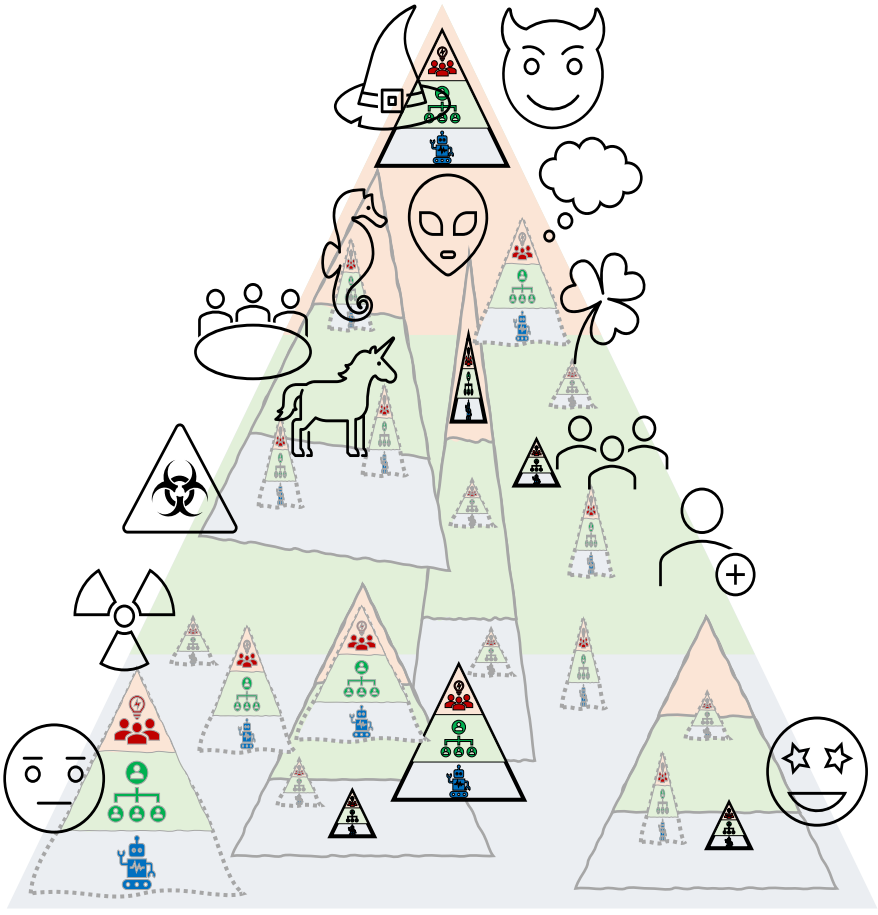
I'd like to add a new sheet

Segurança e Gestão dos Sistemas de Informação

###

Information Systems Management and Security

Lecture Notes



José Borbinha
Instituto Superior Técnico
26 April 2025

Contents

Introduction

Information systems, technology management, and digital governance are no longer confined to technical departments. They have become central concerns of executive leadership, influencing how institutions pursue their missions, respond to risk, deliver services, and interact with evolving regulatory, technological, and societal environments. Whether in public or private organisations, strategic decisions increasingly rely on the ability to interpret and act within a complex digital landscape.

This lecture notes book provides a structured foundation for understanding that landscape, with a particular focus on how executive roles (such as Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Information Security Officer (CISO), and others) operate at the intersection of technology, strategy, and institutional accountability. **The aim is not to train students for these roles, but to equip them with the knowledge and perspective needed to engage effectively with them, especially in consulting and advisory capacities.**

The material is organised around four core themes:

- ***Theme 1****: Organisations, Governance, and Management – Examines structural and cultural dynamics, management systems, and governance practices across sectors.*
- ***Theme 2****: Governance of IT and IT Management – Focuses on how technology is governed, including alignment, cybersecurity, and information management.*
- ***Theme 3****: IT Operations Management – Explores service delivery, process automation, risk management, and performance monitoring.*
- ***Theme 4****: IT, Strategy, and Change – Investigates the role of digital systems in transformation, innovation, and organisational adaptation.*

A preliminary section (Part 0) offers essential background, outlining the historical evolution of organisational forms, public service models, business logic, and IT governance. This context sets the stage for deeper exploration of how organisations manage complexity and make strategic choices.

The notes adopt a conceptual (not procedural) approach. The goal is to develop interpretive capacity: to read institutional structures, recognise governance issues, and engage in informed dialogue across sectoral and disciplinary boundaries. Rather than providing a checklist of solutions, the course fosters a mindset oriented toward alignment, transparency, and ethical reasoning.

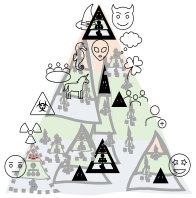
A distinctive feature of this material is its recognition that there is no single linear path through the subject matter. The key concepts are not arranged in a strict sequence but form a dense web of interrelated themes. Designing a narrative structure for these notes has been challenging: every starting point implies certain assumptions and leads in a particular direction, while other equally valid perspectives could lead elsewhere. Governance can be approached through organisational forms, through risk, through compliance structures, or through leadership dynamics (and each route reveals different insights).

Students should therefore treat this material not as a step-by-step guide, but as a map to be navigated. Depending on the initial backgrounds of each individual student, some routes will appear more familiar or intuitive, while others may initially seem distant or abstract. However, the aim is the same for everyone: to foster curiosity, provide orientation, and build a repertoire of concepts that can be used flexibly in practice, especially when working across organisational silos, cultural divides, or between technical and executive roles.

For example, public and private organisations are treated with equal weight, but with attention to their structural differences. These differences (regulatory, cultural, financial, and political) have major implications for how governance and digital strategies are designed and implemented. Understanding this variation is essential for students entering consulting, advisory, or policy-oriented careers, where the ability to tailor advice to sectoral contexts is a core professional skill.

Finally, this course encourages students to critically reflect on the language and frameworks they encounter. Many widely used terms in the digital and governance spheres are ambiguous or contested. Throughout the notes, attention is given to these ambiguities, **not to resolve them definitively**, but to help students recognise them as part of real-world complexity.

This text is a starting point for a professional journey, one that calls for conceptual clarity, institutional awareness, and a commitment to responsible engagement in an increasingly digital world.



0 The Context

Organisations today operate within a dense and evolving landscape of societal expectations, technological advances, regulatory frameworks, and economic pressures. Whether private businesses, public entities, or not-for-profit institutions, their capacity to act coherently and responsibly is shaped by their historical legacies, governance models, and interactions with a wide array of stakeholders.

Understanding this context requires stepping back from specific roles or technologies to examine the broader patterns that have shaped the governance and management of organisations. These patterns include how societies have permitted or constrained the formation of organisations, how economic models have influenced business structures, and how legal and political systems have imposed obligations and enabled autonomy. The resulting institutional arrangements vary across regions and sectors but share certain common threads.

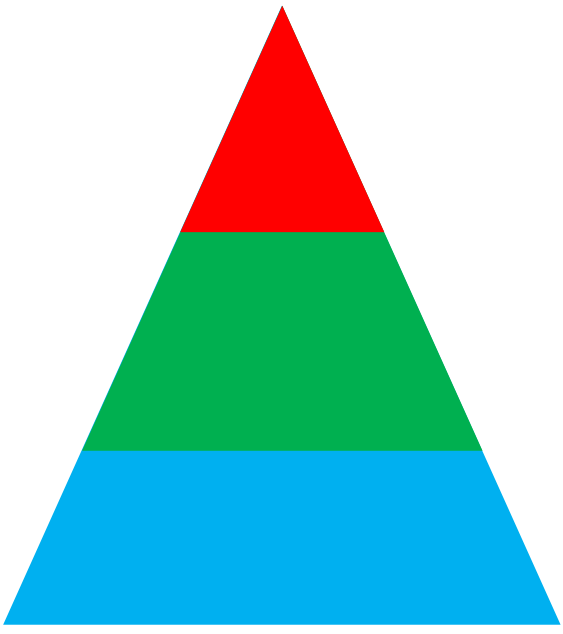
A long view reveals that organisational forms have evolved not only through innovation but also through contestation, regulation, and failure. Moments of disruption (whether due to industrial change, social movements, financial collapse, or technological breakthrough) often prompt new mechanisms of accountability and oversight. These include the emergence of modern corporations, the creation of regulatory authorities, the institutionalisation of management systems, and the formalisation of risk and compliance practices. In the public sector, these shifts have led to transformations in how services are conceived, financed, and delivered.

Digital technologies have added new layers of complexity and possibility. From early data processing systems to cloud computing and algorithmic decision-making, IT has progressively become embedded in organisational structures and processes. This has expanded the scope of what needs to be governed, raising new questions about who decides, who is accountable, and how value is created or compromised in digital contexts.

*In parallel, the **consulting industry** has become a key actor in shaping organisational responses to this complexity. Consultants bring frameworks, benchmarks, and methods that aim to support strategy, reform, or compliance (but they also operate within their own incentives and cultural assumptions). Engaging with senior leadership roles, particularly those responsible for information, technology, or security, requires both technical fluency and institutional awareness.*

This introductory section offers a structured overview of the historical, economic, and institutional dimensions that influence governance and management practices in contemporary organisations. It traces the timelines of business models, organisational forms, public service arrangements, and the role of information technologies. It also addresses the vocabulary and ambiguities that accompany these developments and highlights the significance of legal systems and normative frameworks in shaping organisational conduct.

By situating present-day roles, structures, and challenges within a broader frame, this part prepares the ground for more detailed explorations of governance, management, and strategic engagement in the digital era. It recognises that effective engagement (whether as an internal actor or as a consultant) depends on an ability to navigate both the technical and institutional dimensions of organisational life.



0.1 Organisations as Socio-Technical Constructed Systems

Organisations may be understood either as technical systems designed for coordinated action or as social constructs shaped by shared meaning, culture, and relationships. Each perspective reveals different aspects of how organisations function, evolve, and respond to challenges.

0.1.1 The Organisation as a Technical System

From a systems-oriented view, an organisation is a purposeful structure that transforms inputs into outputs through defined processes. It consists of interrelated components (people, roles, processes, resources, and technology) arranged to achieve specific goals. This approach emphasises clarity, control, and efficiency. Organisations are treated as designed artefacts, where planning and engineering play central roles.

Roles are formalised, responsibilities aligned with workflows, and outcomes measured through indicators and targets. Tools such as organisational charts, business process models, and performance dashboards help monitor, manage, and improve operations. This perspective supports techniques such as enterprise architecture, quality management systems, and workflow automation.

It brings value by enabling structured analysis and optimisation. However, it may understate how people interpret their roles, how informal norms shape action, and how change often emerges from interaction rather than design.

0.1.2 The Organisation as a Social Construct

In contrast, an organisation may also be understood as a socially constructed reality, an evolving product of shared beliefs, norms, and symbolic practices. Rather than being fixed entities, organisations are interpreted, negotiated, and continually reconstructed through communication and interaction.

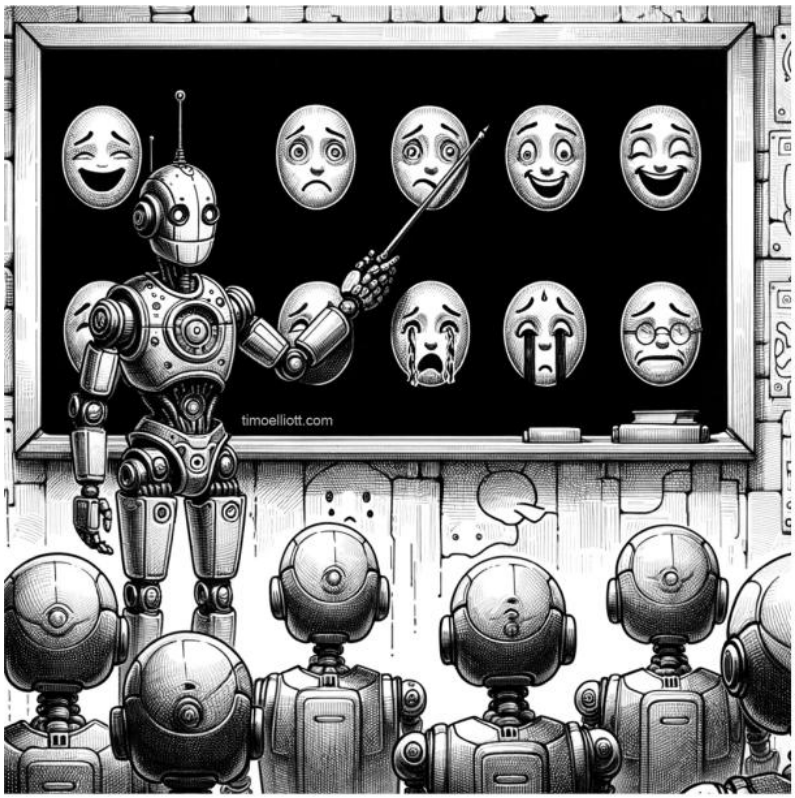
Structures and procedures are seen not as objective facts, but as social agreements, subject to reinterpretation and influenced by culture, history, and context. Roles gain meaning through practice and relationships. Informal networks and tacit understandings often carry more weight than official hierarchies.

This view places attention on leadership, trust, power dynamics, and cultural coherence. It explains why identical organisational charts can lead to different behaviours in different places. It is especially useful for understanding ambiguity, resistance, and change (not as failures of planning, but as signs of multiple perspectives and competing values).

0.1.3 [1]Concluding Note

The technical and social perspectives are not contradictory, but complementary. The former supports design and coordination; the latter illuminates interpretation and adaptation. Both are essential for navigating today's complex organisational environments.

For young engineers, whose training often focuses on designing and optimising systems, this broader view can be both surprising and empowering. Recognising organisations as social as well as technical invites deeper understanding, greater empathy, and more meaningful engagement. Developing the capacity to work fluently across both dimensions equips professionals not only to solve problems but also to contribute to transformation.



Feelings 101: Today's lesson - Why humans say 'It's complicated'

source: https://timoelliott.com/blog/cartoons/artificial-intelligence-cartoons

1

0.2 Timeline of Political and Cultural Freedom of Organising and Operate

The freedom to organise (whether to form a guild, a company, or a public body) has always been conditioned by political power, legal traditions, and cultural values. Organisations do not emerge in isolation; they are social artefacts shaped by how societies view authority, initiative, responsibility, and trust.

0.2.1 Organising Before Modernity

Before the 15th century, organising was mostly governed by tradition or by privilege granted from above. In medieval Europe (c. 1000–1500), organisations such as monasteries, universities, and guilds operated through royal or ecclesiastical charters. The concept of a legal person (a company with rights and obligations independent of its founders) began to take shape slowly during this period, especially in legal theory emerging from Italian city-states.

Supervision was direct and personalised: monarchs, bishops, and lords authorised or dissolved organisations at will. Comparable forms existed in imperial China (Tang and Song dynasties, 7th–13th centuries), where merchant guilds operated under imperial licences, and in West African states such as the Mali Empire (13th–16th centuries), where economic life was mediated through kinship and royal patronage. These early systems show that the impulse to organise socially and economically is both ancient and global.

0.2.2 Expansion, Mercantilism, and Diverging Paths in Europe

From the 15th century onward, European overseas expansion created a demand for large-scale, coordinated organising. In Portugal the "Casa da Guiné"[2] (1443) and the Casa de Contratación[3] (1503) in Castilla served as a supervisory institution for commerce and navigation, which relied on Crown-granted monopolies to administer trade and territory.

England and the Netherlands supported joint-stock companies such as the East India Company[4] (1600) and the VOC[5] (1602). These early multinationals operated with legal personality and wide autonomy. France, particularly under Colbert (1660s–1680s), blended state strategy with commercial privilege.

Colonialism exported these models, often displacing Indigenous forms of organisation. In the Americas, Africa, and Asia, traditional governance systems (communal, kin-based, or spiritual) were marginalised or co-opted. In Oceania, European imperial powers imposed legal-administrative frameworks during the 18th and 19th centuries, though Indigenous organisational principles have endured or re-emerged in modern governance and community structures.

0.2.3 Industrialisation, Liberalism, and Organisational Personhood

The 18th and 19th centuries saw the rise of the modern company. In Britain, the Joint Stock Companies Act (1844) and Limited Liability Act (1855) formalised the company as a legal person. In the United States, state-level incorporation laws and the Sherman Act (1890) laid the groundwork for a capitalist organisational landscape underpinned by freedom of association and antitrust norms. In Canada, a mix of British legal heritage and cooperative innovation led to strong mutuals and credit unions (e.g., Desjardins, 1900). In Japan, the Meiji reforms (1868–1912) enabled large corporate groups (zaibatsu).

In contrast, other reactions to industrialisation took authoritarian forms. For example, Russia (1917) and China (1949) imposed models of collectivised organising, while in Italy (1922–1943), Germany (1933–1945) and Portugal (1928-1974), freedom of organisation was restricted, with independent unions, parties, and associations replaced by state-controlled corporatist structures (organisations existed only insofar as they served state ideology, and pluralism was actively suppressed).

In post-war Europe, the creation of the European Union (from the Treaty of Rome, 1957, to the Maastricht Treaty, 1993) established freedom of establishment and harmonised supervision across borders. This supranational governance allows organisations to operate within a shared legal and economic space.

0.2.4 Supervision and Monopolies in the Modern Era

From the late 19th century onward, democracies developed institutions to regulate organisational power. The FTC (1914) and SEC (1934) in the U.S., the Competition Bureau (1986) in Canada, and EU bodies such as DG COMP and ENISA (among many others…[6],[7]) exemplify structured oversight.

The United Nations system[8], founded in 1945, added a global layer to organisational legitimacy. The Universal Declaration of Human Rights (1948) enshrined freedom of association (Article 20), while agencies like the ILO, UNDP, and UNCTAD helped shape global standards for labour, transparency, and development. The UN Guiding Principles on Business and Human Rights (2011) clarified expectations for private-sector actors worldwide.

Countries from India to South Africa, Brazil, Australia, and New Zealand have since developed national frameworks that blend local traditions with international norms, contributing to an increasingly coordinated and value-driven global regulatory fabric.

0.2.5 Concluding Note

Organisations are human creations, as expressions of ambition, cooperation, and shared purpose. The freedom to form and sustain them reflects deep societal choices. Exploring this timeline across continents and centuries reveals not only what has been done, but what remains possible. The global and European legacies of organising offer future professionals a wide and dynamic landscape from which to learn, innovate, and lead responsibly.

[2] https://en.wikipedia.org/wiki/Casa_da_%C3%8Dndia
[3] https://en.wikipedia.org/wiki/Casa_de_Contrataci%C3%B3n
[4] https://en.wikipedia.org/wiki/East_India_Company
[5] https://en.wikipedia.org/wiki/Dutch_East_India_Company
[6] https://finance.ec.europa.eu/regulation-and-supervision_en
[7] https://www.finma.ch/en/finma/international-activities/policy-and-regulation/european-supervisory-authorities/
[8] https://en.wikipedia.org/wiki/United_Nations_System

0.3 Timeline of Business and Business Models

In early civilisations, economic activity was predominantly local and based on simple exchange logics, such as bartering or standardised weights for goods like grain, wool, or metal. Organised commerce already existed in ancient Mesopotamia, Egypt, and later in the Greco-Roman world, often under the control of temples or state authorities. These entities recorded inputs and outputs, tracked obligations, and controlled surplus, effectively functioning as early forms of enterprise.

Craftsmen, traders, and family-run workshops operated according to informal business models rooted in reputation, trust, and embedded social relationships. Profit, as a guiding objective, was often secondary to stability and continuity, especially in rural or religious contexts.

Interestingly, some of these early models have persisted through the centuries in various forms. A number of businesses operating today were founded in the first or second millennium and still deliver value through craftsmanship, hospitality, or local service provision. These firms, often family-run and deeply rooted in place and tradition, exemplify a business logic focused on heritage, resilience, and intergenerational continuity[9].

0.3.1 The Merchant Model and Intermediated Trade

With the rise of long-distance commerce, especially during the Middle Ages, more structured forms of trade emerged. Merchant families such as the Medici operated models based on arbitrage and financing. They created networks of agents, leveraged economies of scale, and used letters of credit to facilitate transactions.

This period saw the emergence of the intermediated trade model, where value was created not by producing goods but by connecting producers with markets. The organisational structure began to include partners, apprentices, and rotating leadership within merchant guilds.

0.3.2 Early Corporations and the Charter Model

The creation of chartered companies such as the Dutch East India Company (VOC) and the British East India Company introduced the concept of delegating commercial risk to a collective entity. These early cases of **corporation**[10] had monopolies granted by the state and adopted models based on joint investment and shared risk, governed by boards and formal accounting systems.

Business models began to include a global supply chain logic: securing resources in distant colonies, transporting them to Europe, and redistributing goods for sale. Value was captured through control over routes, resources, and political influence.

0.3.3 The Industrial Business Model

The Industrial Revolution introduced the mass production model, built around mechanisation, centralised labour, and standardised outputs. Firms such as Ford or Siemens created vertically integrated operations where value was captured through economies of scale and operational efficiency.

Revenue models were mostly product-based, and pricing was oriented around cost-plus logic. Businesses internalised processes such as sourcing, production, and distribution to reduce dependence on third parties. Management became more formal, often hierarchical, and supported by professional roles in engineering, finance, and operations.

0.3.4 Service and Franchise Models

By the early 20th century, especially in retail and food sectors, the franchise model and service model gained prominence. Organisations like McDonald's or hotel chains began to scale by offering brand and operational standards to independent operators.

In these models, value was often in the brand, the operational method, and the customer experience — not just the product. This shift introduced new risk profiles (brand reputation, service consistency) and led to the creation of operational manuals, audit regimes, and compliance mechanisms across networks.

0.3.5 Platform and Networked Models

The digital revolution introduced platform-based business models, where firms like Amazon, Uber, and Airbnb act as intermediaries that orchestrate transactions between suppliers and customers. These models rely on network effects, data analytics, and user trust.

Here, value is created not by owning assets but by enabling others to use them more efficiently. Monetisation may come from commissions, advertising, subscriptions, or data. Risk and compliance challenges shifted toward algorithmic bias, content moderation, and cybersecurity.

Simultaneously, freemium models, subscription models, and "as-a-service" models emerged, particularly in the software industry. IN platforms and networks, companies focus on building long-term customer relationships rather than one-time transactions.

0.3.6 Business Models and Sustainability

More recently, circular models, shared value models, and impact-driven models are emerging in response to environmental, social, and regulatory pressures. Organisations are expected to deliver financial, social, and environmental value simultaneously.

This evolution brings business models closer to the domains of governance and compliance. Non-financial reporting (e.g. **Environmental, Social, and Governance - ESG**[11]), stakeholder accountability, and regulatory alignment have become key design elements in how business models are structured and evaluated.

[9] https://en.wikipedia.org/wiki/List_of_oldest_companies
[10] https://en.wikipedia.org/wiki/Corporation
[11] https://corporatefinanceinstitute.com/topic/environment-social-governance-esg/

0.4 Timeline of Business Organisations and Governance

Governance, Risk Management, and Compliance (GRC) is a concept expressing the assumption that nowadays organizations must ensure that strategic decisions align with overarching principles and regulations. The origins of governance and risk management can be traced to early trade and statecraft in Mesopotamia, Egypt, and later, the Greco-Roman world. Merchants, monarchs, and religious institutions developed early forms of control and accountability: clay tablets recorded transactions; grain stores were monitored; and tax systems were created to manage state revenue and risks related to scarcity. Compliance, at this stage, referred primarily to adherence to divine or royal decrees.

0.4.1 Medieval Trade and the Rise of Merchant Banks

In the Middle Ages, as commerce expanded across Europe and the Mediterranean, new organisational forms emerged to manage complex financial and reputational risks. The Medici family[12] in Florence pioneered double-entry bookkeeping to track obligations and cash flow, enhancing transparency and internal control.
Guilds and merchant associations created codes of conduct to ensure trust and enforce standards across city-states. Letters of credit and early banking practices were developed to mitigate the risks of long-distance trade.

0.4.2 The Dutch East India Company and Modern Corporations

A pivotal development occurred in the early 17th century with the creation of the Dutch East India Company (VOC), often cited as the first modern corporation. It introduced the concept of joint-stock ownership, delegated decision-making to a board of directors, and pioneered regular financial reporting to shareholders. These practices laid foundational concepts for corporate governance. The VOC was also subject to governmental charters and public scrutiny, highlighting early intersections between private enterprise, state regulation, and public accountability.

0.4.3 The Industrial Revolution and the Formalisation of Risk Management

The 18th and 19th centuries saw the growth of industrial enterprise, large factories, and railways. With these came new organisational risks (workplace accidents, financial speculation, and logistical failures) that demanded more formalised approaches to control.
Insurance markets and actuarial science matured in this period, especially in London. The concept of "**business continuity**" gained ground in response to fire and maritime disasters. Audit functions began to be institutionalised within large organisations, and external financial auditing emerged to assure investors.

0.4.4 20th-Century Governance and Regulation

Following major crises such as the 1929 Wall Street Crash and later corporate scandals, governments and institutions introduced new regulatory frameworks to enforce transparency and stability. In the United States, the Securities Act of 1933 and the creation of the Securities and Exchange Commission (SEC) marked a decisive shift in formal compliance structures.
Corporate governance evolved with the rise of multinational enterprises.
In the 1970s and 1980s, internal control systems and enterprise risk management started to become formal disciplines, particularly in sectors like finance, oil and gas, and aerospace.

0.4.5 The Digital Era and Integrated GRC Frameworks

The late 20th and early 21st centuries witnessed increasing digitalisation of operations and new forms of regulatory complexity. Frameworks such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) and COBIT (Control Objectives for Information and Related Technologies) emerged as references for integrated governance, risk, and compliance into coherent models for IT and finance.
After major corporate collapses like Enron and WorldCom, in the US the Sarbanes-Oxley Act (SOX) in 2002 imposed strict requirements for corporate accountability.
The global financial crisis of 2008 brought renewed attention to systemic risk and the failure of oversight systems.

0.4.6 GRC Today: Beyond Compliance

Today's understanding of GRC encompasses not only internal control and compliance but also strategy, reputation, digital resilience, and stakeholder trust. Cybersecurity, ESG (Environmental, Social, and Governance) metrics, and data privacy regulations such as the **General Data Protection Regulation (GDPR)**[13] have become central.
Organisations are increasingly adopting integrated GRC platforms and management systems to align governance with operational execution, risk anticipation, and regulatory change. Governance is no longer seen only as a legal duty but as a value driver and cultural cornerstone of sustainable business and public administration.

[12] https://en.wikipedia.org/wiki/House_of_Medici
[13] https://eur-lex.europa.eu/eli/reg/2016/679

0.5 Corporate Collapses and the GRC Response

Several major corporate collapses in the early 2000s brought global attention to the consequences of poor governance, ineffective risk management, and weak compliance. Although often associated with US firms such as Enron and WorldCom, similar failures occurred in Europe, revealing systemic vulnerabilities in both corporate and regulatory environments.
Enron, an energy conglomerate based in Texas, used complex accounting structures to conceal debt and inflate profits. Senior executives misled investors and auditors, while the board approved opaque financial instruments without adequate scrutiny. The company collapsed in 2001, followed by WorldCom in 2002, a telecommunications firm that had fraudulently capitalised routine expenses. These events prompted the enactment of the Sarbanes-Oxley Act (SOX) in the United States, introducing stricter rules on executive accountability, auditing independence, and internal control reporting.

0.5.1 The Enron case

Enron, an energy conglomerate based in Texas, used complex accounting structures to conceal debt and inflate profits. Senior executives misled investors and auditors, while the board approved opaque financial instruments without adequate scrutiny. The company collapsed in 2001, triggering widespread financial and reputational losses.
A critical enabler of the deception was its external auditor, **Arthur Andersen**[14], one of the world's leading accounting firms at the time. Andersen not only failed to expose the fraudulent practices but was later found to have destroyed key documents during investigations. The firm's involvement led to its criminal conviction (later overturned on appeal) and its effective disintegration, underscoring the systemic risk posed by conflicts of interest and weak auditor independence.
These events prompted the enactment of the SOX in the United States, introducing stricter rules on executive accountability, auditing independence, and internal control reporting.

0.5.2 European Cases and Global Implications

In Europe, several high-profile failures echoed similar patterns. One of the most notorious was **Parmalat**, an Italian dairy and food group that collapsed in 2003 after it was revealed that a €4 billion bank account supposedly held in the Cayman Islands did not exist. Investigations uncovered massive accounting fraud and falsified transactions, facilitated by weak governance structures and lax oversight by auditors and regulators.
Another example is **Royal Ahold**, a Dutch multinational retail group that overstated profits through improper consolidation of supplier rebates, leading to a €1 billion accounting scandal in 2003. Although the company did not collapse, the crisis resulted in a major loss of shareholder confidence, executive resignations, and lasting reputational damage.
In the UK, **Barings Bank** collapsed in 1995 (an earlier but highly influential case) after a single trader, operating out of Singapore, accumulated losses that exceeded the bank's entire capital. The failure was attributed to poor internal controls, a lack of segregation between front-office and back-office functions, and inadequate operational supervision.
In 2020, **Wirecard**, a German payment services provider, became one of the largest financial scandals in postwar Europe. The company admitted that €1.9 billion in assets were missing. Despite being part of Germany's prestigious DAX index, Wirecard had evaded scrutiny for years, raising questions about regulatory capacity and auditor independence within the European context.

0.5.3 Strengthening GRC Practices

These events catalysed significant changes in how organisations approach governance, risk, and compliance. Regulatory responses included:

- Reinforcement of auditing and financial supervision and reporting standards (e.g. BCBS[15], IFRS[16], ESMA[17], etc.);
- **Enhanced roles for audit committees** and boards in overseeing internal control;
- **Expansion of whistleblower protection**, not only in the US (via SOX) but gradually in European jurisdictions;
- **Greater scrutiny of external auditors**, including mandatory rotation and restrictions on consultancy services.

At the organisational level, these failures contributed to the adoption of integrated GRC frameworks, enterprise risk management, and more structured compliance programmes. Boards are now expected to actively define and monitor risk appetite, and executives are increasingly held accountable not only for financial performance but also for control environments and ethical culture.

0.5.4 Enduring Lessons

Across these cases, common patterns emerge: opaque organisational structures, excessive concentration of authority, deficient oversight, and incentives that favoured short-term performance over long-term sustainability. The absence of effective checks and balances created vulnerabilities that ultimately undermined organisational resilience.
Modern GRC is shaped as much by these failures as by regulatory ambition. They serve as enduring reminders that governance must be active, risk must be visible, and compliance must be meaningful, not merely procedural.

[14] Arthur Andersen collapsed after the Enron scandal due to its role in audit failures and document destruction. Andersen Consulting had already split in 2000 and rebranded as Accenture in 2001. While Arthur Andersen ceased operations, Accenture became a global leader in consulting. The Andersen name survives in limited form through legal and tax networks like Andersen Global.
[15] https://www.bis.org/bcbs/
[16] https://www.ifrs.org/
[17] https://www.esma.europa.eu/

0.6 Timeline of Public Services

The notion of public services is closely linked to the evolving role of the state and the mechanisms through which collective needs are identified and addressed. Public services are not merely instruments of delivery; they reflect deeper ideas about legitimacy, authority, and the social contract. Their development cannot be separated from broader transformations in governance, economic models, and public expectations. This timeline outlines key phases in the evolution of public services, highlighting shifts in their organisation, purpose, and underlying rationales.

0.6.1 Before the modern state

In pre-modern societies, public services were neither systematic nor universal. Functions such as defence, justice, or water management were provided by monarchies, local lords, or religious institutions, often as expressions of power rather than formalised duties. Legitimation of these services derived from tradition, divine sanction, or military dominance. Service provision was fragmented and highly variable, with no consistent framework for rights, access, or accountability. Where present, services were typically delivered as favours, obligations, or acts of charity.

0.6.2 19th century: The liberal state and enabling services

The rise of the liberal state in the 19th century brought with it the idea of limited government intervention. Influenced by Enlightenment thought and classical economic theory, public services were conceived as minimal and functional: maintaining public order, enforcing contracts, providing currency, and supporting infrastructure for commerce. Education and health remained largely decentralised and were often left to churches or private benefactors. Central administration grew modestly, focusing on enabling markets rather than redistributing resources.

0.6.3 Early 20th century: The expansion of basic services

With industrialisation and the growth of urban populations, the limitations of minimalist service provision became more evident. The risks of poverty, epidemics, and labour unrest prompted the state to take on new responsibilities. Education became compulsory in many countries, and public health initiatives were launched to reduce mortality and improve workforce productivity. The expansion of municipal services—such as clean water, waste collection, and housing—was justified in terms of social order and national strength. These developments marked a gradual shift toward a service-oriented conception of the state.

0.6.4 Post–Second World War: The welfare state

After 1945, many governments adopted the welfare state model, positioning the state as a guarantor of key services. Public services such as universal healthcare, pensions, social housing, and comprehensive education systems were rolled out in much of Europe and beyond. This period saw the peak of centralised, tax-funded service provision, often through large bureaucracies. Public servants were tasked with ensuring equity, standardisation, and coverage across entire populations. The legitimacy of the state was increasingly tied to its capacity to deliver predictable and universal services.

0.6.5 1980s–1990s: New Public Management

Rising fiscal constraints, economic liberalisation, and critiques of inefficiency prompted reforms in public administration. New Public Management (NPM) introduced market-inspired mechanisms such as contracting-out, benchmarking, and managerial autonomy. Citizens were reframed as customers, and performance indicators became central to evaluating service quality. While NPM aimed to improve responsiveness and reduce costs, it also raised concerns about equity, coherence, and democratic accountability. The fragmentation of provision and a shift toward short-term performance often conflicted with the long-term goals of public value creation.

0.6.6 21st century: “Digital transformation” and public value

Digital technologies reshaped how services are designed and delivered. Governments increasingly adopted digital platforms to improve accessibility, reduce administrative burdens, and support personalised interactions. Initiatives such as once-only data submission, automated eligibility checks, and real-time dashboards became common. At the same time, new concerns emerged around digital divides, algorithmic bias, and the erosion of face-to-face support. A renewed focus on public value positioned services as a means of fostering trust, inclusion, and ethical governance in complex, data-driven societies.

0.6.7 Current developments and hybrid arrangements

Contemporary service delivery operates in a fluid environment characterised by cross-sector collaboration, real-time data, and rising expectations. The boundaries between public, private, and third-sector actors are increasingly porous, particularly in health, education, and infrastructure. Governments retain responsibility for oversight, coordination, and guaranteeing access, while delegating operational tasks to diverse providers. Current challenges—such as demographic change, ecological transition, and systemic risks—have reinforced the importance of resilient, adaptable service systems that combine efficiency with equity and transparency.

0.7 A Glimpse of the IT Ecosystem

The term *IT ecosystem* refers to the set of interrelated elements involved in the conception, development, operation, and evolution of information systems in an organisation. These elements include technological infrastructure, business processes, governance mechanisms, and, most importantly, the people and roles that shape and support them.

Within an organisation, multiple roles contribute to the governance and use of IT. Executives such as the Chief Information Officer (CIO), Chief Technology Officer (CTO), and Chief Information Security Officer (CISO) lead strategy and oversight, while operational teams carry out the day-to-day tasks of system administration, development, user support, and security. Surrounding this internal structure is a wider environment of external contributors, including technology vendors, service providers, regulatory bodies, and advisory organisations.

Together, these actors form a complex and evolving network.

0.7.1 Internal IT workforce

The internal IT workforce comprises the professionals employed directly by an organisation to manage and operate its information systems. This includes roles in system and network administration, application development, cybersecurity, data analysis, and user support, among others. Depending on the business, organisational size and maturity, these roles may be centralised under an IT department or distributed across business units.

Beyond technical specialisation, internal teams often play a key role in translating business needs into system requirements, managing vendor relationships, supporting compliance efforts, and ensuring the continuity and resilience of services. Their position within the organisation allows for a deeper alignment with strategic priorities and internal culture, although it also requires them to navigate organisational politics, budget constraints, and shifting mandates.

For new professionals, joining the internal workforce (either in IT or in adjacent business functions) means becoming part of the long-term capability of the organisation. It entails not only mastering technical tools but also understanding how to operate within institutional frameworks and contribute to collective goals.

0.7.2 Vendors and technology providers

Vendors provide hardware, software, platforms, and infrastructure services that are critical to most organisations. Their offerings range from enterprise resource planning (ERP) systems to cloud computing platforms, cybersecurity solutions, and specialised vertical applications. Many vendors operate under licensing models or managed service contracts, and some assume responsibility for updates, support, and integration with other systems.

While vendors contribute expertise and economies of scale, their interests and business models may not always align with those of the client organisation. Managing vendor relationships involves careful procurement[18], contract negotiation, performance monitoring, and risk management. Vendor lock-in, limited customisability, and opaque data practices are common challenges.

Understanding the vendor landscape is crucial for professionals working either within the organisation or in consultancy roles. This includes familiarity with the major market players, licensing models, interoperability standards, and the typical lifecycle of vendor-managed solutions.

0.7.3 Consultants and advisory services

Consultants bring external expertise and a broader view of industry practices, often helping organisations frame strategies, specify requirements, evaluate solutions, or manage change. They may be engaged on a short-term basis or through long-term frameworks, and may work independently or as part of larger consultancy firms.

The contribution of consultants can be especially valuable when internal capacity is limited, or when independent assessment is required for governance or accountability. However, consultants do not hold operational responsibility for outcomes. Their work must be integrated into the organisation's internal processes and validated by those with decision-making authority.

Early-career professionals often enter organisations through consultancy roles, particularly in public sector projects. This positioning demands both technical fluency and the ability to listen, analyse, and communicate within institutional environments that are not their own. Developing credibility, understanding the client's context, and respecting internal roles are key to effectiveness in such positions.

0.7.4 Cooperation and boundaries of responsibility

Each actor in the IT ecosystem operates within a set of expectations and boundaries. While internal teams ensure continuity and contextual adaptation, vendors bring scalable solutions, and consultants enable change and reflection. Cooperation across these roles is essential for delivering integrated and sustainable outcomes.

Clear boundaries of responsibility must be maintained to ensure accountability. Operational risk, compliance, data protection, and service quality all depend on understanding who is responsible for what, under which conditions, and with what reporting or escalation mechanisms.

This clarity becomes especially critical in hybrid delivery models, where internal and external contributors jointly manage services. Without well-defined roles, ambiguity can lead to compliance, operational or security issues.

0.7.5 Evolving landscape

The IT ecosystem continues to evolve with developments such as cloud computing, AI-based services, and increased regulatory scrutiny. These shifts affect the distribution of roles, the required skill sets, and the expectations of both public and private organisations.

Professionals must remain adaptable and informed. Whether acting on behalf of an internal unit, a vendor, or a consultancy, understanding the dynamics of the IT ecosystem is essential for making meaningful contributions and supporting sound decision-making.

[18] https://www.investopedia.com/terms/p/procurement.asp

0.8 Consulting Across Borders

Many students in this course already embody a reality that defines today's consulting landscape: cultural diversity, international collaboration, and cross-border organisational complexity. Whether you are an international student, plan to work in a global consulting firm, or engage with public or private sector clients operating across jurisdictions, it is essential to recognise the multinational dimension of information systems management and governance.
It is therefore important to notice that and reflect on cross-border implications of the following topics.

0.8.1 The Multinational as a Structuring Reality

Modern consultancy engagements increasingly involve:

- A **consultant or team based in one country** delivering services to a client in another.
- **Clients who operate internationally**, often with decentralised structures or multinational governance.
- **Suppliers and vendors** from diverse legal and cultural environments.
- **Digital platforms and cloud services** subject to conflicting jurisdictions or regulatory regimes.

While the public–private divide explains many sectoral dynamics, it is the **multinational condition** that often reveals tensions between **legal obligations, cultural expectations, and institutional capacity**.

0.8.2 Legal Diversity and the Importance of Normative Layering

Organisations operating across borders must navigate **heterogeneous legal systems**. For example:

- A Portuguese consulting firm advising a German healthcare group will face differences in **data retention rules, procurement practices, and licensing structures**.
- A platform provider based in the US may not comply automatically with **EU standards on consent and accountability**.

Students should familiarise themselves with the **types of legal instruments** (from EU Regulations like **GDPR** and **DORA**, to national "portarias" or US Executive Orders) because they shape what is possible and required in different contexts.

0.8.3 Organisational and Strategic Implications

Cross-border environments introduce ambiguity in:

- **CxO roles and accountability**, which may be framed differently across countries.
- **Board participation and oversight**, especially in global subsidiaries.
- **Vendor and contract management**, where enforcement and interpretation differ.

Multinational organisations often use **global governance frameworks**, but their **local expression varies**. ISO 27001 or COBIT may be deployed differently in Madrid, São Paulo, or Nairobi, depending on national auditing expectations, institutional maturity, or cultural attitudes towards compliance.

0.8.4 Cultural and Semantic Nuances

Words like "compliance", "audit", or "risk" do not always carry the same **institutional or ethical weight** in different countries. A practice considered normal in one place (e.g. informally resolving IT incidents) may be seen as inadequate or unethical elsewhere.
This has direct implications for **conceptual modelling and stakeholder engagement**, which you will practise in seminar exercises and conceptual maps. Also important is to consider how stakeholder identification and communication strategies must adapt when working across cultural boundaries.

0.8.5 Implications for a Future Professional

An IT professional nowadays will:

- Work in teams with different **cultural styles of decision-making, escalation, and reporting**.
- Be expected to navigate **remote governance chains** or **comply with multiple regulatory frameworks**.
- Translate not only **languages**, but also **concepts** across disciplines, cultures, and legal systems.

Effectiveness in this context will depend on more than technical accuracy, it will hinge on the ability to **contextualise, interpret, and adapt**. This is a key professional skill, especially when interfacing with CIOs, CTOs, or CISOs who operate in multinational ecosystems.

0.8.6 What to Pay Attention to Later

In all four themes, we'll be encouraged to reflect:

- How would this issue change if the organisation were operating in multiple jurisdictions?
- How does governance maturity differ when regulatory obligations are divergent or overlapping?
- What adjustments must a consultant make when advising across borders?

Keep this sheet in mind as you engage especially with:

- (Strategic Alignment, Accountability and Decision Rights.
- Governance of IT Risks and Compliance.
- Regulatory Context, including for AI and Algorithmic Systems.

0.8.7 Conclusion

The multinational is not a complication, it is a reality. Recognising its relevance now will allow you to interpret governance structures more clearly, identify strategic risks more insightfully, and advise with greater credibility. Start early: highlight multinational tensions when you see them in cases, stories, personas, or strategic frameworks. This lens is not optional. It is foundational to your future effectiveness.

0.9 Timeline of IT in Business and Governance of IT

From mainframes to the cloud, IT reshaped business and governance through time.

0.9.1 Early Foundations: the Advent of Business Automation

We can say that the historical journey of Information Technology (IT) in business began with the emergence of programmable machines in the mid-20th century, notably marked by IBM's entry into commercial computing. IBM's 1401 and subsequently the System/360 mainframes (1960s) enabled centralised data processing at scale, supporting administrative and accounting functions in large organisations. Automation was mainly restricted to batch processing of transactions, inventory control, and payroll.

These early systems were closely tied to rigid organisational hierarchies, where centralised IT departments operated under technical command, separate from business strategy. Governance structures were informal, focused primarily on cost control and operational efficiency.

0.9.2 The Rise of Data Management and Governance of IT Awareness

The introduction of Database Management Systems (DBMS), notably IBM's System R in the 1970s, marked a paradigm shift. By supporting the relational model proposed by E. F. Codd, organisations began managing data as a strategic resource. With data independence and query languages like SQL, IT became a more flexible and powerful tool for supporting managerial decision-making.

This era also witnessed the first instances of recognising the importance of aligning IT decisions with business needs. The concept of the Chief Information Officer (CIO) started to emerge, albeit inconsistently, as organisations realised the growing dependency on IT.

0.9.3 Decentralisation: Personal Computing

The 1980s saw the advent of microcomputers and personal computing, with landmark products such as the IBM PC and Apple Macintosh. IT capabilities moved beyond central data centres into departments and individual offices. Spreadsheets like Lotus 1-2-3 and later Microsoft Excel empowered managers to directly interact with data, reducing reliance on IT intermediaries.

Decentralisation introduced new governance challenges, including shadow IT, inconsistencies in software usage, and uncontrolled data replication. Operational autonomy increased, but strategic oversight was often lacking.

0.9.4 Networking and the Emergence of Enterprise-Wide Governance of IT

With the proliferation of local area networks (LANs) in the 1990s and the widespread adoption of enterprise resource planning (ERP) systems, organisations began to recentralise their IT architectures in a more integrated manner. governance of IT matured through structured frameworks, driven in part by the need to coordinate across geographies and functions.

The role of IT in business strategy became clearer. Regulatory compliance also drove formalisation of governance, internal controls, and risk management.

0.9.5 The Internet and the Digitalisation of Business Processes

The rise of the internet and e-commerce at the turn of the millennium transformed customer engagement, supply chains, and marketing. Organisations embraced Business Process Management (BPM) as a discipline, aiming to digitise and optimise processes end-to-end. BPM tools and methodologies allowed for rethinking and redesigning processes with IT as a native enabler.

This was a critical moment for the convergence of governance of IT and business governance, as digital processes required both technological robustness and business adaptability.

0.9.6 Mobile Computing and the Always-On Enterprise

The 2000s introduced mobility as a dominant feature, through smartphones, tablets, and wireless networking. The consumerisation of IT blurred the boundary between personal and enterprise devices, challenging traditional governance approaches. Bring Your Own Device (BYOD) policies, mobile device management, and context-aware security controls became necessary responses.

IT governance expanded to encompass not only internal management but also customer interactions, third-party platforms, and real-time data. The CISO role gained prominence as cybersecurity threats increased with always-connected endpoints.

0.9.7 Cloud Computing and Platform Governance

With the cloud, we have seen a shift towards cloud-native architectures, platform ecosystems, and on-demand scalability. Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) models altered the financial and operational models of IT, transforming capital expenditure (CapEx) into operational expenditure (OpEx), and accelerating the pace of innovation.

Governance frameworks evolved to address shared responsibility models, vendor lock-in, data sovereignty, and service-level agreements. IT management also had to adapt to new challenges, such as multi-cloud strategies, continuous deployment, and agile development practices.

0.9.8 Present Challenges and Future Directions

The governance of IT is nowadays inseparable from corporate governance. AI, edge computing, the Internet of Things (IoT), among many other concepts, continues to expand the scope of digital infrastructures. Governance now encompasses not only compliance and risk, but also ethics, sustainability, and digital sovereignty.

Future trends will likely demand dynamic governance systems capable of responding to technological disruptions, geopolitical shifts, and evolving societal expectations, while maintaining resilience, accountability, and transparency.

0.10 Timeline of IT Services and Consulting

The development of IT services and consulting has closely mirrored the expansion of digital technologies and their growing importance in organisational contexts. This evolution has been marked by successive waves of technological innovation, changing business needs, and the professionalisation of service delivery. While early IT consulting was tightly linked to hardware provision, the scope of services has since broadened to include strategic advisory, digital transformation, and regulatory compliance.

0.10.1 The origins of IT service

The origins of IT service provision date back to the 1950s and 1960s, when mainframe computers began to be deployed in government agencies, universities, and large corporations. Vendors such as IBM played a dual role as technology suppliers and advisors, helping clients configure, operate, and maintain complex systems. Early service engagements were highly technical, often involving custom programming and infrastructure design.

