management** <132>, **data retention** <210>, and **data localization** <207> must also be tightly managed. Tools like **consent mechanisms** <203>, **opt-in models** <221>, and **privacy-by-design** <228> are crucial to uphold trust and legal standards. Ultimately, IT governance in healthcare is not just about technology control but it is about ensuring that digital systems support safe, ethical, and efficient care delivery <103>.



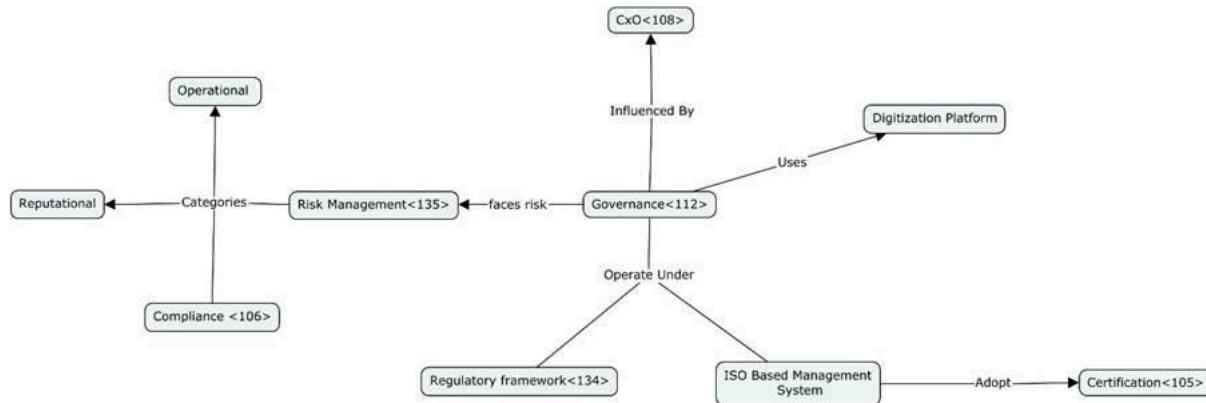
Hospitality

The hospitality and leisure industry encompasses accommodation, food services, entertainment, travel, and recreational activities, all centred on guest experience and service quality. It is highly sensitive to economic fluctuations, seasonal trends, and global events. Governance in this sector must manage brand consistency, local market adaptation, and a wide array of risks, including safety, reputation, and compliance with health, labour, and data privacy regulations. Technology is increasingly integral, from property management and booking systems to mobile apps and loyalty platforms, demanding robust IT governance and cyber resilience.

Hospitality: Governance

The hospitality and leisure sector operates in environments shaped by rapid changes (**<135> Risk**), unclear future outcomes, interconnected challenges, and multiple interpretations of situations. **<112> Governance** directs organizations to address these dynamics through structured frameworks like **<113> GRC (Governance, Risk, and Compliance)**, which integrates **<135> Risk Management** (e.g., mitigating disruptions from geopolitical events) and **<106> Compliance** (e.g., adhering to **<134> Regulatory Frameworks** like GDPR or labor laws). **<103> Business Continuity** ensures operational resilience during crises, supported by **<115> Internal Controls** to monitor processes such as supply chains or digital platforms.