0.10.2 The period of SDLC

During the 1970s and 1980s, IT services expanded to include systems analysis, application development, and business process automation. The emergence of structured methodologies, such as the systems development life cycle (SDLC), introduced a more disciplined approach to designing and implementing informaion systems. Consulting began to intersect with operations research and management science, laying the foundations for enterprise integration and large-scale IT project management.

0.10.3 The period of the ERP

The 1990s brought transformative change with the widespread adoption of enterprise resource planning (ERP) systems and the rise of the internet. IT services providers evolved to address the complexity of multi-site deployments, data migration, and organisational change. Global consulting firms and system integrators emerged as major players, offering end-to-end solutions that combined software, infrastructure, and advisory components. The notion of aligning IT with business objectives gained prominence, along with formal models of governance of IT and portfolio management.

0.10.4 The internet

From the early 2000s onward, the landscape diversified further. Cloud computing, mobility, and software-as-a-service (SaaS) models altered the economics of IT service delivery. At the same time, growing awareness of cybersecurity threats and regulatory obligations (especially in sectors such as finance, healthcare, and public administration) expanded the role of IT services into risk management and compliance. Service providers adapted by offering managed services, security operations, and compliance consulting.

0.10.5 “Digital transformation”

In the 2010s, **digital transformation** became a key buzzword of IT service demand. The concept refers to a structured process of change that repositions an organisation to better achieve its strategic objectives in response to internal or external drivers. **While the idea itself is not new**, it has increasingly shaped strategic thinking through consulting practices that integrate agile delivery models, DevOps automation, and user-centred design. Public sector initiatives in digital government, smart cities, and data interoperability introduced new focuses for challenges and opportunities, often requiring coordination between technology providers, legal advisors, and institutional reformers. Meanwhile, privacy regulations such as the GDPR and the growing relevance of digital identity intensified the need for integrated legal, ethical, and technical expertise.

0.10.6 …and here we are!

Today, IT services and consulting represent a diverse and dynamic field…
Providers range from niche specialists to global integrators, offering services that span infrastructure, applications, strategy, compliance, and innovation. The role of consultants has become more interdisciplinary, combining knowledge of architecture, operations, business models, and regulatory frameworks.
As organisations increasingly depend on digital infrastructure, the demand for trusted, adaptable, and forward-looking service partnerships continues to grow.

0.11 Timeline of Governance of IT in Public Sector Services

Information technology has become progressively central to the organisation and delivery of public services. The governance of IT in the public sector reflects broader changes in public administration, technological capabilities, and expectations of transparency, efficiency, and service quality. This timeline outlines the evolution of governance of IT as it relates to public service provision, from early data processing units to contemporary models of digital governance and data stewardship.

0.11.1 1960s–1970s: Central computing and administrative automation

The initial use of IT in public administration focused on automating repetitive tasks in large bureaucracies. Mainframe computers were introduced in central government departments to handle payroll, taxation, and census data.

These systems were technically complex and capital-intensive, requiring specialised personnel and controlled environments. governance of IT during this period was implicit, centred on procurement procedures and operational reliability, with limited concern for integration or policy alignment.

0.11.2 1980s: Departmental autonomy and early decentralisation

As computing power became more accessible, ministries and agencies began to acquire their own systems, often independently. Personal computers and minicomputers enabled decentralised data processing, but also introduced fragmentation and redundancy.

Governance of IT was still largely technical, oriented around hardware procurement, licensing, and data security. Strategic alignment with organisational goals was seldom explicit. This era also saw the first experiments in IT policy units within ministries of finance or public administration.

0.11.3 1990s: E-government emergence and coordination mechanisms

The 1990s marked the beginning of coordinated efforts to use IT for improving public service delivery. The concept of e-government gained prominence, advocating the use of digital tools to streamline transactions, reduce bureaucracy, and increase transparency.

Governments began to define national IT strategies and establish central coordinating bodies or chief information officers (CIOs). Interoperability and citizen access became policy priorities. Governance of IT shifted from isolated technical management to issues of standardisation, architectural coherence, and cross-agency collaboration.

0.11.4 2000s: Integration, interoperability, and process reengineering

Public administrations pursued deeper integration of back-office systems and interoperability frameworks. Enterprise architecture methodologies began to be adopted to guide large-scale transformations.

Governance of IT structures evolved to include strategic planning, investment oversight, and performance measurement. The creation of shared service centres and common platforms aimed to reduce duplication and improve service coherence. Public sector CIO roles gained visibility, and policy frameworks increasingly emphasised alignment between IT initiatives and organisational objectives.

0.11.5 2010s: Digital government and data-centric governance

Digital government strategies expanded the focus beyond e-services, promoting full digitalisation of processes and the redefinition of service models.

Governance of IT became more complex, encompassing cybersecurity, open data policies, cloud computing, and mobile access. Issues of digital identity, privacy, and regulatory compliance grew in importance. Agile project management and user-centric design were introduced in contrast to earlier waterfall approaches. New roles such as chief data officers (CDOs) emerged to address data governance, analytics, and ethical use of information.

0.11.6 2020s: Resilience, ethics, and public value in digital governance

Recent developments reflect a maturing of governance of IT frameworks in response to crises (e.g., pandemics, cyberattacks) and evolving public expectations. Emphasis has shifted toward resilience, inclusiveness, and ethical use of AI and automation.

Public sector organisations have adopted digital-by-default principles, while also addressing the risks of digital exclusion. Whole-of-government platforms and cross-sector interoperability initiatives highlight the growing complexity of coordination. Governance of IT now encompasses not only technology and service alignment, but also public trust, legitimacy, and responsible innovation.

0.12 Also, Some Ambiguity...

Throughout the evolution of IT in business, certain concepts have gained popularity not because of their clarity, but precisely due to their **fuzziness**. These terms often serve strategic or rhetorical purposes: signalling change, creating alignment around vague aspirations, or supporting consultancy pitches and policy agendas. Many such concepts combine technological innovation with managerial ambition — but without concrete or consistent meaning.

What follows is a historical reflection on **buzzwords and vague constructs** that have shaped the discourse, sometimes usefully, often confusingly.

0.12.1 1970s: "Paperless Office" & "Decision Support Systems"

- The promise of the *paperless office* emerged with word processors and early digital storage. Despite recurring declarations of its arrival, paper usage increased for decades.
- *Decision Support Systems (DSS)* aimed to bring structured and semi-structured decision-making into computing logic. While based on valid needs, implementations were rare and often conflated with simple reporting.

0.12.2 1980s: "Information Systems Strategy" & "Office Automation"

- The term *Information Systems Strategy* became popular as CIOs began to enter executive ranks. However, many of these "strategies" amounted to infrastructure roadmaps or technology acquisition plans, without a business model view.
- *Office Automation* promised seamless electronic workflows. In practice, it often meant replacing typists with PCs, without redesigning underlying processes.

0.12.3 1990s: "Reengineering" & "Knowledge Management"

- *Business Process Reengineering (BPR)*, popularised by Hammer and Champy, advocated for radical process redesign. While it produced meaningful results in some cases, it was often used to justify workforce reductions or imposed top-down reforms without stakeholder engagement.
- *Knowledge Management* aimed to capture and disseminate organisational knowledge. Despite extensive investment, many KM initiatives struggled to go beyond document repositories or intranets.

0.12.4 2000s: "e-*everything" & "Innovation"

- The prefix *e-* (e-business, e-government, e-health) was often applied indiscriminately, even when the initiatives merely digitised paperwork or offered web access to existing services.
- *Innovation* became a catch-all term, increasingly decoupled from actual invention, process improvement, or market impact. It came to refer to any form of "change", whether or not beneficial or evidence-based.

0.12.5 2010s: "Digital Transformation", "Agility" & "Smart"

- *Digital Transformation* began to dominate discourse, but its usage ranged from migrating to cloud services to changing entire business models, often without distinction.
- *Agile* became a management fad beyond its original software development meaning. Organisations branded traditional hierarchies as "agile" by renaming departments or adopting superficial rituals.
- *Smart* cities, smart organisations, and smart solutions became aspirational labels, frequently attached to projects driven more by technology availability than contextual intelligence or local needs.

0.12.6 2020s: "AI-Driven", "Data-Driven" & "Sustainability"

- *AI-Driven* is now a dominant label, even for systems with minimal learning capabilities or human-centred logic. The opacity of what constitutes "AI" facilitates this elasticity.
- *Data-Driven* has become a mantra, yet many decisions remain intuition-based, with data used for post-hoc justification. The challenge of data quality, bias, and governance is often neglected.
- *Sustainability* is increasingly invoked in digital projects, sometimes as a core goal, sometimes as a compliance add-on, often without clarifying the environmental, social, or economic metrics at stake.

0.12.7 Navigating the Ambiguity

Fuzzy terms are not necessarily harmful. They can foster alignment across disciplines, initiate dialogue, or create momentum. However, when left unexamined, they lead to **conceptual inflation**, **unmet expectations**, or **policy drift**. For those engaged in governance of IT and strategy, the challenge is to:

- **Define clearly** what is meant in each context;
- Distinguish rhetoric from capability;
- Understand the historical cycles of management fads;
- Ground discussions in the actual functioning of organisations and systems.

Clarity is not always possible, but critical reflection is always necessary.

0.13 The Rise of Information Security and Cybersecurity

Information security (InfoSec) and **cybersecurity** have undergone a significant transformation along time. What began as a technical issue confined to IT departments has evolved into a central pillar of organisational governance. They are now considered a matter of strategic concern and board-level accountability, especially as digital dependence, regulatory requirements, and reputational risks have grown. This evolution can be traced through distinct phases that mirror technological developments, changing threat landscapes, and shifting governance expectations.

0.13.1 How Information Security and Cybersecurity Relate

InfoSec and **cybersecurity** are closely related but not identical.

Information security focuses on protecting information in all its forms, across physical and digital domains.
Cybersecurity is a subset of InfoSec that concentrates specifically on digital threats and the protection of systems connected to the internet.

While cybersecurity addresses external and malicious threats related to the exposure to the internet, information security also covers internal policies, roles, and controls.

0.13.2 1960s–1970s – Mainframes and Physical Security

Information security was limited to physical access controls and procedural safeguards in centralised computing environments. Mainframes operated in tightly controlled facilities, and the main risk was unauthorised physical access. Passwords were rudimentary, and formalised policies were rare. Security was operationally managed by IT staff, with no institutionalised oversight.

0.13.3 1980s – Personal Computers and Fragmentation

The rise of personal computing decentralised control. Software piracy, viruses, and data loss became prevalent, but responses remained technical and reactive. Antivirus tools and early forms of access control emerged. However, governance remained weak, and information security was not seen as a management concern beyond the IT function.

0.13.4 1990s – Networking and Policy Emergence

With the advent of local and wide area networks, internet connectivity, and shared resources, the attack surface expanded. Firewalls, intrusion detection systems, and corporate security policies were introduced. Information security began to feature in audits, and early roles akin to Chief Information Security Officers (CISOs) appeared in some multinational firms. Security concerns started reaching senior management, though still treated as a support function.

0.13.5 2000s – Regulatory Drivers and Risk Framing

Cybersecurity incidents such as ILOVEYOU and SQL Slammer gained public attention. Regulatory frameworks like SOX (USA), HIPAA (health), and the EU Data Protection Directive introduced formal compliance obligations. Organisations started recognising information security as an element of enterprise risk. Security governance structures developed, CISOs became institutionalised roles, and regular reporting to senior leadership began. Security moved from IT operations into enterprise risk management.

0.13.6 2010s – Strategic Integration and Digital Risk

Cybersecurity was increasingly viewed as a business continuity and reputational risk issue. Large-scale breaches (e.g. Target, Equifax) demonstrated the business consequences of weak security. Risk appetite frameworks began including digital threats. Boards demanded visibility over cyber risk postures. Governance, Risk, and Compliance (GRC) platforms integrated security indicators. Cybersecurity was linked to resilience and regulatory trust.

0.13.7 2020s – Board-Level Accountability and Regulatory Imperatives

Cybersecurity is now regularly addressed by the Board of Directors. Ransomware, supply chain attacks, and geopolitical tensions have made cyber resilience a strategic concern. Regulatory obligations such as the NIS2 Directive, and DORA, for example, as also references such as ISO/IEC 27001 updates formalise board-level responsibilities in relation to InfoSec. InfoSec maturity is nowadays evaluated during **audits**, **due diligence**, and ESG reporting, sometimes with a strong focus on cybersecurity. It now shapes corporate reputation, investor confidence, and institutional trust.

0.13.8 Implications for Governance, Risk, and Compliance (GRC)

InfoSec has become embedded in organisational governance. It intersects with risk management, compliance, and strategic decision-making. Mature organisations no longer treat cybersecurity as a support function but as a strategic domain requiring board engagement, formal roles (e.g. CISO), and integration into management systems.
In private organisations, InfoSec and cybersecurity in special influences investment decisions, vendor selection, and market reputation. In public sector entities, it is fundamental to service continuity, citizen trust, and legal compliance. Across sectors, maturity in cybersecurity governance reflects the broader maturity of GRC structures.

0.13.9 Consulting Relevance

Consultants must assess not only the technical capabilities of an organisation but also the placement of cybersecurity within its governance structure. If cybersecurity lacks executive oversight or is absent from strategic documents, this is a signal of **low maturity**. Clients should therefore be motivated and supported in moving from ad hoc protections to integrated, risk-informed, and auditable security governance models.

0.14 The Rise of Data Privacy

Data privacy refers to the right of individuals to control how their personal information is collected, used, stored, and shared. It encompasses the legal, technical, and organisational measures that ensure personal data is handled in a manner that respects individuals' rights, freedoms, and expectations.

Data privacy has become a defining concern in digital governance, reshaping how organisations collect, process, and share personal information. Like cybersecurity, privacy evolved from a marginal technical topic to a board-level issue. Today, data privacy intersects with strategic risk, operational maturity, public trust, and regulatory compliance.

0.14.1 How Privacy Differs from Security

While closely related, data privacy and InfoSec are distinct. Privacy is concerned with the proper use of personal data: who collects it, why, how it is processed, and with what consent. Security, by contrast, is concerned with protecting data from unauthorised access or harm. A system may be technically secure yet still violate privacy if it collects excessive data or lacks transparency (what might be not intentional, as a consequence of low governance and management maturity, or be intentional, as a consequence of intended business models, or other business goals).

0.14.2 1970s–1980s: Early Legal Recognition

Early privacy laws emerged in response to the growth of computerised databases. The German state of Hesse introduced the first noticed data protection law in 1970. The OECD Guidelines (1980) established foundational principles such as purpose limitation, consent, and transparency.

0.14.3 1990s: European Leadership and Sectoral Laws

The EU Data Protection Directive (1995) set a harmonised framework across Member States. In parallel, the U.S. developed sectoral laws (e.g. HIPAA for health, COPPA for children). In organizations, privacy was starting to be treated as a compliance issue managed by legal departments.

0.14.4 2000s: Web 2.0 and Platform Economy

Mass data collection through social media platforms and search engines introduced new risks. Profiling, behavioural advertising, and opaque terms of service led to increased scrutiny. The role of the Data Protection Officer (DPO) began to emerge in Europe.

0.14.5 2010s: Strategic Relevance and GDPR

The General Data Protection Regulation (GDPR), adopted in 2016 and enforced from 2018, marked a worldwide paradigm shift. It introduced extraterritorial scope, accountability, data subject rights, and heavy fines. Privacy became a board-level concern. Organisational roles (DPO, privacy officers) became institutionalised.

0.14.6 2020s: Globalisation, AI, and Strategic Risk

Dozens of countries have adopted GDPR-inspired laws. Meanwhile, AI, biometrics, and cross-border data flows challenge traditional privacy models. Privacy is now treated as a strategic asset: its mismanagement can lead to loss of trust, reputational damage, and regulatory sanctions. Board engagement and organisational integration are essential.

0.14.7 Implications for GRC

Privacy governance is now part of GRC maturity. Policies must go beyond legal wording to address internal processes, system design, vendor management, and cultural awareness. The concept of "Privacy by Design" embeds controls from the start. Data mapping, risk assessments (DPIAs), consent mechanisms, and user rights interfaces are signs of organisational maturity. Consultants should assess whether privacy is managed by isolated legal units or integrated into enterprise-wide processes. They should also consider if roles in relation to that are symbolic or empowered, and if data protection is reactive or proactive. Many scenarios of tension between providers and costumers arise from misunderstandings in relation to these concerns.

0.15 Vocabulary

The basic vocabulary used to describe "digital things" is often applied inconsistently. The following concepts are frequently used in organisational contexts, yet not always with a shared understanding or agreed definitions, in other words, without a clear ontological commitment[19].

0.15.1 Technology: The Enabler

Technology refers to the **enabling** tools that support digital functions. It includes:

- **Hardware** – physical devices such as servers, laptops, smartphones, and sensors;
- **System Software** – operating systems, virtualisation platforms, device drivers, and other components that manage hardware and provide basic functionality;
- **Infrastructure** – the networks, data centres, cloud environments, and related security mechanisms that enable access, scalability, and resilience.

Technology provides foundational capabilities but does not, by itself, define what the organisation does. It is neutral with respect to business logic or user needs.

0.15.2 Application: The Functional Layer

An application is **a purposeful use of technology designed to meet specific business needs**. It embodies business logic (rules, calculations, and decision paths) and offers interfaces for users or other systems. Applications are where technology becomes *meaningful*. Examples include an invoicing application that calculates taxes and generates payment slips; a hospital scheduling system that matches doctors to shifts and appointments; A university admissions portal that guides applicants through forms and deadlines.

Applications are not just tools, they are *organisational artefacts* that shape and are shaped by internal processes, user expectations, and institutional responsibilities.

0.15.3 System: A Fuzzy but Useful Concept

The term *system* is widely used but not always precisely defined. It may refer to:

- A **technical composition** of interacting components (hardware, software, data).
- An **organisational system** involving roles, procedures, and governance structures.
- A **socio-technical configuration**, where digital elements and human practices are interdependent.

For example, an "HR system" might include a software platform, a set of reporting obligations, defined roles in HR and IT, and a shared understanding of how personnel data is maintained.

Systems are dynamic, partial, and interpreted differently by different actors. From a governance perspective, this ambiguity matters: who defines the system's boundaries? Who owns it? Who is accountable when it fails or evolves?

0.15.4 Service: Delivery with Accountability

A service is the structured delivery of a capability to a user. It involves not only technology and applications, but also service-level definitions, responsibilities, and user expectations. Examples can be a file storage service that offers backup, access control, and user quotas; a tax filing service provided by a public administration; an authentication service that allows single sign-on across systems.

Services are often governed through **service level agreements** (SLAs), which define uptime expectations, response times, escalation paths, and other metrics. Services are central to IT management because they frame what is *delivered*, not just what is *installed*.

0.15.5 Process and Process Automation

A process is a sequence of activities (which might be decomposed in tasks) and decisions through which something is produced. Processes can be manual, automated, or a mix of both.

Digital systems often encode or enforce processes: a loan approval workflow, a payroll cycle, or a citizen identity verification procedure. From a governance point of view, processes define roles, responsibilities, and control points. They are also the basis for performance measurement, audit trails, and compliance validation.

Automation of processes support or replaces manual steps with machine-executed actions, increasing speed, consistency, and traceability. Automation is not always desirable. Inappropriate automation can reduce adaptability, obscure responsibility, or create governance gaps. Decisions about automation require careful reflection on risk, flexibility, and oversight.

Process design and process automation are not just technical concerns, they reflect strategic choices about accountability, risk tolerance, and service quality.

0.15.6 Data, Databases, and Persistence

*Data is the digital representation of facts, events, or **records**. It is stored, processed, and transmitted by systems, and is central to both compliance and value creation.*

Databases are structured environments for managing data, typically using a database management system (DBMS). Persistence refers to the capacity of a system to retain data over time, ensuring that information is not lost between sessions or after failures.

***Data Retention** is the practice of preserving data for a designated period, in line with legal, regulatory, or organisational requirements, to ensure availability, accountability, and compliance.*

0.15.7 Interfaces and Integration

Interfaces are points of interaction between users and applications (user interfaces), or between systems (e.g., APIs). They define how integrated systems communicate, exchange data, or present information. Integration refers to the coordination of separate systems to form a coherent whole. Poor integration results in duplication, inconsistency, and friction. Properly systems support seamless workflows, real-time information access, and collaborative operations.

From a governance perspective, integration raises questions about ownership, compatibility, and resilience.

0.15.8 Conclusion

Understanding how stakeholders define key terms within a specific context, such as technology, application, system, process, and service, is essential for effective engagement. The use of these concepts often varies across business domains and organisations, leading to ambiguity and, at times, ontological confusion. Being mindful of these differences is crucial. It's important to avoid imposing your own definitions unless there is a well-grounded, objective reason for doing so.

[19] https://en.wikipedia.org/wiki/Ontological_commitment

0.16 On Types of Information Systems in Business Contexts

The term "information system" refers not merely to technology, but to purpose-driven arrangements that support decision-making, coordination, compliance, and service delivery. These systems operate within an institutional context: they reflect, reinforce, or challenge how organisations are structured and how they function. While engineers may be familiar with underlying technologies (such as databases, applications, or web services) this course requires a shift in focus: from components to their organisational roles.

This sheet provides a foundational orientation to the types of information systems typically found in business settings. It distinguishes systems not by technical architecture, but by their functional purpose: supporting Governance, Risk, and Compliance (GRC); enabling management coordination and oversight; and executing operational activities.

2. Classification by Organisational Function

Business information systems can be broadly grouped according to their dominant purpose:

- **GRC-Oriented Systems** are used to ensure accountability, transparency, and alignment with internal rules or external regulations. They help manage compliance obligations, institutional risk, and auditability.
- **Management-Oriented Systems** support planning, coordination, performance tracking, and resource allocation across departments. They are often integrated with reporting and business intelligence capabilities.
- **Operations-Oriented Systems** are focused on the day-to-day delivery of services or production of goods. These systems typically automate transactions, manage logistics, or provide customer-facing interfaces.

These categories are not mutually exclusive. In practice, many systems intersect multiple domains (for example, an ERP system may support both operational workflows and internal financial compliance).

3. Examples and Roles of Common Systems

Below is a brief overview of widely adopted names for types of systems, grouped by function (examples are illustrative and vary by sector and organisational scale):

GRC-Focused Systems:

- **Risk Management Systems:** Tools to help identify and assess organisational risks, often integrated with internal controls or audit logs.
- **Compliance and Audit Platforms:** Tolls to track regulatory obligations, generate reports, and support certification processes (e.g., ISO 27001, GDPR).
- **Governance Dashboards:** Tools used by boards or CxOs to monitor policy adherence, role-based access, and control structures.

Management-Focused Systems:

- **Enterprise Resource Planning (ERP):** A fussy concept, used to refer a large spectrum of tools that integrate core functions like finance, procurement, HR, project accounting, etc. Common vendors include SAP, Oracle, Microsoft, etc.
- **Business Intelligence (BI) Tools:** Enable data aggregation, dashboarding, and KPI monitoring. Examples include Tableau, Power BI, and Qlik.
- **Strategy and Performance Platforms:** Support balanced scorecard tracking, portfolio management, and internal benchmarking.
- **Document Management Systems (DMS):** Provide version control, classification, access management, and long-term archiving of business documents subject to retention requirements.

Operations-Focused Systems:

- **Customer Relationship Management (CRM):** Manage customer data, marketing campaigns, etc. Tools like Salesforce or HubSpot are common.
- **Supply Chain Management (SCM):** Coordinate logistics, inventory, and supplier relationships. Frequently integrated with ERP systems.
- **Point of Sale (POS) and ePOS Systems:** For transactions in physical and digital retail contexts, with real-time data feeds into inventory and finance modules.
- **HR Information Systems (HRIS):** Track personnel data, payroll, contracts, and compliance with HR legislation.
- **Case Management Systems (CMS):** Support structured or semi-structured processes centred on individual cases (claims, service requests, investigations, or legal matters) by integrating data, documents, and workflows. Core in knowledge-intensive domains (legal services, criminal investigation, healthcare, etc.).

4. Variations Across Sectors

The relative importance and configuration of these systems vary significantly between organisational contexts:

- **In private sector firms**, CRM and ERP systems are often central, reflecting the importance of customer engagement, revenue tracking, and supplier coordination. In retail, for instance, POS systems are tightly coupled with inventory and analytics platforms to support agile pricing and stock decisions.
- **In public sector organisations**, CMSs and DMSs take precedence, given the need for traceability, procedural fairness, and service accountability. Compliance tools are often tied to specific regulations (e.g., data protection, public procurement) rather than to market competitiveness.
- **In heavily regulated industries** such as banking, energy, or healthcare, governance and audit tools are often embedded within broader management systems, with strict access control and traceability. Here, the distinction between operational, compliance, and governance roles may be blurred (intentionally) for integrated oversight.

Recognising these differences is essential not only for system design or procurement, but also for stakeholder engagement. A system that may be described technically in terms of "workflow automation" or "reporting capability" carries very different organisational meanings de pending on whether it is used to sell a product, issue a tax decision, or manage a patient record.

0.17 On Legal Systems and Normative Layers

Understanding **legal systems** is essential for CxO-level engagement, as strategic decisions, risk management, and regulatory compliance all depend on recognising which norms apply, how they are enforced, and how they shape organisational responsibilities across jurisdictions.

0.17.1 Types of Legal Systems

Legal systems can vary significantly in structure and culture, fallowing in general into these three main traditions.

- **Common Law Systems** (e.g., United Kingdom, United States, Canada): These systems place high value on judicial decisions as sources of law. Statutes are important, but case law (precedent) plays a central role. Regulations and policies are often developed through a mix of legislative acts (e.g., Acts of Parliament, Executive Orders) and judicial interpretation. In the UK, for example, legal acts include *Acts*, *Statutory Instruments*, and *Guidance Notes*, with courts able to influence regulatory meaning through interpretation.
- **Civil Law Systems** (e.g., Brazil, Japan, South Korea): Similar to Portugal, these countries rely on codified laws and place less weight on judicial precedent. Legislative acts are categorised into constitutions, laws, decrees, and regulations, with executive authority playing a key role in implementation.
- **Hybrid and Religious Systems** (e.g., Saudi Arabia, India, South Africa): Some countries combine elements of civil and common law or apply religious law in parallel with secular legal frameworks. For instance, India integrates common law with constitutional norms and significant judicial activism. In contrast, Saudi Arabia's legal system is based on Sharia law, supplemented by royal decrees.

0.17.2 Legal Instruments in the European Union

The European Union (EU) operates through a unique supranational legal system in which its institutions can adopt binding or non-binding **legal acts** that apply to member states and, in some cases, to individuals or organisations directly. These acts are hierarchically structured and vary in scope, purpose, and enforcement mechanisms.

The common types of EU legal acts include:

- **Regulations**: Binding legislative acts that are directly applicable in all member states without the need for national transposition. They override any conflicting national laws and ensure uniformity. For example, the General Data Protection Regulation (GDPR) applies directly across all EU countries.
- **Directives**: Binding as to the results to be achieved, but leave it to member states to decide the form and method of implementation. Directives must be transposed into national law within a specified timeframe. A notable example is the NIS Directive on cybersecurity.
- **Decisions**: Binding only upon those to whom they are addressed (e.g., a member state, a company). These are often used in competition law and state aid cases.
- **Recommendations and Opinions**: Non-binding instruments used to express guidance or policy orientation. Although they carry no legal force, they may influence policy or judicial interpretation.

The European Commission (EC) is primarily responsible for initiating legislation. The Council of the EU (representing governments) and the European Parliament (representing citizens) jointly they **debate, amend, and approve legislation** proposed by the **EC**. Enforcement is carried out by national authorities and, when necessary, through the Court of Justice of the EU (CJEU).

0.17.3 Other Supranational Regulations

Outside the EU, other supranational regulations exist but tend to be sectoral or treaty-based, and enforcement relies on diplomacy, arbitration, or international courts. Examples are the regulations of the World Trade Organization (WTO), conventions by the International Labour Organization (ILO), or data-related rules from the OECD.

0.17.4 EU National Legal Systems

Within the EU, each member state retains its own legal system and constitutional structure. While EU law has supremacy over conflicting national laws, domestic legal instruments remain essential for the implementation of directives and the regulation of areas not harmonised at the EU level. **In Portugal, normative acts are categorised according to their source and hierarchical authority**:

- **"Lei" (Law)**: A general rule adopted by the Assembleia da República (Parliament), used to regulate broad domains of public life, including civil, criminal, administrative, and economic matters.
- **"Decreto-Lei" (Decree-Law)**: A normative act issued by the Government, typically under legislative authorisation from the Parliament, or under its constitutional power during periods when the Assembly is not in session. These are common instruments for day-to-day regulation.
- **"Portaria"**: A ministerial decree, used for more specific or technical regulation, typically to implement a broader law or decree-law. For example, a "portaria" might define procedures, forms, or administrative fees.
- **"Resolução do Conselho de Ministros" (RCM)**: A resolution from the Council of Ministers, often used to approve strategic plans, guidelines, or policy intentions. These are not usually binding in themselves but set the direction for administrative actions. They are an instrument for governance within the government itself and the public services.
- **"Despacho"**: An administrative order issued by a public official, typically within a ministry or public service body. It reflects internal decisions or implementation steps.

These instruments are part of a broader civil law system, where the written law prevails, and legal certainty and predictability are prioritised.

Many other EU countries follow similar civil law traditions, although variations exist. For instance, Germany uses *Verordnungen* (ordinances) and *Gesetze* (laws) with comparable scope. France applies *lois*, *décrets*, and *arrêtés*. Despite differences in terminology and institutional structure, most EU countries maintain a hierarchy of norms under a constitution and integrate EU law through national constitutional mechanisms.

0.17.5 Conclusion

Understanding legal systems is fundamental for analysing the governance of technology and information. Whether engaging with a regulation from the EU, a directive transposed into national law, or a "portaria" defining operational procedures in Portugal, it is essential to recognise the authority, scope, and enforceability of each normative act.

0.18 Knowing, Naming, and Risk: Why Classifying is a Professional Act

In any professional domain, classifying things is not a neutral or purely technical task. It reflects a way of seeing, of simplifying complexity in order to act, and it always carries risk. What counts as a "thing" to be classified is itself shaped by social, organisational, and technical perspectives. These perspectives are often implicit. When we name a thing, define its boundaries, and assign it to a category, we are not just observing the world; we are helping construct a version of it.

This means that classification is always provisional and situated. The categories we use depend on our goals, our tools, and our institutional context. Misunderstandings arise when people assume these categories are self-evident or universal. What one stakeholder sees as a "system", another may understand as a "process" or a "service". These are not just semantic distinctions; they influence decisions about governance, responsibility, and investment.

The challenge becomes even more pronounced in multinational environments. Organisations that span countries or cultures often operate with divergent conceptual frameworks and regulatory assumptions. A term like "platform", "compliance", or even "risk" may carry different institutional weight depending on the legal system, business culture, or public sector structure in a given country. The act of classification is then not only contextual but also cross-cultural — and the stakes of misunderstanding are higher. Consultants and analysts must be aware that their own definitions may not translate cleanly across borders, and that achieving shared understanding requires careful negotiation and sensitivity to local interpretations.

Adding to the challenge is our own perspective. As engineers, analysts, or consultants, we bring assumptions to every analysis. Sometimes we make these assumptions explicit; often we do not. This is especially risky when we are advising others. If we do not clarify how we are seeing the problem, we risk misalignment and unintended consequences.

For example, a consultant who defines a new tool as a "service" may invoke expectations of availability, accountability, and user support. If the organisation sees it only as a "technology component", the necessary governance structures may be absent. This gap can become a source of operational or strategic failure. In such cases, what looks like a technical mistake is in fact a conceptual misalignment.

This course encourages students to approach classification as a reflective, professional act. Rather than assuming we already understand what a "system", "service", or "risk" is, we ask: *what do we mean by this term, in this context, for this purpose?* This mindset fosters intellectual humility and professional caution. It also prepares students to engage responsibly with complexity, especially when working across disciplinary, institutional, or cultural boundaries.

Precision, then, is not about rigid definitions. It is about awareness: being conscious of how we frame the world and the implications of those choices. In professional settings, where decisions have organisational, legal, and human consequences, this awareness is not optional. It is a duty.

Understanding classification as a risk does not mean we avoid it. On the contrary: it means we take it seriously. We reflect, we negotiate meaning with others, and we document our reasoning. Especially in consulting roles, this attitude builds trust and supports the long-term alignment of systems, services, and strategies.

Helping students acquire this awareness is one of the central purposes of this course. *It is not enough to know the definitions; we must understand the stakes of naming. The ability to engage critically and transparently with concepts, classifications, and perspectives (and to do so in diverse, and often multinational, environments) is a professional skill of increasing importance. This course seeks to develop that skill by grounding students in foundational concepts while cultivating reflective, adaptive thinking for real-world consulting and advisory practice.*

0.19 Personas for Exercising...

In a fictional but realistic professional ecosystem, a set of recurring characters has been introduced to support situational reasoning and practical engagement. These personas represent executives and consultants operating in diverse organisational contexts, reflecting variations in leadership style, institutional maturity, and sectoral constraints.
The use of personas enables the formulation of cases and dilemmas grounded in professional dynamics, rather than abstract scenarios. They provide a consistent reference for exercises, discussion, and strategic analysis.

0.19.1 The Executives (Clients)

Public Sector

- **Verónica** – A highly competent public servant executive, known for her integrity and dedication to public value. Methodical and respected, she leads with quiet confidence but may underestimate the inertia embedded in her institution.
- **Lucas** – A visionary executive with strong political instincts. Charismatic and inspiring, but often vague in execution and inattentive to institutional detail. His ambition drives important projects but risks disconnect from operational realities.

Private Sector

- **Alex** – A performance-oriented executive in a competitive business environment. Strategic, focused, and demanding, he rewards competence but has little patience for inefficiency or ambiguity. Operates with high expectations and tight feedback loops.
- **Trish** – A senior executive in a sprawling private organisation. Well-intentioned but overwhelmed, she juggles competing demands with inconsistent follow-through. Tends to delegate without clarifying scope or authority.

0.19.2 The Consultant Teams (External)

Each team is composed of a senior team leader and a junior consultant. These roles enable exercises that explore team dynamics, professional responsibility, and the evolution from technical fluency to institutional insight.

The Dream Team - Known for empathy, strategic clarity, and trust-building, ideal for sensitive environments.

- **Sofia** – Calm and emotionally intelligent, Sofia reads organisations well and builds alignment through diplomacy and structure.
- **Mateus** – Quietly competent and highly responsible, Mateus listens carefully, learns fast, and provides stability. Often the protagonist in public sector scenarios.

The Frenetic Team - Associated with innovation and speed, but often prone to improvisation and risk.

- **Carla** – Dynamic and energetic, Carla excels in pressure environments but may overlook strategic grounding.
- **Tiago** – Creative and enthusiastic, Tiago brings raw energy but lacks maturity. Prone to assumptions and overcommitment.

The Mature Team - Structured and precise, frequently deployed in high-stakes or complex environments.

- **Laura** – Disciplined and principled, Laura brings rigour and coherence to engagements. A natural reference point in certification and compliance contexts.
- **Tomás** – Thoughtful, analytical, and detail-oriented. Tomás delivers depth over speed and models professional preparedness.

The Wildcard Team - Engaged when conventional approaches are unlikely to succeed or when fresh perspectives are essential.

- **Inês** – Brilliant and disruptive, Inês challenges norms and reframes problems. Effective in uncovering blind spots, though not always welcomed by cautious clients.
- **Fábio** – Visionary but unpredictable. Offers insight or confusion depending on context. Requires careful mentoring and boundary-setting.

The Contingent Team - Adaptable and pragmatic, often assigned to fluid, operationally critical, or resilience-focused environments.

- **Ricardo** – A battle-tested senior consultant with strong operational experience. Navigates ambiguity effectively and builds trust through results, not rhetoric.
- **Bruna** – Academically strong and grounded in systems thinking. While still developing fluency in field situations, she brings clarity and structure under pressure.

0.20 Wrap-up…

Below are listed foundational ideas necessary to understand how organisations emerged, evolved, and how they operate today (these concepts frame the historical, legal, and institutional landscape in which information systems governance and management must be interpreted):

- **Organisation as a Technical System** – The view of organisations as purpose-driven structures where processes, roles, and resources are coordinated to achieve defined goals, focusing on efficiency, clarity, and measurable outcomes.
- **Organisation as a Social Construct** – The view of organisations as dynamic entities shaped by shared meaning, norms, power relations, and cultural interpretation, where formal structures are continuously reinterpreted by people.
- **Freedom to Organise** – The historically contingent ability of individuals or groups to create organisations, influenced by political systems, legal traditions, and societal values, not a natural given across time or geography.
- **Business Models** – Conceptual frameworks that describe how organisations create, deliver, and capture value, evolving across history from trade and production to platforms, networks, and sustainable or circular models.
- **Governance, Risk, and Compliance (GRC)** – The interconnected disciplines ensuring that actions are aligned with purpose, manage uncertainty, and respect internal and external obligations, formalised progressively from early commerce to modern corporations.
- **Industrialisation and Organisational Risk** – The transformation of business and governance practices triggered by mass production and technological advancement, leading to the development of risk management and regulatory oversight structures.
- **Public Services Evolution** – The historical progression of state-provided services from ad hoc and fragmented practices to systematic, universal, and rights-based models of service delivery, influenced by societal shifts and economic needs.
- **New Public Management (NPM)** – A late 20th-century movement that introduced private-sector management techniques into the public sector, emphasising efficiency, metrics, and citizen-as-customer perspectives.
- **Digital Transformation in Public Services** – The adoption of digital technologies to redesign and enhance public service delivery, increasing accessibility and transparency but also introducing new risks of exclusion, bias, or loss of trust.
- **IT Ecosystem** – The complex network of actors (internal teams, vendors, consultants, regulators) and technologies that collectively shape how information systems are developed, managed, and governed within organisations.
- **Internal IT Workforce** – The professionals directly employed by organisations to manage, secure, and evolve their information systems, playing a strategic role in aligning technology with organisational priorities.
- **Vendors and Technology Providers** – External organisations supplying hardware, software, platforms, and IT services, whose interests may align with or diverge from the client organisation's strategic goals.
- **Consultants and Advisory Services** – External actors offering expertise, frameworks, and critical analysis to support organisational decision-making, transformation, or compliance, operating within specific contractual and institutional constraints.
- **Cooperation and Boundaries of Responsibility** – The clear definition and management of roles, obligations, and risks across internal and external actors in an ecosystem, essential for resilience and governance maturity.
- **Multinational Complexity** – The additional governance, legal, and cultural challenges faced by organisations and consultants operating across multiple jurisdictions and regulatory environments.
- **Legal Systems Diversity** – The existence of different types of legal systems (common law, civil law, religious or hybrid systems) that shape how organisations are created, governed, and held accountable in different contexts.
- **European Union Legal Instruments** – The specific legal mechanisms (Regulations, Directives, Decisions) that structure cross-border governance in the EU.
- **Normative Layers** – The idea that organisational action is constrained and enabled by multiple overlapping regulatory and normative frameworks (local, national, supranational), which consultants must navigate carefully.
- **Knowing, Naming, and Risk** – The professional responsibility to define and classify concepts carefully, recognising that classification is never neutral and always carries operational and strategic consequences.
- **Cultural Variation in Concepts** – The recognition that seemingly universal concepts (such as "compliance", "risk", "audit") may have different meanings, expectations, and operational significance across different cultural or sectoral contexts.
- **Technological Ambiguity** – The recurrent historical phenomenon where new terms (e.g., "digital transformation," "smart," "AI-driven") are adopted without stable or clear meanings, creating both opportunity and confusion in governance and strategic planning.
- **Historical Evolution of IT** – The journey from early centralised computing through personal computing, networking, internet-driven business models, mobile ubiquity, and now cloud and platform ecosystems, reshaping how organisations think about governance and strategy.
- **Shadow IT** – The use of unsanctioned systems and applications outside formal IT governance structures, reflecting both adaptability and governance risk in dynamic organisations.
- **Information Security versus Cybersecurity** – The distinction between protecting information across all forms and securing digital systems and assets against malicious or accidental harm, both critical to governance today.
- **Privacy versus Security** – The distinction between securing data against breaches (security) and ensuring that personal data is collected, processed, and used lawfully and ethically (privacy), both increasingly regulated and strategic.

Notes:

- "The Context" is not simply background; it shapes what organisations can do, how they are evaluated, and how they manage risk, technology, and change.
- Professionals must interpret organisational environments not only by their formal structures but also by their historical, cultural, and legal contexts.
- When advising or engaging with organisations, recognising underlying assumptions and constraints will be critical to giving credible, context-sensitive advice.

1 Theme: Organizations, Governance, and Management

Understanding how organisations operate requires more than structural analysis. It requires a deep awareness of how authority is distributed, how decisions are made, and how formal systems interact with informal cultures and incentives. Governance and management provide two complementary lenses through which this complexity can be interpreted.

Governance *defines purpose, sets direction, and ensures oversight. It is concerned with legitimacy, accountability, and alignment with external expectations—whether those are legal, financial, societal, or political.*
In contrast, ***management*** *focuses on the design and execution of activities that deliver results. It translates strategic intentions into operational routines and responds to emerging conditions on the ground.*

This theme explores the principles and variations in how governance and management are structured and enacted, particularly in relation to technology. It examines both formal instruments (such as policies, frameworks, and standards) and more fluid dimensions such as culture, leadership styles, and institutional context. Special attention is given to **differences across sectors**: public versus private, regulated versus entrepreneurial, centralised versus distributed. These distinctions matter, especially when assessing governance readiness, designing interventions, or evaluating compliance and risk. A central concept in relation to that is the concept of **Management System**.

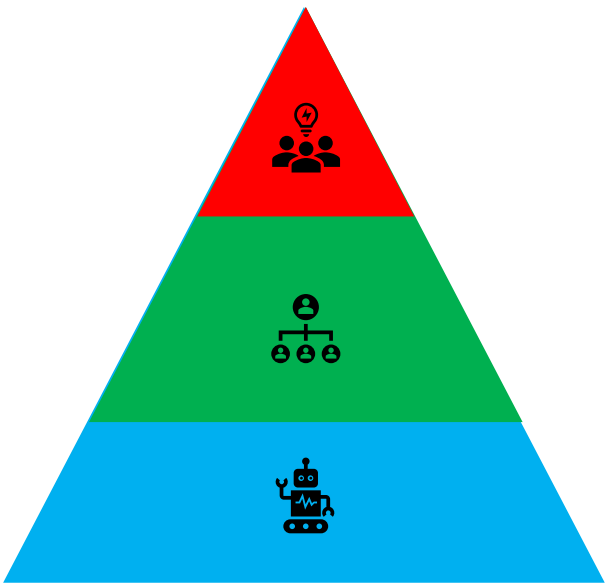
A ***Management System*** *is a structured approach that helps organisations ensure consistency, accountability, and continuous improvement in a specific domain.*

Management systems can be found across domains such as quality, environment, information security, and service delivery. In digital contexts, they are increasingly essential to ensure alignment between business strategy, technological capability, and legal obligations, which also bring the concept of **Integrated Management System**. Together, governance and management form the scaffolding of organisational decision-making. Their effective coordination is a key indicator of organisational **maturity**, a concept that appears throughout this theme and the course as a whole.

Maturity refers to the ability of an organisation to consistently act in a coherent, accountable, and strategic way. Organisations with a high level of maturity have formalised structures, clear role definitions, embedded feedback loops, and are capable of adapting while maintaining purpose and integrity. Organisations with alow level of maturity, by contrast, may rely on improvisation, individual heroics, or ad hoc responses that fail under pressure or change.

Students will also be introduced to organisational roles that operate at the intersection of governance and management, especially those with strategic relevance such as CIO, CTO, and CISO. Learning to interact with these roles as a consultant or analyst requires fluency in both technical and institutional languages (and an understanding of how maturity shapes what is possible, what is fragile, and what can be improved).

Finally, this theme encourages students to think critically about variation and context. The same structure may behave differently in different sectors, cultures, or maturity levels. Recognising such variation is not a complication: it is a core professional competence. For students preparing to engage with executive stakeholders, this means learning to interpret systems not only by their charts and labels, but by their behaviours, incentives, and constraints.



1.1 Corporate Organizations

A corporate organisation, often also named "business organization", is a legal entity that functions as an independent business structure, distinct from its owners. Typically established to conduct commercial activities, generate profit, and deliver goods or services, corporate organisations vary widely in size, from small enterprises to multinational corporations. They may be either publicly listed on stock exchanges or privately held.
These organisations follow a structured hierarchy comprising several key roles:

- **Shareholders** – The owners who provide capital investment.
- **Board of Directors** – Elected representatives tasked with strategic oversight and governance.
- **Executives and Management** – Senior leaders, including the CEO and other managers, responsible for daily action.

Corporate entities operate under **regulatory frameworks** that define their rights, duties, and liabilities, ensuring compliance with financial, labour, and corporate governance laws.

1.1.1 Shareholders and Stakeholders

A **shareholder**, or stockholder, is an individual or institution that owns shares in a company. Shareholders have a financial interest in the company and typically participate in decision-making through voting rights at annual general meetings (AGMs). Their primary focus is on achieving returns, via dividends and share price appreciation.
In contrast, a **stakeholder** is any individual or group affected by or interested in the company's operations. Stakeholders may not hold financial ownership, but they can exert significant influence or be impacted by the company's decisions.
Typical stakeholders include:

- **Employees** – Dependent on the company for income and career development.
- **Customers** – Rely on its goods or services.
- **Suppliers and Business Partners** – Involved in the supply chain and collaborative operations.
- **Governments and Regulators** – Monitor compliance with legal and tax obligations.
- **Local Communities** – May experience the social or environmental consequences of corporate activities.

1.1.2 Corporate Governance

Corporate governance refers to the system of rules, practices, and processes that guide how a company is directed and controlled. It aims to ensure accountability, transparency, and sustainable performance while aligning the interests of various parties—particularly shareholders.
Good governance promotes ethical decision-making, risk management, and long-term value creation. It balances the needs of shareholders with those of broader stakeholders, reinforcing public trust and corporate integrity.

1.1.3 Shareholders' Role

As equity owners, shareholders hold key rights and responsibilities within the governance framework. Their influence varies depending on the company's shareholding structure and applicable legal context.
Shareholders shape governance in several ways:

- **Voting Rights** – Shareholders typically vote on crucial matters, such as electing directors or approving mergers.
- **Board Oversight** – They appoint members to the board of directors, who set strategic direction and oversee executive performance.
- **Dividend and Capital Decisions** – Shareholders influence how profits are used, whether reinvested or distributed as dividends.
- **Major Corporate Actions** – Significant decisions, such as acquisitions or structural changes, often require shareholder approval.
- **Ethical and Social Accountability** – Increasingly, shareholders demand responsible corporate behaviour, including environmental stewardship and adherence to ethical standards.

1.1.4 Types of Shareholders

Corporate governance must accommodate different shareholder types, each with unique priorities and degrees of influence:

- **Institutional Shareholders** – Entities like pension funds and mutual funds often wield substantial voting power and maintain active engagement with boards.
- **Retail Investors** – Individual shareholders with smaller stakes, who collectively represent a significant ownership base in public companies.
- **Controlling Shareholders** – Founders or family groups with majority stakes may significantly influence company strategy and governance.
- **Minority Shareholders** – Though less powerful, they benefit from legal protections that ensure equitable treatment and access to information.