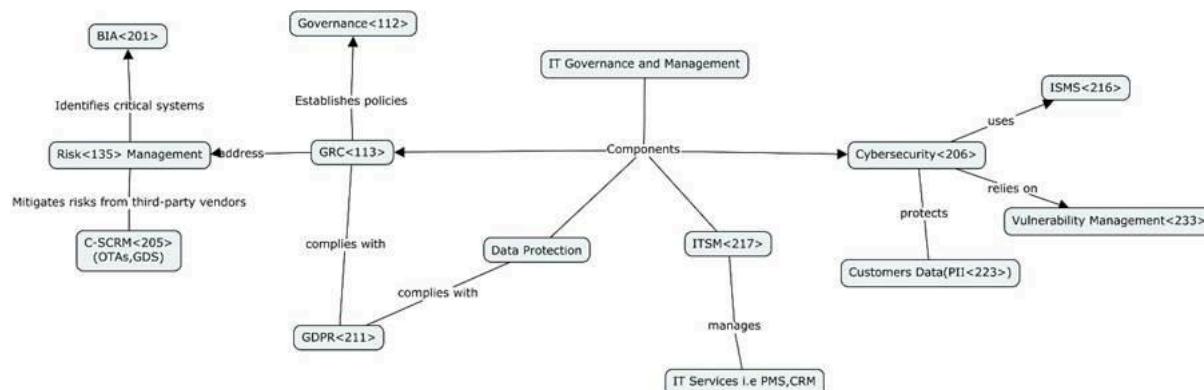
<107> Corporate Governance principles guide collaboration with public authorities in cultural tourism, balancing **<124> Organisational Culture** with regulatory demands. **<105> Certification** (e.g., ISO 22000) and **<123> Management System Standards** standardize practices, while **<109> Documented Information** ensures accountability. **<117> Leadership** roles, including **<108> CxOs**, align IT governance with strategic goals, fostering adaptability in fragmented markets. By embedding **<110> Due Diligence** and **<121> Maturity** into **<120> Management Systems**, organizations navigate complexity, sustain reputation, and align operations with **<122> Mission-driven** objectives.



Hospitality: IT Management

IT management in hospitality and leisure hinges on the principles of **Governance of IT**, aligning digital systems like Property Management Systems (PMS) and Online Travel Agencies (OTAs) with **Governance** frameworks to balance operational efficiency and regulatory demands. **BIA (Business Impact Analysis)** identifies critical systems, such as booking engines and loyalty programs, ensuring continuity amid disruptions like cyberattacks or supply chain failures. This aligns with **Risk Management** strategies that prioritize threats such as data breaches or service interruptions, which are central to the sector's reliance on digital platforms and guest trust. **GRC (Governance, Risk, Compliance)** integrates these efforts, enforcing adherence to **Regulatory Frameworks** like **GDPR**, which mandates stringent protection of **PII (personally identifiable information)** in bookings and payments.

The sector's exposure to cyber risks necessitates robust **Cybersecurity** measures, including **Vulnerability Management** to address weaknesses in IT infrastructure. For example, securing CRM systems and PMS platforms requires **ISMS (Information Security Management System)** frameworks to safeguard guest data and comply with **GDPR**. Public-private partnerships in cultural tourism, highlighted in the case study, further rely on **Governance** to harmonize IT investments with labor laws and sustainability standards. By embedding **BIA** and **GRC**, hospitality entities mitigate operational risks, uphold brand integrity, and adapt to evolving challenges like geopolitical shifts or health crises, ensuring resilience in a fragmented regulatory landscape.



Healthcare vs. Agriculture: Governance

Healthcare governance is characterised by a **highly institutionalised and regulated environment**, with oversight from ministries, hospital boards <102>, and compliance agencies. Governance structures must balance **clinical autonomy**, **financial constraints**, and **public accountability**.

Agriculture, by contrast, operates within **fragmented regulatory frameworks** <134> and often struggles with **dispersed decision-making power**, particularly among smallholders and cooperatives. While **Boards of Directors** <102> and **CxOs** <108> are relevant in large agri-businesses, many decisions depend on **policy enforcement** and **institutional roles** defined by <126> **organisational structure**, especially in public or cooperative sectors.

Both industries use **Management Systems** <120> and **Management Frameworks** <119> to structure governance, but with different emphases. In **healthcare**, these systems are oriented toward **quality assurance** <130>, **risk management** <135>, and **ethics** <111>, often validated through **external certifications** <105> like ISO 9001 or ISO 27799.

In **agriculture**, governance systems are more policy-focused and structured around **compliance** <106> with **environmental and land-use regulations**. While agriculture also uses **audits** <101> and **due diligence** <110>, the emphasis is often on **resource allocation** and **institutional trust**, with maturity reflected in **GRC** <113> integration and **internal controls** <115>, rather than external certifications.

Healthcare vs. Agriculture: IT Management

Healthcare IT is highly sensitive and **safety-critical**, requiring robust **ISMS** <216>, compliance with **GDPR** <211>, and sector-specific standards like ISO/IEC 27799. The sector faces sophisticated threats, making **cybersecurity** <206> and **data privacy** <208> central concerns. Many hospitals operate with formal **RACI** <131> models and **CxO** roles like CIO and CISO <108> to enforce accountability. It deals heavily with **PII** <223>, so **data privacy** <208>, **consent mechanisms** <203>, and **privacy-by-design** <228> are legally and ethically essential. Institutions must manage complex life cycles of patient data including **retention** <210>, **records management** <132>, and **data localization** <207>. Trust in digital systems is directly linked to patient care outcomes <103>.