Together, these dynamics shape how corporate organisations operate, evolve, and respond to the interests of both their owners and the wider society in which they function.

1.2 Public Sector Organisations

A **public sector organisation** is an entity that is owned, funded, and operated by a government or public authority to provide services that benefit society. Unlike private businesses, public sector organisations are not primarily driven by profit but by **public interest, policy objectives, and service delivery**. These organisations can exist at various levels of government, including **local, regional, and national**.
Common types of public sector organisations include:

- **Government Departments** – Ministries or agencies responsible for public administration (e.g., a Ministry of Education).
- **State-Owned Enterprises (SOEs)** – Government-owned corporations operating in commercial sectors (e.g., "RTP - Radio Televisão Portuguesa", the public radio and television enterprise in Portugal).
- **Local Authorities** – Councils responsible for services like education, waste management, and transport (e.g., the "Administração do Porto de Lisboa", the Lisbon Port Authority).
- **Public Utilities** – Organisations providing essential infrastructure services (e.g., water, electricity, transport).

1.2.1 Shareholders vs. Stakeholders

Unlike private businesses, which have **shareholders** who own equity and seek financial returns, public sector organisations do not have **equity investors** in the same way. Instead, they are accountable to the **government and, ultimately, the public**. However, the concept of **stakeholders** is highly relevant in the public sector. Public organisations must consider a diverse range of stakeholders, including:

- **Citizens and Communities** – The primary beneficiaries of public services.
- **Government Authorities** – Overseeing bodies that set policies, regulations, and funding structures.
- **Employees and Unions** – Workers providing public services, often under civil service frameworks.
- **Suppliers and Contractors** – Private entities delivering goods and services under public contracts.
- **Regulators and NGOs (Non-Governmental Organizations)** – Organisations ensuring compliance with legal, ethical, and environmental standards[20].

Since public organisations do not generate profit for shareholders, their success is measured by **efficiency, service quality, and public satisfaction**, rather than financial returns.

1.2.2 On Business Models

While private businesses operate with **commercial business models** focused on revenue generation, public sector organisations adopt models that reflect their **service-driven mandate**. Some common approaches include:

- **Tax-Funded Model** – Services funded directly through taxation, such as healthcare and basic education.
- **Public-Private Partnership (PPP)** – Collaboration between government and private firms to provide public services (e.g., infrastructure projects).
- **State-Owned Enterprise Model** – Public entities operating commercially but reinvesting profits into public services (e.g., The Metro in Lisbon, or the CP in Portugal).
- **User-Fee Model** – Public services that charge fees to users, such as public transport or higher education institutions.

Despite differences from private enterprises, public sector organisations still apply **management principles, performance measurement, and operational efficiency techniques**, adapting business concepts to serve public needs.

1.2.3 Conclusion

Public sector organisations differ from private businesses in their ownership, objectives, and financial structures. While they do not have **shareholders**, they manage complex **stakeholder relationships**, and while their **business models** are not profit-driven, they still require sustainable funding and efficient management to fulfil their public mission.

[20] …a really very interesting stakeholder in this domain: https://noyb.eu

1.3 Not for Profit Organizations

Not-for-profit organizations (NPOs) are entities that operate with the primary objective of achieving a social, cultural, educational, or environmental mission rather than generating profits for owners or shareholders. These organizations reinvest any surplus revenue into their activities to advance their goals, rather than distributing earnings as dividends.

1.3.1 Types of Not-for-Profit Organizations

NPOs exist in diverse sectors and take various forms, including:

- **Charities** – Organizations dedicated to humanitarian aid, poverty alleviation, health, or education (e.g., the Red Cross, Oxfam).
- **Foundations** – Entities that provide funding for research, social causes, or public initiatives (e.g., the Gulbenkian Foundation, the Bill & Melinda Gates Foundation).
- **Associations and Societies** – Member-based organizations that promote professional, cultural, or recreational interests (e.g., the IEEE, the ACM, the Engineers Guild[21], sports federations).
- **Cooperatives** – Member-owned organizations that operate in the interests of their participants, commonly found in agriculture, banking, and retail (e.g., credit unions).
- **Non-Governmental Organizations (NGOs)** – Independent organizations that work on international development, human rights, or environmental protection (e.g., Greenpeace, Amnesty International).
- **Public Benefit Institutions** – Organizations that provide essential services like healthcare, research, or education, often in partnership with governments (e.g., public universities and hospitals with non-profit mandates).

1.3.2 Governance and Stakeholders in Not-for-Profit Organizations

Unlike corporate organizations, NPOs do not have shareholders but are accountable to a variety of stakeholders, including:

- **Donors and Granting Entities** – Individuals, foundations, or governments that fund NPO activities.
- **Beneficiaries** – The communities or individuals who receive services or support from the organization.
- **Volunteers and Employees** – Those who contribute their time and expertise to the organization's operations.
- **Regulatory Bodies** – Authorities that oversee compliance with legal and fiscal requirements for non-profits.
- **The General Public** – Since many NPOs serve broader societal interests, public perception and trust are crucial to their sustainability.

To ensure accountability, NPOs typically have governing boards that oversee operations, manage financial resources, and safeguard the organization's mission. Governance frameworks such as the **Principles for Good Governance and Ethical Practice**[22] help ensure transparency, ethical management, and compliance with legal obligations.

1.3.3 Business Models in Not-for-Profit Organizations

While NPOs do not operate for profit, they still require sustainable financial models to function effectively. Common approaches include:

- **Donor-Based Model** – Relying on donations from individuals, philanthropic foundations, or corporate sponsorships.
- **Grants and Public Funding** – Securing funds from government agencies or international bodies to finance projects.
- **Social Enterprise Model** – Running revenue-generating activities that support the organization's mission, such as charity shops or fair-trade businesses.
- **Membership-Based Model** – Collecting fees from members who receive benefits or services in return (e.g., professional associations).
- **Endowment and Investment Income** – Managing long-term funds that generate interest or investment returns to sustain operations.
- **Fee-for-Service Model** – Offering services for a fee, often at reduced rates, in areas such as education, healthcare, or consultancy (e.g., non-profit hospitals, training programs).

Despite their non-commercial nature, NPOs must apply financial management principles, strategic planning, and performance measurement techniques to remain sustainable and impactful. Many adopt corporate-style management practices to ensure operational efficiency, risk management, and stakeholder engagement.

1.3.4 Challenges and Ethical Considerations

Not-for-profit organizations face unique challenges, including:

- **Financial Sustainability** – Dependence on donations and grants can make revenue streams unpredictable.
- **Accountability and Transparency** – Public and donor trust requires clear reporting, governance, and ethical standards.
- **Mission Drift** – The risk of shifting priorities due to funding conditions rather than strategic intent.
- **Volunteer and Workforce Management** – Balancing professionalization with reliance on volunteer contributions.
- **Regulatory Compliance** – Adhering to tax regulations, reporting requirements, and sector-specific laws.

Many NPOs address these challenges through good governance practices, financial diversification, and partnerships with governments or private sector entities.

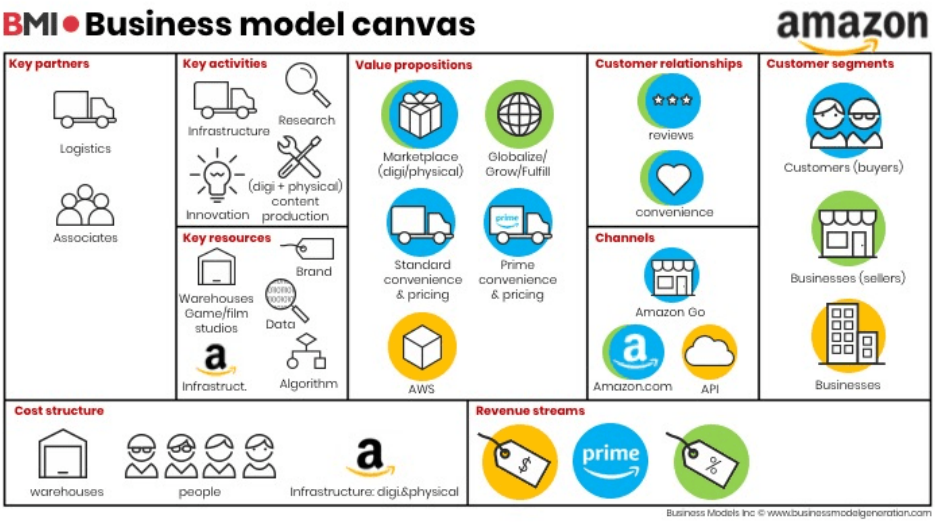
1.3.5 Conclusion

NPOs play a vital role in society, addressing gaps in social services, research, and advocacy. Though they differ from corporate and public sector organizations in their profit motives and governance structures, they still require effective management, financial sustainability, and accountability. By leveraging diverse funding models and strategic partnerships, NPOs can enhance their long-term impact while remaining aligned with their mission-driven objectives.

[21] Ordem dos Engenheiros

[22] https://independentsector.org/resource/principles-for-good-governance-and-ethical-practice-resource-center/

1.4 Organizations and Business Models



Every organisation, regardless of sector or size, operates based on an underlying **business model**, a conceptual framework that explains how it creates, delivers, and captures value.

A **business model** sets out how an organisation structures its resources, relationships, and activities to achieve its objectives. For corporate entities, these objectives typically centre around profitability, market share, and shareholder value; in public sector the focus is on policy outcomes, service delivery, and accountability to citizens; not-for-profits prioritise social impact and mission fulfilment.

1.4.1 Key Components of a Business Model

Many frameworks exist to express business models[23], but the Business Model Canvas (BMC) is eventually the most cited. The BMC comprises several common components[24,2526]:

- **Value Proposition**: The unique value an organisation offers to its customers, beneficiaries, or stakeholders.
- **Target Segments**: The specific audiences or markets served.
- **Channels**: How value is delivered (e.g., physical locations, digital platforms).
- **Revenue Streams**: The means by which income is generated (e.g., sales, taxes, donations).
- **Cost Structure**: The key operational expenses required to deliver value.
- **Key Activities and Resources**: The critical tasks and assets involved in delivering services or products.
- **Partnerships**: Strategic collaborations that enhance efficiency or reach.

1.4.2 Business Models in the Private Sector

Private sector organisations often adopt one or more of the following generic models, depending on their industry and strategic focus[27,28,29]:

- **Product-Based Model**: Organisations manufacture or source physical or digital products and sell them directly to consumers or intermediaries. Examples include retailers, manufacturers, and software vendors.
- **Service-Based Model**: Businesses provide intangible offerings such as consulting, legal advice, financial services, or maintenance. The value lies in expertise, reliability, and personalisation.
- **Subscription Model**: Customers pay a recurring fee (e.g., monthly or annually) for continuous access to a product or service. Common in media, software (SaaS), and membership-based services.
- **Platform Model**: These organisations create digital or physical platforms that facilitate interactions between two or more user groups, such as buyers and sellers (e.g., Uber, Airbnb, eBay). The platform earns revenue through transaction fees, advertising, or premium features.
- **Franchise Model**: A central organisation (the franchisor) licenses its brand and business system to independent operators (franchisees), who deliver services locally in exchange for fees and royalties.
- **Freemium Model**: Popular in the tech sector, this model offers a basic version of a service for free while charging for advanced features or premium usage.

1.4.3 Public and Not-for-Profit Sector Models

In the public and not-for-profit sectors, business models are adapted to reflect missions of service and public value. Instead of generating profit, these organisations aim to optimise resource use, improve outcomes, and maintain legitimacy. Common models include:

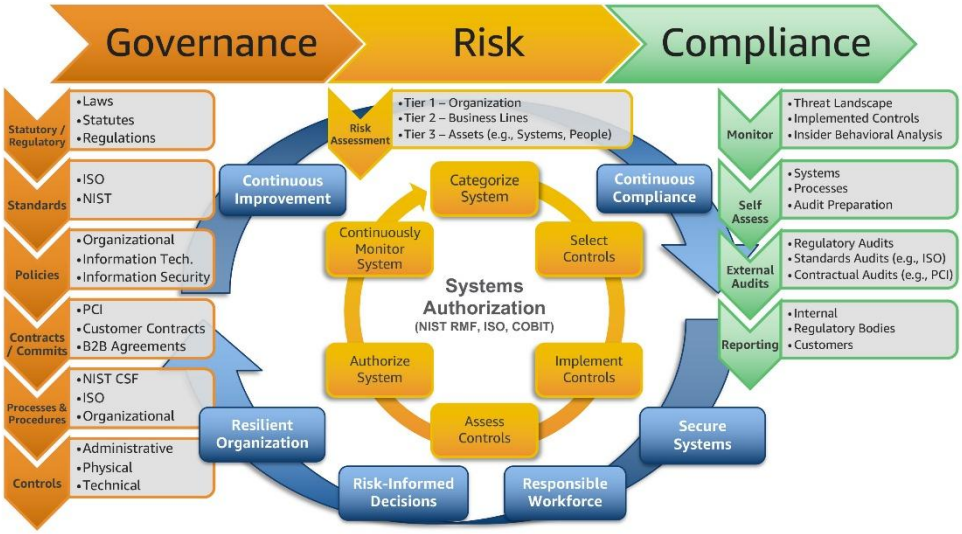
- **Tax-Funded Model**: Government-funded services such as healthcare, education, or public safety.
- **Fee-for-Service Model**: Organisations charge for services, often subsidised or offered at cost, such as university tuition or museum admissions.
- **Grant-Based Model**: Activities funded by external donors or foundations, typical in international development or research.
- **Social Enterprise Model**: Combines commercial activity with a social mission, reinvesting profits into community impact.

1.4.4 Conclusion

Understanding an organisation's business model is essential for effective governance, strategic alignment, and stakeholder engagement. Business models not only define how value is created and delivered but also influence financial sustainability, risk exposure, and innovation capacity. In an increasingly dynamic environment, successful organisations regularly reassess and adapt their business models to remain relevant, efficient, and impactful.

[23] https://en.wikipedia.org/wiki/Business_model
[24] https://businessmodelanalyst.com/
[25] https://businessmodelanalyst.com/types-of-business-models/
[26] Amazon BMC example from: https://www.si2blue.com/business-model-canvas/
[27] https://www.investopedia.com/terms/b/businessmodel.asp
[28] https://online.hbs.edu/blog/post/types-of-business-models
[29] https://startupmindset.com/types-of-business-models/

1.5 Governance, Risk and Compliance



Modern organisations operate in a complex environment of regulatory obligations, financial risks, technological advances, and stakeholder expectations. **Governance, Risk, and Compliance (GRC)** is a structured approach that ensures organisations achieve their objectives reliably, address uncertainties effectively, and act with integrity. GRC integrates corporate governance, risk management, and regulatory compliance into a unified framework that aligns with strategic goals, operational needs, and ethical considerations.

1.5.1 Risk Management

Risk management is the structured process of identifying, analysing, and mitigating potential threats that could impact an organisation's strategic, operational, financial, or reputational standing:

- **Strategic Risks:** Arise from business decisions that impact long-term objectives, such as entering new markets or adopting emerging technologies.
- **Operational Risks:** Stem from failures in internal processes, human error, or system malfunctions.
- **Financial Risks:** Fluctuations in revenue, currency exchange rates, credit exposure, etc.
- **Regulatory and Compliance Risks:** Non-compliance with legal, regulatory, or ethical requirements.
- **Cybersecurity and Information Risks:** Concern data breaches, cyber threats, and IT system vulnerabilities[30].

Effective risk management enables organisations to anticipate and respond to challenges while seizing opportunities for growth. For that, the adoption of structured risk management frameworks ensures consistency and effectiveness. For example, **COSO ERM (Enterprise Risk Management)** is a framework integrating risk management into corporate governance and decision-making. By systematically managing risks, organisations enhance resilience, improve the chances of maintain **business continuity**, and protect stakeholder interests.

Risk management must be addressed as a process. A comprehensive risk management approach typically follows these steps, as recommended by the **ISO 31000**.

1.5.2 Compliance

Compliance ensures that an organisation operates within legal, regulatory, and industry frameworks while maintaining ethical integrity. Failure to comply with laws and standards can result in financial penalties, reputational damage, operational restrictions, and legal liabilities. Compliance can arise from multiple dimensions, such as:

- **Regulatory Compliance:** Organisations must adhere to jurisdiction-specific regulations that govern financial practices, data protection, consumer rights, and industry-specific requirements. Examples include the **GDPR (General Data Protection Regulation)** that governs data privacy and protection in the EU, and in the US the **Sarbanes-Oxley Act (SOX)** that regulates financial reporting and corporate accountability and the **HIPAA (Health Insurance Portability and Accountability Act)** for health information security.
- **Corporate Compliance:** Internal policies and procedures, adherence to industry best practices, etc.
- **Third-Party and Supply Chain Compliance:** Ensure that partners, vendors, and suppliers comply with relevant regulations and corporate standards.
- **Ethical Compliance:** Beyond legal requirements, organisations are increasingly held accountable for ESG practices[31].

To manage compliance effectively, organisations implement structured policies, internal controls, and monitoring mechanisms. These typically include:

- **Compliance Policies and Codes of Conduct:** Establish guidelines for ethical behaviour, data protection, anti-bribery, and fair competition.
- **Audits and Regulatory Reporting:** Internal and external audits assess adherence to regulations, identifying compliance gaps and corrective actions.
- **Training and Awareness Programmes:** Employee education ensures understanding of compliance obligations, reducing the risk of violations.
- **Compliance Technology and Automation:** Many organisations leverage compliance management software and AI-driven monitoring systems to streamline regulatory tracking and reporting.

1.5.3 Conclusion

Risk and compliance are fundamental components of organisational success in an increasingly complex business environment. Risk management enables organisations to anticipate and mitigate potential threats, while compliance ensures regulatory adherence and ethical conduct. By integrating risk and compliance management into governance frameworks, organisations can achieve strategic objectives, maintain business continuity, and uphold stakeholder trust (the image here presented shows how Amazon sees this issue in relation to its could business AWS[32]).

[30] An interesting tale of information security from before the Internet:
- https://en.wikipedia.org/wiki/Crypto_AG
- https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

[31] https://en.wikipedia.org/wiki/Environmental,_social,_and_governance

[32] https://aws.amazon.com/blogs/security/scaling-a-governance-risk-and-compliance-program-for-the-cloud/

1.6 Risk and Risk Management

Risk is defined as the effect of uncertainty on objectives. It arises from the possibility that an event or condition will occur and impact the achievement of strategic, operational, financial, reputational, or compliance goals.
While risk can result in both positive and negative outcomes, the emphasis in practice is often placed on anticipating and mitigating adverse consequences.
In information-related domains, risk is typically understood through the interaction of three core concepts:

- **Threat**: A potential cause of an unwanted incident, which may result in harm.
- **Vulnerability**: A weakness or gap that could be exploited by one or more threats.
- **Consequence**: The outcome or impact that would result if a threat successfully exploits a vulnerability.

Complementing this triad is a fourth element central to many practical models:

- **Risk Event**: The actual occurrence where a threat acts upon a vulnerability, triggering a specific impact scenario.

These elements underpin many risk analysis methods, especially in domains like cybersecurity, where a threat such as a cyberattack may target a vulnerability like poor access control, leading to data leakage or system compromise.

1.6.1 Risk Management Process

Risk management involves a structured set of activities for identifying, analysing, evaluating, treating, and monitoring risk. According to ISO 31000 (Risk Management), these activities are:

- **Risk Identification**: Detecting and describing potential risks, threats, and vulnerabilities.
- **Risk Analysis**: Assessing the likelihood and consequences of each risk scenario.
- **Risk Evaluation**: Comparing assessed risks with organisational risk appetite or acceptance criteria.
- **Risk Treatment**: Selecting and applying actions to mitigate, transfer, avoid, or accept risk.
- **Monitoring and Review**: Regularly tracking risk status and the effectiveness of controls.
- **Communication and Consultation**: Engaging internal and external stakeholders to ensure understanding and transparency.

The risk management process is iterative and should be embedded across management functions such as operations, project governance, and strategic planning.

1.6.2 Types and Domains of Risk

Risks manifest in different domains and require context-sensitive approaches.

Common categories include:

- **Strategic risks**: Arising from long-term policy decisions or misalignment with institutional mission.
- **Operational risks**: Stemming from failures in internal processes, systems, or human error.
- **Compliance risks**: Related to failure in meeting legal, regulatory, or contractual obligations.
- **Security and privacy risks**: Involving threats to the confidentiality, integrity, or availability of information.
- **Reputational risks**: Resulting from incidents that damage stakeholder trust or public credibility.
- **Financial risks**: Such as funding instability, market volatility, or fraud.
- **Regulatory risks**: Emerging from changes in the legal or regulatory environment, or from failure to meet evolving regulatory expectations, especially in complex or cross-border contexts.

Regulatory risk deserves particular attention in governance and compliance-sensitive environments. It may arise from:

- Introduction of new laws or standards (e.g. GDPR, DORA, NIS2),
- Diverging regulations across jurisdictions,
- Shifting interpretations by regulatory bodies,
- Failure to keep internal practices aligned with external expectations.

While often framed under compliance, regulatory risk also relates to **strategic positioning**, **reputational exposure**, and the **cost of non-compliance**, including fines, sanctions, and lost business opportunities.

1.6.3 Integration and Maturity

Risk management should not be isolated from other organisational systems. It must be integrated into governance models, management systems (e.g. ISO/IEC 27001, ISO 22301), and quality or audit programmes. ISO 31000 provides a generic reference point, applicable across all domains and organisational types.

Mature organisations display:

- A consistent methodology for risk identification and evaluation,
- Clear articulation of risk appetite and tolerance,
- Role-based responsibilities for monitoring and escalation,
- Integration of risk considerations into planning, investment, and design.

Less mature organisations may rely on ad hoc judgement, leading to inconsistent responses and limited capacity to deal with complex or emerging threats.
A strong risk culture enables both resilience and agility. It helps organisations anticipate disruption, make informed decisions under uncertainty, and adapt with confidence to regulatory, technological, or strategic change.

1.7 Governance, Management and Operations

Every regular organisation, regardless of its size or sector, operates through three levels of control and execution: **Governance, Management, and Operations**. Each level has distinct roles and responsibilities, and must work together to ensure strategic alignment, effective coordination, and efficient execution of tasks.

1.7.1 Governance: Setting Direction and Oversight

Governance represents the highest level of decision-making in an organisation. It is primarily concerned with defining strategic goals, establishing policies, and overseeing overall organisational performance.
Key responsibilities of governance include:

- **Defining organisational mission and vision** – Establishing the fundamental purpose and long-term aspirations of the organisation.
- **Setting strategic direction** – Ensuring that management decisions align with overarching goals.
- **Risk management and compliance** – Implementing frameworks to mitigate risks and ensure adherence to regulations.
- **Stakeholder engagement** – Balancing the interests of shareholders, employees, customers, and regulatory bodies.
- **Performance oversight** – Monitoring management activities (e.g., towards audits) and ensuring accountability.

Governance is typically exercised by one or more bodies, which set long-term objectives and **evaluate risks and opportunities, such as a Board of Directors, an Executive Committee, or other** governing bodies. Governance frameworks (see "1.13 Management Systems and Frameworks") provide structured approaches to effective governance practices.

1.7.2 Management: Planning and Coordination

Sitting between governance and operations, management translates strategic directives into actionable plans. Managers ensure that operational activities align with strategic objectives, allocate resources effectively, and monitor performance to achieve desired outcomes. Management is typically structured in **hierarchical layers**, such as senior, middle, and frontline management.
Key functions of management include:

- **Planning** – Developing plans that bridge high-level governance decisions with operational execution.
- **Resource allocation** – Distributing financial, human, and technological resources efficiently.
- **Process optimisation** – Improving workflows and removing inefficiencies.
- Performance measurement – Monitoring **key performance indicators (KPI)** to track progress.
- **Leadership and communication** – Motivating teams, resolving conflicts, and fostering a productive work culture.

Management methodologies and systems help organisations enhance efficiency and effectiveness in this domain.

1.7.3 Operations: Execution and Delivery

Operations represent the **execution layer** of an organisation, where employees and automated systems perform the day-to-day activities that generate value. This level is focused on efficiency, quality, and meeting customer or stakeholder demands. Key characteristics of operations include:

- **Task execution** – Carrying out routine activities and services.
- **Service and product delivery** – Ensuring goods and services meet predefined requirements.
- **Process adherence** – Following established procedures and guidelines to maintain consistency.
- **Customer interaction** – Addressing client needs and providing support.
- **Continuous improvement** – Identifying inefficiencies and implementing process enhancements.

Operations are often structured into **departments or functional units** (e.g., finance, human resources, IT, manufacturing, logistics) that directly contribute to the organisation's core objectives.

1.7.4 Relating Governance, Management, and Operations

These three levels are interdependent:

- **Governance defines the strategic vision**, ensuring compliance and risk mitigation.
- **Management translates this vision** into actionable strategies and monitors execution.
- **Operations execute these strategies**, delivering products and services efficiently.

For an organisation to function effectively, these levels must be aligned, ensuring that day-to-day operations contribute to long-term strategic goals while being well-managed and compliant with governance policies.

1.7.5 Conclusion

Governance, management, and operations are fundamental layers of any organisation's structure. **Governance sets direction and oversight, management ensures planning and coordination, and operations execute daily activities.** When these levels work together cohesively, organisations achieve greater efficiency, sustainability, and strategic success.

1.8 Role and Responsibility Frameworks

Responsibility Assignment Matrices are structured methods used to clearly define and communicate roles, responsibilities, accountability, and decision-making authority among stakeholders.

Specifically, these matrices are part of:

- **Governance frameworks**, clarifying authority and decision-making roles.
- **Management frameworks**, organizing and streamlining work responsibilities.
- **Project management methodologies**, ensuring clarity of who does what.

1.8.1 RACI

The acronym RACI stands for Responsible, Accountable, Consulted, and Informed, providing clarity on who does what in IT processes, projects, or operational tasks, thus ensuring effective governance, decision-making, and risk management:

- Responsible (R) identifies the individuals who execute the work. Within governance of IT, these are typically team members or IT specialists performing tasks such as system implementations, software maintenance, security updates, or data management. Several individuals can be designated as responsible, each contributing directly to achieving IT-related objectives.
- Accountable (A) signifies the person who ultimately answers for task completion and outcomes. In governance of IT, the accountable individual is typically a senior manager, such as a CIO, IT director, or IT service owner. Crucially, only one individual can hold accountability per task, ensuring clear ownership and decision-making authority, such as approving budgets, authorising major changes, or ensuring compliance with IT standards and regulations.
- Consulted (C) refers to stakeholders whose input, expertise, or perspective must be sought before making IT-related decisions or completing critical tasks. Examples include security officers, compliance managers, enterprise architects, or external consultants who provide guidance on technical standards, compliance issues, or best practices. Consulting these stakeholders helps ensure alignment of IT initiatives with strategic goals and compliance requirements, reducing the risk of costly errors.
- Informed (I) comprises individuals or groups who must be kept updated on progress or decisions in IT processes but do not participate actively in execution or approval. Within governance of IT contexts, informed stakeholders may include senior executives, business users, audit teams, or regulators. Keeping these stakeholders informed ensures transparency, enables oversight, and enhances trust and confidence in the organisation's IT management practices.

Typically, organisations apply the RACI model through a matrix, in the form of a simple, structured table listing IT tasks or processes against specific roles or stakeholders, clearly specifying who is Responsible, Accountable, Consulted, or Informed.

In governance of IT, the effective use of RACI directly can support accountability, enhances decision-making quality, strengthens risk management, and promoting regulatory compliance. It also facilitates organisational alignment by clarifying the interactions between technical teams and business stakeholders, essential for successful complex IT initiatives.

However, successful adoption of RACI requires ongoing maintenance and review. Governance of IT environments frequently evolve, meaning roles and responsibilities must be revisited regularly to remain relevant and effective. Open discussions and clear communication among stakeholders are crucial for keeping the RACI matrix accurate, up-to-date, and genuinely useful.

1.8.2 Besides RACI

Besides the RACI framework, several alternative responsibility assignment matrices (RAMs) are widely used, each with specific strengths.
The **RASCI** model expands RACI by adding **Support (S)**, explicitly identifying team members providing assistance without direct responsibility.
The **DACI** framework clarifies decision-making roles by distinguishing a **Driver (D)** who leads the task, an **Approver (A)** who makes final decisions, **Contributors (C)** providing input, and **Informed (I)** stakeholders.
Another approach, **RAPID**, emphasises decision clarity by identifying who **Recommends (R)** solutions, who must **Agree (A)** formally, who **Performs (P)** the tasks, who provides **Input (I)**, and crucially, who ultimately **Decides (D)**.
The **CAIRO** model adds an explicit "Out of the Loop (O)" category, clarifying who should remain uninvolved, reducing unnecessary communication.
These alternative frameworks enable organisations to tailor responsibility definitions according to specific governance or operational needs, enhancing decision-making clarity and organisational effectiveness.

1.9 Organisational Models and Control Structures

Organisational models define how authority, responsibilities, and workflows are structured within an organisation. These models influence everything from decision-making and communication to accountability and agility. **Control structures**, in turn, are the mechanisms by which governance and management monitor, direct, and enforce compliance with rules, objectives, and performance expectations. Together, these elements shape the organisation's ability to execute its strategy, manage risk, and respond to change.

Understanding different organisational models and their associated control structures is essential for designing effective governance systems that suit the organisation's context, culture, and complexity.

1.9.1 Common Organisational Models

Organisations can adopt various structural models depending on their size, sector, and goals. The most common include:

- **Functional Structure** - Departments are organised by specialised functions such as finance, marketing, IT, or operations. This model promotes efficiency and expertise but can create silos and reduce cross-functional collaboration.
- **Divisional Structure** - The organisation is divided into autonomous units based on products, regions, or customer segments. Each division has its own functions and operates semi-independently. This model is useful in large, diversified companies but can lead to duplication of effort.
- **Matrix Structure** - Combines functional and project-based lines of authority. Employees may report to both a functional manager and a project or product lead. While this model promotes flexibility and collaboration, it can create ambiguity in decision-making and accountability.
- **Flat or Horizontal Structure** - Reduces hierarchical layers to promote faster decision-making and greater employee empowerment. Common in start-ups and agile environments, it relies heavily on a strong **organisational culture** and informal control.
- **Networked or Platform-Based Structure** - Built around flexible partnerships, ecosystems, or digital platforms. Often found in digitally native companies, this model enables rapid innovation and responsiveness but requires robust coordination mechanisms.
- **Holacratic and Self-Managed Structures** - In more experimental models like holacracy, authority is distributed across self-organising teams. While promoting autonomy and innovation, these models challenge traditional notions of governance and require high levels of maturity and trust.

1.9.2 Control Structures and Mechanisms

Control structures ensure that the organisation operates in line with its mission, policies, and regulatory obligations. These include both **formal controls** (**documented information**, defined processes, defined roles, reporting lines, and oversight bodies) and **informal controls**, such as organisational culture, peer influence, and leadership tone.

Key components of control structures include:

- **Lines of Authority and Accountability** - Clear reporting relationships and decision rights are essential to ensure that responsibilities are understood and monitored.
- **Policies and Procedures** - Standard operating procedures, codes of conduct, and governance frameworks define how work is done and what behaviours are expected.
- **Performance Management Systems** - Objectives and key results (OKRs), key performance indicators (KPIs), and regular performance reviews provide mechanisms for monitoring progress and enforcing accountability.
- **Internal Controls and Audits** - Financial controls, risk registers, compliance checks, and audit trails ensure that the organisation adheres to internal and external standards.
- **Board Committees and Oversight Bodies** - Structures such as audit committees, risk committees, and ethics boards provide independent oversight of critical areas of governance.
- **Culture and Informal Norms** - An organisation's culture (its shared values, assumptions, and behaviours) acts as a powerful informal control system. Ethical leadership, open communication, and mutual trust can reinforce or undermine formal structures.
-

1.9.3 Aligning Structure with Governance Needs

The choice of organisational model and control structure should reflect the organisation's size, complexity, strategic focus, and regulatory environment. For example:

- A regulated financial institution may favour a hierarchical, control-heavy structure with detailed risk oversight.
- A digital start-up might adopt a flat or matrix structure to encourage speed and innovation, supported by agile governance mechanisms.

Regardless of the model, effective governance requires that roles are clear, controls are proportionate, and oversight is robust yet adaptable.

1.9.4 Conclusion

Organisational models and control structures are fundamental to how governance is enacted in practice. They influence agility, accountability, and performance. By carefully designing and evolving these structures, organisations can ensure that their governance frameworks remain fit for purpose in a changing and often uncertain environment.

1.10 Control: The Three Lines of Defence

The **Three Lines Model**, developed by the **Institute of Internal Auditors (IIA)**[33], is a widely recognised framework for structuring roles and responsibilities in governance, risk management, and control. It clarifies how different organisational actors contribute to achieving objectives, managing risk, and ensuring accountability, while maintaining independence where required.

The model replaces earlier linear interpretations of "defence" with a more integrated view, where collaboration and clarity of roles are prioritised over rigid boundaries. It is particularly relevant for organisations aiming to demonstrate effective governance and internal control systems in regulated or high-risk environments.

1.10.1 Structure of the Three Lines

The model distinguishes **three core roles**, aligned with the organisation's overall governance structure:

1. First Line: Management and Operational Functions
   - Responsible for **delivering products and services**, while **managing risks directly** as part of day-to-day operations.
   - Includes business unit leaders, process owners, project managers, and IT or security managers.
   - Owns and manages risks, and is responsible for **designing and implementing controls**.
2. Second Line: Risk, Compliance, and Oversight Functions
   - Provides expertise, guidance, monitoring, and challenge to the first line.
   - Includes roles such as risk managers, compliance officers, information security coordinators, data protection officers (DPOs), and controllers.
   - Supports the development of risk frameworks and policies, tracks performance, and ensures consistent application of standards.
3. Third Line: Internal Audit
   - Provides **independent and objective assurance** to the governing body (e.g. Board of Directors or Audit Committee).
   - Evaluates the effectiveness of governance, risk management, and internal controls, without taking part in day-to-day decision-making.
   - Must remain **functionally independent**, with direct access to the board or its oversight committees.

In simple terms:

- The 1st line is closest to the activities being governed. It has the most immediate understanding of how risks arise and evolve.
- The 2nd line reinforces accountability by ensuring that risks are being identified and managed in line with expectations and regulations.
- The 3rd line helps ensure that governance and risk systems are working as intended, and that earlier lines are operating effectively and transparently.

1.10.2 Governance and the Role of the Board

Overarching all three lines is the role of **governing bodies** (e.g. the Board of Directors or equivalent), which are accountable for:

- Setting direction and strategy,
- Ensuring organisational purpose is achieved ethically and legally,
- Overseeing risk, control, and assurance activities.

The board relies on input and assurance from each of the three lines, while also enabling those functions to perform their roles without interference.

1.10.3 Coordination and Communication

The IIA's model emphasises **collaboration**, not separation. Effective governance depends on:

- **Clear role definitions** and lines of reporting,
- **Flow of information** between the three lines and the board,
- **Mutual respect** between operational, oversight, and assurance roles.

Conflicts arise when roles are unclear, for example, when compliance functions report through the same managers they are meant to oversee, or when audit recommendations are ignored due to a lack of authority or independence.

1.10.4 Application in Practice

For a CISO, CIO, or any other CxO role, the model provides a way to:

- Understand how assurance is layered across the organisation,
- Position governance tools and functions appropriately,
- Respond to internal audit findings constructively,
- And justify governance maturity to regulators, partners, or clients.

In many organisations, **second line functions** are being strengthened to meet rising demands for compliance (e.g. data protection, sustainability, ethics), while **third line functions** are becoming more strategic, offering insights beyond mere conformance.

1.10.5 Conclusion

The model of the three lines of defence offers a practical lens for structuring governance and risk responsibilities[34]. It enables alignment between operational control, risk oversight, and independent assurance, all under the strategic supervision of the governing body. By clarifying who does what, and why, the model supports better decision-making, stronger accountability, and a more resilient organisational posture.

Three lines of defence

[33] https://www.theiia.org/

[34] Image form: https://www.nordea.com/en/about-us/nordea-in-society/three-lines-of-defence

1.11 Management

While governance is responsible for setting strategic direction and ensuring accountability, management serves as the critical intermediary that translates these goals into plans and coordinates their execution.

Management is both a function and a system within organisations, operating within the strategic parameters defined by governance but focused on enabling results, efficiency, and improvement through operational leadership.

Management ensures that the decisions taken by the Board or senior governing bodies are enacted through coherent planning, resource allocation, and monitoring. It also acts as the feedback mechanism, informing governance structures of performance, risks, and emerging issues. The interplay between governance and management is essential for organisational agility and responsiveness, especially in dynamic or regulated environments.

1.11.1 Management Roles

Management roles are typically named after "Chief something Office", with an acronym in the form "**CxO**". In each organisation those roles are structured across several levels of responsibility and scope, where the most common levels are:

- **Executive Management**: Includes roles such as Chief Executive Officer (CEO) or Managing Director, who are responsible for overall performance and act as the link between governance and the organisation's operations. They often represent the organisation to external stakeholders and oversee all other management layers.
- **Middle Management**: Manages teams, departments, or functional areas. This level ensures the translation of strategic and corporate-level plans into operational processes and objectives. Middle managers are typically responsible for monitoring team performance, ensuring resource alignment, and resolving issues that arise during execution.
- **Front-Line Management**: Supervises day-to-day activities and personnel, ensuring operational tasks are carried out effectively and in line with procedures. These roles are often closest to customers, systems, or production, making them critical for feedback and continuous improvement.

The clarity of role definition, authority, and accountability across these levels supports organisational stability and performance.

1.11.2 IT Management Roles

In the context of information systems and digital operations, specialised management roles are increasingly significant.
These include:

- **Chief Information Officer (CIO)**: Responsible for aligning IT strategy with organisational goals. A CIO oversees the IT function, including architecture, systems, infrastructure, and service delivery.
- **Chief Technology Officer (CTO)**: Focuses on technological innovation, architecture design, and the long-term evolution of systems and platforms. The CTO is often more externally oriented, preferred to CIO in product-driven organisations.
- **Chief Information Security Officer (CISO)**: Oversees cybersecurity and information assurance. The CISO manages risks related to data protection, regulatory compliance, and business continuity, and increasingly plays a strategic role at board level. Usually, the CISO is under other CxO role (having the role of CISO under CIO or CTO is considered not a best practice, due to the risk of conflict of interests)
- **IT Managers and Service Managers**: Operate at departmental or operational levels, managing IT teams, contracts, applications, and infrastructure. These roles ensure technical operations align with service levels and support business objectives.

These roles reflect the critical position of technology in achieving resilience, efficiency, and innovation. IT management requires a balance of technical literacy, stakeholder communication, and risk awareness.

1.11.3 Management and Operations

While management and operations are distinct, they are also interdependent. Management is primarily concerned with planning, controlling, and guiding activities, whereas operations are focused on execution and delivery. However, many organisations blur these boundaries through the adoption of lean or agile approaches, where managers are also involved in continuous improvement, performance coaching, and incident handling.

A mature organisation often features management that is empowered, supported by systems of metrics and dashboards, and capable of using operational data to refine processes and anticipate issues. In such contexts, management can become a driver of innovation and resilience, not just a supervisory function.

1.11.4 Conclusion

Management plays a pivotal role in ensuring that strategic intentions are realised through coordinated execution.

It operates as the organisational engine that mobilises **people, technology, and processes** to achieve goals defined by governance. In modern organisations, management is increasingly data-driven, responsive, and cross-functional (particularly in the domain of IT, where rapid change and complex risks demand strong, integrated leadership). By understanding the layered roles and responsibilities of management, one gains insight into how organisations function effectively and sustainably in their operational contexts. Also, management it is not a static thing[35]…

[35] "Where Have All the Managers Gone? Companies' quest to purge bosses is seizing up job and promotion opportunities. Workers have had to adjust" - https://www.wsj.com/lifestyle/careers/management-jobs-shrinking-white-collar-workers-cc761cb7

1.12 Management and Maturity

Maturity, in the context of management, refers to the extent to which organisational processes, structures, and behaviours are formally defined, consistently applied, and continuously improved. An organisation with an high level of maturity operates with predictability, accountability, and strategic alignment, which is characterised by documented procedures, integrated decision-making, measurable objectives, and feedback loops for learning and adaptation.

Maturity is not just a qualitative label. It can be assessed through structured models such as CMMI, COBIT, ISO/IEC 33000 series, and others. These models describe maturity across defined levels, enabling benchmarking and structured progression. A key terminological point must be emphasised: in professional and academic contexts, we should avoid using the term "immaturity". Instead, the technically appropriate term is "low maturity" or "low maturity level". These expressions refer to identifiable, structured states within maturity models, free from rhetorical or emotional overtones. "Immaturity" carries imprecise connotations and is not analytically useful in professional discourse.

1.12.1 Management Systems and Maturity

Management systems play a critical role in enabling maturity. A management system is a set of interrelated or interacting elements that organisations use to establish policy and objectives and to achieve those objectives. It includes planning, implementation, monitoring, and continuous improvement. Management systems in relation to maturity typically exhibit several key features:

- **Systematisation of activities** — documented procedures and defined roles;
- **Performance monitoring** — use of indicators and regular assessments;
- **Alignment mechanisms** — integration between strategic, operational, and compliance objectives;
- **Review cycles** — management reviews and corrective/preventive actions.

A low maturity level is often associated with the absence of a structured management system, or with a system that exists on paper but without operational practice. There may be reliance on informal routines or personal knowledge, minimal documentation, and weak feedback mechanisms. Again, such situations should be described precisely as exhibiting "low maturity", not "immaturity".

Maturity can be scoped across domains: quality, security, risk, IT, environmental performance, and others. Integrated management systems seek to unify multiple domains under a coherent structure, which is itself a sign of higher maturity.

1.12.2 Management Systems and Assessment

Maturity assessment can be qualitative, quantitative, or hybrid. Methods include:

- **Self-assessments** using checklists or guided interviews;
- **Internal or external audits** based on standards (e.g., ISO 9001, ISO/IEC 27001);
- **Benchmarking** against peers or frameworks;
- **Capability maturity evaluations**, using maturity models.

Such assessments serve different purposes: diagnostic (to identify gaps), strategic (to guide investment), or compliance-driven (to demonstrate adherence to a standard).

Maturity models provide structured ways to evaluate and enhance organisational capabilities, usually considering five progressive levels:

1. **"Level 1" - Initial (Ad Hoc, Reactive):** Processes are unstructured, inconsistent, and unpredictable. Success depends on individual efforts rather than repeatable methodologies. Risk management and compliance are reactive rather than proactive.
2. **"Level 2" - Repeatable (Basic Process Established):** Fundamental management processes are documented and repeatable. There is some level of **control and standardisation**, but effectiveness varies. Risk management and compliance practices exist but may not be consistently applied.
3. **"Level 3" - Defined (Standardised and Formalised)**: Management systems are **established and formally documented**, following structured methodologies such as ISO-based frameworks. Performance measurement and feedback mechanisms support improvement. Compliance is embedded in operational processes.
4. **"Level 4" - Managed (Quantitatively Controlled and Measured):** Processes are measured, monitored, and optimised using data-driven approaches. Continuous improvement is embedded in the management culture. Risk management and compliance are **proactively integrated** into decision-making.
5. **"Level 5" - Optimised (Continuous Improvement and Innovation)**: The organisation actively seeks improvements based on performance data, innovation, and strategic alignment. Governance, risk, and compliance (GRC) functions are fully integrated into all aspects of management. Agility, resilience, and adaptability define decision-making.

1.12.3 Conclusion

Management in organisations is not just about planning, coordination, and execution, but also about continuous improvement and achieving higher levels of organisational maturity. Maturity is a core organising principle in modern management frameworks. It allows organisations to measure their capabilities, benchmark practices, and identify pathways for growth. One of the key frameworks supporting organisational maturity is the **Management System** approach, as defined by various ISO standards. A **Management System** establishes structured policies, processes, and controls to guide an organisation toward its strategic and operational goals.

In consultancy settings, framing observations through maturity language enables constructive conversations. For example, one can point out that an organisation is at a "low maturity level" in incident response planning, rather than stating that it is "immature" (the latter risks being interpreted as judgemental or personal). Consultants and professionals must be precise in their terminology: use of "low maturity" or "low maturity level" aligns with technical models and promotes clarity. Avoiding vague or colloquial alternatives such as "immaturity" ensures communication remains constructive and analytical.

Maturity reflects the degree of self-awareness the organisation has about its goals, systems, risks, and capabilities, and its ability to act coherently based on that awareness.

1.13 Management Systems and Frameworks

A **Management System (MS)** provides a structured framework through which an organisation establishes policies, sets objectives, and implements processes to achieve those objectives effectively and consistently. These systems are essential for translating governance principles into operational reality, enabling organisations to meet regulatory obligations, manage risks, and pursue continuous improvement. **Management Systems** do not operate in isolation, they are embedded within broader organisational practices, supported by a combination of documentation, roles, controls, and performance monitoring. Their strength lies in the ability to create repeatable, auditable, and adaptable processes that align with strategic goals. Commonly formalised through international standards such as ISO, they are applicable across a wide range of domains, including quality, information security, business continuity, environmental responsibility, and privacy.

1.13.1 Common ISO-Based Management Systems

A number of ISO standards define Management Systems that are widely adopted in both public and private sector organisations[36],[37]. Examples include:

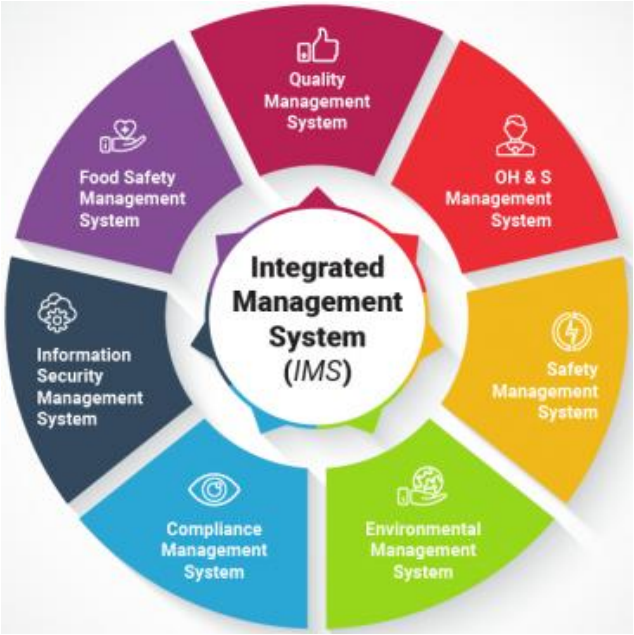
- **ISO 9001** – Quality Management System (QMS): Consistent processes for product and service delivery, customer satisfaction, and continuous improvement.
- **ISO/IEC 27001** – Information Security Management System (ISMS): Provides a framework for managing information security risks, including access control, **ICT asset management**, and incident response.
- **ISO 22301** – Business Continuity Management System (BCMS): Focuses on organisational resilience and the ability to maintain operations during disruptions.
- **ISO 14001** – Environmental Management System (EMS): Enables organisations to manage their environmental impact, compliance, and pursue sustainability.
- **ISO/IEC 27701** – Privacy Information Management System (PIMS): An extension to ISO/IEC 27001, supporting the management of personal data in alignment with privacy regulations such as GDPR.
- **ISO 37001 - Anti-bribery Management Systems**.
- **ISO 50001 - Energy Management Systems**.

These systems share a common structure based on the "Plan-Do-Check-Act" (PDCA)[38] cycle, facilitating integration and scalability across functions.

1.13.2 The Role of Frameworks

In addition to formal standards, organisations frequently adopt **management frameworks** to provide guidance, structure, and best practices in specific areas. Unlike standards, which define what must be achieved (and may be subject to certification), frameworks often describe how to implement practices, offering tools, maturity models, and reference processes. Examples include:

- **COBIT** (Control Objectives for Information and Related Technologies): Focuses on governance and management of enterprise IT, aligning IT operations with business needs.



- **ITIL** (Information Technology Infrastructure Library): Provides detailed guidance on IT service management, covering lifecycle stages such as incident, change, and service level management.
- **NIST Cybersecurity Framework**: Offers a comprehensive structure for identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents.
- **TOGAF** (The Open Group Architecture Framework): Supports enterprise architecture planning and governance, aligning technology and business capabilities.

Frameworks are often combined with management systems to enhance implementation. For example, ISO/IEC 27001 may be used alongside NIST guidelines for cybersecurity, or COBIT may inform the design of processes governed by ISO/IEC 38500.

1.13.3 Integrated Management Systems

Organisations with high levels of maturity typically adopt **multiple management systems and frameworks** in an integrated manner[39]. This integration avoids duplication, ensures consistency, and supports holistic governance:

- Quality and security management systems can share risk assessment procedures.
- Business continuity planning may rely on shared asset inventories and incident response plans from the ISMS.
- Audit and compliance functions can report across domains using common indicators and dashboards; integrated systems facilitate certification and reporting.

1.13.4 Conclusion

Standards such as those defined by ISO, offer internationally recognised models for quality, security, and continuity, while frameworks like COBIT and ITIL provide methods and tools to operationalise these models. By adopting and integrating these systems (see image above[40]), organisations build resilience, trust, and capability (key attributes for sustainable success in complex and digitally dependent environments.

[36] https://www.iso.org/management-system-standards.html
[37] https://www.iso.org/management-system-standards-list.html
[38] https://en.wikipedia.org/wiki/PDCA
[39] https://www.iso.org/news/ref2347.html
[40] Image from: https://qsmgroup.com.au/integrated-management-systems/

1.14 ISO Management System Standards

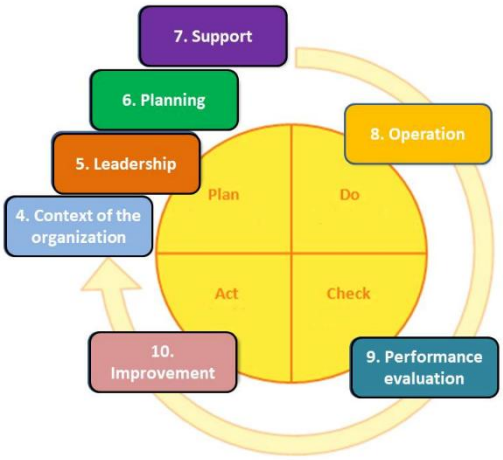
A **management system**, in ISO terminology, refers to a structured set of policies, processes, and procedures used by an organisation to achieve specific objectives. A **Management System Standard (MSS)** provides the normative requirements and guidance to develop and operate such systems. These standards do not prescribe specific technologies or tools; instead, they define what must be in place to ensure consistent, effective, and continually improving practices in a given domain.

Management systems can be applied to a wide range of organisational goals: ensuring quality, managing environmental impact, securing information, ensuring occupational health, or protecting personal data. While each domain has its own requirements, ISO has harmonised the structure of these standards to allow integration and consistency across management areas.

1.14.1 Integrated Management Systems

Since 2012, ISO has adopted a **High-Level Structure (HLS)**, now referred to as the **Harmonised Structure**, for all new and meanwhile revised MSS.

This structure includes common clauses in relation to the PDCA cycle (such as context of the organisation, leadership, planning, support, operation, performance evaluation, and improvement; see image[41]), making it easier to implement **integrated management systems (IMS)**, which is especially important in large or regulated organisations managing multiple compliance and assurance areas simultaneously.



An **IMS** combines multiple management systems (such as those for quality, information security, environment, or occupational health) into a unified framework. Instead of managing each domain separately, an IMS aligns their policies, processes, and controls under shared objectives, roles, and procedures. This integration is enabled by the common structure used in modern ISO management system standards, which include shared clauses for leadership, planning, support, performance evaluation, and continual improvement. The purpose of an IMS is to reduce duplication, improve coordination, and enable more effective governance across disciplines. For example, risk assessments, internal audits, and training programmes can be streamlined when managed through a single system. An IMS is particularly valuable in complex organisations where overlapping requirements, such as those from ISO 9001 (quality), ISO/IEC 27001 (information security), and ISO 14001 (environment), need to be met efficiently. While integration may be full or partial, depending on organisational structure and scope, the approach supports greater consistency, accountability, and transparency. It can also improve responsiveness to change and reduce audit fatigue. Whether for public or private entities, an integrated management system reflects a mature, strategic view of governance and continuous improvement.

1.14.2 Certifications

Many MSS allow for **independent third-party certification**. Certification provides formal recognition that an organisation conforms to the requirements of a given standard. It is conducted by accredited certification bodies and typically involves periodic audits and surveillance visits. Certification serves various purposes:

- **Demonstrating compliance** to regulators, partners, and customers
- **Enabling market access**, especially in public procurement or regulated sectors
- Supporting internal governance and continuous improvement

However, certification only applies to the **defined scope** of implementation. This may cover the entire organisation, or only specific functions, sites, services, or business units.

1.14.3 Examples of Widely Adopted MSS

Below are some widely used and certifiable standards (these are often used in combination, depending on priorities and stakeholder requirements; for example, ISO 9001 and ISO/IEC 27001 jointly address quality and security in service delivery):

Standard	Domain	Notable Features
ISO 9001	Quality Management	The first and most widely adopted MSS globally
ISO 14001	Environmental Management	Focus on environmental impacts and compliance
ISO/IEC 27001	Information Security Management	Core standard in the ISO 27xxx family
ISO 45001	Occupational Health and Safety	Replaced OHSAS 18001
ISO/IEC 20000-1	IT Service Management	Aligned with ITIL practices
ISO 22301	Business Continuity Management	Addresses preparedness and resilience
ISO 50001	Energy Management	Supports energy performance improvement
ISO/IEC 27701	Privacy Information Management	Extension to ISO/IEC 27001 (certifiable as an extension)

1.14.4 Strategic Value

The adoption of MSS contributes not only to compliance, but also to improved internal coherence, risk awareness, and accountability. For public administrations, MSS adoption signals commitment to transparency and good governance. For private enterprises, it may serve as a market differentiator and a foundation for scaling operations securely and reliably.

[41] Image from: https://www.qualitiso.com/en/hls-high-level-structure/

1.15 Management Oversight

Effective oversight is necessary to ensure that organisational actions are consistent with strategic goals, legal obligations, and ethical standards. Compliance processes, performance assessments, and audits provide the structured mechanisms through which this oversight is exercised, enabling management to detect deviations, ensure accountability, and drive continuous improvement.

1.15.1 Compliance

Compliance requirements can be grouped into three broad categories:

- **Legal and Regulatory**: National or international laws and sector-specific regulations (e.g. GDPR, labour law, public procurement rules).
- **Contractual**: Commitments made through contracts or agreements with clients, suppliers, or partners.
- **Voluntary or Internal**: Adoption of standards, codes of conduct, or policies set by the organisation itself (e.g. ISO standards, ethics codes, internal procedures).

1.15.2 Roles and Responsibilities

Effective compliance relies on clearly assigned roles and institutional support:

- **Executive management** sets the tone and ensures resources for compliance initiatives.
- **Compliance officers**, **internal auditors**, or **risk managers** coordinate assessments and provide oversight.
- **Operational staff and process owners** are responsible for embedding compliance into daily activities and maintaining records in relation to that.
- **Specialised roles**, such as Data Protection Officers (DPOs), are required by law in some contexts and act as key points of contact with regulators.

Clear accountability, supported by appropriate training and communication, strengthens compliance at all levels.

1.15.3 Compliance Assessment and Audits

In many cases, organisations operate under a combination of these layers. Public sector bodies, in particular, are subject to comprehensive legal frameworks that demand transparency, accountability, and traceability in service delivery.

Compliance assessment refers to the process of evaluating whether a system, process, or organisation meets the applicable requirements. This may take different forms:

- **Internal audits and self-assessments**: Conducted by internal functions, such as audit, quality, or compliance teams.
- **External audits or inspections**: Performed by regulators, supervisory authorities, or independent assessors.
- **Continuous compliance monitoring**: Supported by automated tools and dashboards, especially in operational contexts.

Assessment and **audit** are both structured evaluations, but they differ in purpose, scope, and formality:

- **Assessment** is a flexible evaluation process used to understand how well an organisation meets certain expectations, such as maturity levels, best practices, or readiness for change. It may be internal or external, and its goal is often to support improvement, benchmarking, or strategic planning. Assessments may be qualitative, quantitative, or mixed.
- **Audit** is a formal, systematic examination conducted against predefined criteria, often a standard or regulation (e.g. ISO/IEC 27001, GDPR). Audits follow established procedures, are usually carried out by independent parties, and aim to verify **conformity** (in certification audits) or **compliance** (in legal or regulatory audits). Audit findings may lead to certification, corrective actions, or penalties.

1.15.4 Certification

When compliance with a formal set of requirements is externally validated by a recognised body, the result can lead to **certification**. Certification provides independent assurance that specific requirements (typically defined in international standards) have been systematically implemented and maintained. For instance:

- ISO 9001 certification attests to the presence of a quality management system aligned with best practices.
- ISO/IEC 27001 certification demonstrates conformity to information security management system requirements.

Certification may be mandatory in some business or public procurement contexts. It also serves as a competitive differentiator in the private sector. It typically requires initial assessment, surveillance audits, and periodic recertification.

1.15.5 Compliance Culture and Integration

Compliance should not be treated as an isolated function. It must be integrated with broader governance mechanisms and aligned with risk management and internal control systems. This integration enables a more coherent response to overlapping issues, such as security incidents that may trigger both legal and operational consequences.

Mature organisations foster a compliance culture, in which obligations are understood not only as constraints but as instruments for quality, trust, and value creation. Certification efforts often support this culture by formalising practices, improving documentation, and promoting continuous improvement. The ability to demonstrate compliance (through assessment, audit, or certification) is as important as the substantive adherence itself, especially in environments subject to oversight or public scrutiny.

Regulatory Technology (RegTech) solutions enable real-time monitoring, automated reporting, and improved risk detection, reducing the burden of manual processes and increasing reliability, illustrating the increasing reliance on digital tools to meet compliance requirements efficiently (particularly in sectors with high compliance obligations, such as finance or health, these tools play a growing role in aligning operations with regulatory standards).

1.16 Management Assurance: Auditing

Auditing is a core mechanism of management oversight. It provides assurance that an organisation's activities are being conducted as intended, in compliance with internal policies, legal requirements, and strategic goals. In the context of formal Management Systems, audits are essential for verifying the effectiveness of controls, the adequacy of risk responses, and the consistency of performance across processes.

Audits help identify deviations, inefficiencies, and improvement opportunities, thereby reinforcing the "Check" phase of the Plan–Do–Check–Act (PDCA) cycle that underpins many ISO management systems standards. More broadly, auditing serves to build internal accountability and external trust, both of which are vital in regulated, competitive, and high-risk sectors.

1.16.1 Due Diligence and the Role of Auditing

Auditing also plays a critical role in demonstrating that due diligence has been exercised.

Due diligence refers to the structured and proactive assessment of risks, obligations, and potential impacts before or during decision-making. It is a fundamental principle of responsible governance and is expected in areas such as procurement, outsourcing, compliance, mergers, strategic initiatives, and third-party engagements.

Audits provide the documentary evidence that due diligence has not only been considered but also operationalised and verified. For CxO roles and those who advise them, this is especially relevant: the ability to demonstrate that decisions were taken with foresight and care may significantly reduce liability and reinforce institutional credibility.

1.16.2 Types of Audits

Organisations typically employ multiple types of audits, depending on the scope, purpose, and audience, such as:

- **First-Party (Internal) Audits**: Conducted typically through internal audit teams or process owners. to support **self-assessment**, monitor internal controls, and prepare the organisation for external evaluation (focus on compliance, risk management, and operational efficiency).
- **Second-Party Audits**: Performed by clients, customers, or partners to assess **compliance with contractual obligations**, service expectations, or supply chain requirements[42],[43].
- **Third-Party (External) Audits**: Carried out by independent certification bodies or regulatory authorities to assess conformity with formal standards (e.g. ISO 27001, ISO 9001), financial and legal requirements, or sector-specific regulations; often result in certifications, regulatory approvals, or public assurances of governance maturity.

Each audit type has a specific function within the broader governance and compliance ecosystem.

1.16.3 Audit Planning and Execution

A robust audit process typically follows a structured methodology:

- **Planning** – Define objectives, scope, criteria, and schedule. Select auditors with appropriate competence and independence.
- **Execution** – Collect and examine evidence (interviews, observations, sampling, and document reviews).
- **Reporting** – Record findings, highlight non-conformities or risks, and provide recommendations.
- Follow-up – Track corrective actions, reassess risks, and verify closure of findings. Audit cycles should feed into management reviews and continuous improvement initiatives.

In formal Management Systems (e.g. ISO/IEC 27001), internal audits are mandatory and must be performed at planned intervals, based on risk and organisational changes.

1.16.4 Audit Functions and Organisational Roles

In large or regulated organisations, auditing is usually embedded within a broader governance, risk, and compliance (GRC) function. Key roles include:

- **Internal Audit Department** – Reports to the board or audit committee. Focuses on independent review of risk controls, financial integrity, and compliance.
- **Line Managers and Process Owners** – Responsible for preparing for audits and responding to findings. They play a critical role in demonstrating process maturity and taking corrective actions.
- **CxO Roles** – CIOs, CISOs, and other executives are often subject to audits concerning governance of IT, data protection, or cybersecurity. Their visibility and cooperation with auditors are essential for demonstrating accountability and institutional due diligence.

1.16.5 Value Beyond Compliance

While audits are often seen as compliance tools, they also offer strategic value:

- **Risk Awareness** – Audits expose latent risks, emerging vulnerabilities, or ineffective controls that may not be visible in day-to-day operations.
- **Performance Insight** – Metrics and findings provide feedback on whether strategic goals are being achieved through operational practices.
- **Cultural Reinforcement** – A well-conducted audit process encourages ethical behaviour, transparency, and engagement with continuous improvement.

To realise this value, organisations must approach auditing as a learning opportunity—not merely a box-ticking exercise.

1.16.6 Conclusion

Auditing is a fundamental instrument of management assurance: It provides verifiable evidence that governance structures are functioning, that controls are effective, and that strategic risks are being managed responsibly.
By integrating the concept of due diligence, audits reinforce not only regulatory compliance but also the quality of decision-making at all levels.

For senior leadership and those who support them, audits are not just oversight, they are an essential part of earning and sustaining trust.

[42] https://redresscompliance.com/sap-audit-defense-faq/

[43] https://www.ikea.com/global/en/stories/sustainability/the-iway-auditing-process-ten-principles-for-building-a-responsible-supply-chain-230619/

1.17 Management Excellence: Certifications

Certifications are formal attestations issued by recognised third-party bodies, verifying that something meets a specified standard. In the context of management systems, certifications provide external validation of the capability to deliver consistent, compliant, and high-quality outcomes within a defined scope.
Contrary to popular perception, certifications rarely apply to an organisation as a whole. They are typically granted to a specific function, process, product line, department, or physical facilities.

For example, a company may be certified for its information security management practices in a particular data centre, or for its quality management system in relation to the development of a specific product or service.

1.17.1 Organisational Certifications

Organisations may pursue various certifications to demonstrate alignment with best practices in areas such as quality, security, environmental performance, or service continuity. Examples include:

- **ISO 9001** – Quality Management Systems: Confirms the presence of systematic practices for delivering products and services that meet established requirements.
- **ISO/IEC 27001** – Information Security Management Systems: Demonstrates structured control over risks to confidentiality, integrity, and availability of information.
- **ISO 14001** – Environmental Management Systems: Focuses on reducing environmental impact and complying with environmental regulations.
- **ISO 22301** – Business Continuity Management Systems: Validates preparedness for operational disruptions and ability to maintain critical services.
- **ISO/IEC 20000-1** – IT Service Management: Aligns IT service delivery with business needs through structured management and continuous improvement.
- **ISO/IEC 27701** – Privacy Information Management Systems: Supports GDPR compliance and privacy risk management, as an extension to ISO/IEC 27001.

Each certification applies only to a clearly defined scope, subject to regular surveillance and renewal. This scope must be understood when evaluating maturity claims or when integrating certified capabilities into broader governance frameworks.

1.17.2 Professional Certifications

Individuals also can obtain certifications that validate their knowledge, competence, and commitment to recognised standards and practices. These certifications are valuable for building credibility, demonstrating readiness for specific responsibilities, and aligning teams with shared methodologies. Examples include:

- **CISA** (Certified Information Systems Auditor) – Focused on auditing, control, and assurance of information systems.
- **CISM** (Certified Information Security Manager) – Emphasises leadership in enterprise information security programmes.
- **CISSP** (Certified Information Systems Security Professional) – Recognised for technical and managerial expertise in cybersecurity.
- **ITIL Certifications** – Cover IT service management practices across lifecycle stages.
- **COBIT Certifications** – Validate understanding of enterprise governance of IT.
- **PRINCE2[44],[45] and PMP[46] (Project Management Professional)** – Focus on project management methodologies and frameworks.

1.17.3 Certification Bodies and Accreditation

Certifications are issued by accredited certification bodies that operate under internationally recognised principles of impartiality and competence. In Portugal, na exemple is **APCER** (Associação Portuguesa de Certificação). At the international level, accreditation is overseen by bodies such as **IAF** (International Accreditation Forum). In regulated sectors, additional oversight may be exercised by supervisory authorities or sector-specific regulators.

1.17.4 Strategic Benefits of Certification

When properly interpreted and integrated, certifications deliver multiple benefits:

- **Market Access and Competitiveness** – A prerequisite for participating in public procurement or regulated markets.
- **Risk Reduction and Assurance** – Uncover weaknesses and promote control mechanisms that reduce exposure to operational and compliance risks.
- **Stakeholder Trust and Reputation** – Third-party validation reinforces transparency, reliability, and commitment to quality and integrity.
- **Process Maturity and Learning** – Certification audits promote internal discipline and continuous improvement, particularly when combined with management dashboards and review cycles.

However, certifications must not be overstated. The fact that one part of an organisation is certified does not imply that others are, or that certified practices are uniformly adopted. For executives, clients, or partners interpreting certification claims, it is critical to ask: *What exactly is certified? Who maintains the scope? How is conformance verified and sustained?*

1.17.5 Conclusion

Certifications are valuable indicators of management excellence, **but only within their defined scope**. They do not certify an entire organisation in a generic sense, but rather a specific system, activity, or context. Certifications offer assurance, credibility, and structure, but their true impact depends on integration with broader governance, risk, and compliance efforts. When aligned with organisational purpose and monitored through robust oversight, certifications become not only a badge of maturity, but a tool for sustained improvement.

[44] https://www.prince2.com/eur/what-is-prince2
[45] https://www.prince2portugal.pt/
[46] https://www.pmi.org/standards/pmbok

1.18 Governance and Ethics

Ethics and responsible governance are essential foundations for trustworthy, sustainable, and legitimate organisational conduct. While governance establishes structures, policies, and processes for oversight and decision-making, ethics and **ethical values** provide the moral compass that guides how those decisions should be made and implemented. In modern organisations, ethical considerations are no longer optional; they are a strategic imperative.

1.18.1 The Role of Ethics in Governance

Ethics in governance refers to the application of moral principles (such as integrity, fairness, transparency, and accountability) in the leadership and management of organisations. Ethical governance helps ensure that decision-making processes respect not only legal standards but also social norms and stakeholder expectations. Ethical principles support:

- **Trust and Reputation** – Ethical behaviour fosters public and stakeholder trust, a critical asset for any organisation.
- **Long-Term Value Creation** – Ethical organisations are more likely to adopt sustainable practices that benefit society and the environment.
- **Internal Cohesion** – A strong ethical culture promotes employee engagement, loyalty, and compliance with internal policies.

While laws define minimum acceptable standards, ethics often go further, addressing issues where regulations may be ambiguous or lag behind societal expectations.

1.18.2 Elements of Responsible Governance

Responsible governance expands the scope of traditional corporate governance by integrating ethical values and social responsibilities into strategic oversight. Key elements include:

- **Integrity in Decision-Making** – Governance should uphold honesty, transparency, and consistency, avoiding conflicts of interest and ensuring that decisions serve the organisation's mission rather than personal gain.
- **Accountability and Oversight** – BoD members and CxOs must be accountable for their actions and for the organisation's performance. This includes transparent reporting and responsiveness to stakeholders.
- Respect – valuing the dignity, rights, and contributions of individuals
- Fairness – making decisions impartially and without bias
- Trustworthiness – being reliable and dependable in actions and communications
- **Sustainability and Social Responsibility** – Boards are increasingly expected to consider the long-term social and environmental impacts of their decisions. Responsible governance encourages alignment with frameworks such as the UN Sustainable Development Goals (SDGs).
- **Anti-Corruption and Whistleblower Protection** – Organisations should implement robust mechanisms to prevent fraud, bribery, and unethical behaviour, as well as protect individuals who report misconduct.

1.18.3 Environmental, Social, and Governance Considerations

In recent years, Environmental, Social, and Governance (ESG) criteria have become central to responsible governance. These factors are used by investors, regulators, and the public to assess how well organisations manage their non-financial risks and obligations.

- **Environmental** – Includes energy use, waste management, emissions, and environmental impact.
- **Social** – Covers labour practices, human rights, community engagement, and consumer protection.
- **Governance** – Focuses on board structure, ethical leadership, executive remuneration, and transparency.

Integrating ESG principles into governance frameworks helps organisations anticipate regulatory change, reduce reputational risk, and attract socially conscious investors and partners.

1.18.4 Embedding Ethics in Organisational Culture

Ethical governance is most effective when supported by a values-based organisational culture.
This involves:

- **Codes of Ethics or Conduct** – Clearly articulating expected behaviours and responsibilities.
- **Training and Awareness** – Ensuring that staff at all levels understand and apply ethical standards in their daily work.
- **Leadership by Example** – Senior figures must model ethical behaviour consistently.
- **Mechanisms for Dialogue** – Establishing safe channels for raising concerns, discussing dilemmas, and reporting unethical practices.

1.18.5 Conclusion

Ethics and responsible governance are not abstract ideals; they are practical tools for building resilient, credible, and forward-looking organisations. In a world of growing scrutiny and complex challenges, ethical leadership is essential to balance performance with purpose, ensuring that organisations act not only in accordance with the law, but in service of the common good[47,48,49].

[47] *Interesting extra reading*: **Backdating: Insight Into a Scandal - Deception, greed, and corporate accountability in options trading** - https://www.investopedia.com/articles/optioninvestor/09/backdating-insight-scandal.asp

[48] 007: Accused Tech Spy Says Rival CEO Recruited Him With Offer to Be Like James Bond - Former employee of payroll-services firm Rippling says executives at Deel directed him to steal corporate secrets - https://www.wsj.com/tech/accused-tech-spy-says-rival-ceo-recruited-him-with-offer-to-be-like-james-bond-793483e1

[49] When there is too much money: The World's Biggest Construction Project Is a Magnet for Executives Behaving Badly - Saudi Arabia's Neom project contends with corruption, worker deaths, racism and misogyny - https://www.wsj.com/business/the-worlds-biggest-construction-project-is-a-magnet-for-executives-behaving-badly-9accd37b

1.19 Governance and Organisational Culture

Governance and culture are deeply interconnected, shaping the way organisations establish and enforce policies, make decisions, and interact with stakeholders. While governance provides the structural framework for oversight, accountability, and strategic direction, organisational culture influences how governance mechanisms are perceived, implemented, and sustained.

1.19.1 The Role of Organisational Culture in Governance

Organisational culture *can be understood as the shared values, beliefs, norms, and behaviours that define how individuals within an organisation interact and work together.*

Effective governance is not solely about rules, policies, and formal structures, as it also depends on a culture that supports ethical behaviour, transparency, and accountability. Without alignment between governance and culture, even the most robust governance frameworks may fail in practice.

Key aspects of organisational culture that influence governance include:

- **Ethical Standards** – A strong ethical culture encourages compliance with governance policies and fosters responsible decision-making at all levels.
- **Transparency and Openness** – Cultures that value openness facilitate better information flow and accountability, reducing the risks of corruption or poor governance.
- **Risk Awareness** – An organisation's risk culture determines how governance frameworks address uncertainty, balancing innovation with regulatory compliance.
- **Leadership and Tone at the Top** – Senior leadership plays a critical role in setting cultural expectations, as employees often model behaviours based on executive attitudes and decisions.

A governance framework that ignores cultural dynamics risks being ineffective, as employees and stakeholders may not internalise or adhere to governance principles in daily operations.

1.19.2 Governance Models and Cultural Variations

Governance structures vary across organisations, industries, and national contexts, often reflecting underlying cultural differences. For instance:

- **Corporate vs. Public Sector Governance** – Private sector governance typically prioritises shareholder interests and financial performance, while public sector governance focuses on public accountability and service delivery. Cultural attitudes towards risk-taking, transparency, and decision-making authority differ significantly between these environments.
- **Regulatory and Legal Influences** – National governance models are shaped by legal traditions, such as common law systems (e.g., the UK and US) versus civil law systems (e.g., most of continental Europe). These legal foundations reflect broader cultural norms related to regulatory enforcement and corporate responsibility.
- **Organisational Size and Industry Factors** – Start-ups and technology firms often have flatter hierarchies and more agile governance structures, while large financial institutions or government bodies may have rigid, compliance-driven governance models. These differences arise from variations in organisational culture, industry norms, and regulatory expectations.

Understanding cultural influences on governance is essential for organisations operating across multiple regions, as governance mechanisms must be adapted to fit local expectations without compromising core ethical and operational principles.

1.19.3 Aligning Governance and Organisational Culture

For governance to be effective, it must be embedded in the organisation's culture, rather than treated as a separate or purely procedural function. Strategies to achieve this alignment include:

- **Developing a Governance-Oriented Culture** – Organisations should promote awareness of governance principles through leadership commitment, regular communication, and employee engagement initiatives.
- **Training and Awareness Programmes** – Ethical training and compliance education ensure that governance frameworks are understood and integrated into daily activities.
- **Incentives and Reinforcement Mechanisms** – Aligning performance metrics and rewards with good governance practices encourages adherence to policies and ethical standards.
- **Continuous Monitoring and Adaptation** – Governance structures should be reviewed regularly to ensure they evolve alongside cultural and operational changes within the organisation.

By embedding governance within an organisation's culture, companies and institutions enhance their ability to manage risks, ensure compliance, and achieve strategic goals in a sustainable manner.

1.19.4 Conclusion

Governance and culture are interdependent forces that shape organisational effectiveness. While governance provides the rules and structures for oversight, culture determines how these are applied in practice. Successful organisations recognise that governance is not merely a compliance function but a dynamic process that must be integrated into their cultural fabric. Fostering a governance-conscious culture can strengthen accountability, ethical decision-making, and long-term resilience.

1.20 Cultural Variation in Management and Governance

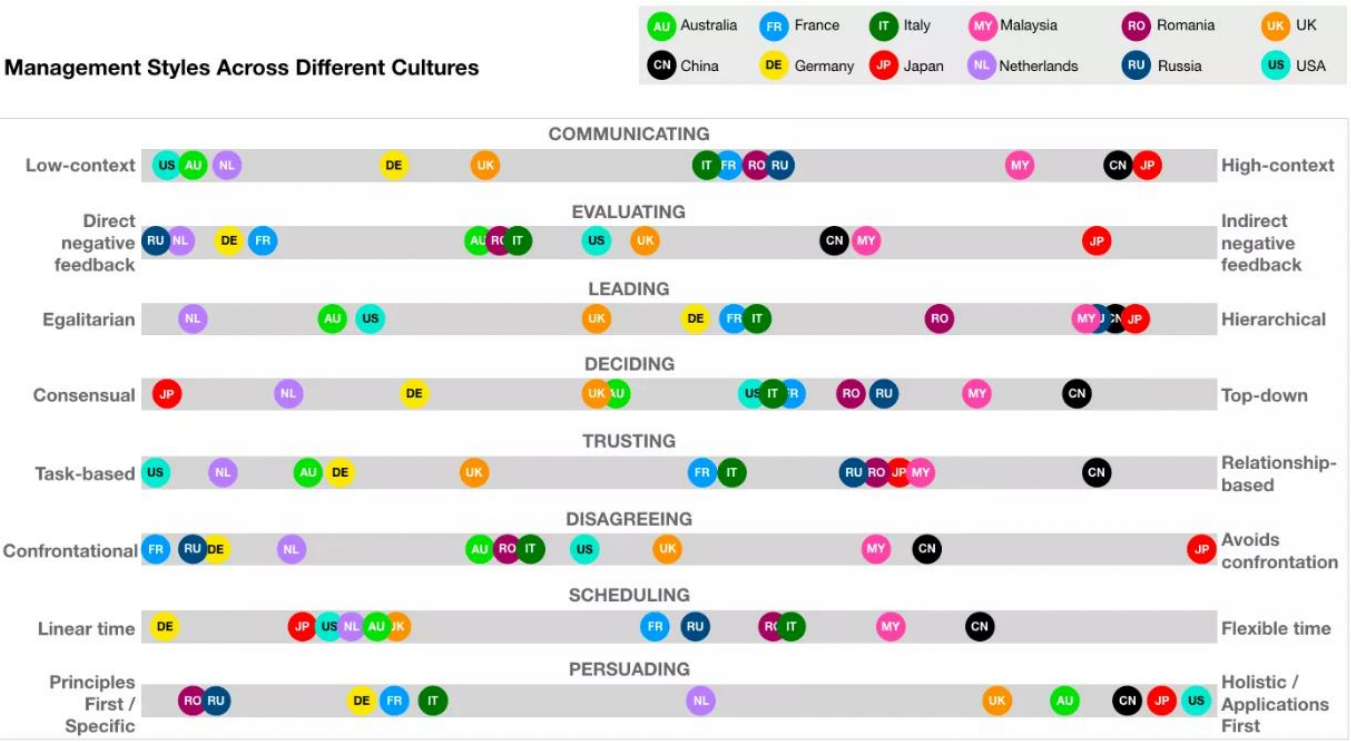
Cultural context significantly shapes how organisations communicate, lead, build trust, and make decisions. Formal governance and management systems often operate alongside informal norms rooted in national or institutional cultures. Recognising these patterns is essential for interpreting organisational dynamics and ensuring that practices and frameworks are applied effectively across diverse environments.

Erin Meyer's work, *The Culture Map*[50], outlines eight dimensions of cultural variation, which she presents as relevant to professional settings:

- **Communicating**: Low-context cultures favour explicit, direct communication. High-context cultures rely on implicit understanding and shared context…
- **Evaluating**: Some cultures give direct negative feedback; others use more indirect, face-saving approaches…
- **Persuading**: Reasoning may start from principles (deductive) or from practical examples (inductive), influencing how arguments and reports are framed…
- **Leading**: In egalitarian contexts, authority is informal and accessible. Hierarchical cultures value clear status and structured delegation…
- **Deciding**: Some environments favour consensus-based decisions; others rely on top-down authority…
- **Trusting**: In task-based cultures, trust arises from competence. In relationship-based settings, it develops through personal connection…
- **Disagreeing**: Confrontational cultures tolerate open challenge. Others avoid conflict to preserve group harmony…
- **Scheduling**: Linear-time cultures prioritise punctuality and planning. Flexible-time cultures adapt, sequencing to the situation…

These patterns are not rigid rules but observable tendencies. Cultural variation can affect how strategy is communicated, how compliance is ensured, and how digital transformation or risk governance is approached. For instance, a control mechanism seen as routine in one context may be perceived as intrusive in another.

Cultural awareness is thus not simply interpersonal, it is institutional. *Governance models that succeed across contexts often adapt how roles are defined, how procedures are introduced, and how authority is exercised. Understanding these differences enhances alignment, reduces friction, and supports trust across diverse organisational and regulatory settings.*



Source: Erin Meyer, The Culture Map. Decoding HowPeople Think, Lead, And Get Things Done Across Cultures

[50] https://erinmeyer.com/books/the-culture-map/

1.21 Board Dynamics and Governance Structures

*The **Board of Directors (BoD)** is the organisation's highest governance authority, responsible for setting direction, overseeing management performance, and ensuring accountability to stakeholders.*

The BoD plays a central role in governance, serving as the link between shareholders or other stakeholders and the executive leadership of an organisation.
The composition, structure, and internal dynamics of the BoD significantly influence the effectiveness of oversight, strategic direction, and ethical conduct. Understanding different governance structures and the dynamics within boards is essential for assessing the strength and maturity of any organisation's governance model.

1.21.1 Roles and Responsibilities of the Board

The primary responsibilities of a board of directors include:

- **Strategic Oversight** – Approving long-term goals, business plans, and major investments.
- **Performance Monitoring** – Evaluating executive performance and organisational outcomes.
- **Risk Management and Compliance** – Ensuring that appropriate risk frameworks and internal controls are in place.
- **Ethical and Legal Accountability** – Upholding fiduciary duties, compliance with laws, and alignment with ethical standards.
- **Stakeholder Engagement** – Representing shareholder or public interests and balancing stakeholder expectations.

Boards must strike a careful balance between supporting executive management and providing independent oversight.

1.21.2 Board Composition and Roles

Effective boards typically comprise a mix of **executive directors** (involved in day-to-day operations) and **non-executive directors (NEDs)**, who provide external, independent judgement. The ideal board should offer diversity in expertise, experience, and background.
Key roles within the board include:

- **Chairperson** – Leads board meetings, ensures balanced discussion, and facilitates strategic consensus.
- **Chief Executive Officer (CEO)** – Often a board member, responsible for operational leadership and executing board-approved strategies.
- **Company Secretary** – Advises on corporate governance obligations and ensures proper board procedures.
- **Board Committees** – Sub-groups such as audit, risk, remuneration, or sustainability committees allow for focused oversight of specific areas.

Strong board performance requires mutual trust, clarity of roles, and open communication between members.

1.21.3 Governance Structures

There are two dominant structural models of corporate governance, which differ in how they separate oversight and management:

- **Monistic Model (Unitary Board)** – A single board of directors includes both executive and non-executive members. This model is common in Anglo-Saxon countries like the UK and the US. It encourages close collaboration but may blur lines between oversight and execution.
- **Dualistic Model (Two-Tier Board)** – Separate supervisory and management boards exist, as seen in countries like Germany and the Netherlands. The supervisory board focuses on governance and accountability, while the management board handles operations. This model emphasises independence but can introduce complexity and slower decision-making.

The choice of structure often reflects national legal frameworks and cultural preferences regarding corporate control and stakeholder inclusion.

1.21.4 Board Dynamics and Performance

Beyond formal structures, **board dynamics** (the interactions, relationships, and behavioural patterns within the board) are critical to effective governance.
Factors that influence board dynamics include:

- **Diversity and Inclusion** – A diverse board (in gender, culture, expertise) can foster broader perspectives and reduces groupthink.
- **Independence** – Truly independent directors are more likely to challenge assumptions and hold executives accountable.
- **Information Quality** – Timely and relevant reporting enables better decision-making and reduces reliance on intuition.
- **Constructive Challenge** – Boards must encourage healthy debate and critical questioning while maintaining collegiality.
- **Board Evaluation and Development** – Regular performance reviews and high-level training enhance the effectiveness and adaptability of the board.

Boards that function as active strategic partners (rather than passive overseers or micro-managers) add tangible value to the organisation.

1.21.5 Conclusion

The effectiveness of governance is shaped not just by formal board structures, but by the quality of leadership, independence, and interpersonal dynamics within the boardroom. Whether in a corporate, public, or not-for-profit context, a well-composed and well-functioning board is essential for ethical oversight, risk control, and long-term strategic success.

1.22 Governance and Change

"Digital transformation" is a too generic term, which it usually refers to the strategic integration of digital technologies into all areas of an organisation, fundamentally changing how it operates, delivers value, and engages with stakeholders. The success of it is not guaranteed by technology alone. It requires effective **governance** to ensure that digital initiatives align with organisational goals, manage risk, and uphold ethical and legal responsibilities.

1.22.1 Challenge in Digital Change

Digital change often involves complex, cross-functional change, including:

- The adoption of new technologies (e.g., cloud computing, AI, IoT)
- The redesign of business processes and customer experiences
- The evolution of organisational culture and capabilities
- The redefinition of value creation and competitive advantage

Without strong governance, such changes can become fragmented, misaligned with strategy, or expose the organisation to unnecessary risk. Governance provides the structure and discipline to manage this change responsibly and effectively.

1.22.2 Aligning Strategy and Purpose

Governance ensures that change programmes support (and not distract from) the organisation's core mission.

This involves:

- **Strategic alignment** – Ensuring that digital initiatives are prioritised based on their contribution to long-term goals, whether commercial, public service, or social impact.
- **Benefit realisation** – Defining clear value propositions and outcomes for digital projects, and tracking their realisation.
- **Stakeholder engagement** – Involving users, employees, partners, and regulators early and throughout the transformation process.

Senior leadership, including the board, must provide ongoing oversight and challenge to ensure that digital ambitions remain grounded in organisational purpose and reality.

1.22.3 Managing Risk and Compliance in a Digital World

Changes in a digital context often increases exposure to risks, particularly in areas such as cybersecurity, data protection, regulatory compliance, and operational continuity. Effective governance addresses these risks by:

- Embedding risk management into the design of digital initiatives
- Defining clear accountability for digital risks, including emerging risks from artificial intelligence, automation, or algorithmic bias
- Ensuring compliance with evolving legal frameworks, such as the GDPR, the Digital Services Act (DSA), or sector-specific standards

Many organisations now include digital risks in their broader Governance, Risk and Compliance (GRC) frameworks, recognising their strategic importance.

1.22.4 Cultural and Organisational Readiness

Governance also plays a critical role in shaping the organisational culture needed for successful changes This includes:

- **Leadership and tone from the top** – Leaders must demonstrate commitment to digital innovation while upholding values such as transparency, accountability, and inclusion.
- **Capability development** – Governance structures should support investment in digital skills, agile ways of working, and continuous learning.
- **Change governance** – Change often involves shifting mindsets and workflows. Governance must manage this process with sensitivity, ensuring that transitions are inclusive, well-communicated, and supported by change management practices.

1.22.5 Agile Delivery

Traditional governance approaches may not be well suited to fast-paced, iterative digital initiatives. Increasingly, organisations are adopting **adaptive or agile governance** models, which maintain accountability while allowing for experimentation and rapid feedback.

Characteristics include:

- Short, frequent decision cycles
- Empowered teams with clear guardrails
- Dynamic prioritisation based on real-time data and outcomes

This hybrid approach blends strategic oversight with operational flexibility, enabling governance to facilitate rather than constrain transformation.

1.22.6 Conclusion

Engaging in change in a digital context offers significant opportunities, but also demands a disciplined and forward-looking approach to governance. By integrating digital objectives into strategic oversight, managing new risks, fostering cultural readiness, and adopting more adaptive governance models, organisations can navigate transformation with purpose, integrity, and resilience. Ultimately, governance ensures that digital change serves the organisation, rather than the other way around.

1.23 Emerging Global Norms

In an increasingly interconnected and complex world, governance cannot be viewed solely within the boundaries of individual organisations or national jurisdictions. A growing body of **emerging global norms** is shaping expectations around transparency, sustainability, digital responsibility, and stakeholder engagement. These norms often go beyond legal compliance, setting ethical and strategic benchmarks that influence how organisations operate across borders.
Global norms emerge through a combination of international agreements, soft law, voluntary frameworks, civil society pressure, and market expectations. While not always legally binding, they carry considerable weight, particularly for organisations with international operations, global supply chains, or public accountability.

1.23.1 Drivers of Global Norms

Several global developments are fuelling the emergence and evolution of governance-related norms:

- **Sustainable Development and ESG Pressures** - There is growing pressure for organisations to integrate **Environmental, Social, and Governance (ESG)** considerations into decision-making. Investors, regulators, and the public increasingly expect transparent reporting on sustainability, human rights, and ethical business conduct.
- **Digital Globalisation** - As data and digital platforms cross borders, so too must governance frameworks. Issues such as **data sovereignty**, cross-border privacy protection, and algorithmic accountability now demand international coordination.
- **Geopolitical Shifts and Regulatory Convergence** - Trade agreements, regional alliances, and transnational crises (e.g., climate change, pandemics, cyber threats) are encouraging greater alignment in governance approaches, while also creating new tensions between national autonomy and international obligations.
- **Stakeholder Empowerment** - A more informed and vocal public, amplified by digital media and activism, is holding organisations to account on issues such as diversity, corporate ethics, and environmental impact—regardless of what the law requires.
-

1.23.2 Examples of Influential Global Norms and Frameworks

- **United Nations Sustainable Development Goals (SDGs)** - These 17 goals provide a global blueprint for peace, prosperity, and sustainability by 2030. Many organisations now align their governance and reporting practices with relevant SDGs, such as climate action, gender equality, and responsible consumption.
- **OECD Guidelines for Multinational Enterprises** - These non-binding principles offer recommendations on responsible business conduct, covering areas such as labour rights, environmental impact, bribery prevention, and disclosure.
- **UN Guiding Principles on Business and Human Rights** - These outline the duty of states and the responsibility of businesses to respect human rights, providing a framework for due diligence and remediation.
- **Global Reporting Initiative (GRI)** - The GRI standards enable organisations to measure and disclose their environmental, social, and governance performance in a transparent and comparable way.
- **ISO Standards with Global Reach** - Standards such as **ISO 26000** (Social Responsibility) and **ISO 37000** (Governance of Organisations) promote ethical and sustainable governance practices that can be applied across cultures and industries.
- **EU Digital Regulations with Global Influence** - Regulations like the **General Data Protection Regulation (GDPR)** and proposed **AI Act** have extraterritorial effects, setting benchmarks for global data protection and digital ethics.

Emerging global norms require organisations to think beyond compliance and embrace a more proactive, values-driven approach to governance. Implications include:

- Adopting **voluntary frameworks** that demonstrate commitment to global best practices
- Enhancing **transparency and reporting** to international standards
- Building **cross-border governance capabilities**, particularly in multinational operations
- Engaging with **stakeholders globally**, including through multilateral dialogues, partnerships, and public commitments

Boards and senior leaders must stay attuned to these evolving expectations and ensure that governance structures are adaptable, inclusive, and globally aware.

1.23.3 Conclusion

Emerging global norms reflect the shifting landscape of accountability, ethics, and strategic risk in the 21st century. While often soft in legal terms, they are hard in impact—shaping reputations, investment decisions, and stakeholder trust. By aligning governance practices with these norms, organisations can demonstrate leadership, resilience, and legitimacy in a globalised world.

1.24 Governance Frameworks

Governance frameworks provide structured models to help organisations define, implement, and monitor governance practices in a consistent and effective manner. These frameworks support accountability, strategic alignment, and compliance, offering tested principles and methodologies for managing complex organisations. Whether applied to corporate governance or Governance of IT, such frameworks act as reference points that enable organisations to benchmark and mature their governance capabilities.
Governance frameworks are not one-size-fits-all. They are selected and adapted based on the organisation's size, sector, regulatory context, and strategic objectives.

1.24.1 Corporate Governance Frameworks

Corporate governance frameworks focus on the overall system by which organisations are directed and controlled, especially in relation to stakeholders, leadership structures, and ethical behaviour.
Key examples include:

- **OECD Principles of Corporate Governance** - Widely adopted across the public and private sectors, these principles provide a global standard for good governance. They emphasise shareholder rights, transparency, board responsibilities, and equitable treatment of stakeholders.
- **UK Corporate Governance Code** - Applied to companies listed on the London Stock Exchange, this code promotes leadership, accountability, remuneration transparency, and board effectiveness. It operates on a "comply or explain" basis, offering flexibility while maintaining expectations.
- **King IV Report (South Africa)** - Known for its integrated approach, King IV focuses on outcomes-based governance, emphasising ethical leadership, sustainability, and stakeholder inclusiveness.
- **Sarbanes-Oxley Act (SOX)** - A legal framework in the United States, SOX enforces strict standards for financial reporting and internal controls in public companies. While not a voluntary framework, it shapes governance practices globally, especially around accountability and auditing.

These frameworks help organisations establish clear roles and responsibilities, improve board performance, and build stakeholder confidence through transparency and ethical leadership.

1.24.2 Governance of IT Frameworks

Information technology governance frameworks provide structured guidance for ensuring that IT supports business objectives, manages risk effectively, and delivers value. These frameworks are especially relevant in organisations undergoing in change or operating in highly regulated environments.

- **COBIT (Control Objectives for Information and Related Technologies)** - Developed by ISACA, COBIT is one of the most comprehensive frameworks for governance of IT and management. It provides a process model, performance metrics, and maturity models to guide decision-making, control, and continuous improvement. COBIT 2019 introduces flexible governance components that align IT goals with enterprise objectives.
- **ISO/IEC 38500** - This international standard sets out principles for the effective governance of IT. It is intended for board members and senior executives, promoting strategic alignment, performance, resource management, and risk control. It emphasises governance as a responsibility distinct from day-to-day IT management.
- **ITIL (Information Technology Infrastructure Library)** - ITIL is a widely used framework for IT service management (ITSM). While focused more on operational processes than strategic governance, ITIL includes governance-related components such as service strategy, continual service improvement, and service level management.
- **TOGAF (The Open Group Architecture Framework)** - TOGAF is primarily an Enterprise Erchitecture framework, but it includes governance mechanisms to ensure that architecture decisions align with business strategy and standards. It helps coordinate technology development within large organisations and across value chains.

These frameworks are not mutually exclusive. Many organisations combine elements from multiple frameworks to build governance models suited to their specific needs, often integrating governance of IT within broader enterprise governance structures.

1.24.3 Conclusion

Governance frameworks offer valuable structure and guidance to organisations striving for transparency, accountability, and strategic coherence. Whether corporate or IT-focused, these frameworks enable consistency, maturity, and risk awareness across the organisation. By adopting and adapting appropriate governance frameworks, organisations can enhance performance, build stakeholder trust, and navigate complexity with greater confidence.

1.25 On CxO Roles in Governance and Strategic Engagement

In contemporary organisations, particularly those undergoing digital transformation, CxO roles (executive functions denoted by "Chief x Officer") represent key leadership positions that shape strategic direction, operational priorities, and governance frameworks. Understanding these roles is essential for professionals seeking to contribute effectively to projects, consultations, or service engagements involving technology and organisational change (see more details in relation to IT I the section “2.2 Leadership Roles and Governance Posture”).