Agriculture, while increasingly digital, faces **lower data sensitivity** but **greater variability in IT readiness**. Many organisations rely on **MSPs** <219> and **MDR** <218> services due to limited in-house capabilities. Cybersecurity is still important but infrastructure and funding limitations often reduce maturity. Tools like **IAM** <214> and **C-SCRM** <205> are growing, but not yet widely standardised. It also processes personal and operational data, but often without the same legal burden. **GDPR** <211> still applies, but implementation varies. **Consent mechanisms** <203> and **data privacy practices** are emerging—especially as platforms expand—but many rural or smallholder contexts rely on **informal trust** more than codified policies. The focus remains on enabling access, not restricting it.

Agriculture vs. Hospitality: Governance

Governance <112> in agriculture and hospitality and leisure shares core principles like transparency, accountability, and **compliance** <106>, but differs in focus and execution. Agricultural governance emphasizes sustainable development, environmental **compliance** <106>, and inclusive stakeholder engagement, especially smallholder farmers. It addresses resource sustainability, climate-related **risks** <135>, and fragmented **regulatory frameworks** <134> in land use and food safety. Tools such as **internal controls** <115>, **due diligence** <110>, and **audit** <101> mechanisms support accountability. **Corporate governance** <107>, through the **BoD** <102> and **CxO** <108> **leadership** <117>, aligns strategy with **ethical values** <111> and long-term goals. **Management frameworks** <119> and performance audits are used to develop governance **maturity** <121> and resilient food systems.

Conversely, **governance** <112> in hospitality and leisure focuses on resilience, adaptability, and service quality amid uncertainty and complexity. It uses **GRC** <113> frameworks to manage **risk** <135>, ensure **compliance** <106>, and maintain **business continuity** <103>. The sector involves diverse stakeholders such as tourists, employees, and public authorities, addressing geopolitical risks, market volatility, and legal shifts like **GDPR** <211>. Internal monitoring, **documented information** <109>, **certifications** <105> (e.g., ISO 22000), and **management system standards** <123> reinforce governance. **Corporate governance** <107> aligns **CxO** <108> strategies with IT and **organisational culture** <124>, while digital platforms enable real-time oversight. **Governance maturity** <121> grows through **leadership** <117>, robust systems, and alignment with **mission**<122>-driven goals.

Agriculture vs. Hospitality: IT Management

IT Governance and Management in agriculture and hospitality and leisure are based on **Governance of IT** <212> principles but differ in focus. In agriculture, IT governance aligns digital tools with farming goals to improve productivity and decision-making. **ISMS** <216> safeguards critical data like crop health and market trends, upholding the **CIA triad** <202>. External **MSPs** <219> are vital in resource-limited settings, often using **MDR** <218> for real-time threat detection. With growing digital reliance, strong **Data Privacy** <208> and **Consent mechanisms** <203> protect **PII** <223> in line with **GDPR** <211>. Resilience is further supported by managing ecosystem **risks** <135> through **C-SCRM** <205> and enforcing **IAM** <214>.

In hospitality and leisure, IT governance emphasizes integration of systems like PMS and OTAs within **Governance** <112> structures to enhance efficiency while meeting regulations. **BIA** <201> identifies key systems (e.g., booking engines, loyalty programs) to ensure continuity during disruptions, while **Risk Management** <135> addresses cyber threats and service integrity. **GRC** <113> frameworks ensure compliance with **Regulatory Frameworks** <134>, particularly **GDPR** <211>, protecting **PII** <223> in customer interactions. High cyber risk necessitates strong **Cybersecurity** <206> strategies, including **Vulnerability Management** <233> and secure infrastructure under **ISMS** <216>. Public-private efforts in cultural tourism rely on **Governance** <112> to align IT with labor and sustainability goals. By embedding **BIA** <201> and **GRC** <113>, the sector mitigates risk, ensures compliance, and protects brand trust.