- Chief Executive Officer (CEO)
    - The CEO holds ultimate responsibility for the organisation’s performance and direction. This role articulates vision, leads the executive team, and ensures coherence between strategy and execution.
    - *Engagement clue:* Understand the organisation’s purpose and political landscape. Offer insights that link your contribution to measurable value and long-term goals.
- Chief Financial Officer (CFO)
    - The CFO manages financial planning, reporting, and risk. This includes oversight of budgets, investment analysis, and often, procurement strategy. It is usually the most influential role after the CEO (in many organizations, the BoD is made solely by the CEO and the CFO).
    - *Engagement clue:* Clarify cost implications of your proposals. Distinguish between CapEx and OpEx when appropriate, and show awareness of return on investment (ROI) or total cost of ownership (TCO).
- Chief Operating Officer (COO)
    - The COO oversees day-to-day operations, ensuring that strategic plans are translated into effective execution. This role often supervises business continuity, process optimisation, and cross-departmental coordination.
    - *Engagement clue:* Show how your work improves operational reliability, scalability, or responsiveness to demand.
- Chief Information Officer (CIO)
    - The CIO leads the organisation’s IT strategy and ensures that technology supports business objectives. This role often governs enterprise architecture, IT service management, and major digital programmes.
    - *Engagement clue:* Align your input with strategic IT priorities. Use shared vocabulary (e.g., "service levels," "digital capability") and show sensitivity to governance structures.
- Chief Technology Officer (CTO)
    - The CTO focuses on technological innovation and systems architecture. In product-oriented organisations, the CTO may also drive R&D and platform evolution. **It is rare to find an organization having a CIO plus a CTO, as usually only one of those roles is preferred, depending on the industry and the vision.**
    - *Engagement clue:* Emphasise scalability, interoperability, and technical feasibility. Show awareness of trends, but be pragmatic about adoption readiness.
- Chief Information Security Officer (CISO)
    - The CISO oversees information security, cybersecurity, and privacy. This role ensures that digital assets are protected and that risks are understood at the executive level.
    - *Engagement clue:* Frame security as a business enabler, not just a constraint. Demonstrate awareness of risk management principles, regulatory obligations, and incident response.
- Chief Risk Officer (CRO)
    - The CRO coordinates enterprise risk management across domains such as finance, operations, cybersecurity, and compliance. This role is particularly relevant in regulated environments.
    - *Engagement clue:* Use structured thinking around risk appetite, likelihood, and impact. Refer to established frameworks (e.g., ISO 31000) and risk treatment plans.
- Chief Data Officer (CDO)
    - The CDO manages the organisation’s data assets, including governance, quality, analytics, and ethical use. In many public organisations, the CDO also oversees data transparency and interoperability.
    - *Engagement clue:* Speak to data as a strategic asset. Acknowledge stewardship responsibilities and compliance with data protection or sovereignty requirements.
- Chief Digital Officer (CDO)
    - In organisations undergoing transformation, the Chief Digital Officer may lead digital strategy, innovation, and organisational change. This role often serves as a bridge between business and IT.
    - *Engagement clue:* Demonstrate sensitivity to organisational maturity. Link digital initiatives to cultural readiness, user needs, and public value or customer impact.
- Chief Compliance Officer (CCO)
    - The CCO is responsible for ensuring that the organisation operates in accordance with applicable laws, regulations, and internal policies. This role oversees the design and implementation of compliance programmes, coordinates audits and regulatory reporting, and promotes ethical conduct across the organisation. In many sectors, especially finance, healthcare, energy, and the public sector, the CCO is a key figure in risk prevention and governance alignment.
    - *Engagement clue:* Show that you understand the compliance landscape relevant to the organisation, whether it involves GDPR, anti-corruption measures, procurement rules, or sector-specific standards. When proposing technical or organisational changes, be prepared to discuss compliance implications and how to embed controls in processes without obstructing value creation.

1.26 CxO Titles: Naming Variations Across Sectors and Languages

While the term "CxO" is widely used in English-speaking contexts to refer to senior executive roles (e.g., CEO for Chief Executive Officer), these roles often appear under different titles depending on industry, language, tradition, and sector-specific governance models.
Understanding these variations is essential for cross-cultural collaboration and for interpreting organisational charts and stakeholder maps in international settings.

1.26.1 Lusophone Countries

In Portugal and other Portuguese-speaking contexts (such as Brazil, Angola, or Mozambique), the English "CxO" terminology is increasingly recognised in multinational and technology-driven environments.
However, traditional terms are still common:

- **CEO**: Presidente Executivo, Diretor Executivo or simply Presidente do Conselho de Administração (if executive). In the public sector, the equivalent may be Presidente, Diretor-Geral, or Secretário de Estado.
- **COO**: Diretor de Operações or Diretor Executivo de Operações.
- **CFO**: Diretor Financeiro or Diretor Executivo de Finanças.
- **CIO**: Diretor de Sistemas de Informação or Diretor de Informática. In public administration: Diretor de Serviços de Tecnologias de Informação.
- **CTO**: Diretor de Tecnologia or Diretor Técnico. In some sectors, Engenheiro-Chefe or Responsável Técnico.
- **CISO**: Responsável pela Segurança da Informação, or formally Encarregado de Segurança da Informação.
- **CDO (Chief Data Officer)**: Diretor de Dados, Gestor de Dados, or Responsável pela Governança de Dados.
- **CDO (Chief Digital Officer)**: Sometimes Diretor de Transformação Digital, Diretor Digital, or Responsável pela Inovação Digital.
- **CRO**: Diretor de Riscos, Gestor de Riscos, or Responsável pela Gestão de Risco.
- **CCO**: Common titles include *Diretor de Conformidade*, *Diretor de Compliance*, or *Responsável pela Conformidade*. In some contexts, especially in regulated industries, you may also find *Responsável de Compliance e Ética*

Brazilian Portuguese often adopts the English acronyms more liberally, especially in financial and tech sectors, though local equivalents coexist.

1.26.2 Spanish

In Spanish-speaking countries, local titles are more common in traditional sectors, though multinationals may retain English acronyms:

- **CEO**: Director General, Presidente Ejecutivo, or Consejero Delegado (in Spain).
- **COO**: Director de Operaciones.
- **CFO**: Director Financiero.
- **CIO**: Director de Sistemas de Información or Responsable de TI.
- **CTO**: Director de Tecnología.
- **CISO**: Responsable de Seguridad de la Información.
- **CDO (Data)**: Director de Datos or Gestor de Datos.
- **CDO (Digital)**: Director de Transformación Digital.
- **CRO**: Director de Riesgos.
- **CCO**: *Director de Cumplimiento Normativo*, *Oficial de Cumplimiento*, or *Responsable de Cumplimiento y Ética*. In Latin America, "Oficial de Cumplimiento" is widely used in financial and legal contexts.

In Latin America, usage tends to blend English and Spanish, depending on sector and formality.

1.26.3 French

French-speaking contexts, including France, Belgium, Canada (Québec), and West Africa, typically use French titles in official communication, though English CxO acronyms are increasingly used in private-sector and digital contexts:

- **CEO**: Président Directeur Général (PDG) in France, Administrateur Délégué in Belgium.
- **COO**: Directeur des Opérations.
- **CFO**: Directeur Financier.
- **CIO**: Directeur des Systèmes d'Information (DSI).
- **CTO**: Directeur Technique or Responsable de la Technologie.
- **CISO**: Responsable de la Sécurité des Systèmes d'Information (RSSI).
- **CDO (Data)**: *Chief Data Officer* is often retained, but also *Directeur des Données*.
- **CDO (Digital)**: Directeur du Numérique or Directeur de la Transformation Digitale.
- **CRO**: Directeur des Risques.
- **CCO**: Responsable de la Conformité, Directeur de la Conformité, or in some sectors, Responsable Éthique et Conformité.

1.26.4 English-Speaking Variants

Even in English, terminology may vary:

- In public sector or NGOs: *Executive Director* instead of CEO; *Chief Administrative Officer (CAO)* is also used.
- In UK public services: *Permanent Secretary* or *Director-General* may be top administrative roles.
- In universities or research: *Provost*, *Registrar*, or *Chief Academic Officer* may functionally align with CxO roles.
- In relation to CCO, some organisations use *Chief Ethics and Compliance Officer* (CECO) or *VP of Compliance*. In public sector or university environments, the equivalent role may be referred to as *Compliance Manager*, *Ethics Officer*, or *Regulatory Affairs Lead*.

1.26.5 Takeaway

CxO roles are functionally comparable across contexts, but their labels adapt to local governance models, legal traditions, and organisational cultures. When engaging with unfamiliar organisations:

- Focus first on **responsibilities**, not titles.
- Ask for or map out **decision rights** and reporting lines.
- Use **clear, respectful language**, avoiding assumptions based solely on acronyms.

Being culturally and linguistically aware is key to understanding power structures, building trust, and proposing meaningful solutions.

1.27 On Some CxO Dilemmas

Governance systems are designed to create clarity, consistency, and control, but in practice, they often expose tensions between competing priorities. These tensions emerge as dilemmas, which cannot be resolved by rules alone but require judgement, contextual awareness, and organisational maturity. The following sections outline typical dilemmas faced by CxO-level roles and those who support them.

1.27.1 Executive Accountability for Misconduct

CxO Dilemma: If an employee commits a serious error or policy violation, to what extent is the executive leadership (such as the CEO, CIO, or CISO) accountable for the outcome?

This is a fundamental dilemma in governance: when misconduct occurs, does it indicate an individual failure or a systemic flaw?

- If appropriate governance mechanisms were in place (with documented policies, clear delegation, training, and oversight) and the employee clearly violated them, accountability may remain with the individual.
- If governance was unclear, or inadequately enforced, leadership may be held responsible for enabling or failing to prevent the incident.
- In some sectors (e.g. finance, healthcare, data protection), laws impose strict or presumed liability on leadership, regardless of intent or direct involvement.
- The ability to demonstrate **due diligence** becomes a key defence and governance asset.

Understanding the traceability between governance design, behavioural expectations, and oversight is essential for managing personal and institutional responsibility at the top.

1.27.2 Transparency vs. Confidentiality

CxO Dilemma: How much internal or external transparency should be maintained without exposing the organisation to unnecessary risk or violating confidentiality obligations?

Governance demands openness (in reporting, accountability, and responsiveness) but this must be balanced against legal, contractual, and strategic constraints.

- Excessive transparency can expose vulnerabilities or lead to misinterpretation.
- Excessive secrecy can reduce trust, increase internal friction, or trigger non-compliance.
- CxOs must decide what to disclose, when, and to whom, whether in internal investigations, audit responses, public communication, or regulator interactions.

This balance is especially sensitive in areas such as cybersecurity, whistleblowing, procurement, and internal audit.

1.27.3 Central Control vs. Local Autonomy

CxO Dilemma: To what extent should governance structures enforce centralised control, versus allowing units or subsidiaries to adapt governance practices to local realities?

Multisite or multinational organisations must reconcile uniformity with flexibility:

- Centralised control ensures consistency, compliance, and traceability.
- Local autonomy enables responsiveness, cultural adaptation, and operational agility.
- Misalignment between central policies and local practices can lead to ineffective or symbolic governance.

Executives must often choose between enforcing uniform procedures and supporting differentiated local solutions — or finding a hybrid governance model that accommodates both.

1.27.4 Outsourcing and Third-Party Risk

CxO Dilemma: When critical processes or systems are outsourced, how can responsibility be retained without undermining operational efficiency or innovation?

External providers introduce dependencies that affect governance:

- Contractual terms define accountability, but not all risks can be transferred.
- Failures by third parties (e.g. cloud providers, cybersecurity partners) can damage the reputation and compliance standing of the organisation itself.
- CxOs must ensure oversight mechanisms, exit strategies, and incident response procedures are in place.

This is particularly relevant in IT, data processing, facilities management, and customer-facing services.

1.27.5 Compliance vs. Innovation

CxO Dilemma: How can the organisation adopt new technologies or business models while remaining within the limits of regulatory and policy frameworks that may not yet accommodate them?

Innovation often moves faster than regulation:

- Emerging technologies may lack clear legal treatment (e.g. AI, biometrics, blockchain).
- Overly rigid compliance can stifle experimentation or delay competitive advantage.
- Loosely governed innovation can result in regulatory breaches, ethical lapses, or reputational harm.

CxOs must create governance models that support **controlled experimentation**, where innovation can proceed within monitored boundaries and with clear escalation mechanisms.

1.27.6 Governance Maturity and Organisational Culture

CxO Dilemma: How can governance be enforced without creating resistance, disengagement, or excessive bureaucracy?

Even well-designed systems fail without a supporting culture:

- Employees must understand not only what is required, but why it matters.
- Middle management plays a critical role in translating governance into behaviour.
- Governance maturity includes leadership example, feedback loops, and continuous adaptation.

For CxOs, the challenge is to institutionalise good governance without reducing organisational agility or motivation, striking a balance between structure and empowerment.

1.28 Oops…

1.28.1 A Clean Process… Or So It Seemed

Mateus is a newly hired junior consultant on **The Dream Team**. In his first client engagement, he joins his team leader, **Sofia**, to support a public sector agency led by **Verónica**, a highly respected executive in public administration.

Verónica is admired for her integrity and commitment to public service. She leads a mid-sized agency responsible for delivering essential services to citizens. Recently, she launched a digitisation initiative to modernise procedures and improve transparency. Confident that her internal teams are aligned with the mission and that governance structures are functioning well, she has asked Sofia and Mateus to help prepare an implementation plan. In her view, the strategic groundwork has already been done — this is just about execution.

Sofia, as usual, begins by setting up brief interviews with key managers and asking for internal documentation. She encourages Mateus to listen carefully, take notes, and reflect on what he observes.

At first glance, the organisation seems well-intentioned and orderly. But within a few days, inconsistencies begin to surface. Different departments have very different interpretations of the agency's mission. Some speak passionately about empowering citizens; others see their role as strictly administrative. A few departments have started building IT tools on their own, unaware of what others are doing. When asked who has the authority to make key decisions, most middle managers shrug or refer vaguely to "how things have always been done."

There is no shared view of decision rights, and governance seems to rely more on habit than structure. Some staff even express quiet scepticism about the digitisation initiative, fearing it may threaten their roles or create more work without clear benefits.

In one meeting, Mateus turns to Sofia and whispers, "Everyone's working hard, but not necessarily together."

At the end of the week, Sofia and Mateus prepare a short debrief for Verónica. Sofia presents the findings gently, framing them as an opportunity. She explains that while the agency has strong values and dedicated people, the current state shows signs of fragmentation and ambiguity. To ensure success, she suggests a lightweight governance framework to clarify roles, responsibilities, and shared objectives before any technical rollout.

Verónica is taken aback. She had believed alignment was already achieved. But Sofia's tone is constructive and respectful, and Verónica listens. After a moment of reflection, she agrees that this step is needed and invites the team to continue.

Let us now play Mateus! You are entering an organisation that seems ethical and orderly, but you begin to see cracks in the foundation.

What would you do?

This scenario shows that even competent, well-meaning organisations can suffer from invisible misalignments. It reminds us that **governance is not just a policy, it is the practice of shared understanding**, and junior consultants can play a key role in making that visible.

1.28.2 "Just Make It Work"

For their next assignment, Mateus and Sofia are called into a very different setting: a chaotic private-sector company led by **Trish**, a senior executive with a fast-paced style and a long to-do list.

Trish is friendly, always says yes, and loves to "keep things moving", but her attention is scattered and her decisions often incomplete.

The company has hired the consultants to implement a new internal reporting system, supposedly to streamline communication and reduce duplicated efforts.

"The system's already bought," Trish says breezily. "We just need to roll it out. Don't overthink it."

To Mateus, this initially sounds like a simple implementation job. But Sofia, cautious as always, requests a few stakeholder interviews before defining the project scope.

Very quickly, they discover the organisation is running on reactive energy. No one is quite sure who requested the system in the first place. No one has been appointed to manage it. The IT department resents the project because they were not consulted. Team leaders worry it will lead to more oversight without helping their actual work. Several have already built their own spreadsheets or tools to work around the confusion.

In one tense meeting, a department head tells Mateus bluntly, "We've tried versions of this three times. Nothing sticks. What makes you think this one will?"

When Sofia gently asks Trish who will approve key decisions and what authority the consultants will have, Trish waves it off. "Let's not get stuck in politics. Just make it work. People will adjust."

Let us now play Mateus.

You're watching your team leader navigate a situation where there's no clarity, no ownership, and no meaningful definition of success. And the client wants it done yesterday.

What would you do?

This scenario shows the risks of moving too fast without strategic grounding. It highlights how **governance is not only about structure, but also about leadership discipline**, and how difficult it can be to challenge a client who doesn't want to hear bad news.

But it also shows that even junior consultants can help improve the situation — not by solving everything, but by **asking the right questions**, noticing what others miss, and giving their team the insight needed to respond with care and integrity.

1.29 …what?…

1.29.1 The Plan Behind the Plan

Mateus and **Sofia** are hired to support **Lucas**, a public sector executive known for his big ideas and inspiring speeches. His agency has just been awarded funding for an innovation programme focused on community engagement and digital participation.

Lucas presents the brief with confidence: "We already know what we want to do. The project is aligned with the national strategy. We just need help structuring the action plan and measuring results."

It sounds simple enough: a technical engagement with clear goals. But from the first internal meetings, Sofia senses the ground shifting. While Lucas is visionary, his teams are unsure of the objectives. Managers seem unclear about who's in charge. When Mateus asks for existing documentation, he gets slide decks filled with inspirational quotes and political slogans, but no actual process definitions.

Behind closed doors, staff express doubts about feasibility. "Lucas means well," one coordinator says, "but he jumps to the next idea before this one lands."

Mateus begins to feel overwhelmed. He's tempted to say, "This isn't what we were told." But Sofia calmly reframes the situation. She tells Mateus: "When strategy is vague, we build clarity by listening."

Over the next week, Sofia facilitates short working sessions with department leads, asking concrete questions about capacity, decision-making, and reporting. She includes Mateus in every step, assigning him the task of capturing the real, current state of operations, what's working, what's missing, and who's actually involved.

Slowly, a picture emerges. With Sofia's guidance, the team translates Lucas's vision into a grounded, step-by-step programme plan, with clear timelines and a small set of indicators tied to real deliverables. Lucas is relieved. "This is exactly what I meant," he says, even if it wasn't what he said.

Let us now play Mateus.

You're working with a charismatic executive who speaks in vision but struggles with structure. The organisation has energy, but no map. Your job is to listen, observe, and help your team turn ambiguity into action.

What would you do?

This scenario shows that even when the starting point is unclear, competent consultants can **build clarity** and **deliver value**, as long as they observe carefully, stay grounded, and work with humility.

1.29.2 A Slide Too Far

This time, **Carla** and **Tiago** from the **Frenetic Team** are hired to support **Trish**, an overextended executive in a large company. The request is to create a business case for a new internal platform that will "boost productivity and innovation." Trish assures them: "We've already done the thinking. You just need to package it."

The team jumps into action. Carla sees it as a fast-turnaround presentation job and tells Tiago to start drafting slides while she schedules stakeholder interviews. Tiago is excited — this seems like a high-impact opportunity — and he starts creating diagrams and writing "key messages" based on Trish's vague notes.

But as they start talking to staff, it becomes clear: there is no actual business model, no defined process, and no stakeholder alignment. When Carla realises this, she changes the plan — now the goal is to "help them think through their ideas," but she doesn't pause the project to clarify expectations.

Tiago, eager to impress, keeps designing polished materials, even when he doesn't fully understand the content. He avoids asking questions, afraid of seeming unprepared.

When Sofia (from another project) happens to glance at his slides, she frowns. "You're presenting assumptions as facts."

At the final meeting, Carla presents the deck to Trish and her senior team. The slides look good, but the message falls flat. Trish's team starts pointing out inconsistencies. "Where did these numbers come from?" "This isn't how our processes work." Carla is defensive. Tiago sits in silence.

The meeting ends awkwardly. No decisions are made. Later, Trish writes back: "Thanks for the effort. We may revisit this later."

Let us now play Tiago.

You were excited to work on a big project, but you didn't ask enough questions, and now the client doesn't trust the work. Your materials were polished, but not grounded. What went wrong?

This scenario shows how **consultant competence matters**, especially when the client doesn't provide clarity. The best consultants ask difficult questions early. The worst deliver slick documents that fall apart under scrutiny.

As a junior consultant, your role is not just to execute, it's to think. Not to assume, but to verify. And above all, to make sure that what looks good also makes sense.

1.30 …OK!

1.30.1 Aligned from the Start

Mateus is once again working with Sofia on a new engagement, this time in a public sector organisation led by **Verónica**. It's a follow-up project, after a previous initiative helped the agency clarify its mission and establish a new governance model.

This time, the request is straightforward: Verónica wants help designing a performance dashboard for internal use.

The goal is to make results more visible across departments and encourage a culture of shared accountability. The strategy is clear, leadership is aligned, and middle management is engaged.

From the very first meeting, Mateus feels something is different.

There is no confusion about who the stakeholders are.

Meetings start on time.

People have read the briefing documents.

When Sofia asks about decision-making authority, Verónica lays it out clearly, supported by a simple, visual governance chart.

Mateus is assigned to help gather user requirements and sketch initial indicators for the dashboard.

As he interviews staff from different teams, he's surprised (pleasantly) that everyone is on the same page. They know what the organisation is trying to achieve and how their work contributes. They raise thoughtful suggestions without defensiveness. Many say, "We've been waiting for something like this — we're glad it's happening now."

Midway through the project, Mateus proposes a simple idea: to include a qualitative comment field in each department's monthly self-assessment, so teams can explain challenges or context behind their numbers. Sofia supports the idea, and when they present it to Verónica, she agrees instantly. "That's the kind of nuance we need. Good thinking, Mateus."

The project proceeds as planned, on time and without escalation. The consultants help shape the structure and visual design of the dashboard, while the client's internal teams handle data integration and adoption. When they wrap up the assignment, Verónica thanks them, not just for the technical work, but for the way they helped strengthen internal dialogue.

Let us now play Mateus.

You are stepping into a well-governed, mature public institution. Your job is not to fix problems, but to **contribute**, to **learn**, and to **build trust** through thoughtful, practical input. What would you do?

- How can you bring value in an organisation that already works well?
- What can you learn from their structure and culture?
- How do you ensure that even small contributions are meaningful and well-placed?
- What can you do to build credibility as a junior consultant in a successful engagement?

This story shows that consultants are not only crisis responders — they can also help high-functioning organisations reach the next level. And it reminds us that clear goals, shared purpose, and good governance make consulting work not only easier, but also more rewarding.

1.30.2 A Well-Oiled Machine

This time, the Dream Team has been hired by **Alex**, a sharp and demanding executive in a competitive business sector. Alex is known for being intense, but also fair (if you deliver, he'll respect you; if not, he'll move on).

The company is launching a new service line, and Alex wants the consultants to help map the business processes and ensure operational readiness across departments. He gives Sofia a clear mandate: "I need clarity, speed, and no nonsense."

Despite the pressure, Mateus feels energised. From day one, things run like a machine. Alex provides crisp instructions and connects them with key decision-makers. All stakeholders know their roles. Everyone they meet has clear responsibilities and is fully engaged. No one tries to dodge accountability; they ask smart questions and move fast.

Sofia assigns Mateus to work with operations and IT, interviewing staff to trace how the new service will flow from request to delivery. In just two days, Mateus builds a detailed outline of the key touchpoints and dependencies. He proposes a checklist-based coordination tool to prevent handover errors between teams.

Sofia helps him refine it and shares it with Alex. Alex nods and replies, "Good. That's exactly what we need to tighten. Let's put it into testing next week."

The team moves forward smoothly. No urgent meetings, no major surprises. Each department adopts their part of the new process, and within three weeks, the pilot is running. When a minor issue arises (a mismatch in service tracking codes) it is resolved quickly through a joint call between Mateus and the IT lead.

At the final review, Alex gives rare but sincere praise: "You didn't just deliver. You improved the thinking along the way. Well done."

Let us now play Mateus.

You are working in a high-performance business with clear leadership and strong internal culture. The pace is fast, **but the structure supports it**. Your role is to **stay sharp**, **add value**, and **not get in the way**. What would you do?

- How do you manage your time and focus in a fast-paced but organised environment?
- What habits or practices make this company work so well?
- What can you contribute as a junior consultant under pressure?
- What signals tell you that your ideas are welcomed — or not?

This story shows that **governance and execution go hand in hand**. In a high-functioning private business, clarity and pace can coexist. Consultants are not just problem-solvers, but **value creators**, helping successful teams go even further.

1.31 Wrap-up…

Key high-level concepts introduced in Theme 1 are listed (they can be reference points when interpreting governance structures, evaluating management maturity, and engaging with public or private sector organisations):

- **Organisation -** A coordinated system of people, processes, and resources structured to achieve defined goals. Organisations may be private, public, or not-for-profit, and vary in their governance, culture, and operational maturity.
- **Governance -** The framework of rules, practices, processes, and relationships through which an organisation (or part of it) is directed and controlled. Governance, when made explicitly, ensures accountability, defines purpose, and aligns organisational activities with strategic and external expectations.
- **Management -** The set of activities concerned with planning, organising, leading, and controlling resources to achieve specific objectives. Management operates within the strategic direction set by governance.
- **Management System -** A structured approach used by organisations to manage a set of interrelated elements (e.g., processes, policies, responsibilities) that help achieve objectives consistently and efficiently. Examples include ISO-based systems for quality, environment, or information security.
- **Governance, Risk, and Compliance (GRC) -** An integrated set of capabilities that enable an organisation to achieve objectives, address uncertainty, and act with integrity. GRC frameworks ensure that governance structures address risk and regulatory requirements cohesively.
- **Risk and Risk Management -** Risk is the effect of uncertainty on objectives. Risk management is the coordinated activities to direct and control an organisation with regard to risk, including identification, assessment, mitigation, and monitoring. In context of high maturity levels, risk management is a process well defined, executed by a respective risk management system.
- **Compliance -** The state of adhering to legal, regulatory, contractual, and internal obligations. Compliance ensures that organisational actions conform to required standards and reduces exposure to legal and reputational risks.
- **Maturity (in Governance and Management) -** The degree to which an organisation has formalised, structured, and optimised its governance and management practices. High maturity signals consistency, accountability, and adaptability; low maturity indicates reliance on improvisation or personality-driven practices.
- **Role and Responsibility Frameworks -** Tools that define who is responsible, accountable, consulted, and informed (e.g., RACI model) in decision-making and operations. Clear frameworks are indicators of governance maturity.
- **Organisational Models -** The structural configurations that determine how activities, roles, and hierarchies are arranged within an organisation (e.g., functional, divisional, matrix structures).
- **Control Structures -** Mechanisms for monitoring and guiding organisational activities to ensure they meet governance objectives. Examples include internal audits, risk committees, and compliance reporting lines.
- **Three Lines of Defence -** A model for structuring internal control and risk management responsibilities across three layers: operational management, risk and compliance functions, and internal audit.
- **Board of Directors -** The group of individuals responsible for overseeing the governance of an organisation, ensuring that executive actions align with strategic objectives and stakeholder interests.
- **Shareholders and Stakeholders -** Shareholders are equity owners in a company, primarily concerned with financial returns. Stakeholders include all individuals or groups affected by the organisation's activities, such as employees, customers, regulators, and communities.
- **Public Sector Organisations -** Entities owned and operated by government bodies to provide public services, guided by principles of transparency, equity, and public value rather than profit.
- **Not-for-Profit Organisations -** Organisations that pursue missions of social, cultural, or environmental value without distributing profits to owners. Governance focuses on accountability to donors, beneficiaries, and society.
- **Business Model -** The conceptual framework that explains how an organisation creates, delivers, and captures value. Business models differ substantially between private, public, and non-profit sectors.
- **Corporate Governance -** A subset of governance concerned specifically with the structures and relationships that determine corporate direction and performance in an organization, especially in relation to shareholder and stakeholder interests.
- **Organisational Culture -** The set of shared values, beliefs, assumptions, and practices that shape behaviour within an organisation. While some aspects of culture con be formally expressed (such as mission statements or codes of conduct), much of it operates implicitly through habits, norms, and unwritten rules. Culture strongly influences the effectiveness of governance and management systems, often in ways that formal structures alone cannot predict.
- **Maturity Models -** Frameworks used to assess and guide the development of management capabilities across areas such as leadership, operations, risk, and compliance. Maturity models help organisations benchmark their practices and plan improvements.

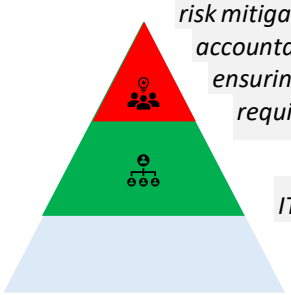
Notes:

- These concepts are interrelated: understanding maturity, for instance, requires interpreting how governance structures, management systems, and culture interact.
- In consulting roles, recognising the signs of maturity, misalignment, or cultural barriers is as important as knowing the formal definitions.

2 Theme: Governance of IT and IT Management

As organisations grow increasingly dependent on digital systems, the need for deliberate governance of IT becomes more pressing. Information technologies influence not only operational efficiency but also strategic agility, regulatory exposure, and reputational risk. For this reason, IT governance and IT management must be understood as distinct but interrelated practices.

Governance of IT is the set of mechanisms by which the use of technology is directed, controlled, and evaluated in alignment with organisational goals. It ensures that decisions about technology contribute to value creation, risk mitigation, and compliance. This includes defining accountabilities, overseeing major investments, and ensuring that ethical, legal, and strategic requirements are consistently addressed.



IT Management, on the other hand, concerns the planning, development, operation, and continuous improvement of information systems. It encompasses technical architecture, service delivery, security operations, user support, and the coordination of internal and external resources. It is where day-to-day decisions are made, and operational resilience is sustained.

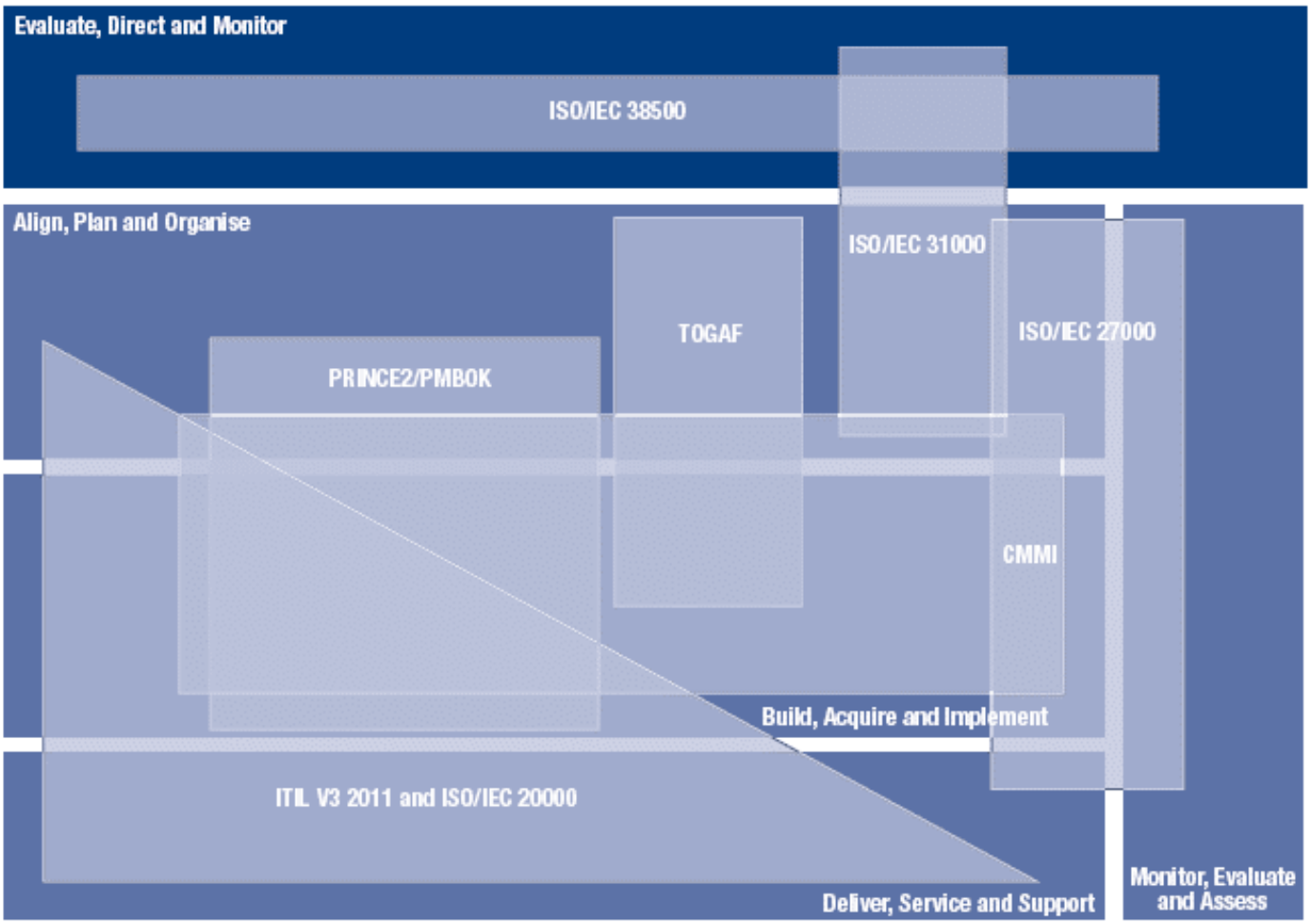
In practice, governance sets the "why" and "what," while management focuses on the "how."

Yet the distinction is often blurred, especially in organisations with low maturity structures or unclear boundaries between strategic and operational responsibilities.

This theme examines how these roles are distributed, formalised, and enacted. It introduces reference models such as COBIT, ISO/IEC 38500, and ITIL, which provide vocabulary, principles, and guidance for designing governance and management systems (**see the picture**[51]). These frameworks do not prescribe a single model but offer building blocks that can be adapted to specific organisational contexts, whether centralised or decentralised, private or public, regulated or unregulated.

Attention is also given to the relationship between IT and business leadership. Effective governance of IT requires participation beyond the IT department, involving senior executives and stakeholders who understand the business impact of technological decisions. Where governance is weak, IT may become reactive, fragmented, or misaligned with organisational priorities.

By framing IT as both an enabler and a source of risk, this theme highlights the need for clear structures, well-defined roles, and transparent processes. It encourages critical reflection on how organisations ensure that technology contributes sustainably and responsibly to their evolving missions.



[51] Image from: https://blog.itil.org/2013/10/governance-over-it-service-management-processes-using-cobit-5-0/

2.1 Business Governance versus Governance of IT

Business governance refers to the frameworks, processes, and decision-making structures that guide an organisation's strategic direction, ethical standards, and risk oversight. It encompasses how leadership ensures accountability, aligns interests across stakeholders, and sets priorities in pursuit of the organisation's mission (whether profit-driven, public-oriented, or mission-based).
In contrast, governance of IT is a subset of corporate governance, concerned specifically with the strategic alignment, value delivery, risk management, and resource stewardship of information technology. It provides the structures through which organisations ensure that IT supports and enables business goals, while also managing the specific risks, costs, and opportunities associated with technology.
Although distinct in scope, these two layers of governance must operate in tight coordination. In a digital economy, IT is no longer a support function but a strategic enabler. As such, governance of IT must be embedded within, and responsive to, business governance.

2.1.1 Strategic Alignment

One of the central challenges for CIOs, CTOs, and similar roles is ensuring alignment between IT strategy and business objectives. This requires more than technical competence, it demands active engagement with business leaders to understand commercial priorities, service goals, or public policy mandates.
Strategic alignment involves:

- Ensuring that IT investments contribute to business value.
- Prioritising technology initiatives based on organisational impact.
- Balancing innovation with operational stability and regulatory compliance.

Frameworks such as COBIT and ISO/IEC 38500 emphasise that governance of IT must begin with business needs and cascade downward into planning, execution, and monitoring. Without alignment, IT risks becoming a cost centre or bottleneck, rather than a driver of transformation.

2.1.2 Accountability and Decision Rights

Effective governance clarifies **who decides what**, and on what basis. Business governance typically rests with the board of directors, which delegates authority to executives.
Similarly, governance of IT defines specific roles (such as CIO, CTO, or enterprise architect) with decision rights and accountability for technology-related domains.
Tensions can emerge when IT decisions are made in isolation from business oversight, or when boards lack sufficient understanding of technological risk. For this reason, many governance models now emphasise shared accountability across both business and IT leaders. For example, IT steering committees often include representatives from both domains to ensure integrated decision-making.
Mature organisations also invest in governance mechanisms such as project portfolio boards, benefits realisation tracking, and service-level dashboards (tools that make IT performance visible and measurable in business terms).

2.1.3 Risk and Compliance Integration

While business governance manages enterprise-wide risks, governance of IT must address the increasingly complex landscape of technology risks, including cybersecurity, data privacy, system resilience, and third-party dependencies.
The role of the **Chief Information Security Officer (CISO)** is particularly relevant here. The CISO must bridge operational security concerns with board-level awareness and strategic risk appetite.
This includes:

- Reporting on threat trends and vulnerabilities.
- Framing cybersecurity as a business risk, not only a technical issue.
- Ensuring that IT controls align with regulatory obligations and ethical standards.

As cyber and data-related risks grow, governance of IT is progressively integrated into broader risk management and compliance structures. Many organisations now treat information security and digital resilience as matters for board oversight.

2.1.4 Conclusion

The relationship between business governance and governance of IT is foundational to effective leadership in the digital era. While business governance sets the broader direction, governance of IT ensures that digital capabilities are managed strategically, ethically, and in alignment with organisational goals. For roles such as CIO, CTO, or CISO, success depends on navigating both domains, acting as a translator between technical potential and strategic imperatives. In this way, governance of IT becomes not only a matter of control but a driver of value, innovation, and trust.

2.2 Leadership Roles and Governance Posture

The organisational placement of senior technology roles such as the Chief Information Officer (CIO), Chief Technology Officer (CTO), and Chief Information Security Officer (CISO) provides important signals about the organisation's governance model and strategic orientation toward digital, technological, and risk-related matters.

2.2.1 Board-Level Participation as Indicator of Strategic Integration

When a CIO or CTO sits on the Board of Directors (BoD), or equivalent governing body, this typically reflects a governance model in which IT is not merely a support function, but an intrinsic component of organisational strategy. In such settings, digital capabilities are seen as drivers of innovation, resilience, and value creation. This is consistent with the concept of **governance of IT**, where technology is subject to the same oversight and strategic deliberation as finance, operations, or legal affairs.

By contrast, when the CIO or CTO reports to another executive who sits on the board (such as the CFO or COO), IT is more likely to be treated as an enabling or subordinate function. This arrangement may reflect a narrower view in which IT governance is exercised through management hierarchies, with a primary focus on efficiency, cost control, and technical delivery. In such contexts, the expression **IT governance** often denotes internal processes, service management, or project oversight, rather than strategic deliberation at board level.

The difference is not purely semantic. It corresponds to how decision rights, accountability, and strategic influence are distributed within the organisation. The position of the CIO or CTO within the hierarchy can serve as a proxy for the maturity and ambition of the organisation's governance of IT arrangements.

2.2.2 The Role of the CISO and Independence of Oversight

The CISO's position is equally telling, though framed through the lens of risk and assurance. A CISO who reports independently to the CEO or to a board-level committee (e.g., audit or risk committee) is in a position to provide objective assessments of information security, resilience, and regulatory compliance. This placement aligns with governance practices that emphasise checks and balances, visibility of risk, and integration of security concerns into strategic oversight.

However, in many organisations, the CISO reports to the CIO or CTO. While this may offer technical cohesion, it also introduces a potential conflict of interest, especially if the same line of command is responsible for both delivering and auditing security-related initiatives. Such arrangements risk downplaying governance of information security in favour of operational convenience. In regulated sectors or high-risk environments, this structure may be seen as part of an organization with low maturity or inadequate governance.

The independence of the CISO role, and its access to executive forums, therefore, signals whether the organisation treats information security as a board-level concern or a technical subdomain. This distinction becomes particularly relevant in contexts of legal exposure, fiduciary responsibility, and public trust.

2.2.3 Implications for Governance of IT

The relative position of the CIO, CTO, and CISO within the organisational hierarchy can be interpreted as a diagnostic element of the organisation's broader governance maturity:

Role Placement	Likely Governance Posture
CIO/CTO sits on the BoD	Strong governance of IT integration; IT seen as strategic
CIO/CTO reports to CFO/COO	IT seen as a service or cost centre; limited strategic voice
CISO reports to CEO or Risk Committee	Independent assurance; security treated as governance priority
CISO reports to CIO/CTO	Security embedded in IT operations; possible conflict of interest

These configurations are not prescriptive, but indicative. Organisational culture, sectoral constraints, and legal requirements also shape governance arrangements. Nevertheless, attention to reporting lines and role positioning offers a valuable lens through which to assess the organisation's strategic intent and its capacity to align digital, operational, and risk-related concerns with its overall mission.

2.2.4 Conclusion

In governance, structure matters. The position of the CIO, CTO, and CISO (whether on the BoD, reporting to it, or operating within another domain) can reveal how seriously the organisation engages with the governance of IT, and whether risk, innovation, and resilience are seen as shared executive responsibilities.

Governance maturity is not only about documents and processes, but mainly about who sits at the table, with what authority, and to what purpose.

2.3 Conjugating “Governance” and “IT”

The term “governance of IT” is increasingly prevalent in professional and academic literature, often appearing alongside or in place of the more concise expression “IT governance”. While both are widely used, they are not entirely interchangeable. Understanding the distinction between the two is essential for engaging critically with different frameworks, standards, and organisational perspectives.

2.3.1 “Governance of IT”

“Governance of IT” is a prepositional phrase that emphasises the domain being governed: information technologies and their role within the organisation. It aligns directly with the language of ISO/IEC 38500, which defines itself as a standard for the **governance of information technology**. The formulation underscores that the principles, structures, and processes of governance are being applied to the organisation’s use of IT, situating it clearly within the broader scope of corporate or public governance.

> *“This Standard provides guiding principles for members of governing bodies of organisations on the effective, efficient and acceptable use of information technology (IT) within their organisations. It applies to the governance of management processes and decisions relating to the current and future use of IT.”*
> *— ISO/IEC 38500:2015, Introduction*

2.3.2 “IT Governance”

By contrast, the expression “IT governance” is a nominal compound that functions as a label for a recognised field of practice. It is widely adopted by frameworks such as COBIT, and is common in consulting, management discourse, and professional certification schemes. As a syntactic construction, it compresses meaning, and in doing so, may obscure the fact that governance is an overarching function being exercised over IT—not by IT, nor exclusively within IT departments.

> *“Governance is the system by which the enterprise is directed and controlled. In the context of this framework, governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against agreed-on direction and objectives (EDM).”*
> *— COBIT 2019 Framework: Governance and Management Objectives, p. 12*

2.3.3 Why it matters

The distinction becomes especially relevant when discussing the distribution of responsibilities.

> *Governance of IT implies that executive and board-level actors are accountable for setting direction, monitoring performance, and ensuring responsible IT behaviour across the organisation. It helps avoid the misconception that this is the responsibility of IT professionals alone. In fact, the effective governance of IT typically depends on the integration of technical, managerial, and strategic perspectives.*

This terminological precision also aids in maintaining coherence across governance domains, such as the governance of risk, the governance of data, or the governance of cybersecurity. In each case, the prepositional form places focus on the object of governance, supporting modularity and interoperability between governance systems.
While in many contexts the two expressions may be used interchangeably without confusion, the prepositional form offers clearer alignment with systemic thinking and formal governance structures. For this reason, many organisations and authors adopt “governance of IT” when aiming for conceptual clarity, particularly in policy development, academic writing, and communication with non-specialist stakeholders.

> *In summary, both terms refer to the same general concern: ensuring that the use of IT supports and does not undermine organisational goals.* ***However, the expression “governance of IT” offers a more explicit and flexible formulation****, especially when framing governance as a shared executive function rather than an operational matter confined to the IT function.*

2.4 The Focus of the Concern

Governance of IT encompasses a broad spectrum of responsibilities, but at its core lies a crucial and recurring question: what, exactly, is being governed?

This question is not merely semantic. It defines the scope, priorities, structures, and success criteria of governance mechanisms. Whether in private enterprises or public administrations, clarity around the object of governance (the "focus of the concern") is essential to avoid fragmentation, misalignment, or governance structures that are too narrow or too vague to be effective.

2.4.1 Governance of What?

Governance of IT is not about controlling individual technologies, systems, or projects in isolation. Rather, it concerns the set of organisational capabilities that enable digital services, ensure information integrity, support operations, and deliver value. These capabilities include not only the enterprise IT infrastructure and applications, but also the processes, policies, roles, and relationships through which technology is deployed and maintained.

In mature settings, the focus of the governance of IT is not on technology itself, but on what technology enables: business capabilities, public services, regulatory compliance, trust relationships, and strategic adaptation. This requires governance structures that are not focused only in the IT departments, but engage business owners, risk officers, finance directors, and executive leadership.

2.4.2 Core Objects of Governance

The object of governance may vary by context, but commonly includes:

- **Digital Assets and Services** – Applications, platforms, and digital channels that support the organisation's mission.
- **Information** – As a strategic asset, subject to quality, security, privacy, and regulatory requirements.
- **Technology Investments** – Portfolios of projects, platforms, and licences, subject to prioritisation, return-on-investment analysis, and lifecycle management.
- **Operational Capabilities** – The people, processes, and service management practices that enable IT performance and resilience.
- **Risk and Compliance Posture** – Including cybersecurity, data protection, procurement dependencies, and audit readiness.

These objects are interrelated. Governance that focuses too narrowly on one (e.g. infrastructure costs) without considering others (e.g. data protection or user needs) risks blind spots and unintended consequences.

2.4.3 From Control to Value Creation

In early or compliance-driven implementations, governance of IT is often framed in terms of risk containment and cost control. Over time, however, the focus tends to evolve.

Mature organisations increasingly see governance as a driver of coherence, innovation, and long-term value. The question becomes not just how to control IT, but how to ensure that IT contributes meaningfully to organisational purpose.

This evolution is reflected in frameworks such as COBIT, which frame governance around value creation, risk optimisation, and resource management. **Similarly, ISO/IEC 38500 defines governance of IT as a set of high-level responsibilities for ensuring that IT use is aligned with business goals, performance expectations, and ethical standards**.

2.4.4 Sectoral and Organisational Variations

In the private sector, the focus of IT governance is often tied to competitive advantage, operational efficiency, and customer engagement. Metrics may include service availability, agility in product delivery, or innovation throughput. In public sector organisations, the concern typically centres on accountability, continuity of service, public trust, and legal compliance. Here, governance may need to accommodate more stakeholders, procedural transparency, and institutional constraints.
In either case, the definition of what is being governed must be explicit, regularly reviewed, and translated into roles, decision rights, and performance indicators.

2.4.5 Conclusion

The focus of the concern in governance of IT is not technology for its own sake, but the organisational capabilities and outcomes that technology makes possible. Clarity about what is being governed — and why — is essential to designing governance structures that are effective, legitimate, and adaptive. By framing the concern around strategic contribution rather than technical control, organisations can better align digital initiatives with their mission, manage risks coherently, and deliver value that is meaningful and measurable.

2.5 Governance and Information Technology

Information Technology (IT) plays a central role in enabling organisational capabilities, supporting innovation, and delivering services across all sectors. As such, IT must be governed with the same rigour as financial and human resources. **Governance of IT**, when done in awareness of the main guidelines (see image[52]), ensures that technology investments are aligned with strategic objectives, deliver value, and are managed responsibly in terms of risk, compliance, and performance.

Governance of IT is a subset of corporate governance, focused on the decision rights and accountability frameworks related to the use of IT. It addresses the question: *Are we doing the right things with technology, and are we doing them the right way?* Key goals include:

- **Strategic alignment** – Ensuring that IT initiatives support the organisation's mission and long-term plans.
- **Value delivery** – Maximising the return on IT investments and ensuring that technology contributes to desired outcomes.
- **Risk management** – Identifying and mitigating IT-related risks, including cybersecurity, project failure, or regulatory non-compliance.
- **Resource optimisation** – Making efficient and responsible use of technology assets, infrastructure, and talent.
- **Performance measurement** – Using metrics and reporting to track IT effectiveness, efficiency, and contribution to business goals.

Well-governed IT is essential for successful change, regulatory compliance, and maintaining stakeholder trust.

2.5.1 Structures and Responsibilities

Effective governance of IT requires a clear structure that defines responsibilities, authority, and processes:

- **Board Oversight** – The BoD should receive regular updates on IT strategy, major initiatives, risks, and performance.
- **CIO** – Leading governance of IT at the executive level, ensuring coordination between IT and business units (in some business the role might have other designation, as for example CTO or CDO).
- **IT Steering Committees** – Cross-functional groups that evaluate, prioritise, and monitor technology investments and initiatives.
- **Enterprise Architecture and Portfolio Management** – Frameworks that support coherent, efficient, and adaptable technology landscapes.

In larger organisations, owning complex infrastructures and systems, formal governance roles may also include a Chief Information Security Officers (CISO).

2.5.2 Governance of IT Risks and Compliance

The governance of IT must include robust processes for managing technology-related risks and meeting compliance obligations. Common focus areas include:

- **Cybersecurity Governance** – Defining security policies, monitoring threats, and ensuring incident response capabilities.
- **Data Protection and Privacy** – Complying with laws such as the GDPR, and implementing controls to safeguard sensitive information.
- **Business Continuity and Disaster Recovery** – Ensuring that critical IT systems can withstand disruption and recover swiftly.
- **Project and Change Governance** – Evaluating and controlling IT projects to prevent scope creep, budget overruns, or stakeholder misalignment.

IT risks are increasingly integrated into enterprise-wide risk management (ERM) frameworks, reflecting their critical impact on reputation, operations, and compliance.

2.5.3 Ethical Governance in Information Systems

Beyond efficiency and risk, governance of IT must address **ethical dimensions** of digital technologies. Topics of growing relevance include:

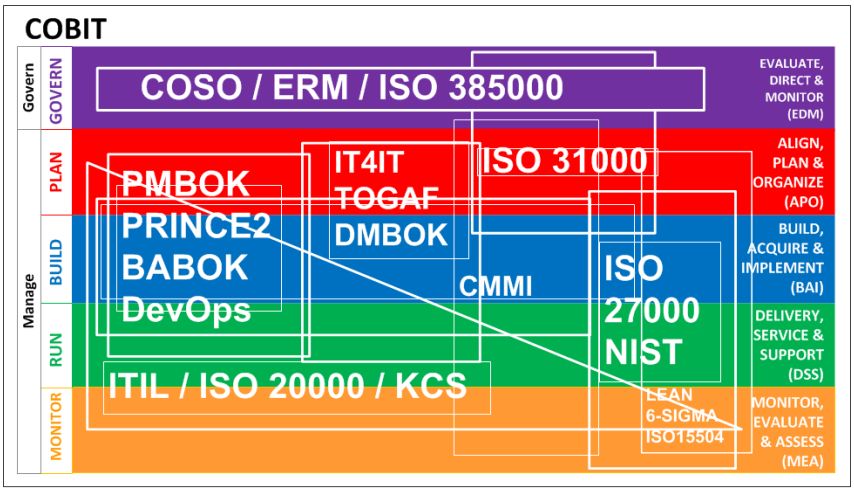
- **AI and Algorithmic Accountability** – Ensuring transparency, fairness, and non-discrimination in automated decision-making.
- **Digital Rights and Access** – Respecting users' rights to privacy, consent, and inclusion.
- **Environmental Sustainability** – Considering the ecological footprint of IT operations and digital infrastructure.

These issues are often addressed through ethical guidelines, responsible innovation policies, and stakeholder engagement processes.

2.5.4 Conclusion

Information Technology is too integral to modern organisations to be managed in isolation from governance structures. governance of IT ensures that technology is used responsibly, strategically, and ethically, in alignment with organisational goals and societal expectations. As changes accelerates, robust governance of IT becomes not only a technical necessity but a key enabler of trust, resilience, and long-term success.

Map - IT Standards, Frameworks & Guidance



Context, structure and content
Where do you fit in?

[52] Image from: https://grcmusings.com/a-beginners-guide-to-information-security-frameworks/

2.6 Multiple Faces of IT and Governance Implications

In many organisations, particularly those operating in complex or regulated environments, the notion of Information Technology (IT) as a single, unified domain does not reflect operational reality. Instead, IT often comprises multiple **segregated subdomains**, each with distinct technologies, governance demands, and professional cultures. These include, but are not limited to, operational technology, safety-critical systems, scientific computing, communications infrastructure, and embedded digital components in physical assets.

While often interconnected at a technical level, these domains may differ significantly in **risk posture**, **compliance obligations**, **performance requirements**, and even in **temporal logic** (some operate in real time, others over long procurement and deployment cycles). As a result, governance structures must be attuned to these divergences, and **executive roles** may need to adapt accordingly.

2.6.1 Operational Technology and the IT/OT Interface

Operational Technology (OT) encompasses systems that monitor and control physical infrastructure, such as those found in energy networks, manufacturing lines, and transportation systems. These systems are traditionally engineered for safety, reliability, and deterministic control. Their convergence with IT brings benefits but also introduces cyber risks and integration challenges. In these contexts, the **CIO** may share governance responsibilities with other roles, such as an **OT Director**, **Chief Operations Officer**, or **Chief Risk Officer**. Where cyber-physical risks are prominent, the **CISO** may require specific expertise or delegated authority over OT security, a domain with its own standards and incident dynamics.

2.6.2 Safety-Critical Systems

In sectors such as aerospace, automotive, and healthcare, some digital systems are subject to strict regulatory oversight, with traceability, formal verification, and certification as standard requirements. These systems differ from general-purpose IT in both design and accountability. Organisations operating in such environments may require a **Chief Safety Officer**, or assign safety oversight to a **CTO**, particularly where software is embedded in regulated products. In these scenarios, the role of **CIO** might not exist, or may be limited to the broader digital environment, while the product-centric governance follows its own chain of assurance.

2.6.3 Communications Technology and Infrastructure

Large-scale communications infrastructures, such as telecommunications networks or national emergency services, require governance distinct from traditional IT. Responsibilities for lawful intercept, spectrum regulation, and service continuity often fall outside the remit of a CIO role. In such cases, the organisation may appoint a **Chief Network Officer** or equivalent, or extend the scope of the **CTO** to cover both application-level and network-level technology domains. Regulatory liaison functions may also be assigned to the **CCO** or **Legal Counsel**, especially in public or cross-border contexts.

2.6.4 Embedded IT and Infrastructure-Integrated IT

In domains such as smart cities, transport infrastructure, or utilities, IT is increasingly embedded in long-lived physical assets. These systems must balance digital evolution with physical durability, often operating in environments where change is slow, and risks are systemic. Governance in such contexts may involve several leaders in coordinated models. The **CxO constellation** is not static: new roles may emerge, such as **Chief Digital Infrastructure Officer**, reflecting the growing importance of hybrid systems that span digital and physical layers.

2.6.5 Scientific Computing and Research IT

Universities, laboratories, and research-intensive organisations often support both general administrative IT and specialised scientific computing environments. The latter may prioritise performance, experimentation, and user configurability over standardisation or central control. Here, governance may be shared between a **CIO** and a **Director of Research Infrastructure** or **Chief Scientific Computing Officer**. The CIO focuses on institutional IT governance and compliance, while the latter ensures alignment of research IT with scientific priorities, funding requirements, and data stewardship practices.

2.6.6 Governance Considerations

Recognising the differentiated nature of IT subdomains enables more effective governance and risk management. It may also influence the **design of executive roles**, especially in large or multi-mission organisations. Critical considerations include:

- Clarifying scope and boundaries of CxO responsibilities across domains;
- Ensuring risk, compliance, and assurance processes reflect domain-specific needs;
- Establishing governance interfaces across organisational silos;
- Avoiding fragmentation through shared principles while respecting divergence;
- Designing escalation, funding, and reporting lines that are domain-aware.

These adaptations are not solely structural. They reflect the operational reality that **not all IT is the same**, and that governance maturity depends on recognising (and managing) this diversity.

2.7 Stakeholder Management and Information Systems

In any organisation, **stakeholders** are individuals or groups with an interest in or influence over the organisation's actions, objectives, or outcomes. Stakeholders may be internal (e.g., employees, management, board members) or external (e.g., customers, suppliers, regulators, shareholders, or the public).
Stakeholder management involves identifying these actors, understanding their expectations, and ensuring that organisational activities take their interests into account in a balanced and transparent manner.
Effective stakeholder management is not merely a communication exercise, but a key component of governance and strategic alignment. This is especially relevant in the context of information systems (IS), where data flows and system changes can affect or depend on multiple stakeholders.

2.7.1 Stakeholders in Information Systems

Information systems interact with a diverse range of stakeholders, each with specific concerns:

- **Users**: Focused on system usability, availability, and functionality.
- **Managers**: Concerned with performance, reporting, alignment with business processes, and return on investment.
- **IT Staff**: Responsible for operations, maintenance, and technical compliance.
- **Security and Compliance Officers**: Interested in access control, auditability, and regulatory conformity.
- **External Partners and Clients**: May require interoperability, service levels, or access to shared platforms.
- **Regulators and Authorities**: Expect systems to comply with data protection, transparency, or sector-specific legislation.

Conflicting expectations are common. For example, a business unit may seek fast deployment of new features, while the information security officer prioritises risk mitigation and formal validation. Stakeholder management helps mediate such tensions by clarifying priorities and shared objectives.

2.7.2 Role of Information Systems in Stakeholder Management

Information systems themselves can support stakeholder management by enabling:

- **Visibility and Transparency**: Dashboards, portals, and reporting tools provide stakeholders with relevant and timely information, improving accountability and trust.
- **Participation and Engagement**: Collaboration platforms, feedback mechanisms, and participatory tools (e.g., user surveys, workflow approvals) allow stakeholders to be involved in shaping and evaluating processes.
- **Access Control and Personalisation**: Systems can be designed to reflect role-based access, ensuring that stakeholders receive information tailored to their responsibilities and rights.
- **Traceability and Compliance**: Information systems support audit trails, documentation of decisions, and evidence of policy enforcement—all important for regulatory stakeholders.

By integrating stakeholder awareness into system design and management, organisations can align digital tools with both operational needs and governance principles.

2.7.3 Challenges and Risks

Stakeholder management in the context of IS is not without complications:

- **Stakeholder Misidentification**: Failure to recognise key actors (e.g., legal, data protection officers) can lead to blind spots in risk analysis.
- **Overload or Conflict**: Attempting to satisfy too many stakeholder demands without prioritisation can lead to system complexity, delay, or failure.
- **Lack of Communication**: Technical decisions made without engaging affected users or external parties can result in resistance, lack of adoption, or reputational damage.
- **Data Sensitivity and Ethics**: Systems that collect or process personal or sensitive data must address stakeholder concerns about privacy and fairness.

Addressing these issues requires both structured processes (e.g., stakeholder mapping, impact analysis) and cultural awareness of communication, ethics, and participation.

2.7.4 Conclusion

Stakeholder management is integral to effective governance, particularly when information systems are involved. Systems affect a wide range of actors, each with distinct expectations and responsibilities. By proactively identifying, engaging, and supporting stakeholders through well-designed processes and digital tools, organisations enhance alignment, reduce resistance, and build trust. In doing so, they also improve the likelihood that information systems contribute meaningfully to strategic and operational goals.

2.8 Information Governance and Management

Information governance establishes the overarching policies, accountability structures, and decision rights that determine how information is used, protected, and controlled.
Information management focuses on the practical implementation of those policies through systems, processes, and daily practices that govern the information lifecycle. Governance defines the "what" and "why"; management ensures the "how".

2.8.1 Principles and Frameworks

Sound information governance and management rest on principles such as:

- **Value**: Information is recognised as an asset that supports performance and innovation.
- **Integrity**: Information must be trustworthy, with controls to prevent unauthorised modification or loss.
- **Availability**: Information should be accessible to those with legitimate need.
- **Accountability**: Responsibilities must be clearly defined and monitored.
- **Compliance**: Information must be handled in accordance with legal, regulatory, and policy requirements.

Frameworks that support these principles include ISO 15489 (records management), ISO/IEC 27001 (information security), ISO/IEC 27701 (privacy information), and COBIT (governance of enterprise IT).

2.8.2 Key Domains and Lifecycle

Effective **information governance and management** require attention across several domains:

- **Data Ownership and Stewardship**: Clarity over who owns and who stewards data is critical. Stewards are tasked with ensuring accuracy, consistency, and policy adherence.
- **Information Quality and Integrity**: Reliable data is essential for risk management, reporting, and decision-making.
- **Privacy and Data Protection**: Compliance with regulations such as the GDPR involves protecting personal data and respecting individual rights.
- **Security and Access Control**: Controls must be in place to prevent unauthorised access, including encryption, access logging, and authentication.
- **Records Retention and Disposal**: Data must be retained or deleted in accordance with retention schedules that reflect legal and operational requirements.
- **Transparency and Ethics**: Organisations are expected to use information fairly, avoid bias, and be transparent in automated decision-making.

These domains are enacted through the information lifecycle:

1. **Creation and Capture** – Information is generated or received and should be registered, classified, and attributed.
2. **Storage and Use** – Information is stored in repositories where it can be accessed securely and used effectively.
3. **Sharing and Distribution** – Information is shared under clear rules governing recipients, methods, and purposes.
4. **Retention and Disposal** – Timely deletion or archiving is necessary to avoid unnecessary risk and cost.
5.

2.8.3 Organisational Roles and Responsibilities

Information governance and management involve actors at multiple levels:

- **Senior Executives**: Define strategic direction, allocate resources, and ensure compliance.
- **CxOs (e.g., CIO, CISO, CDO)**: Lead governance frameworks and supervise implementation across domains.
- **Data Owners and Stewards**: Operationalise policies and oversee data domains.
- **Records Managers and Archivists**: Ensure continuity, legal admissibility, and compliance with records obligations.
- **Legal and Compliance Officers**: Interpret regulatory requirements and advise on information risks.

Public sector entities often face additional transparency and archival obligations, and must align with public records laws, freedom of information regimes, and long-term preservation mandates.

2.8.4 Strategic and Risk Dimensions

Information governance and management are integral to broader organisational strategy. Benefits include:

- **Informed Decision-Making**: Reliable information enhances the quality of strategic and operational choices.
- **Risk Mitigation**: Weak governance can lead to legal penalties, data breaches, and reputational harm.
- **Innovation and Agility**: High-quality, well-managed data enables digital services and analytics.

Conversely, failures in information governance and management expose organisations to regulatory breaches, inefficiencies, and loss of stakeholder trust, which include:

- ***Data Residency**: The physical location where data is stored, often selected for legal or strategic reasons.*
- ***Data Localisation**: Mandatory legal requirements for data to remain within specific jurisdictions. These concerns are particularly relevant to cloud adoption and international operation in regulated sectors.*

2.8.5 Institutional Integration

Mature organisations increasingly establish Information Governance Councils or Committees to integrate policy, coordinate responsibilities, and align information use with strategic goals. They also invest in enterprise content management systems, metadata standards, and integrated management systems.

2.8.6 Conclusion

Information governance and management are fundamental enablers of compliance, trust, and value creation. Governance provides the rules and oversight; management delivers implementation and continuity. Together, they ensure that information is a strategic, secure, and well-used resource throughout its lifecycle. Embedding that within organisational governance structures ensures consistency, accountability, and strategic coherence.

2.9 Information Security

Information security, of **InfoSec**, refers to the preservation of the confidentiality, integrity, and availability (CIA) of information, as well as other properties such as authenticity, accountability, non-repudiation, and reliability. Its primary objective is to protect organisational information assets from threats that may result in harm to operations, assets, individuals, or reputation.

The scope of information security extends beyond digital systems. It encompasses physical security, human behaviour, organisational structures, and third-party relationships. It is an essential component of organisational resilience and a prerequisite for maintaining trust with stakeholders.

2.9.1 Core Principles and Terminology

The fundamental model for information security is often framed around the **CIA triad**:

- **Confidentiality**: Ensuring that information is accessible only to those authorised to have access.
- **Integrity**: Safeguarding the accuracy and completeness of information and processing methods.
- **Availability**: Ensuring that authorised users have access to information and associated assets when required.

These are supported by additional principles such as accountability (traceability of actions), authenticity (verifying identity and origin), and non-repudiation (ensuring actions or communications cannot be denied later). Key terms include:

- **Threat**: A potential cause of an unwanted incident.
- **Vulnerability**: A weakness that can be exploited by a threat.
- **Risk**: The potential impact, or consequence, of a threat exploiting a vulnerability, considering the likelihood and consequences.

2.9.2 Standards and References

Numerous standards and frameworks guide the implementation of information security. Among the most prominent are:

- **ISO/IEC 27001**: Specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).
- **ISO/IEC 27002**: Provides guidelines for information security controls.
- **NIST Cybersecurity Framework (CSF)**: Offers a risk-based approach to managing cybersecurity.
- **ENISA Guidelines**: From the EU Agency for Cybersecurity, providing sector-specific and cross-sector guidance.

Organisations often adopt combinations of these frameworks, tailoring them to their size, industry, and regulatory context.

2.9.3 Governance and Policy

Effective information security requires governance mechanisms that define roles, responsibilities, and decision-making processes. This includes the development and enforcement of security policies, the establishment of risk management procedures, and the alignment with broader organisational objectives.

*The governance of security is typically overseen by roles such as the **Chief Information Security Officer (CISO)**, supported by committees, risk officers, internal audit, and IT teams. A well-defined governance structure helps ensure that security measures are not only technically sound but also supported and enforced throughout the organisation.*

2.9.4 Controls and Implementation

Information security controls can be preventive, detective, or corrective. They span technical, physical, and organisational measures. Examples include:

- **Technical controls**: Encryption, firewalls, access control systems, intrusion detection.
- **Physical controls**: Access badges, surveillance systems, secure facilities.
- **Organisational controls**: Policies, training, incident response plans, background checks.

Implementation requires a risk-based approach, prioritising controls according to the value of the information and the level of threat. Control effectiveness should be monitored and reviewed as part of a continuous improvement process.

2.9.5 Emerging Trends and Challenges

Organisations face a constantly evolving threat landscape, including cybercrime, insider threats, state-sponsored attacks, and supply chain vulnerabilities. The increasing use of cloud services, mobile devices, and remote work introduces new challenges for securing data and maintaining control over infrastructure.

Emerging technologies such as artificial intelligence, blockchain, and quantum computing create both opportunities and risks for information security. Threat intelligence, automation, and zero-trust architectures are among the evolving responses to these challenges.

Security is no longer confined to IT departments; it is a strategic concern requiring awareness, engagement, and responsibility at all levels of the organisation.

2.10 Records Management

Records management is a foundational function in all organisations. It underpins accountability, legal compliance, continuity of service, and cultural memory. Although often perceived as a support activity, it forms a core part of business governance and institutional responsibility. However, its growing entanglement with digital systems, regulatory obligations, and lifecycle governance of information makes it core to governance of IT.

2.10.1 Core Concepts

*A **record** is any information created or received by an organisation in the course of its activities, preserved as evidence or for its operational, legal, or historical value.*

Records may be physical or digital and span formats as diverse as correspondence, databases, images, forms, or video. A **recordkeeping system** encompasses the policies, procedures, and tools used to manage these records throughout their lifecycle.

An archive refers specifically to records of enduring value. These may be preserved for legal accountability, institutional memory, research, or public access.

Many traditions reflect the recognition of distinct phases in a record's lifecycle. In Lusophone contexts, the model of *arquivo corrente* (active use), *arquivo intermédio* (semi-active or temporary retention), and *arquivo permanente* (long-term or historical preservation) remains influential. Other jurisdictions refer to similar phases as current, semi-current, and archival.

2.10.2 International Standards

ISO 15489 remains the foundational international standard for records management, defining principles for the creation, capture, and control of records. More recently, the ISO 30300 series introduce a management system perspective, aligning recordkeeping with broader organisational governance structures. These standards emphasise policy-driven lifecycle management, clearly assigned roles, defined retention rules, and documented procedures for access, security, and disposal. Records management, in this view, becomes part of a broader accountability system, embedded into organisational maturity models and management system audits.

2.10.3 The Challenge of Digital Preservation

Preserving records over time presents significant challenges. File formats, metadata, and system dependencies may degrade or become obsolete. Institutional knowledge may be lost. Even when storage capacity is available, the usability and authenticity of digital records are not guaranteed without active curation. The risks of data loss, of altered meaning, or of legal inadmissibility must be weighed against the value of retention. Preservation is not only a technical exercise; it requires governance clarity, resource allocation, and long-term planning. Public institutions face particular pressures. They may be required to preserve certain classes of records permanently; even as digital transformation initiatives shift platforms and formats. Sectoral regulations, funding constraints, and political change can further complicate preservation efforts.

2.10.4 Sectoral Distinctions and Public Interest

In the private sector, records management is often driven by risk mitigation, operational continuity, and compliance with contractual or fiscal obligations. Decisions to retain or dispose of information are primarily shaped by business value and legal exposure.

In the public sector, however, records carry an additional weight: they may embody citizen rights, administrative transparency, and institutional legitimacy. Archival functions often intersect with the principle of public access to information, especially where decisions affect lives, entitlements, or public trust. **The long-term stewardship of public records is thus not merely a technical concern, but a social responsibility.** In Portugal, the *Lei de Acesso aos Documentos Administrativos* (LADA) grants access rights to administrative records[53].

2.10.5 Regulatory Tensions: Deletion vs Retention

The principle of retention limitation is enshrined in multiple regulatory frameworks. The General Data Protection Regulation (GDPR), for example, requires that personal data be kept no longer than necessary. ISO/IEC 27001:2022, the international standard for information security, includes a specific control on *Information Deletion*, requiring organisations to define and enforce deletion rules for data no longer needed.

However, such controls can come into conflict with archival and legal obligations that mandate indefinite or conditional retention, especially in public administration, justice, or scientific domains.

These tensions have created friction in practice. Records professionals and archivists may advocate for indefinite retention of certain categories of records, citing legal, evidentiary, or historical value. Meanwhile, security auditors may treat any record without a defined deletion date as a compliance failure. The resulting policy conflicts must be managed with care, avoiding both excessive risk aversion and indiscriminate data destruction.

2.10.6 Governance and Coordination Across Roles

Records management must not be marginalised or siloed. Its relevance extends across procurement, HR, finance, and digital services. In a governance of IT context, recordkeeping should be addressed not only as a storage issue, but as part of strategic information governance and risk management. Alignment with security and privacy frameworks is essential, but so too is preserving institutional memory and respecting rights to information. Addressing that requires collaboration between legal, security, compliance, IT, and records management functions. Each brings a legitimate perspective: risk, regulation, efficiency, and accountability. Only through coordinated governance (backed by clear roles, retention schedules, and exception handling) can a coherent policy be sustained.

2.10.7 Conclusion

Archives and records management are far more than routine filing or compliance chores. They are manifestations of how organisations understand responsibility, time, and value. The systems and policies that govern records shape how decisions are remembered, how rights are upheld, and how trust is sustained. In organisations, especially in public institutions, records management must be integrated into governance structures, reconciled with security requirements, and supported by long-term investment. It is both a strategic function and a societal obligation.

[53] https://www.cada.pt/

2.11 Information Privacy

Information privacy refers to the rights and expectations individuals have regarding the collection, use, and disclosure of their personal data. In both public and private organisations, safeguarding personal information is not only a matter of legal compliance but also one of trust, ethics, and risk management. The complexity of digital ecosystems has expanded the potential for misuse, loss, or unauthorised disclosure of personal data, thereby intensifying the focus on privacy governance. At the heart of privacy concerns is the concept of Personally Identifiable Information (PII), which includes any data that can be used to identify a specific individual. This may include names, identification numbers, location data, online identifiers, and even factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity.

2.11.1 Key Roles in Privacy

Three key organisational roles define how PII is handled:

- **PII Principal**: This is the individual to whom the personal information relates. The principal is the subject of the data, and modern privacy frameworks aim to reinforce their rights over how their information is processed, shared, and stored.
- **PII Controller**: The controller is the entity, often an organisation, that determines the purposes and means of processing PII. The controller holds primary responsibility for ensuring that the collection and handling of personal data comply with applicable legal and ethical standards. In public administration, ministries, municipalities, or national agencies often act as controllers when processing citizen data.
- **PII Processor**: The processor is a third party that processes data on behalf of the controller, without determining the purposes or essential means of the processing. Examples include cloud service providers, outsourcing firms, or contracted analytics services. Processors must act only under the instructions of the controller and are also subject to compliance obligations.

Clear delineation of these roles supports accountability, a central principle of most privacy regulations. It also helps define who is responsible in cases of data breaches or privacy violations.

2.11.2 Privacy by Design and Risk Orientation

Beyond roles, privacy governance requires organisations to implement policies, procedures, and technologies that ensure lawful, fair, and transparent processing of personal data. These include practices such as data minimisation, purpose limitation, storage limitation, and ensuring data subject rights are respected. Techniques like anonymisation, pseudonymisation, and encryption are also relevant to reduce exposure to risk.

Public entities face additional complexity, as they often manage sensitive data at a large scale and under higher public scrutiny. They must also reconcile privacy obligations with transparency mandates and the delivery of essential services. The relationship between privacy and national security, public health, or administrative efficiency frequently creates tensions that must be managed carefully.

A key approach to embedding privacy into organisational processes is the principle of **privacy by design**, which calls for the integration of privacy considerations into the architecture of systems, services, and operations from the outset. This implies a proactive stance, in contrast to reactive or corrective measures taken after privacy risks materialise.

Privacy risk management involves identifying the potential harms associated with the processing of personal data, assessing their likelihood and severity, and applying appropriate controls. Risk may arise from over-collection, lack of purpose limitation, insufficient data security, or unintended disclosure. Data Protection Impact Assessments (DPIAs), where required, provide a structured mechanism for assessing and mitigating such risks and are further addressed in section 4.8.

2.11.3 Governance, Roles, and International Standards

As data becomes increasingly central to strategic operations and transformation efforts, information privacy must be approached as an ongoing responsibility. This includes continuous assessment of risks, regular updates to privacy policies, training of personnel, and the establishment of privacy-by-design practices across systems and services

Beyond the General Data Protection Regulation (GDPR), several international standards contribute to privacy governance. ISO/IEC 29100 provides a high-level privacy framework, while ISO/IEC 27701 extends information security management systems to incorporate privacy. ISO/IEC 27550 addresses privacy engineering, offering support for operationalising privacy controls. Organisations operating across jurisdictions may also need to align with other national or regional frameworks, such as the California Consumer Privacy Act (CCPA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), or Brazil's Lei Geral de Proteção de Dados (LGPD). Although principles often converge, requirements and enforcement mechanisms can vary.

2.11.4 Strategic and Organisational Considerations

Privacy management must be embedded into the organisation's broader strategy and culture. This includes ensuring alignment with data governance, security, and risk management frameworks.

Privacy training and awareness, transparency with stakeholders, and mechanisms for addressing complaints and exercising data subject rights are essential components.

Public sector organisations may face additional considerations, such as balancing transparency and accountability with the protection of personal data, or managing consent and information rights in contexts where services are mandatory.

2.12 General Data Protection Regulation

Building upon the broader discussion of information privacy, this section details the General Data Protection Regulation (GDPR), the central legal instrument governing personal data protection within the European Union. Adopted in 2016 and applicable since May 2018, the GDPR replaces earlier directives to establish a harmonised and enforceable framework across Member States.

The regulation aims to strengthen data subject rights, promote accountability among organisations, and ensure that the protection of personal data is embedded into the design and operation of systems and services. Its extraterritorial scope means that any organisation processing personal data of individuals located in the EU must comply, regardless of where the organisation is established.

2.12.1 Principles of Data Processing

The GDPR is underpinned by a set of principles that apply to all personal data processing activities:

- **Lawfulness, Fairness and Transparency**: Processing must be based on a lawful basis, conducted fairly, and communicated clearly to data subjects.
- **Purpose Limitation**: Data must be collected for specified, explicit, and legitimate purposes and not processed in a manner incompatible with those purposes.
- **Data Minimisation**: Only data necessary for the intended purposes may be collected.
- **Accuracy**: Reasonable steps must be taken to ensure that data is accurate and kept up to date.
- **Storage Limitation**: Data should not be retained for longer than necessary for the purposes for which it was processed.
- **Integrity and Confidentiality**: Appropriate security measures must protect data against unauthorised or unlawful processing and accidental loss or damage.
- **Accountability**: Data controllers must not only comply with the above principles but also be able to demonstrate such compliance.

These principles guide the entire lifecycle of personal data and are foundational to organisational compliance efforts.

2.12.2 Rights of Data Subjects

The GDPR provides data subjects with a comprehensive set of rights that organisations must respect and facilitate, which include:

- The **right of access** to personal data held by a controller.
- The **right to rectification** of inaccurate or incomplete data.
- The **right to erasure** ('right to be forgotten') under specified conditions.
- The **right to restrict processing** under certain circumstances.
- The **right to data portability**, allowing individuals to obtain and reuse their data.
- The **right to object** to processing based on legitimate interests or direct marketing.
- Rights in relation to automated decision-making, including profiling.

Organisations must establish processes to respond to data subject requests within mandated timeframes, and must be able to demonstrate that appropriate mechanisms are in place.

2.12.3 Organisational Obligations and Roles

Under the GDPR, organisations are categorised as either **data controllers** or **data processors**, with distinct responsibilities:

- **Controllers** determine the purposes and means of processing personal data. They are accountable for compliance and must implement appropriate technical and organisational measures, including record-keeping, data protection by design and by default, and, where required, DPIAs.
- **Processors** act on behalf of controllers and must adhere to written contracts and implement security measures. They are directly liable for breaches of their own obligations.

Certain organisations are required to appoint a Data Protection Officer (DPO), especially when data processing is large-scale, systematic, or involves sensitive personal data. The DPO must act independently, free from managerial influence or conflicts of interest, to oversee compliance, advise on obligations, and liaise with supervisory authorities. Although the DPO reports to top management, the role demands full autonomy in judgment and action.

To meet this highly specialised requirement, many organisations opt to outsource the function, commonly known as "DPO as a Service", and the emergence of service providers for that[54,55]. This provides access to expert knowledge but still requires the DPO to have sufficient authority, insight into internal operations, and unimpeded access to relevant information and decision-makers.

2.12.4 Enforcement and Sectoral Considerations

Enforcement of the GDPR is carried out by independent **Supervisory Authorities (SAs)** in each Member State, coordinated at the European level by the **European Data Protection Board (EDPB)**. Penalties for non-compliance can be significant, up to €20 million or 4% of the organisation's global annual turnover.

While the GDPR applies uniformly across sectors, public organisations face specific challenges. These include reconciling privacy with transparency obligations, managing data subject requests in public service contexts, and ensuring consistent practices across decentralised units. Public bodies are typically required to appoint a DPO and often operate under additional national rules in areas such as health, education, or justice.

The GDPR has also served as a model for data protection frameworks beyond the EU, influencing regulatory developments globally and reinforcing the role of privacy as a core component of modern governance.

[54] https://www.dpo-portugal.pt/

[55] https://www.portaldodpo.pt/

2.13 Consent Mechanisms: Opt-In and Opt-Out

Consent is a cornerstone of data protection law. Under the General Data Protection Regulation (GDPR), organisations must have a lawful basis for processing personal data, and **consent** is one of the most frequently discussed, yet often misunderstood, bases. Understanding **opt-in** and **opt-out** mechanisms is critical for the governance and management of information systems, particularly in the design of user interfaces, privacy policies, and service configurations.
Engineers and consultants working in both public and private sectors must be able to identify when consent is required, how it must be obtained, and the organisational and technical implications of using opt-in or opt-out models.

2.13.1 Opt-In

Opt-in refers to a consent mechanism that requires the **data subject to take an explicit affirmative action** before any processing of their personal data occurs:

- Under GDPR, valid consent must be **freely given, specific, informed, and unambiguous**, typically through actions such as ticking an unchecked box or clicking "Accept."
- Opt-in is mandatory for most non-essential data processing, such as:
    - Direct marketing
    - Behavioural tracking
    - Data sharing across services
    - Processing of special categories of data

Failing to implement a compliant opt-in mechanism can result in severe regulatory penalties, reputational damage, and invalidated data collection.

2.13.2 Opt-Out

Opt-out mechanisms presume consent by default, but offer the user a chance to decline or withdraw. This approach is **not compliant for most use cases under GDPR** unless:

- A different legal basis than consent is applicable (e.g., legitimate interest — and even then, subject to balancing tests).
- The processing is strictly necessary and covered by other lawful grounds.

Opt-out mechanisms are still found in:

- Cookie banners (for non-essential cookies, under specific configurations)
- Subscription management (e.g., "unsubscribe" links)
- Public sector legacy systems (often under legal or administrative justifications)

In systems using opt-out, **transparency and ease of refusal** are critical. Failure to offer clear opt-out options may lead to enforcement action.

2.13.3 Strategic and Sectoral Relevance

Public vs Private Sector:

- Public sector systems typically require **explicit opt-in**, especially in areas like health, taxation, or welfare, where trust and transparency are essential.
- Private sector platforms may **attempt opt-out models** (e.g., pre-ticked boxes), but risk legal exposure — particularly in marketing or cross-border contexts.

CxO Considerations:

- CIOs must ensure that systems record and enforce consent preferences.
- CISOs are accountable for compliance monitoring and breach prevention linked to unauthorised processing.
- CTOs may influence how user interfaces operationalise opt-in/opt-out mechanisms, which affects user trust and system integrity.

Consultants must assess:

- Whether consent is required at all
- Whether it is validly collected
- Whether the mechanism is **auditable and enforceable**

2.13.4 Governance and Compliance Implications

Consent mechanisms should be addressed within information governance and management, in special GDPR obligations and ISO/IEC 27001 certification. They must be documented, tested, and subject to internal audits. They should also be considered in frameworks for InfoSec and risk management, particularly in Data Protection Impact Assessments (DPIAs) and privacy-by-design approaches.

2.13.5 Final Notes

Consent is not merely a checkbox — it is a **legal, organisational, and ethical commitment**. Choosing between opt-in and opt-out is not a matter of convenience but of governance, accountability, and legitimacy. Organisations that trivialise consent risk technical non-compliance and loss of public trust.
In digital governance, how consent is implemented is as important as **why** it is sought.

2.14 Personal Data

Sensitive categories of personal data refer to specific types of information deemed particularly vulnerable due to their potential to result in discrimination, harm to personal dignity, or intrusion into fundamental rights and freedoms. Under Article 9 of the General Data Protection Regulation (GDPR), the processing of such data is generally prohibited unless specific conditions are met. These categories are subject to heightened protection due to their nature and social implications.

The GDPR defines these categories to include personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data that uniquely identifies a natural person
- Health data
- Individual's sex life or sexual orientation

In addition, national laws may extend this list or establish further restrictions depending on jurisdictional context. For example, in Portugal, specific attention is also given to judicial data or data related to criminal offences, even when not directly covered under Article 9[56].

2.14.1 Examples and Risk Considerations

The potential misuse of sensitive data poses severe ethical and legal risks. Examples include:

- Discrimination in employment or insurance based on health or genetic data
- Surveillance or profiling based on religious or political beliefs
- Identity theft involving biometric data (such as facial recognition or fingerprints)
- Social or psychological harm stemming from the exposure of sexual orientation or personal beliefs

Even where consent is given, it must be explicit and informed, with clear safeguards. Certain contexts (such as public administration, health systems, or biometric access control) raise additional complexity, as individuals may have limited ability to refuse without adverse effects.

2.14.2 Legal Exceptions for Processing

Processing of sensitive categories of personal data is only lawful under specific exceptions outlined in Article 9(2) of the GDPR.

These include, among others:

- Explicit consent of the data subject
- Obligations in employment, social security, or social protection law
- Vital interests of the data subject or others, particularly when the person is incapable of giving consent
- Processing by not-for-profit organisations with appropriate safeguards
- Data made public by the data subject
- Legal claims or defence
- Reasons of substantial public interest, based on Union or Member State law
- Preventive or occupational medicine, or public health reasons
- Archiving, research, or statistical purposes under strict conditions

Each of these grounds requires proportionality, necessity, and suitable measures for data protection, such as pseudonymisation, access control, and minimisation of exposure.

2.14.3 Governance and Accountability

Organisations processing sensitive personal data must be able to demonstrate compliance through documentation, risk assessment, and internal controls.

Typical measures include:

- Conducting a Data Protection Impact Assessment (DPIA)
- Assigning clear responsibilities to data controllers and processors
- Restricting access to authorised personnel
- Logging and auditing access to sensitive data
- Ensuring lawful basis is documented and monitored

In many cases, the involvement of a Data Protection Officer (DPO) is mandatory, especially in public sector bodies or organisations engaging in large-scale processing of sensitive categories.

2.14.4 Sectoral and Technological Implications

In healthcare, education, research, and public administration, sensitive data is pervasive. The use of AI and biometric technologies further complicates compliance, particularly when automated decision-making or profiling is involved. Systems must be designed with privacy and fairness in mind—this includes "Privacy by Design" approaches and robust auditability.

In the private sector, marketing, employment screening, or customer profiling based on sensitive attributes is highly restricted and often unlawful. Legitimate interests are not considered a valid basis for processing sensitive data under Article 6(1)(f) of the GDPR.

2.14.5 Conclusion

Sensitive categories of personal data require enhanced governance, ethical vigilance, and robust safeguards. Their misuse not only violates legal norms but undermines trust, accountability, and social cohesion. Organisations must not only comply with legal definitions and exceptions but must also adopt a risk-aware, rights-centred approach to the management of sensitive information.

[56] https://tecnico.ulisboa.pt/pt/noticias/inteligencia-artificial-vai-agilizar-digitalizacao-de-acordaos-e-facilitar-o-seu-acesso/

2.15 The Ecosystem of Cybersecurity

Cybersecurity is not solely a technical or internal matter; it is embedded in a complex ecosystem of institutions, frameworks, providers, and cooperative mechanisms at the international, national, and organisational levels. A mature cybersecurity posture relies not only on internal capabilities but also on external partnerships, regulatory guidance, specialised service providers, and sectoral cooperation. Understanding the ecosystem is critical for the Chief Information Security Officer (CISO) and others involved in information risk governance.

2.15.1 Supranational and International Bodies

Cybersecurity policies and practices are increasingly shaped by international standardisation bodies, cooperation frameworks, and information-sharing entities, such as:

- **ENISA (European Union Agency for Cybersecurity)** – The EU's agency dedicated to supporting member states and EU institutions on cybersecurity policy, operational cooperation, threat intelligence, capacity building, and certification schemes. ENISA publishes guidance, threat landscapes, and maintains central roles in implementing the NIS Directive and the EU Cybersecurity Act.
- **NIS Cooperation Group** – A forum established under the NIS Directive to support strategic cooperation and the exchange of best practices among EU member states.
- **EU-CERTs Network** – A network of national CSERT entities, designated under the NIS Directive, facilitating cross-border response coordination.
- **Standardisation Bodies** – Organisations such as **ISO**, **IEC**, **ETSI**, and **NIST** contribute through technical standards and guidelines (e.g. ISO/IEC 27000 series, NIST CSF).
- **International Cybercrime and Cooperation Forums** – Entities such as **Interpol**, **Europol (EC3)**, and **Council of Europe (Budapest Convention)** provide frameworks for international law enforcement and legal harmonisation in cybersecurity-related crimes.

2.15.2 National Authorities and Coordination

In each country, the cybersecurity architecture reflects its regulatory model, sectoral priorities, and institutional maturity. In Portugal, the key formal actors include:

- **CNCS (Centro Nacional de Cibersegurança)** – The national authority for cybersecurity, responsible for coordinating policy, sectoral oversight, issuing alerts and guidance, and promoting awareness and resilience. CNCS plays a central role in implementing the NIS Directive, operating the national CSIRT, and supporting public and critical infrastructure entities.
- **GNS (Gabinete Nacional de Segurança)** – The National Security Office, which oversees national classified information systems, crypto security, and accreditation of systems and personnel. GNS handles security clearances and coordinates protective measures for national defence and critical state systems.
- **CISOs of Public Administration and Critical Operators** – In Portugal, specific obligations apply to operators of essential services (OES) and digital service providers (DSP) under national transpositions of the NIS Directive. These include mandatory notification of incidents and adoption of risk management practices.

Depending on the sector, additional bodies such as the Bank of Portugal, ERSE (energy), or the Health Ministry may have cybersecurity supervisory roles.

2.15.3 Providers and External Support Actors

The operational execution of cybersecurity strategies often depends on a mix of in-house capabilities and external service providers. Typical actors in this landscape include:

- **Managed Security Service Providers (MSSPs)** – Offer outsourced security services such as monitoring, incident detection and response (MDR), vulnerability scanning, firewall and SIEM management, often with 24/7 operation centres.
- **Cybersecurity Consultancies** – Provide advisory services in areas such as risk assessment, compliance audits, penetration testing, strategy development, and business continuity planning.
- **Forensics and Incident Response Firms** – Specialised providers that support organisations during or after a security breach, including technical analysis, containment, recovery, and post-incident review.
- **Cybersecurity Product Vendors** – Suppliers of software or hardware solutions such as endpoint protection, **identity and access management (IAM)**, encryption, secure communications, etc.
- **Threat Intelligence and Sharing Platforms** – Services, communities and platforms that facilitate the exchange of indicators of compromise, vulnerabilities, and threat actor tactics. Examples include ISACs (Information Sharing and Analysis Centers), CERT networks, and commercial threat feeds.
- **Cybersecurity Training and Certification Bodies** – Organisations that offer training, simulations, certification exams, and professional development in cybersecurity roles and standards.

2.15.4 Cyberinsurance

Cyberinsurance has emerged as a financial risk-transfer mechanism within the cybersecurity ecosystem. It enables organisations to hedge against financial losses associated with cyber incidents, including data breaches, ransomware attacks, business interruption, and legal liability.

Policies vary widely in coverage, limitations, and conditions. Typical considerations include:

- Preconditions such as compliance with basic security hygiene.
- Requirements for incident reporting and third-party involvement.
- Exclusions for nation-state attacks or internal negligence.

From a governance perspective, cyberinsurance can be part of a risk treatment strategy, alongside mitigation, transfer, and acceptance. For CISOs, engaging with insurers can offer insights into actuarial risk models, breach cost estimation, and required controls, often reinforcing the case for investments in prevention and detection.

2.15.5 Conclusion

For a CISO, navigating the cybersecurity ecosystem is essential not only for achieving technical resilience but also for demonstrating due diligence, aligning with national expectations, and engaging with sector-wide threat intelligence. Engaging and building trusted relationships within this landscape enhances the organisation's capacity to prevent, detect, respond to, and recover from cyber threats in a manner consistent with legal, strategic, and societal expectations.

2.16 Security Challenge: Bring Your Own Device

The increasing ubiquity of personal computing devices and the widespread use of cloud-based applications have led many organisations to have to face the Bring Your Own Device (BYOD) dilemma, which has implied the definition of policies. BYOD refers to the practice of allowing employees, contractors, or other authorised individuals to use their personal smartphones, tablets, laptops, or other devices to access organisational systems, applications, or data. **While this model can improve flexibility, satisfaction, and productivity, it also raises complex issues related to security, governance, privacy, and compliance**.

2.16.1 Rationale and Adoption

BYOD initiatives often emerge as a response to user expectations for mobility and flexibility. Users familiar with specific devices or applications may prefer to use their own equipment rather than adapt to centrally provided solutions. From the organisation's perspective, BYOD may reduce direct hardware costs and streamline onboarding processes, particularly for temporary staff or third-party collaborators. However, these perceived benefits must be weighed against the increased complexity of securing a diverse and uncontrolled device landscape.

2.16.2 Governance and Policy Frameworks

A BYOD environment must be supported by well-defined policies that address roles and responsibilities, acceptable use, technical requirements, and support boundaries. Policies typically define which types of devices and operating systems are supported, what security configurations are required (e.g. device encryption, lock screen, anti-malware), and what types of data access are permitted. Users are often required to accept terms of use that clarify the organisation's right to monitor, restrict, or remotely wipe organisational data on personal devices.

The scope of support provided by IT departments for personal devices also needs to be established. Some organisations adopt a "best effort" model, where IT provides limited guidance but does not guarantee compatibility or resolution of issues. Others invest in more formalised BYOD support structures, often tied to a Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) platform.

2.16.3 Security and Risk Management

BYOD significantly expands the organisation's attack surface. Personal devices may lack adequate security configurations or may be shared with unauthorised individuals. The risk of data leakage increases, particularly in cases of device theft, malware infection, or unintentional exposure through cloud synchronisation. Security controls must therefore be tailored to this model.

Common security practices include:

- Enforcing strong authentication and encryption for remote access.
- Implementing MDM/EMM tools to enforce compliance with baseline security policies.
- Segregating personal and organisational data through containerisation or virtualisation.
- Restricting access to sensitive applications or data to devices that meet predefined security criteria.

The organisation's incident response and business continuity plans must also take BYOD scenarios into account, including procedures for revoking access and managing lost or compromised devices.

2.16.4 Privacy and Legal Considerations

BYOD environments blur the boundary between personal and organisational domains. Monitoring or controlling personal devices may raise concerns under data protection laws, including the General Data Protection Regulation (GDPR). Care must be taken to distinguish between organisational and personal data, and to apply technical and organisational measures that respect privacy principles such as data minimisation, purpose limitation, and transparency.

User consent is typically required before installing monitoring or control tools on personal devices. In some jurisdictions, labour law and collective bargaining agreements may also impose restrictions on BYOD implementation.

2.16.5 Alternatives and Variants

Several variations of the BYOD model have emerged:

- **COPE (Corporate-Owned, Personally Enabled)**: Devices are owned and managed by the organisation, but users are allowed to use them for personal purposes.
- **CYOD (Choose Your Own Device)**: Users select from a predefined set of approved devices, which are then managed by the organisation.
- **HYOD (Here's Your Own Device)**: The organisation purchases and gifts the device to the user, allowing full personal control with minimal organisational oversight.

These models seek to balance user flexibility with organisational control and accountability.

2.16.6 Strategic Implications

The adoption of BYOD must be aligned with the organisation's digital workplace strategy, security posture, and risk tolerance. While potentially cost-effective and empowering, BYOD introduces non-trivial challenges in governance, compliance, and operational resilience. In public sector contexts, additional considerations may include auditability, procurement constraints, and the need to conform with national standards or shared service policies.

2.17 Frameworks for InfoSec and Risk Management

Frameworks provide structured approaches to managing information security, enabling organisations to assess risk, implement controls, ensure regulatory compliance, and build resilience. They offer common language, principles, and best practices that can be tailored to the organisation's context, regulatory environment, and strategic objectives.

Unlike technical specifications or tools, frameworks are high-level and generally technology-agnostic. They help organisations align security efforts with business priorities and communicate risk and control strategies to both technical and non-technical stakeholders.

2.17.1 ISO Standards for InfoSec

The ISO/IEC 27000 family of standards provides a comprehensive framework for managing information security risks across organisations. At its core is the **ISO/IEC 27xxx**, for an Information Security Management System (ISMS).

Beyond that, several other ISO standards complement information security governance and operational practices. **ISO 31000** offers guidance on general risk management, while **ISO 22301** focuses on business continuity and resilience. **ISO 9001**, although primarily for quality management, contributes to procedural consistency and continuous improvement, often integrated into security operations. **ISO 20000-1** addresses IT service management, with close ties to secure service delivery. **ISO 37301** and **ISO 37001** provide frameworks for compliance and anti-bribery, reinforcing integrity and trust.

These standards can be adopted individually or integrated into broader management systems, enabling alignment across governance, security, privacy, and operational resilience. Formal certification is available for many of these standards, offering independent assurance and demonstrating organisational maturity to partners, regulators, and stakeholders.

2.17.2 NIST Cybersecurity Framework (CSF)

Developed by the US National Institute of Standards and Technology (NIST), the **Cybersecurity Framework (CSF)** provides a flexible structure for managing cybersecurity risks, particularly for critical infrastructure sectors. It is widely adopted internationally, even beyond its original regulatory scope.

The CSF is structured around five core functions:

1. **Identify**: Understand business context and risk…
2. **Protect**: Develop safeguards for delivery of services.
3. **Detect**: Implement monitoring to identify events.
4. **Respond**: Act regarding incidents.
5. **Recover**: Restore capabilities and services.

Each function contains categories and subcategories, with mappings to other standards such as ISO/IEC 27001, COBIT, and NIST SP 800-53. CSF is particularly useful as a **communication tool** between technical teams and executive leadership.

2.17.3 NIST SP 800 Series

The NIST Special Publication (SP) 800 series includes detailed guidance on implementing technical and organisational security measures. Among the most relevant documents:

- **SP 800-53**: Security and privacy controls for federal information systems.
- **SP 800-30**: Risk assessment methodology.
- **SP 800-61**: Computer security incident handling guide.

These publications are often used in sectors that require high assurance, such as defence, healthcare, and finance.

2.17.4 COBIT

COBIT (Control Objectives for Information and Related Technologies) is a governance framework that includes strong emphasis on risk management and control. Its most recent versions support integration with ISO and NIST frameworks and can be used to support alignment between IT strategy and enterprise governance.

Although broader in scope than information security, COBIT defines governance and management objectives related to information security risk, such as:

- **EDM03**: Ensure risk optimisation.
- **BAI09**: Manage assets.
- **DSS05**: Manage security services.

2.17.5 Choosing and Combining Frameworks

Frameworks are often **complementary**, not mutually exclusive. For example:

- ISO/IEC 27001 can serve as a certifiable ISMS foundation.
- NIST CSF can guide internal maturity assessment and improvement planning.
- COBIT can provide alignment with enterprise governance structures.
- Sector-specific regulations may require reference to particular NIST SPs or ISO guidelines.

Selection depends on the organisation's size, sector, jurisdiction, and maturity level. Many organisations blend elements of multiple frameworks in their security architecture.

2.17.6 Strategic Implications

Frameworks are not static checklists but evolving reference models. Even if they are not required (as compliance requirements) their value lies in guiding organisations toward resilient, risk-aware, and responsive security practices. They provide the scaffolding for:

- Developing and maintaining a security strategy.
- Communicating with auditors, regulators, and partners.
- Aligning security investments with business risk appetite.
- Demonstrating due diligence and accountability.

2.18 The ISO/IEC 27xxx Family

The ISO/IEC 27xxx family defines a comprehensive framework for managing information security, privacy, risk, and continuity in a structured and auditable manner. Developed by ISO and IEC, this family promotes international alignment on the governance of information-related risks and supports both public and private organisations in establishing trustworthy and resilient systems.

At its core, the 27xxx family enables the implementation of an **Information Security Management System (ISMS)**, a structured set of policies, processes, roles, and controls for managing information security risks in a continuous improvement cycle.

As of early 2025, the **ISO/IEC 27xxx family** includes **over 60 published standards**, technical reports, and technical specifications[57].

2.18.1 ISO/IEC 27001: Requirements and Certification

ISO/IEC 27001 is the central and certifiable standard of the family. It specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS. Unlike many guidelines or codes of practice, ISO/IEC 27001 allows organisations to undergo an independent **certification process**, demonstrating conformity with international best practices in information security management.
Certification is usually voluntary but often pursued for strategic reasons, such as improving internal governance, gaining competitive advantage, responding to regulatory expectations, or qualifying for public or international tenders. The certification process involves external audit by an accredited body and typically includes annual surveillance and periodic recertification.
ISO/IEC 27001 is applicable to organisations of any size or sector, but its implementation and certification are scoped. This means that certification can apply to a specific process, service, department, or business unit rather than the organisation as a whole. The standard is particularly valued in contexts where the confidentiality, integrity, and availability of information are critical to operations or compliance. Public administrations and regulated industries often adopt ISO/IEC 27001 as part of broader strategies to enhance trust, meet contractual obligations, or demonstrate accountability in high-risk or high-visibility domains.

2.18.2 Supporting and Extension Standards

ISO/IEC 27002 complements 27001 by providing implementation guidance for the controls listed in its Annex A. It supports the selection and adaptation of controls based on the organisation's risk profile.

Several other standards in the family address specific needs:

- **ISO/IEC 27000** – Terminology and foundational concepts.
- **ISO/IEC 27005** – Risk management methods for ISMS contexts.
- **ISO/IEC 27004** – Measurement and metrics for assessing ISMS performance.

Extensions to privacy include:

- **ISO/IEC 27701** – An add-on to ISO/IEC 27001 that defines a **Privacy Information Management System (PIMS)**, aligning ISMS practices with privacy obligations such as those under GDPR.
- **ISO/IEC 27018** – Guidelines for protecting personal data in cloud computing services.

2.18.3 Sectoral Applications and Integration

The family also includes specialised standards for areas such as cloud services (27017, 27018), supply chain security (27036), and incident management (27035). These allow tailored approaches that maintain consistency with the 27001 framework.
A major strength of ISO/IEC 27001 lies in its compatibility with other ISO management system standards, including ISO 9001 (quality), ISO 22301 (business continuity), and ISO 14001 (environmental). This enables integrated management systems across diverse risk domains.

2.18.4 Global Relevance and Strategic Value

With growing demand for transparency, resilience, and interoperability, the ISO/IEC 27xxx family is increasingly adopted as a foundation for both compliance and strategic positioning. Certification in ISO/IEC 27001 is often a prerequisite in partnerships, procurement, and outsourcing, particularly where trust and data sensitivity are at stake.
By structuring security and privacy governance through internationally recognised standards, organisations improve not only their operational robustness but also their legitimacy in the eyes of regulators, clients, and society.

[57] https://en.wikipedia.org/wiki/ISO/IEC_27000_family

2.19 Certification on ISO/IEC 27001

Certification on ISO/IEC 27001 refers to a formal, third-party attestation that an organisation has established, implemented, maintained, and improved an information security management system (ISMS) in conformity with the requirements of the ISO/IEC 27001 standard. It signals that the organisation adopts a systematic approach to managing sensitive information, based on risk management principles, and subject to continuous evaluation and improvement.

2.19.1 What Certification Means

ISO/IEC 27001 certification does not certify technology, nor does it guarantee that no security incidents will occur. Instead, it confirms that a robust management system is in place to identify, assess, and mitigate risks to information assets.

Certification is issued by accredited certification bodies after a successful audit process. It covers a defined *scope*, which must be explicitly declared. The scope may be narrow (e.g., a specific department or service) or organisation-wide, but certification only applies to what is included. Misunderstanding or overstating the scope can lead to reputational or contractual problems.

2.19.2 What It Requires

To achieve certification, an organisation must establish an ISMS that complies with the normative clauses of ISO/IEC 27001. These include:

- Context of the organisation – understanding internal and external issues, interested parties, and the scope of the ISMS.
- Leadership – top management must demonstrate commitment and define roles, responsibilities, and the information security policy.
- Planning – includes the identification of risks and opportunities, and definition of security objectives and risk treatment plans.
- Support – resources, competence, awareness, communication, and controlled documentation must be in place.
- Operation – the organisation must plan, implement, and control its information security processes, including risk management activities.
- Performance evaluation – monitoring, measurement, internal audits, and management reviews are required to assess ISMS effectiveness.
- Improvement – the organisation must take corrective actions and pursue continual improvement.

In addition, the organisation must implement the appropriate *Annex A* controls (or justify exclusions) based on its own risk assessment and the *Statement of Applicability*. These controls range from access control and cryptography to supplier relationships, physical security, and information deletion.

2.19.3 The Certification Process

Certification follows a structured process:

- **Gap analysis (optional):** An initial assessment by a consultancy or pre-audit service to evaluate readiness.
- **Stage 1 audit:** A review of documentation and preparedness by the certification body.
- **Stage 2 audit:** A more detailed assessment of implementation and effectiveness across the defined scope.
- **Issuance of certificate:** If conformity is confirmed, a certificate is issued for a period of three years.
- **Surveillance audits:** Conducted annually to verify that the ISMS is being maintained.
- **Recertification audit:** At the end of the three-year cycle, a full reassessment is required to renew certification.

2.19.4 Strategic and Operational Implications

Achieving and maintaining certification has both internal and external implications. Internally, it demands a structured governance model for information security, cross-functional collaboration, and continuous improvement. It may require changes to roles, processes, risk registers, and documentation practices.

Externally, ISO/IEC 27001 certification is often a precondition for participating in tenders, forming partnerships, or demonstrating compliance with legal or sectoral obligations. It strengthens trust among stakeholders and reduces the need for detailed security due diligence in business relationships.

For public sector organisations, certification supports transparency and accountability. For private sector entities, it often functions as a differentiator in competitive markets. For both, it provides a benchmark against which security maturity and governance practices can be measured.

2.19.5 Common Challenges and Misunderstandings

Certification according to a MSS can be misunderstood as a purely technical or IT-driven concern. In reality, it always requires executive commitment, organisational alignment, and cultural adaptation. Common pitfalls, especially in relation to ISO/IEC 27001, include:

- Treating ISO/IEC 27001 as a one-time project rather than a continuous cycle.
- Delegating responsibility solely to IT teams, without engaging business units.
- Using generic documentation templates without tailoring them to real practices.
- Misrepresenting the scope or control coverage in external communication.

Successful certification on ISO/IEC 27001 reflects not only the existence of documented controls, but also their effective integration into the organisation's governance, planning, and day-to-day activities.

2.19.6 Conclusion

ISO/IEC 27001 certification is a structured demonstration of security governance maturity. It affirms that an organisation understands the risks to its information assets, has planned and implemented suitable controls, and is committed to monitoring, reviewing, and improving its security posture. More than a compliance label, it is a signal of organisational discipline and risk awareness in an increasingly complex digital environment.

2.20 Shadow IT

Shadow IT refers to the use of information technologies, such as applications, devices, or cloud services, within an organisation without formal approval or oversight by the central IT function.
While often perceived as a risk, shadow IT also reflects evolving user needs and operational pressures, and may reveal gaps between official IT offerings and actual work practices. Effective governance of shadow IT involves not only detection and control, but also dialogue, adaptation, and alignment.

2.20.1 Origins and Drivers

The emergence of cloud-based tools, mobile applications, and easy-to-use digital services has lowered the threshold for adoption outside the traditional IT procurement and deployment cycle. Users may turn to unofficial tools due to perceived delays, rigidity, or lack of functionality in authorised systems. Examples include using personal email accounts for work communication, subscribing to online file-sharing services, or deploying third-party collaboration platforms within teams.
In many cases, these choices aim to improve productivity or address immediate operational challenges. Shadow IT can thus be understood as both a symptom of unmet needs and a signal of digital initiative among users.

2.20.2 Risks and Challenges

The informal adoption of technology solutions introduces significant risks, including:

- **Security vulnerabilities**: Unvetted tools may lack proper authentication, encryption, or update mechanisms, creating entry points for cyber threats.
- **Data leakage**: Sensitive or personal data may be stored in uncontrolled environments, exposing the organisation to breaches and regulatory non-compliance.
- **Inconsistencies and fragmentation**: Parallel systems may create inconsistencies in data, duplicate efforts, or complicate integration and reporting.
- **Undermined governance**: Lack of visibility overshadow IT impairs the organisation's ability to enforce policies, manage risk, and respond to incidents.

In regulated environments, including much of the public sector, shadow IT may also compromise auditability and accountability, potentially leading to legal or reputational consequences.

2.20.3 Detection and Visibility

Organisations must balance control with awareness. Detection of shadow IT can be supported through network traffic analysis, endpoint monitoring, and surveys. However, aggressive surveillance may raise ethical or legal concerns. It is therefore essential to establish a governance approach that promotes transparency and encourages disclosure rather than secrecy.
Clear communication of acceptable use policies and a non-punitive posture toward unauthorised tools can help uncover shadow IT without damaging trust. In many cases, shadow solutions provide valuable insight into user preferences and unmet requirements.

2.20.4 Response Strategies

Approaches to managing shadow IT include:

- **Containment**: Blocking or restricting unauthorised tools, often through network controls or policy enforcement.
- **Integration**: Evaluating and formally adopting popular tools after security and compliance assessment.
- **Substitution**: Providing sanctioned alternatives that meet user needs while preserving control and oversight.
- **Dialogue**: Engaging users to understand their motivations and co-create better solutions.

The choice of strategy depends on the nature of the tools in use, the criticality of the associated risks, and the organisation's maturity in governance of IT.

2.20.5 Cultural and Organisational Dimensions

Shadow IT is not merely a technical issue, it reflects organisational culture, trust in IT services, and the agility of internal processes. In some organisations, shadow IT emerges as a workaround for bureaucracy or perceived inefficiency. Addressing these root causes may involve reviewing service catalogues, simplifying approval processes, or adopting more user-centric design practices.

2.20.6 Public Sector Considerations

In public administrations, shadow IT can conflict with procurement rules, data protection obligations, and interoperability requirements. The use of unapproved cloud services, for example, may violate contractual restrictions or national cybersecurity guidelines.

2.20.7 Strategic Implications

Shadow IT should not be viewed solely as a threat, but as an opportunity to realign IT services with evolving user needs. Its presence signals gaps in governance or agility that may require strategic attention. A mature approach combines detection, engagement, and integration into a broader change effort.

2.21 Management of Information Systems

Information systems are not merely technological tools; they are critical organisational assets that support decision-making, enable service delivery, enhance communication, and sustain competitive or operational advantage. Their management requires more than technical maintenance; it involves strategic planning, governance alignment, risk oversight, and service performance.

As organisations become more dependent on digital infrastructures and data, the effective management of information systems becomes a key driver of resilience, agility, and stakeholder satisfaction. Poorly managed systems can lead to inefficiencies, vulnerabilities, and loss of trust (while well-managed systems contribute to excellence, innovation, and compliance).

2.21.1 Core Dimensions of IS Management

Managing information systems encompasses several interdependent dimensions, which include:

- **Strategic Planning**: Aligning IS initiatives with organisational goals. This involves prioritising projects, budgeting for long-term IT investments, and ensuring interoperability with future architectures.
- **IT Operations Management**: Maintaining availability, performance, and reliability of systems. This includes capacity planning, system monitoring, incident management, and change control.
- **Data Management**: Ensuring the quality, integrity, availability, and security of data. Data is often one of the most valuable outputs of information systems and must be governed accordingly.
- **Security and Compliance**: Protecting systems against threats and ensuring they meet legal, regulatory, and contractual obligations. This includes implementation of access controls, audits, encryption, and logging.
- **Vendor and Contract Management**: Overseeing relationships with software providers, cloud platforms, and service integrators. This is especially important in environments where key systems are delivered through third parties.
- **User Support and Experience**: Managing helpdesk functions, training, and feedback channels. User satisfaction is a key metric in the success of many internal information systems.

Each of these domains requires specific competencies, tools, and governance mechanisms. Integration across them is necessary for a coherent management approach.

2.21.2 Lifecycle Management of Information Systems

Information systems should be managed across their entire lifecycle, typically structured in phases:

1. **Conception and Requirements** – Identifying business needs, stakeholder expectations, and regulatory constraints.
2. **Design and Acquisition** – Developing or selecting appropriate technologies and architectures.
3. **Implementation** – Deploying the system, often involving data migration, change management, and user onboarding.
4. **Operation and Maintenance** – Running the system under controlled conditions, resolving issues, and applying updates.
5. **Evaluation and Optimisation** – Assessing system performance and identifying improvement opportunities.
6. **Decommissioning** – Phasing out outdated systems, ensuring data preservation or disposal, and managing transition risks.

Effective lifecycle management reduces total cost of ownership, mitigates technical debt, and ensures system relevance over time.

2.21.3 Governance Interfaces

The management of information systems is closely connected to organisational governance structures. For example:

- The **CIO** typically leads IS strategy and governance alignment.
- The **CISO** ensures that security controls are applied throughout the system lifecycle.
- **Audit and compliance teams** may review IS processes, configurations, and performance records.
- **Business owners** of systems are responsible for functional requirements, funding, and value realisation.

Clarity in these roles and their interdependencies is a prerequisite for effective system management.

2.21.4 Management References

Modern IS management relies on a variety of tools and reference models, including:

- **ITIL** (Information Technology Infrastructure Library): Framework for service management, particularly for operations and support.
- **COBIT**: Supports governance of enterprise IT and aligns IS processes with strategic objectives.
- **ISO/IEC 20000**: Standard for IT service management.
- **Configuration Management Databases (CMDBs)**, **Monitoring Systems**, and **ITSM Platforms**: Support visibility, control, and efficiency in managing complex environments.

The selection and implementation of techniques, frameworks or tools should be driven by business needs, maturity level, and resource availability.

2.21.5 Conclusion

Managing information systems is a complex task requiring technical proficiency, governance awareness, and continuous alignment with organisational priorities. It extends beyond IT operations management to encompass strategic planning, stakeholder engagement, risk management, and compliance. As digital infrastructures grow in scale and importance, mature IS management becomes essential for operational continuity, innovation, and trustworthiness. A structured and lifecycle-based approach, supported by recognised frameworks and clear accountability, enables organisations to realise the full value of their information systems.

2.22 IT Providers

Organisations rarely operate in technological isolation. Most rely on a range of external IT providers to supply infrastructure, develop applications, manage systems, or deliver specialised services. **The nature of these relationships reflects not only technical needs but also the organisation's sector, size, regulatory context, strategic posture, and internal maturity.** Understanding the different classes of IT providers (and how they relate to the organisation's business base) is essential for informed governance, risk management, and decision-making.

2.22.1 A Glimpse of Types of Providers

IT providers can be classified not only by the type of service offered, but also by the strategic role they play within the organisational ecosystem. Some are operational enablers, others are strategic partners, and some serve as compliance-critical dependencies.

- **Commodity Providers:** These suppliers deliver standardised, widely available technology products or services. Examples include providers of network connectivity, cloud infrastructure (IaaS), endpoint hardware, or generic office software (e.g., email, word processing). **Their offerings are typically commoditised, price-sensitive, and subject to competitive procurement.** While often taken for granted, they represent operational dependencies and can introduce risk in areas such as availability, data residency, or vendor lock-in.
- Managed Service Providers (MSPs): MSPs take responsibility for the operation and monitoring of a defined set of IT functions (such as user support, data backup, infrastructure management, or cybersecurity monitoring) under contractual terms. These arrangements are common where internal capacity is limited or where predictable service levels are required. The relationship is based on service-level agreements (SLAs), and effectiveness depends on governance maturity on both sides. In regulated sectors or public services, the choice of MSPs may also be shaped by compliance and procurement constraints. Some vendors have special support (and their own certifications) for MSPs[58,59,60,61].
- **Application and Platform Providers:** These providers offer business-critical applications, such as enterprise resource planning (ERP), customer relationship management (CRM), sector-specific platforms (e.g. health records, education management systems), or software-as-a-service (SaaS) tools. **They influence the organisation's business logic and operational processes. Switching costs can be high, and dependence on proprietary data structures or workflows requires careful vendor governance**.
- **Development Partners and System Integrators**: When bespoke systems are needed, or when integrating diverse technologies into a coherent architecture, organisations often engage external development teams or system integrators. These providers may work under fixed contracts, agile frameworks, or long-term collaborations. **Their role often goes beyond coding or implementation, they help shape solutions, negotiate requirements, and mediate between technical possibilities and business expectations**. The success of such engagements hinges on shared understanding, project governance, and clear role definitions.
- Strategic Advisory and Consultancy Providers: These providers offer high-level guidance, assessment, or planning services. They support decision-making through technology roadmaps, due diligence, feasibility studies, or risk reviews. Their influence is often significant in moments of change: digital transformation initiatives, restructuring, compliance reform, or crisis recovery. While they do not operate systems directly, their recommendations shape long-term technology trajectories. The relationship requires transparency, contextual knowledge, and an ability to navigate organisational culture and politics.
- Public Sector and Mission-Specific Providers: In public administration or mission-driven environments, additional classes of providers exist. These include national infrastructure platforms, shared service centres, inter-municipal cooperatives, or supranational providers such as EU-level digital platforms. In these cases, the client organisation may have little or no market choice, and the relationship is shaped by policy, regulation, or funding mechanisms. The provider may itself be a public body, which alters accountability and escalation paths.
- **Start-ups and Innovation Providers**: In both private and public sectors, some organisations engage emerging technology providers (such as start-ups, research labs, or pilot initiatives) as a way to explore new models or rapidly prototype solutions. **These relationships carry high uncertainty but can generate innovation and agility**. The governance challenge here is to balance experimentation with oversight, ensure learning, and manage intellectual property or continuity risks.

2.22.2 Provider Relationships and Maturity

The nature of IT provider relationships is not static.

As organisational maturity increases, so does the ability to shape provider strategy, evaluate risks, and embed performance monitoring into ongoing operations:

- *Less mature organisations may accept provider terms passively or fail to articulate their own governance requirements.*
- *More mature organisations co-design accountability structures, negotiate meaningful SLAs, and integrate provider performance into internal management dashboards.*

2.22.3 Conclusion

IT providers are not neutral suppliers, they are embedded in the organisation's strategic, operational, and compliance fabric. Understanding the different classes of providers, and their relationship to the business base, supports better alignment, clearer contracts, and more resilient service ecosystems. Whether operating in the private or public sector, recognising the diversity and role of providers is critical to effective governance of IT.

[58] https://partner.microsoft.com/en-US/solutions/managed-services
[59] https://aws.amazon.com/partners/programs/msp/
[60] https://cloud.google.com/partners/msp-initiative
[61] https://partner.ovhcloud.com/en/managed-services-provider/

2.23 Vendor and Contract Management

In an era where digital ecosystems are increasingly interdependent, the management of external providers—especially those supplying technology, services, and platforms—has become a critical function. For roles such as CIO, CTO, and CISO, effective vendor and contract management is essential not only for ensuring service delivery and innovation but also for maintaining control, accountability, and compliance within complex organisational settings.

2.23.1 Strategic Relevance of Vendor Relationships

Vendor relationships often represent more than operational outsourcing or procurement: they are strategic extensions of the organisation. In domains like cloud computing, cybersecurity services, or enterprise systems, external providers may directly influence the organisation's capability to adapt, secure its operations, and innovate. Strategic alignment between the organisation's goals and vendor capabilities is thus central. This requires clarity on expectations, performance indicators, risk-sharing models, and governance mechanisms.

For CxOs, vendor governance is not merely about managing contracts; it involves ongoing evaluation of vendor performance, technological roadmaps, ethical practices, and long-term viability. Vendors should be seen as partners, but with well-defined accountability frameworks.

2.23.2 Contractual Frameworks

Contracts formalise expectations and allocate responsibilities. Key elements typically include service level agreements (SLAs), key performance indicators (KPIs), rights to audit, clauses for data protection and privacy, intellectual property rights, and provisions for dispute resolution or termination.

From a security and compliance perspective, contracts must align with internal controls and legal frameworks such as the GDPR or NIS2 Directive. The role of the CISO is particularly relevant in ensuring that cybersecurity and incident reporting obligations are contractually embedded, especially for suppliers managing critical infrastructure or sensitive data.

Long-term engagements benefit from flexible contracting models such as outcome-based contracts, risk-sharing arrangements, or modular contracts that evolve over time. However, flexibility must not compromise control.

2.23.3 Risk and Dependency Management

Vendor dependency introduces systemic risk. A vendor failure, data breach, or misalignment in values (e.g. in ESG or compliance) can rapidly affect the organisation's resilience or reputation. Therefore, vendor risk assessments (performed at onboarding and regularly throughout the relationship) are vital.

Typical assessments include operational, financial, technical, and legal risks. Concentration risk should also be considered: reliance on a single vendor across multiple services can increase exposure, especially in globalised supply chains.

For high-risk providers, additional governance measures may include enhanced monitoring, independent assurance, or business continuity clauses.

2.23.4 Collaboration Across Organisational Roles

Vendor and contract management intersects with multiple roles.

Typically, the CIO is often responsible for IT procurement strategy and lifecycle management. When the role is defined as CTO, it might be more focused on ensuring technical compatibility and futureproofing of vendor solutions. The CISO provides guidance on security, privacy, and regulatory compliance. Procurement teams and legal departments offer critical support in negotiation, due diligence, and enforcement.

These roles must coordinate effectively, particularly during procurement, contract negotiation, incident response, or vendor offboarding. Governance bodies (such as steering committees or supplier performance boards) can structure this coordination.

2.23.5 Emerging Trends

Recent trends include increased use of third-party risk management platforms, integration of ESG criteria into vendor assessments, and contractual provisions for AI-related responsibilities. Open ecosystems, such as those based on APIs or multi-cloud architectures, increase the complexity of managing dependencies.

Cyber supply chain risk is gaining attention, especially under regulatory frameworks like the EU Cybersecurity Act or DORA (Digital Operational Resilience Act). Proactive vendor oversight is becoming not only a good practice but also a legal obligation.

2.24 External Services and Operational Challenges

As organisations evolve in complexity and scale, they increasingly rely on a diverse array of external service models and workforce arrangements to support their operations, improve resilience, and meet strategic objectives.
These dependencies, while often beneficial in terms of agility and cost-efficiency, introduce layered risks and governance challenges that must be addressed systematically.

The increasing reliance on external services and workforce arrangements underscores the importance of robust vendor and **contract management** and attention to **supply-chain risks**. It also highlights the need for effective coordination between internal roles such as the CIO, CISO, and procurement or legal departments, who must jointly evaluate not just performance, but also exposure and resilience.

Addressing these dependencies requires more than contractual safeguards, as it demands integrated governance frameworks, continuous risk assessment, and clear delineation of responsibilities. As digital ecosystems expand, managing external operational actors becomes a core element of organisational maturity and strategic control.

2.24.1 Contingent Workforce

Contingent Workforce refers to non-permanent personnel such as contractors, freelancers, agency workers, or consultants, brought in to provide specialised expertise or support temporary workload increases.
They are typically hired to meet short-term needs or provide specialised expertise without being part of the organisation's permanent headcount. Managing a contingent workforce often involves different governance, compliance, and risk considerations than managing full-time employees, especially with regard to access to information, systems, and physical facilities.
While this model enhances flexibility and accelerates access to rare skills, it also poses risks to organisational cohesion, information security, and long-term capability development related with knowledge retention.

2.24.2 Managed Service Providers

A common model is the use of **Managed Service Providers (MSPs),** which deliver operational support for **enterprise IT infrastructure**, networks, cloud platforms, and end-user environments.
The concept of MSP enable organisations to shift from internal service delivery models to externally managed environments, often supported by service-level agreements (SLAs) and performance indicators. This arrangement aligns closely with the concerns **IT Sourcing** and **Supplier Risk**, where the choice of externalising services must be balanced with an assessment of strategic dependency, contract robustness, and long-term adaptability.

2.24.3 Managed Security Service Providers

For cybersecurity functions, organisations increasingly engage Managed Security Service Providers (MSSPs). These providers offer services such as threat monitoring, firewall and endpoint management, vulnerability scanning, and compliance support.
MSSPs are distinct from general MSPs in their focus on security-specific functions and regulatory alignment, which links them to concerns of **Information Security** and **Security Operations and Monitoring**.
Effective use of MSSPs requires clarity about incident response roles and a shared understanding of risk thresholds.

2.24.4 Managed Detection and Response

A more specialised variant of MSSP is Managed Detection and Response (MDR). This focuses on advanced threat detection and rapid incident response. MDR providers integrate automated tools with expert human analysis to offer real-time insights and recommendations, often supported by a **security operations centre (SOC**).
While overlapping with MSSPs in function, MDRs typically emphasise proactive detection, response workflows, and forensics, making them particularly relevant for organisations facing persistent or advanced threats. Their effectiveness depends on integration with internal processes, which relates to **Incident Management** and **Business Continuity and Resilience**.

2.25 IT Supply-Chain

In the digital economy, the concept of supply chain extends beyond the movement of physical goods; it now encompasses digital services, platforms, software, data, and infrastructure components.
For roles such as CIO, CTO, and CISO, understanding and managing the digital supply chain of their business is crucial for ensuring operational continuity, regulatory compliance, and strategic alignment. As organisations increasingly depend on interconnected systems and outsourced services, vulnerabilities within the supply chain can rapidly escalate into systemic risks.

2.25.1 The Digital Supply Chain

The digital supply chain includes not only traditional vendors of hardware and software, but also cloud service providers, platform operators, maintenance teams, software development partners, open-source component contributors, and data suppliers, for example.
These elements form a complex and often opaque network of dependencies. Modern IT services frequently integrate components from multiple third parties, many of which are invisible to the end user.
This complex ecosystem complicates the identification of origin, responsibility, and resilience in case of disruption. A failure or compromise in a seemingly distant or minor supplier can propagate upstream and affect core business services.

2.25.2 Roles and Responsibilities

Within the organisation, responsibility for managing supply chain risk does not belong to a single role. A CIO typically accountable for establishing supply chain governance practices aligned with organisational strategy. A CTO tends to be more focuses on technical dependencies and integration choices, ensuring that architecture decisions account for supply resilience. The CISO plays a critical role in identifying and mitigating cyber risks within the supply chain, including data handling practices, software integrity, and third-party access.
In practice, supply chain considerations are often embedded into procurement, vendor management, compliance, and incident response processes, requiring cross-functional coordination.

2.25.3 Risk and Resilience

Supply chain risk encompasses a range of scenarios, including vendor failure, geopolitical instability, component obsolescence, software vulnerabilities, and malicious interference. From a security standpoint, the introduction of malicious code, compromised libraries, or unauthorised access via third-party service providers are growing concerns.
Resilience measures include diversified sourcing, vetting of third-party code, contractual obligations for business continuity and incident reporting, and the use of **software bills of materials (SBOM**) to enhance traceability. Cybersecurity frameworks such as NIST SP 800-161 or ISO/IEC 27036 provide guidance on supply chain risk management.
Importantly, resilience is not just about redundancy, it also involves visibility and response capacity. For example, knowing whether a specific service relies on a third-party platform in a foreign jurisdiction can be critical in crisis management.

2.25.4 Cyber Supply Chain Risk Management

C-SCRM stands for **Cyber Supply Chain Risk Management**. It refers to the set of processes and practices used to identify, assess, and mitigate risks associated with the **cybersecurity of products and services across the supply chain**. C-SCRM has become a critical focus area in both public and private sectors, particularly after high-profile incidents involving third-party vulnerabilities (e.g. SolarWinds, Log4j). Public entities and regulated industries are increasingly required to demonstrate due diligence and transparency in how they manage supply chain cybersecurity risks.

2.25.5 Regulatory and Strategic Implications

Several regulatory frameworks now explicitly address supply chain risk. In the EU, the Digital Operational Resilience Act (DORA) and the Cybersecurity Act require financial entities and critical infrastructure operators to monitor and manage ICT third-party risk.
Similarly, the NIS2 Directive expands obligations around the security of supply chains across various sectors.
From a strategic viewpoint, supply chain decisions influence agility, innovation potential, and cost structures. The emergence of sovereign cloud initiatives, data localisation requirements, and geopolitical tensions has led many organisations to revisit supplier portfolios and sourcing strategies.
CxOs must balance innovation and efficiency with risk awareness and compliance. For example, relying heavily on a dominant hyperscaler may offer efficiency, but can introduce risks related to dependency, cost evolution, or regulatory exposure.

2.25.6 Monitoring and Governance

Effective supply chain governance requires ongoing monitoring of supplier performance, geopolitical developments, and technological shifts. It also calls for structured internal processes, such as risk classification of suppliers, integration of risk controls into procurement, and periodic review of exposure across key services.
Automation tools, threat intelligence platforms, and third-party risk management services can enhance monitoring capabilities. However, internal coordination and leadership commitment remain the foundation of supply chain resilience.

2.26 IT Security and Safety

Security and safety in digital systems are closely intertwined, particularly in contexts involving third-party vendors and complex supply chains. As organisations increasingly rely on external services, platforms, and components, the boundaries of trust and control become blurred. For organisational leaders such as CIOs, CTOs, and CISOs, maintaining security and safety across these extended ecosystems presents both strategic and operational challenges.

Security refers here to the protection of systems, data, and services from intentional threats, such as cyberattacks or unauthorised access.

Safety refers to the assurance that systems will behave as intended and will not cause harm, which is especially important in critical sectors such as healthcare, transportation, or manufacturing, where IT systems interact with the physical world.

2.26.1 Supply Chains and Expanding Risk Surfaces

The integration of multiple external elements into organisational systems introduces new attack vectors and vulnerabilities. A third-party software library might be compromised, a firmware update might include malicious code, or a vendor might suffer a data breach affecting the organisation indirectly. These risks are often difficult to detect in advance, and traditional perimeter-based security models are inadequate in this context.

This broader risk surface includes not only direct suppliers but also their own subcontractors and open-source dependencies. As a result, ensuring end-to-end security and safety requires visibility and controls beyond the organisation's own systems.

2.26.2 Role of Governance and CxO Leadership

CxO leadership plays a pivotal role in integrating security and safety principles into vendor and supply-chain management. The CISO is central in defining third-party risk management policies, conducting security assessments, and enforcing contractual controls related to cybersecurity and incident response.

A CIO or CTO must ensure that procurement and architecture decisions consider long-term implications for resilience, availability, and data protection, while also considering technical integration points, code provenance, and update mechanisms.

Effective governance includes not only due diligence before onboarding a vendor but also continuous monitoring, regular reassessments, and coordinated responses in the event of incidents. Contracts should include detailed clauses on security responsibilities, audit rights, data handling, and coordinated response mechanisms.

2.26.3 Safety Considerations in Digital Components

When IT systems directly influence physical processes (as in operational technology (OT), embedded systems, or Internet of Things (IoT) environments), safety becomes inseparable from digital security. A vulnerability in a connected medical device, vehicle control system, or industrial sensor can lead to physical harm or regulatory breach.

Vendors supplying such components must meet stringent standards, often including certification under safety-critical frameworks (e.g. ISO 26262 for automotive systems or IEC 61508 for industrial safety). Organisations must ensure that updates, patches, and system changes do not unintentionally compromise safety conditions.

CxOs must foster collaboration between IT, OT, safety engineering, and vendor management teams to address these cross-cutting concerns.

2.26.4 Legal and Regulatory Dimensions

Security and safety responsibilities are increasingly being shaped by regulation. The EU's NIS2 Directive, the Digital Operational Resilience Act (DORA), and sector-specific frameworks all impose requirements for managing third-party risk, reporting incidents, and ensuring resilience.

In regulated sectors, failure to ensure vendor compliance can lead to legal liabilities or reputational damage. Clauses related to encryption, data localisation, lawful access, or critical infrastructure classification must be carefully managed within contracts and operational practice.

Furthermore, safety standards may require traceability of all software components used, especially if they can influence critical functions.

2.26.5 Building a Resilient and Safe Ecosystem

A resilient and safe ecosystem does not depend on trust alone; it must be supported by systematic controls, layered defences, and collaborative governance. This includes:

- Maintaining inventories of all third-party components (including transitive dependencies);
- Requiring vendors to disclose vulnerabilities and provide update mechanisms;
- Validating software integrity through code signing and SBOMs;
- Performing regular penetration testing, including supply chain elements;
- Ensuring coordinated disclosure and response plans across the ecosystem.

Organisations must strike a balance between the benefits of outsourcing and the risks of losing visibility or control. While absolute safety and security may be unachievable, robust frameworks, proactive governance, and clear accountability can significantly reduce exposure.

2.27 Metrics and Performance Indicators in IS Governance

Information Systems governance involves directing and controlling the use of IT to support the organisation's goals, manage risk, and ensure value delivery. To be effective, governance must be measurable. Metrics and performance indicators provide the basis for monitoring progress, assessing outcomes, and enabling informed decision-making.

Well-chosen indicators transform abstract principles into operational feedback mechanisms. They support transparency, drive accountability, and offer evidence for regulatory compliance or strategic alignment. However, selecting appropriate indicators is not trivial: poor metrics can obscure reality, incentivise the wrong behaviours, or foster complacency.

2.27.1 Types of Metrics and Indicators

In the context of IS governance, metrics and performance indicators generally fall into three broad categories:

- **Strategic indicators**: These relate to business alignment, investment performance, innovation outcomes, or contribution to mission. Examples include IT portfolio value contribution, project success rate, or digital maturity assessments.
- **Operational indicators**: These focus on efficiency, availability, or service delivery. Examples include system uptime, mean time to repair (MTTR), or service desk response times.
- **Risk and compliance indicators**: These capture exposure, control effectiveness, or regulatory performance. Examples include number of unpatched vulnerabilities, audit findings, data breach incidents, or compliance coverage for key controls.

Depending on the governance framework defined (that might be inspired by COBIT, ITIL, or ISO/IEC 27001) organisations may adopt standard indicator sets or customise them to their context.

2.27.2 Characteristics of Good Indicators

For metrics to be useful in governance, they must be:

- **Relevant** to governance objectives and decision-making needs;
- **Actionable**, meaning they can trigger corrective or improvement actions;
- **Reliable**, based on accurate and reproducible data;
- **Comparable**, either over time or across units;
- **Balanced**, avoiding over-optimisation of one area at the expense of others.

Indicators should be integrated into governance dashboards, periodic reviews, and strategic planning processes. Moreover, the number of indicators should be manageable: too many metrics dilute focus, while too few may oversimplify complex dynamics.

2.27.3 CxOs and Perfiormance Indicators

CxOs use performance indicators not only to assess internal capabilities, but also to communicate with stakeholders, justify investments, and shape long-term priorities. For instance:

- A **CIO** might be motivated to monitor IT service quality, investment ROI, and digital enablement metrics.
- A **CTO** may focus on system scalability, architecture efficiency, or innovation throughput.
- The **CISO** uses indicators such as threat detection times, incident resolution performance, control maturity, or user awareness levels.

In many cases, governance indicators are shared with the board, regulators, or external partners. CxOs must ensure consistency and clarity in such reporting.

2.27.4 Emerging Trends and Challenges

With the growing adoption of agile and DevOps practices, traditional metrics are being complemented by new forms of continuous measurement, including deployment frequency, change failure rates, and user experience metrics.

At the same time, regulatory environments increasingly require evidence-based compliance.

Frameworks such as NIS2, DORA, or the GDPR introduce formal reporting requirements and risk-based thresholds, which often can be supported by metrics.

Challenges persist in areas such as:

- Measuring intangible outcomes like trust, innovation, or culture;
- Integrating data from fragmented tools or services;
- Avoiding metric manipulation or focusing on vanity metrics.

Organisations must also adapt metrics as their governance priorities evolve.

2.27.5 Metrics in Practice

Good governance metrics are not static: they evolve alongside strategy, technology, and risk landscapes. Periodic review and stakeholder input help ensure their continued relevance. Automation, data integration, and real-time analytics are increasingly important in enabling timely insights.

Ultimately, the value of metrics lies not in the numbers themselves, but in how they are interpreted and acted upon. Mature organisations use indicators to create shared understanding, prioritise efforts, and learn from performance patterns—both in success and failure.

2.28 Frameworks for Information Systems Management

Frameworks play a foundational role in structuring how organisations manage and govern their information systems. They offer reference models, standardised practices, and guidance for aligning technology with business objectives, managing risk, ensuring compliance, and delivering value. For those in key governance and management roles, familiarity with relevant frameworks is essential to promote coherence, transparency, and maturity across digital initiatives.

Rather than imposing rigid procedures, frameworks help create shared language and structured thinking. Their adoption also facilitates external benchmarking, certification, and communication with auditors, regulators, and stakeholders.

2.28.1 Types of Frameworks and Their Purposes

Different frameworks address different aspects of information systems management. The most widely used can be grouped into several categories:

- Governance and management of IT:
  - *COBIT* (Control Objectives for Information and Related Technologies) focuses on governance, value delivery, and risk management of enterprise IT.
  - *ITIL* (Information Technology Infrastructure Library) provides best practices for IT service management (ITSM), including service lifecycle, roles, and continuous improvement.
  - *ISO/IEC 38500* offers high-level principles for corporate governance of IT.
- Security and risk management:
  - *ISO/IEC 27001* is a globally recognised standard for information security management systems (ISMS).
  - *NIST Cybersecurity Framework (CSF)* provides a flexible model for managing and improving cybersecurity posture.
  - guides risk management practices are, for example, *ISO/IEC 31000 (generic reference), ISO/IEC 27005 (information security)*, and *COSO ERM* (Enterprise Risk Management).
- Architecture and systems development:
  - *TOGAF* (The Open Group Architecture Framework) supports enterprise architecture development.
  - Frameworks exist for *Agile* and *DevOps*, as guide for adaptive, iterative approaches to development and operations integration.
- Regulatory and sector-specific frameworks:
  - *GDPR* and the *NIS2 Directive* provide legal obligations related to data protection and cybersecurity in the EU.
  - *DORA* addresses operational resilience in the financial sector.
  - Specific standards apply in domains such as healthcare (e.g. HL7), energy, and transportation.

Each framework reflects particular assumptions, cultural models, and target audiences. Their application depends on organisational context, maturity level, and sector-specific needs.

2.28.2 Selecting and Adapting Frameworks

No single framework addresses all aspects of information systems management. Most organisations adopt a **hybrid approach**, combining elements from several frameworks to meet their objectives. The CIO and their governance team are often responsible for selecting which frameworks to adopt, how to integrate them into internal policies, and how to monitor compliance and effectiveness.

Frameworks must be adapted to the scale, complexity, and regulatory environment of the organisation. Overly rigid implementation may lead to bureaucratic overhead, while informal adoption may reduce their effectiveness. Maturity models (e.g. CMMI) can support phased implementation and continuous improvement.

2.28.3 Benefits and Challenges

Leadership plays a vital role in setting the tone for meaningful adoption and integration into everyday management. The benefits of using established frameworks include:

- Structured guidance for policy development and process design;
- Improved alignment between IT and organisational strategy;
- Consistency in risk and compliance management;
- Greater credibility and trust with external stakeholders;
- Facilitated audits and certifications.

However, challenges include:

- Misalignment between framework assumptions and organisational culture;
- Resistance to change or process formalisation;
- Fragmentation when multiple frameworks are poorly integrated;
- Superficial adoption driven by compliance rather than internal commitment.

2.28.4 From Formalism to Organisational Learning

Frameworks stimulate shared language across business and IT, clarify responsibilities, and create space for dialogue about value, risk, and priorities. However, frameworks are not ends in themselves, but tools. Their true value lies in **embedding structured reflection and disciplined thinking**. Therefore, mature organisations use frameworks not as checklists, but as instruments of organisational learning and sources to define their own management systems. Ultimately, effective information systems management depends not only on which frameworks are chosen, but on how they are used to guide decisions, allocate responsibility, and support continuous improvement.

2.29 International and National Governance of Cybersecurity

Cyber Resilience refers to the capability of an organisation to prepare for, respond to, and recover from cyber threats and incidents while continuing to deliver essential services and maintain critical operations. It extends beyond traditional notions of cybersecurity by integrating risk management, business continuity, and organisational adaptability. A cyber-resilient organisation anticipates disruptions, protects its information assets, detects intrusions, and adapts its operations to ensure rapid recovery. Rather than aiming solely to prevent breaches, the focus is on sustaining operational integrity under persistent and evolving threats and related **Cybersecurity**.

Cybersecurity is not only a technical challenge, but also a matter of governance, policy, and institutional coordination. In the European context, the implementation of cybersecurity measures is embedded in a multi-level governance framework. Supranational institutions such as the European Union play a central role in shaping regulatory frameworks and supporting Member States. At the national level, specialised cybersecurity centres are established to coordinate the implementation of national strategies, provide operational support, and foster collaboration between the public and private sectors.

The integration of governance structures at both European and national levels reflects the increasing importance of cybersecurity to digital sovereignty, resilience of critical infrastructures, and trust in digital services.

2.29.1 ENISA and the European Cybersecurity Governance Framework

The European Union Agency for Cybersecurity (ENISA) is the key institution supporting the development of a high level of cybersecurity across the EU. Established in 2004 and significantly reinforced by the Cybersecurity Act (Regulation (EU) 2019/881), ENISA operates with a dual mandate: it acts both as a centre of expertise and as a facilitator for cooperation among Member States, EU institutions, and stakeholders.

Core responsibilities of ENISA include:

- Supporting the development and implementation of EU cybersecurity policy and legislation, including the NIS2 Directive.
- Coordinating cybersecurity capacity-building across the EU, notably through support for the Computer Security Incident Response Teams (CSIRTs) Network.
- Managing the EU Cybersecurity Certification Framework, which provides harmonised schemes for ICT product and service assurance.
- Facilitating the exchange of threat intelligence and promoting the development of good practices and guidelines.

ENISA also organises the “Cyber Europe” exercise, one of the largest cybersecurity simulation events in the world, and publishes threat landscape reports that inform policymakers and industry stakeholders.

2.29.2 National Cybersecurity Centres in the EU

All EU Member States are required to designate national competent authorities for cybersecurity, in line with the NIS2 Directive. Most have established dedicated cybersecurity centres or agencies that serve as focal points for strategy, coordination, incident response, and stakeholder engagement. These centres typically:

- Lead the implementation of national cybersecurity strategies.
- Coordinate with critical infrastructure operators and essential service providers.
- Operate or host national CSIRTs.
- Promote awareness, training, and education.
- Engage in international cooperation, especially with ENISA and other Member States.

The existence of such institutions enables a harmonised yet locally adapted approach to cybersecurity, and supports the development of national capacities aligned with European strategic objectives.

2.29.3 The Portuguese National Cybersecurity Centre (CNCS)

In Portugal, the National Cybersecurity Centre (Centro Nacional de Cibersegurança – CNCS) is the national authority responsible for cybersecurity policy coordination and implementation. It operates under the supervision of the High Council for Cybersecurity and is an entity integrated within the National Security Office (Gabinete Nacional de Segurança), which:

- Coordinates the **National Cybersecurity Strategy** and monitors its execution.
- Supports the definition and implementation of security requirements for operators of essential services.
- Hosts the national CSIRT (CERT.PT), responsible for managing cybersecurity incidents and supporting public administration, critical sectors, and private entities.
- Provides guidance, training, and awareness activities across sectors.
- Acts as Portugal’s liaison with ENISA and contributes to EU-wide initiatives and policies.

The CNCS also fosters collaboration with academia and industry, promoting innovation in cybersecurity and contributing to national resilience in the face of evolving threats.

2.29.4 Strategic Relevance and Governance Maturity

Institutions such as ENISA and the CNCS play a pivotal role in advancing governance maturity. Their actions go beyond operational response, enabling a strategic and systemic approach to managing cybersecurity risk. They foster alignment between national and EU strategies, promote consistency in standards and practices, and create a governance environment in which CxO roles can operate with clarity and purpose.

2.30 Cybersecurity Governance in Portugal

The Portuguese National Cybersecurity Centre (Centro Nacional de Cibersegurança – CNCS) is the national authority for cybersecurity, operating under the High Council for Cybersecurity and integrated in the National Security Office (Gabinete Nacional de Segurança). Its mission is to contribute to the operational security of cyberspace in Portugal, supporting the implementation of national cybersecurity strategies and promoting resilience in critical sectors.
The CNCS plays a central role in both strategic coordination and operational support. It acts as a trusted point of contact for EU institutions such as ENISA, and facilitates communication and cooperation among national stakeholders, including public administration, critical infrastructure operators, and private sector organisations.

2.30.1 Public Administration Obligations

Entities within the Portuguese public administration have defined responsibilities in relation to cybersecurity and the CNCS, namely:

- **Implementation of cybersecurity measures** as defined in national strategies and technical guidelines issued by the CNCS.
- **Cooperation with CERT.PT** (the national incident response team) in the detection, reporting, and management of cybersecurity incidents.
- **Mandatory reporting of incidents** classified as significant, in line with national legislation and EU directives such as NIS2.
- **Participation in national cybersecurity exercises**, awareness programmes, and capacity-building activities promoted by the CNCS.
- **Designation of security contact points**, particularly for entities operating critical or essential services.

The CNCS also provides guidelines and frameworks to support compliance, and monitors adherence to security baselines. Public administration bodies are encouraged to integrate cybersecurity principles early in service design and infrastructure planning.

2.30.2 Private Sector and Operators of Essential Services

Private organisations, particularly those classified as **Operators of Essential Services (OES)** or **Digital Service Providers (DSPs)** under national transposition of the NIS Directive, are subject to regulatory obligations coordinated by the CNCS. These obligations include:

- **Risk management and incident prevention**, with a duty to implement adequate technical and organisational security measures.
- **Incident notification obligations**, including thresholds for mandatory reporting and cooperation with CNCS and CERT.PT.
- **Audit and compliance**, which may include assessments or inspections carried out under CNCS coordination.
- **Alignment with national and European cybersecurity frameworks**, including participation in certification schemes and adoption of security standards.

Beyond OES and DSPs, the CNCS engages with a broader set of business organisations through awareness campaigns, training programmes, and sectoral partnerships, especially in finance, health, energy, and transport.

2.30.3 Guidance, Capacity Building and Strategic Support

In addition to its supervisory and regulatory functions, the CNCS also has an important **supportive and educational role**. It publishes:

- **Guidelines and technical documentation** on risk assessment, cloud security, supply chain risk, and resilience.
- Annual threat landscape reports and trend analyses.
- **Training and certification programmes**, including the National Cybersecurity Skills Framework.

It also contributes to national and EU research initiatives, promotes cooperation between academia and industry, and plays a key role in strengthening national cyber capacity.

2.30.4 Cybersecurity and Governance Maturity

The activities coordinated by the CNCS contribute to a more mature governance environment in Portugal. By aligning cybersecurity practices with governance frameworks, the CNCS supports not only compliance but also strategic risk management, operational continuity, and public trust in digital services.
Public and private organisations that proactively engage with CNCS guidance and frameworks tend to demonstrate greater maturity level in cybersecurity governance and overall digital resilience.

2.31 CxO Dilemmas

The management of information systems within complex organisations often requires navigating tensions between competing goals, constraints, and risks. As digital ecosystems evolve to rely more heavily on external vendors, intricate supply chains, formalised frameworks, and data-driven decision-making, new challenges arise, both strategic and operational. This sheet explores recurring dilemmas faced by those in roles of CxO, particularly in the governance of digital dependencies and performance.

2.31.1 Control vs. Dependence

A central dilemma is the balance between leveraging external capabilities and maintaining internal control. Outsourcing to vendors offers flexibility, cost-efficiency, and access to innovation, but it also introduces dependency and reduces direct oversight. CIOs and CISOs may find themselves accountable for outcomes they cannot fully control, particularly when core services are delivered through cloud platforms, offshore development, or third-party data processors.

The challenge is compounded when subcontractors or open-source components are embedded deep within the supply chain, making accountability diffuse. Mechanisms such as contracts, audits, and monitoring tools help, but do not eliminate the structural vulnerability.

2.31.2 Compliance vs. Agility

CxOs must ensure that systems and services comply with an expanding landscape of regulations, including data protection, cybersecurity, resilience, and safety standards. At the same time, organisations must remain agile to respond to market shifts, adopt emerging technologies, and innovate.

This creates tension between procedural rigidity (often introduced by frameworks or audit requirements) and the need for adaptive, experimental approaches. Agile, DevOps, or continuous delivery challenge traditional governance models, especially when performance indicators are tied to pre-defined plans rather than outcomes or learning.

2.31.3 Measuring What Matters

Metrics are essential for governance, but selecting and interpreting them poses several dilemmas. Some metrics are easy to collect (e.g. uptime, incident counts) but may offer limited insight. Others, like user trust or strategic alignment, are harder to quantify but potentially more meaningful.

There is a risk of **metric distortion**, where teams optimise for what is measured rather than what matters, or where vanity metrics obscure poor performance. Moreover, performance indicators that work well in stable environments may mislead in turbulent or innovative contexts.

2.31.4 Integration of Frameworks

Frameworks provide structure and credibility, but their integration can be difficult. Organisations often attempt to apply multiple frameworks simultaneously (such as COBIT for governance, ITIL for service management, ISO 27001 for security, and Agile for delivery) without a coherent overarching model.

This can result in duplication, contradictions, or gaps in responsibility. CIOs and governance bodies must often mediate between formal requirements and operational realities, choosing what to standardise and where to allow flexibility.

2.31.5 Transparency vs. Confidentiality

Vendor oversight and supply chain risk management require transparency about components, dependencies, and practices. Yet vendors may resist disclosing such details, citing intellectual property or security concerns. Organisations must negotiate access to audit information, code provenance, or third-party dependencies while respecting confidentiality.

This dilemma becomes more acute in regulated environments or when public trust is involved. Transparency is essential for due diligence and incident response, but it must be managed with care to avoid legal or reputational consequences.

2.31.6 Accountability in Shared Ecosystems

Digital service delivery often takes place within **shared ecosystems**, such as cloud infrastructures, software platforms, or federated data spaces. When something fails, it is not always clear who is responsible, particularly in multi-tenant or multi-supplier scenarios.

CxOs must often navigate contractual ambiguity, overlapping roles, and fragmented governance. Establishing clear escalation paths, joint governance boards, and shared incident handling procedures can help—but require investment in coordination and trust.

2.31.7 Final Reflection

The governance of information systems is not only a technical or procedural challenge—it is a socio-technical one. It involves choices under uncertainty, trade-offs between competing goals, and coordination across organisational boundaries. There are no perfect solutions, only informed positions that balance risk, opportunity, and accountability.

Mature organisations do not eliminate dilemmas; they manage them with foresight, transparency, and adaptive governance structures. For a CxO, this means not only mastering frameworks and metrics, but also developing judgment, influence, and institutional learning capacities.

2.32 Oops…

2.32.1 The Chain of Trust That Broke Itself

Tomás, a junior consultant on the **Mature Team**, is assigned to assist a well-established financial institution implementing a new data governance framework.

The institution, led by CFO **Helena**, prides itself on precision, legacy, and control. The assignment seems structured: the framework has been chosen, responsibilities charted, and a steering committee is already in place. Tomás is tasked with helping define performance indicators and assist in documentation.

As weeks pass, it becomes clear that implementation is slow. Steering committee meetings are postponed. Risk managers show up unprepared. Legal and IT teams exchange conflicting interpretations of retention policies. Most concerning: no one seems to know who has final authority to resolve disputes.

Laura, the senior consultant, probes gently. Helena insists the plan is solid, just delayed. But Tomás, quietly observant, notices something deeper: the governance structure exists on paper, but lacks lived ownership. People comply, but without conviction. When asked why a rule exists, staff often respond with, "It was in the last audit report," rather than any strategic rationale.

Tomás proposes a workshop to explore why the project matters and who needs to lead. Helena agrees, reluctantly. The workshop is revealing: the core issue is a collapse in cross-departmental trust. Legal doesn't trust IT's enforcement; IT doesn't trust that business owners will maintain their registries; business units don't see why they should change at all.

The team steps back. With Helena's support, Laura and Tomás reshape the approach, not by changing the framework, but by re-establishing purpose and clarifying what "good governance" means for this specific organisation. The new focus is on shared understanding, not just compliance.

The implementation eventually resumes, but the delay served a purpose. It highlighted that a governance initiative cannot succeed without cultural alignment and interpersonal trust. For Tomás, it was a lesson in the difference between procedural authority and authentic leadership.

2.32.2 The Vendor Took the Lead — And Ran With It

Bruna, the junior consultant from the **Contingent Team,** joins a late-stage implementation of a cloud-based case management platform in a public health agency.

The vendor has been chosen, the platform is being configured, and project milestones are being celebrated by leadership. Bruna's role is to support final stage testing and help draft operational guidance.

As she observes daily briefings, Bruna grows uneasy. The vendor appears unusually dominant: they drive meeting agendas, control timelines, and decide priorities. The internal IT team is reduced to logistics, while operational leads defer to the vendor's project manager.

Bruna flags this dynamic to **Ricardo**, her senior. Together, they dig deeper. They discover that key data governance decisions (about access rights, retention policies, and audit trails) have been made unilaterally by the vendor team. No formal change requests were logged. Internal responsibilities are unclear. In one alarming case, sensitive personal data was being mirrored in a test environment without proper anonymisation.

Ricardo calls an urgent alignment session. Agency leadership is surprised. "They're the experts," someone says of the vendor. "We assumed they'd follow best practices." But no one had verified which practices were being followed, or whether they met the agency's legal obligations.

With diplomacy and rigour, Ricardo and Bruna help the client reassert control. Governance roles are reassigned. Data protection officers and internal IT regain visibility. The vendor is kept on board, but under stricter contract terms and clearer reporting duties.

The project is delayed, but reputational damage is avoided. Bruna reflects that what seemed like mere coordination at first glance was actually a deep issue of accountability. Expertise can be helpful—but only when it operates within a clear framework of oversight.

These stories serve as reminders that governance failures are not always dramatic. Often, they emerge quietly, through unchallenged assumptions, neglected trust, or outsourced control. But even in such scenarios, attentive consultants and thoughtful clients can recalibrate direction before harm is done.

2.33 …What? …

2.33.1 Same Ambition, Different Endings

Carla and **Laura** are each engaged in a consulting role on behalf of **WiseConsult** to help a costumer in the private sector eager to adopt new AI tools to automate decision-making in customer service. The goal are reduce costs, streamline interactions, and stay competitive. The outcomes, however, are not.

The CIO in the costumer is **Alex**, a fast-moving executive who wants results "by next quarter."

Carla, energised by the urgency, skips the usual stakeholder analysis and dives into prototyping with the AI vendor. She trusts the AI engine's training data, provided by the client's marketing team, and quickly delivers a chatbot model to demo. Alex is impressed by the speed and greenlights the rollout.

But weeks after launch, complaints flood in. Customers say the chatbot gives inconsistent answers and avoids escalation. A regulatory audit reveals that the model was trained on biased historical data, leading to discriminatory outcomes in how complaints were prioritised. Carla scrambles to respond, but the project is suspended, and the company faces reputational harm.

Laura, meanwhile, faces the same brief, but approaches it differently. Her first move is to assemble a cross-functional working group, including customer service, compliance, and IT security. She challenges the AI vendor's off-the-shelf solution, asking for transparency in the training data and model assumptions.

Progress is slower, but when rollout begins, the system includes an escalation matrix, logging for auditability, and feedback loops for learning. An internal review even praises the project as a benchmark for responsible innovation. The CEO highlights the initiative in the company's ESG report.

Carla's takeaway: speed without structure can amplify harm. Laura's lesson: governance is not the opposite of innovation, it's what makes innovation sustainable.

2.33.2 When Data Protection Is Just a Word

Inês and **Lucas** are each engaged in a consulting role on behalf of **WiseConsult** supporting public sector clients undergoing digital transition.

Both engagements involve personal data processing and require privacy impact assessments. The clients are politically visible and under public scrutiny.

Inês is working with **Lucas**, a visionary executive frustrated by what he calls "paperwork rituals." He wants to launch a citizen-facing mobile app before the next fiscal review.

Inês, captivated by the opportunity to "make real impact," decides to fast-track the project. She encourages her team to draft basic documentation but skips formal Data Protection Impact Assessment (DPIA) procedures, assuming they can be completed retroactively.

When the app launches, civil society groups raise concerns over geolocation tracking and lack of clear consent mechanisms. The national data protection authority opens an inquiry. The press picks up the story. Lucas distances himself from the consultants, and the project's reputation is tarnished.

Meanwhile, Sofia is working with **Verónica**, a cautious executive in another public agency. From the outset, Sofia insists on including the DPO and legal team in design discussions. She explains how DPIA is not just a checklist but a process that protects the organisation from later disruptions.

The process adds a few weeks, but results in clearer choices: anonymisation in reporting dashboards, opt-in for sensitive features, and a fallback plan for data minimisation. The rollout is uneventful. A year later, the project wins a national award for digital inclusion.

Inês's lesson: skipping governance may feel bold, but it often leaves others to clean up the mess. Sofia's success reminds us that even under pressure, procedural rigour can enable trust and resilience.

In each story, the same types of challenges (AI adoption, data governance, pressure to deliver) lead to diverging outcomes. The difference is not in technical capacity, but in how governance is treated: as a constraint to dodge, or as an enabler to embrace. These contrasting narratives show that sustainable impact requires not just ideas and drive, but discipline and care.

2.34 OK!

2.34.1 Everything Lined Up, Almost

Sofia and Mateus from the Dream Team are brought into a mid-sized public agency to help restructure its internal risk management process. The executive sponsor, Verónica, is respected for her clarity and measured leadership.

The timing is favourable: a new strategic plan is being finalised, and staff morale is high. Everyone agrees the time is right to update the risk register and align it with digital transformation priorities.

The engagement begins smoothly. Stakeholders are engaged, workshops are well attended, and the agency's governance team is responsive. The consultants help map risks across strategic, operational, and compliance domains. A new dashboard is designed, blending qualitative assessments and KPIs from various departments.

Then, just before final approval, an issue arises: two departments disagree over how to classify a recurring data handling exception. It's a small technical point but becomes politically sensitive because it touches on past incidents.

Sofia suggests a short facilitated session with both teams. She asks Mateus to prepare a neutral scenario to discuss consequences, not blame. The meeting is productive. A compromise is reached, and more importantly, a procedural fix is identified that prevents future recurrence.

The updated risk register is adopted, and the executive board praises the process as a model of internal collaboration. Verónica later reflects that while the issue was minor, the way it was handled avoided a major political distraction.

Lesson learned: even when alignment exists, governance requires active listening, early detection of friction points, and a commitment to integrity in small decisions, not just big ones.

2.34.2 Walking the Tightrope, with a Net

Ricardo and Bruna from the Contingent Team are engaged in a critical infrastructure company operating under strict regulatory oversight.

The task: review operational resilience in one of the company's distributed facilities, recently affected by extreme weather. A new European directive is pushing organisations to adopt more robust resilience frameworks, and the company wants to be ahead of the curve.

Bruna is responsible for mapping interdependencies across systems, some legacy, others cloud-based. She quickly notices that the existing documentation is outdated, but rather than raising alarm, she suggests using a simple dependency graph to visualise current workflows before any recommendations are made. Ricardo encourages her to present the draft in a joint meeting with IT, facilities, and operations leads.

To their surprise, the graph becomes a conversation starter, highlighting one previously unnoticed single point of failure involving a cooling system and a poorly documented backup protocol.

The finding does not cause panic. Instead, it triggers a constructive response. The team agrees to update contingency plans and invest in a secondary alert mechanism. Bruna is thanked for "making it visible before it became a reportable incident."

The audit later confirms compliance, and the company uses the work as a case study to demonstrate proactive governance to its supervisory board.

Lesson learned: being technically correct is not enough; clarity, timing, and the ability to communicate potential risk in non-threatening ways are essential parts of a mature governance posture.

These two stories show that "success" in governance and IT management is not just about avoiding failure. It's about how risks are framed, how relationships are nurtured, and how attention to detail creates resilience. Even when things go well, there's always more to learn, especially about the human side of structured decision-making.

2.35 Wrap-up…

Below is a list that summarises the foundational concepts for Theme 2 (understanding these ideas is essential for interpreting how organisations govern their technology assets, manage digital risk, and align IT with strategic objectives):

- **Governance of IT** – The structures, processes, and leadership responsibilities that ensure IT supports and extends an organisation's goals, while managing associated risks and complying with external obligations.
- **IT Management** – The planning, development, delivery, and monitoring of IT services and resources to meet organisational needs, typically focused on operational efficiency, service quality, and resource control.
- **Strategic Alignment** – The process of ensuring that IT initiatives, investments, and services directly support and enable the broader business or organisational strategy.
- **Accountability and Decision Rights** – The formal assignment of authority and responsibility for IT-related decisions, ensuring that governance structures clearly define who is empowered to act and who is responsible for outcomes.
- **Risk and Compliance Integration** – The embedding of IT risk management and regulatory compliance into broader organisational governance structures, ensuring that digital risks are addressed proactively and transparently.
- **Leadership Roles and Governance Posture** – The influence of senior leadership, especially CxO roles such as CIO and CISO, on setting the tone, structure, and priorities of IT governance within the organisation.
- **CxO Participation at Board Level** – The involvement of senior IT leadership roles in strategic decision-making forums or in direct reporting to the Board of Directors. While they may not hold formal board seats (occasionally the CIO or CTO might seat, but really rarely that is the case of the CISO), their proximity to the board and their influence on strategic discussions serve as important indicators of IT governance maturity and strategic integration.
- **Business Governance versus IT Governance** – The distinction between overall organisational governance (mission, strategy, stakeholder engagement) and the specific governance of IT assets, capabilities, risks, and services.
- **Governance of IT Risks** – The identification, assessment, and mitigation of risks arising from IT activities, including cybersecurity, data protection, operational continuity, and third-party dependencies.
- **Information Governance** – The strategic management of information assets, including data quality, ownership, lifecycle control, privacy, and regulatory compliance.
- **Information Security Governance** – A subset of IT governance focused specifically on protecting information assets against threats and vulnerabilities, aligning security activities with risk appetite and strategic objectives.
- **Privacy Governance** – The structures and responsibilities ensuring that personal data is collected, used, stored, and shared in compliance with applicable laws (such as GDPR) and ethical standards.
- **Vendor and Contract Management** – The governance and management of third-party IT providers, ensuring that contractual relationships are structured to support strategic goals, manage risk, and maintain accountability.
- **IT Governance Frameworks** – Reference structures that organisations use to guide their governance of IT, such as COBIT, ISO/IEC 38500, or national public sector frameworks.
- **Operational Technology (OT) Governance** – The governance of technology systems that monitor or control physical processes (such as in manufacturing or energy sectors), addressing convergence and conflict between traditional IT governance and industrial operations.
- **Sectoral and Regulatory Contexts** – Recognition that IT governance practices vary significantly between industries (e.g., healthcare, finance, public sector) depending on regulatory obligations, risk profiles, and service expectations.
- **Ethical Governance in Information Systems** – The responsibility to ensure that IT decisions and systems respect human rights, fairness, transparency, and societal values, beyond mere compliance.
- **Governance of Algorithmic Systems** – The application of governance principles to systems driven by algorithms, especially AI, addressing risks of bias, opacity, lack of explainability, and decision-making accountability.
- **Data Governance Maturity** – The extent to which an organisation has formalised and embedded practices for managing its data assets, including quality, ownership, security, and compliance.
- **Governance Indicators and Metrics** – Tools and measurements used to assess the health, maturity, and effectiveness of IT governance structures, providing evidence for decision-making and continuous improvement.

Notes:

- Governance of IT is not about technology management alone; it is fundamentally about **strategic decision-making, accountability, and risk visibility** in the scope of the overall business
- Sector-specific differences matter: the way IT is governed in a hospital is not the same as in a retail company or a city council.
- In consulting or advisory roles, we must be able to **recognise governance gaps**, **evaluate maturity**, and, when in a role for that purpose (what itself requires an high level of maturity in consulting and advising), **propose improvements** using appropriate concepts and frameworks.

3 Theme: IT Operations Management

IT operations management encompass the practices, tools, and organisational roles that ensure the stable, secure, and efficient functioning of information systems and digital services. This theme explores the operational backbone of IT environments, highlighting the importance of structured service management, operational governance, risk mitigation, and responsiveness to change.

At the heart of IT operations management lies IT Service Management (ITSM), often guided by frameworks such as ITIL. These frameworks support consistent service delivery through processes like incident management, change control, problem resolution, and service level agreements (SLAs). SLAs define expectations around availability, performance, and response times, and are essential for accountability in both internal and outsourced contexts.

The theme also addresses change management, an area of growing complexity in dynamic digital environments. Structured approaches to change are needed to balance agility with stability, especially when adopting DevOps and continuous delivery models. These models blur traditional boundaries between development and operations, enabling faster deployment cycles while introducing new coordination and governance demands.

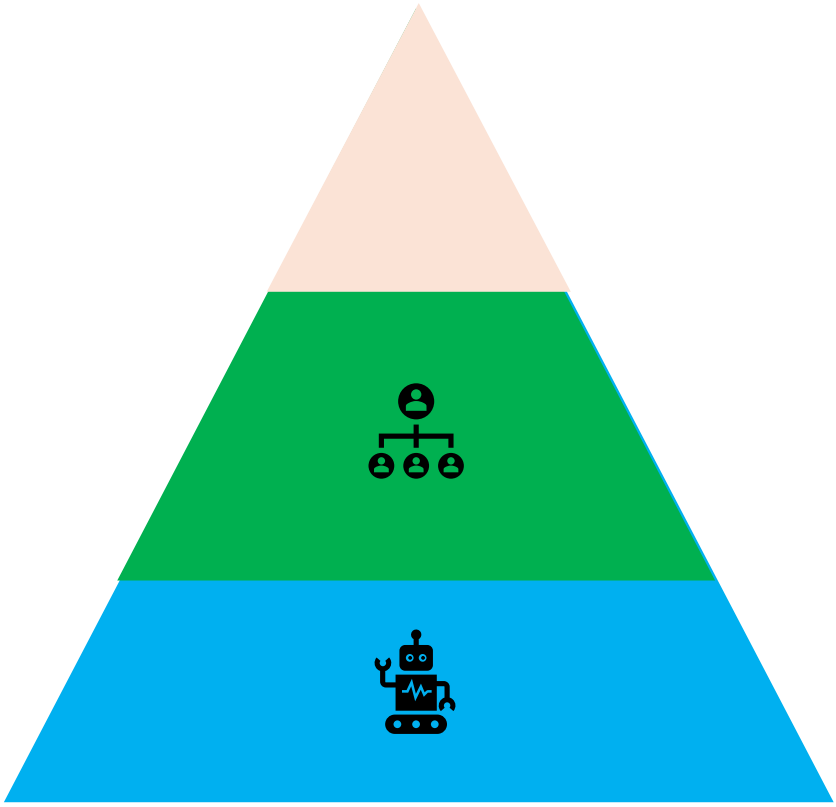
Operational maturity is examined through tools such as performance indicators, dashboards, and lifecycle management practices. Mature organisations monitor system health, track configuration changes, and ensure alignment between IT services and organisational priorities. This involves not only technical practices, but also cultural readiness and cross-functional collaboration.

Licensing models are another critical aspect of IT operations management. Organisations must navigate a mix of perpetual, subscription-based, and consumption-based licences, often across on-premises and cloud platforms. This affects budgeting, compliance, and long-term flexibility. Multi-tenant environments, especially in cloud contexts, introduce additional governance challenges related to data segregation, service continuity, and regulatory compliance.

Security and resilience are foundational concerns. Threat monitoring, incident response planning, and backup strategies are operational necessities in a landscape marked by cyber threats and increasing regulatory scrutiny. Operational governance includes not just technical controls, but also reporting structures and escalation paths for decision-making.

The theme recognises the differences between public and private sector operational contexts. Public services must balance cost-efficiency with equity, transparency, and accountability. Meanwhile, private sector entities may prioritise speed and competitiveness but face risks from service failures or reputational damage.

In sum, IT operations management are not merely technical. They are strategic, integrative, and deeply tied to organisational risk posture and value delivery. High-functioning operations depend on clear roles, mature processes, robust infrastructure, and governance mechanisms that adapt to evolving demands.



3.1 IT Service Management

IT Service Management (ITSM) refers to the structured approach organisations use to design, deliver, manage, and improve the way IT services are used. It places emphasis on aligning IT services with the needs of the business and delivering value through a combination of people, processes, and technology. While IT operations management traditionally focused on systems and infrastructure, ITSM encourages a more holistic view, treating IT as a service provider that supports business outcomes.

At the core of ITSM is the idea that IT services should not only be reliable and efficient, but also demonstrably contribute to the strategic goals of the organisation. To this end, ITSM frameworks help organisations manage incidents, problems, changes, service requests, configurations, and more, using standardised procedures and continuous improvement mechanisms.

3.1.1 The Role of Frameworks in ITSM

Over time, various frameworks and standards have emerged to support ITSM. Among the most influential are ITIL (Information Technology Infrastructure Library) and ISO/IEC 20000, and others like COBIT. While some are standards with certification schemes (e.g., ISO/IEC 20000), others are collections of best practices (e.g., ITIL).

ITIL, in particular, has become the de facto global standard for ITSM. First developed by the UK Government's Central Computer and Telecommunications Agency (CCTA) in the 1980s, ITIL has evolved through several iterations, most recently ITIL 4, which reflects the need for greater flexibility, agility, and integration with most recent approaches such as Agile, Lean, and DevOps.

3.1.2 Foundations of ITIL

ITIL 4 is structured around a service value system (SVS), which integrates multiple components and activities to facilitate value creation through IT-enabled services.

Key concepts introduced in ITIL 4 include:

- **Service**: A means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks.
- **Value**: The perceived benefits, usefulness, and importance of something.
- **Service Management**: A set of specialised organisational capabilities for enabling value for customers in the form of services.

ITIL 4 highlights seven guiding principles, drawn from earlier versions and contemporary methodologies:

1. Focus on value
2. Start where you are
3. Progress iteratively with feedback
4. Collaborate and promote visibility
5. Think and work holistically
6. Keep it simple and practical
7. Optimise and automate

These principles are intended to support decision-making and guide behaviour at all levels of the organisation.

3.1.3 Processes and Practices in ITIL

ITIL distinguishes between **practices** (sets of organisational resources for performing work or accomplishing an objective) and traditional **processes** (which tend to be more linear and task-driven).

Examples of practices in ITIL 4 include:

- **Incident Management**: Restoring service operation as quickly as possible.
- **Problem Management**: Identifying and addressing the root causes of incidents.
- **Change Enablement**: Ensuring that changes are made with minimal risk and disruption.
- **Service Request Management**: Handling requests from users.
- **Service Level Management**: Ensuring services meet agreed performance standards.
- **Continual Improvement**: Ongoing identification and implementation of improvements.

These practices support the broader **service value chain**, which includes activities such as planning, improving, engaging, designing and transitioning, obtaining/building, and delivering/supporting.

3.1.4 Strategic Relevance of ITSM

In organisations where IT is critical to operations, ITSM plays a central role in ensuring operational stability, customer satisfaction, and regulatory compliance. However, it also has a strategic dimension: mature ITSM capabilities allow the organisation to better manage complexity, respond to change, and align technology investment with business priorities.

From the perspective of CxO executive roles, ITSM provides both a language and a mechanism for ensuring that service delivery is efficient, controlled, and oriented toward outcomes that matter to the organisation. When well implemented, ITSM becomes a foundational enabler of change management and innovation.

3.2 Business Process Management

Business Process Management (BPM) *refers to the structured approach to analysing, designing, executing, monitoring, and optimising business processes to achieve organisational goals. It serves as both a management discipline and a technological practice, enabling organisations to align operations with strategic objectives, increase efficiency, and improve service quality.*

At its core, BPM aims to make work visible, measurable, and adaptable. It treats business processes as organisational assets to be actively managed over time, rather than as fixed routines or informal practices. This shift is especially relevant in complex or regulated environments, where traceability, performance, and continuous improvement are critical.

3.2.1 Understanding Business Processes

A business process is a structured set of activities or tasks that, when executed in a defined sequence, produce a specific outcome or value for internal or external stakeholders. Processes can be operational (e.g. processing claims), managerial (e.g. budget planning), or supporting (e.g. IT maintenance).

Processes often cut across departmental boundaries, involving multiple roles, systems, and information flows. Mapping and analysing these interactions is essential for identifying bottlenecks, redundancies, or compliance risks. Effective BPM requires understanding not just the sequence of steps, but also their purpose, dependencies, and performance metrics.

3.2.2 BPM Lifecycle

The BPM discipline is typically structured around an iterative lifecycle that includes:

- **Design**: Mapping the current ("as-is") process and modelling the desired ("to-be") process, often using notations such as BPMN (Business Process Model and Notation).
- **Implementation**: Executing process changes, which may involve automation, system integration, or changes in organisational roles and rules.
- **Execution**: Running the process using either manual procedures, digital tools, or Business Process Management Systems (BPMS).
- **Monitoring**: Collecting performance data to track effectiveness, efficiency, and compliance.
- **Optimisation**: Identifying opportunities for refinement or transformation, based on real-world feedback and strategic shifts.

This lifecycle promotes agility by enabling organisations to adapt processes in response to internal changes or external pressures.

3.2.3 BPM and Governance of IT

In the context of governance of IT, BPM is a foundational tool for aligning technology investments with business needs. By articulating what the organisation does and how it does it, BPM provides a structured context for identifying IT requirements, justifying projects, and evaluating impacts. It supports the requirements for compliance with standards and frameworks such as ISO 9001 (quality), ISO/IEC 27001 (information security), or ITIL (service management).

Moreover, BPM enables the identification of automation opportunities, such as Robotic Process Automation (RPA), and facilitates the integration of IT systems across silos. In large organisations or public administrations, explicit BPM approaches support transparency, accountability, and service evoluation.

3.2.4 Public Sector Relevance

In public sector entities, BPM plays a critical role in improving service delivery, ensuring compliance with administrative law, and implementing digital government strategies. Many public services are legally defined as processes and must be executed with consistency and traceability. BPM helps identify gaps between legal norms and operational practices, and supports initiatives such as process standardisation or interoperability across administrative units.

Public sector BPM efforts are often aligned with initiatives promoted by central agencies or shared service platforms, such as those coordinated by ESPAP or AMA in Portugal. BPM also supports audit readiness and performance evaluation, essential for managing public trust and institutional legitimacy.

3.2.5 Tools and Techniques

BPM can be supported by a range of tools and methodologies, including:

- Process modelling languages such as BPMN, EPC, or UML Activity Diagrams.
- Workflow and orchestration platforms (BPMS).
- Analytical techniques such as time-and-motion studies, value stream mapping, or process mining.
- Process performance indicators (PPIs) and dashboards.

Selection and application of tools should be adapted to the organisation's maturity, culture, and strategic priorities.

3.2.6 Strategic Implications

BPM is not merely a technical exercise, but a strategic capability. It enables organisations to shift from reactive problem-solving to proactive management of operations. When integrated with risk management, enterprise architecture, and change management, BPM becomes a central enabler of organisational agility and resilience.

3.3 Change Management

In any digitally dependent organisation, **change is continuous**, from updates to infrastructure and applications to transformations in business processes, regulatory requirements, or service delivery models.

Change management refers to the structured approach for ensuring that changes are introduced in a controlled and coordinated manner, with minimal risk to stability, security, and performance.

Change management is a critical function within **operational governance**, especially in environments subject to compliance obligations, public scrutiny, or safety requirements. It provides assurance that changes are assessed, authorised, documented, and reversible where necessary.

3.3.1 Types of Change

Changes vary widely in scope and impact. They can be classified into:

- **Standard changes**: Pre-authorised and low-risk, such as routine updates or configuration changes.
- **Normal changes**: Subject to formal assessment, approval, and scheduling processes.
- **Emergency changes**: Implemented quickly to resolve critical incidents, often followed by retrospective review.

Effective classification supports prioritisation and appropriate levels of control.

3.3.2 Change Management Lifecycle

A mature change process typically includes:

1. **Request for change (RFC)**: Initiated by technical teams, business owners, or external triggers.
2. **Impact assessment**: Technical and business evaluation of risks, dependencies, downtime, and compliance.
3. **Authorisation**: Decision by a change advisory board (CAB) or delegated authority.
4. **Implementation and testing**: Carried out by designated personnel, following defined procedures.
5. **Review and documentation**: Verifying that the change was successful and updating configuration records.

This process must be **embedded in operational workflows**, supported by tools such as IT service management platforms (e.g. ITSM, CMDBs), and aligned with standards such as **ITIL**, **ISO/IEC 20000**, or **COBIT**.

3.3.3 Change Control and Risk

Change is a leading source of operational incidents and security vulnerabilities. Inadequate change control may result in:

- Service disruption or degraded performance
- Configuration drift and loss of system integrity
- Security gaps or non-compliance
- Reputational damage

To mitigate these risks, organisations implement **segregation of duties**, **rollback procedures**, **test environments**, and **audit trails**. In regulated sectors, change documentation may be subject to external audits or reporting obligations.
Change management must be coordinated with **incident management**, **release management**, **ICT asset management**, and **configuration management**. This is especially critical when involve cloud environments, multi-tenant platforms, and hybrid infrastructures.

3.3.4 Organisational and Strategic Dimensions

Change management is not only a technical concern but also an **organisational capability**, which effectiveness depends on:

- **Leadership support** and alignment with strategic priorities
- Clear roles and responsibilities across business and IT units
- **Cultural readiness** for change, including communication and training
- **Balance between agility and control**, especially in DevOps or agile environments

In public sector contexts, additional constraints such as procurement procedures, legal accountability, or policy cycles may influence how change is managed and communicated.

3.3.5 Continuous Improvement

Change management itself must evolve. Metrics such as **change success rate**, **number of emergency changes**, or **mean time to implement change** can inform improvements. Automation and integration with development pipelines (e.g. in DevOps or GitOps[62] contexts) can also streamline governance without sacrificing control.
Ultimately, change management enables organisations to respond effectively to both planned initiatives and unforeseen challenges—without compromising the reliability, trust, and security of their digital operations.

[62] https://www.atlassian.com/br/git/tutorials/gitops

3.4 Models for Acquiring IT Solutions

When acquiring hardware or software solutions, organisations must evaluate not only technical and financial aspects but also the legal and strategic consequences of different acquisition models. These models influence long-term control, cost structures, upgrade paths, and compliance obligations. Understanding the licensing and ownership landscape is essential for aligning procurement decisions with organisational strategy, operational needs, and public sector policies.

3.4.1 Perpetual Licensing

Perpetual licensing grants indefinite usage rights upon payment of a one-time fee. Typically associated with on-premises installations, this model provides full access to a particular software version, with optional annual support or maintenance contracts. It ensures autonomy and control but may lead to higher upfront costs. Without a maintenance agreement, access to updates or security patches may be limited, increasing technical debt over time.

3.4.2 Subscription Licensing

Subscription models allow time-bound access to software or platforms, usually through monthly or annual payments. This structure ensures continuous updates, technical support, and improved scalability. Common in SaaS (Software-as-a-Service) environments, subscription licensing can reduce initial investment and align costs with usage. However, it implies ongoing dependency on the vendor and may result in higher total expenditure in stable environments with low variability.

3.4.3 Consumption-Based Licensing

In this model, payment is based on actual usage metrics—such as computing time, storage capacity, or API calls. Widely used in IaaS and PaaS contexts, this approach offers significant flexibility and cost-efficiency for variable or experimental workloads. It requires robust monitoring to avoid unexpected costs and is best suited to organisations with advanced operational governance.

3.4.4 Device-Based vs. User-Based Licensing

Licensing conditions often vary depending on the unit of usage. Device-based licences tie usage rights to specific hardware, while user-based licences follow named or active users. In organisations with fixed workstations or shared access, device-based models may be more efficient. In contrast, user-based licences favour highly mobile workforces and individual productivity tools. Some vendors also offer concurrent-user licences, where a maximum number of simultaneous sessions is defined.

3.4.5 Enterprise Licensing Agreements (ELA)

Large-scale customers often negotiate bundled licensing agreements that cover multiple products and services under a single contract. These ELAs may offer volume discounts, favourable upgrade paths, and audit protections. For example, in Portugal, the public sector benefits from framework agreements coordinated by ESPAP (Entidade de Serviços Partilhados da Administração Pública), which streamlines procurement, ensures standardised conditions, and promotes financial efficiency[63]. Entities opting into these agreements benefit from pre-negotiated legal terms and public sector compliance.

3.4.6 Contracted Development vs. Licensed Products

An important distinction arises between licensing a ready-made product and contracting the custom development of a software solution. In the licensing model, the intellectual property (IP) remains with the vendor; the client merely obtains usage rights under the agreed terms. This limits modification and redistribution, and places the client in a dependent position regarding maintenance and evolution.

In contrast, commissioning a software development project—often under a work-for-hire or service contract—can allow the client to retain full ownership of the resulting codebase. This includes the right to modify, reuse, or redistribute the software. However, it also transfers long-term responsibility for maintenance, security, and compliance. Clarity around IP ownership clauses is critical in such contracts, particularly in public procurement, where legal obligations and future vendor independence must be preserved.

3.4.7 Open Source and Community Licensing

Adopting open-source solutions under community licences[64],[65] (such as MIT, Apache, or GPL) offers low acquisition costs and high flexibility. These licences permit usage, modification, and redistribution, with varying conditions. While open-source adoption reduces vendor lock-in, it shifts responsibility for integration, support, and security to the organisation or to its third-party providers.

3.4.8 Strategic Considerations

The choice among these models depends on several factors: the stability and predictability of operations, regulatory obligations, IT maturity, available skills, and the role of the software in critical business processes. Public sector organisations must align choices with procurement law and long-term sustainability. Ownership, control, and exit strategy should be considered early in the acquisition process to avoid technical and legal entrapments.

[63] https://www.espap.gov.pt/FrontEnd/Paginas/Areas/SP_CP/SNCP/AcordosQuadro_tpl_1.aspx
[64] https://en.wikipedia.org/wiki/Open-source_license
[65] https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses

3.5 Technical Debt and System Evolution

Technical debt is a metaphor used to describe the long-term consequences of decisions that prioritise short-term convenience over long-term quality in system development and maintenance. These decisions may involve bypassing architectural rigour, reducing documentation, limiting testing, or delaying upgrades. While such choices can accelerate initial delivery or reduce immediate costs, they often accumulate hidden liabilities that impact the adaptability, security, performance, and maintainability of systems.

This concept is applicable to both software systems and broader socio-technical systems, including hardware infrastructure, data management practices, and process automation. Technical debt arises in contexts ranging from software development to enterprise architecture, and from public sector IT to private enterprise platforms.

3.5.1 Types and Sources of Technical Debt

Technical debt can be categorised in multiple ways, such as **deliberate vs accidental**, or **strategic vs inadvertent**:

- Deliberate debt may be accepted as part of a time-sensitive delivery plan, with the intention of repayment through refactoring or system redesign.
- Inadvertent debt, on the other hand, often results from a lack of knowledge, inadequate documentation, or poor design choices.

Sources of technical debt include:

- Hasty implementation due to time pressure or budget constraints
- Lack of adherence to architectural standards
- Inadequate testing or automation
- Poorly defined requirements or unstable specifications
- Use of outdated technologies or unsupported components
- Misalignment between system evolution and organisational strategy

3.5.2 Impacts on System Evolution

The presence of technical debt affects the capacity of an organisation to evolve its systems effectively. It can lead to:

- Increased cost and effort for future development or maintenance
- Decreased system reliability or performance
- Greater vulnerability to security threats
- Reduced team morale due to the difficulty of working with complex, fragile systems

When unaddressed, technical debt can constrain innovation and delay responses to new regulatory, market, or user demands. **It is especially problematic in large-scale or long-lived systems, where cumulative effects can dominate lifecycle costs**.

3.5.3 Governance and Management of Technical Debt

Managing technical debt requires visibility, measurement, and strategic planning. Practices may include:

- Incorporating technical debt analysis into architectural reviews
- Tracking known debt items in the same way as defects or features
- Prioritising refactoring or modernisation tasks within project backlogs
- Integrating technical debt metrics in project dashboards and executive reporting

In mature organisations, the management of technical debt is aligned with broader governance of IT and risk management frameworks. This ensures that decisions about deferring improvements or repaying debt are not made in isolation, but as part of strategic portfolio management.

3.5.4 Public versus Private Sector Considerations

In public sector contexts, technical debt often interacts with procurement constraints, legacy interoperability requirements, and changing legislative environments (that can create contradictory requirements, etc.). The visibility of technical debt may be lower due to outsourcing or limited internal technical capacity. However, its consequences can be far-reaching, constraining the future quality of services.

In the private sector, technical debt is frequently associated with innovation speed and time-to-market pressures. Organisations that effectively manage technical debt can respond more rapidly to new opportunities, while those that accumulate unmanaged debt may find themselves unable to scale or pivot when needed.

3.5.5 Conclusion

Technical debt is an unavoidable aspect of complex systems, but it can be managed with appropriate architectural foresight, governance practices, and lifecycle planning. Recognising its presence and impact is essential for ensuring the sustainable evolution of socio-technical systems over time.

3.6 Threat Monitoring

As organisations increasingly depend on digital technologies to conduct their operations, the risk landscape they face becomes more complex and dynamic. Threat monitoring is a fundamental component of information security management, aimed at identifying, assessing, and responding to potential security threats in real time or near-real time.

While preventative controls such as firewalls and access policies are important, they are not sufficient on their own. Threats evolve rapidly, often exploiting unknown vulnerabilities, insider misuse, or configuration weaknesses. Continuous monitoring allows an organisation to detect anomalies and potential intrusions early, helping to mitigate the impact of security incidents and reduce recovery times.

3.6.1 Core Concepts and Objectives

Threat monitoring involves the systematic collection, analysis, and interpretation of data from various sources to detect signs of malicious activity. The objectives include:

- Detecting unauthorised access attempts or policy violations.
- Identifying indicators of compromise (IoCs).
- Monitoring for data exfiltration, malware activity, and lateral movement.
- Supporting incident response and forensic investigations.
- Providing situational awareness to support risk-based decision-making.

Monitoring must be both comprehensive and context-aware. It requires not just technical signals, but also integration with asset inventories, threat intelligence feeds, and business priorities.

3.6.2 Sources of Data

Effective threat monitoring depends on the availability and correlation of diverse data sources.

Typical inputs include:

- **Logs**: From systems, applications, firewalls, and network devices.
- **Endpoint telemetry**: Including process activity, file changes, and registry access.
- **Network traffic analysis**: Detection of unusual patterns, data transfers, or command-and-control traffic.
- **Authentication records**: Login attempts, failed access, privilege escalation.
- **Threat intelligence**: Feeds describing known attack patterns, vulnerabilities, or indicators from external sources.

Data must be collected, normalised, and stored securely, enabling correlation and pattern recognition over time.

3.6.3 Tools and Platforms

Threat monitoring activities can be support by tools. Among the most common are:

- **Security Information and Event Management (SIEM)** systems: Aggregate log data from multiple sources, apply correlation rules, and generate alerts.
- **Endpoint Detection and Response (EDR)**: Focus on detecting and responding to threats at the device level.
- **Network Detection and Response (NDR)**: Monitor network traffic for suspicious behaviour.
- **User and Entity Behaviour Analytics (UEBA)**: Apply machine learning to detect deviations from normal usage patterns.
- **Threat Intelligence Platforms (TIPs)**: Aggregate and curate threat data for integration with monitoring tools.

The effectiveness of these platforms depends not only on their capabilities, but also on the quality of configuration, rule tuning, and integration with broader security processes.

3.6.4 Operational Considerations

For threat monitoring to be valuable, it must be part of a broader security operations strategy and ecosystem.

This includes:

- **Security Operations Centres (SOCs)**: Dedicated teams responsible for real-time monitoring, triage, and response.
- **Alert prioritisation**: Use of risk scores and contextual data to reduce false positives and avoid alert fatigue.
- **Integration with incident response**: Clear workflows to escalate and manage confirmed incidents.
- **Continuous improvement**: Feedback loops to refine detection rules and response playbooks over time.

Organisations must also address challenges such as encryption visibility, cloud monitoring, and integration across hybrid environments.

3.6.5 Strategic Role

From the viewpoint of roles such as CISO or CIO, threat monitoring is both an operational necessity and a strategic asset. It provides visibility into the current risk posture, supports compliance with legal and regulatory requirements, and builds resilience against disruption. Furthermore, it serves as an early warning system, enabling proactive measures to protect critical assets and maintain stakeholder trust.

As threats become more sophisticated, organisations must evolve from reactive to proactive monitoring approaches, including threat hunting and behavioural analytics. The goal is not only to detect and contain threats, but also to inform broader governance, risk, and compliance decisions.

3.7 Service Level Agreements

A **Service Level Agreement (SLA)** is a formalised commitment between a **service provider** and a client that defines the expected level of service. It articulates measurable performance targets and responsibilities, serving both as a governance tool and a reference point for managing expectations, risk, and accountability.

SLAs are central to managing relationships between internal organisational units (e.g. IT and business teams) as well as external contracts with third-party providers. They define not only the services to be delivered, but also the metrics used to assess delivery, procedures for reporting, penalties or escalation paths for non-compliance, and provisions for revision or termination.

SLAs are especially critical in **outsourcing** arrangements, **cloud services**, and **managed service** contexts, where operational dependency on external providers must be balanced with mechanisms for transparency and control.

3.7.1 Components of an SLA

The specificity and enforceability of an SLA depend on the maturity of both parties and the criticality of the service involved. A typical SLA includes:

- **Scope of services**: What is covered, and what is excluded
- **Service levels**: Quantified performance targets (e.g. availability, response times)
- **Measurement methods**: Tools and data sources for verifying compliance
- **Roles and responsibilities**: Both for service providers and customers
- **Escalation and remediation**: What happens in case of breach
- **Review and revision**: Frequency and procedures for updates

3.7.2 Operational Metrics and Monitoring

Operational metrics are the foundation for SLA management. These metrics must be clearly defined, measurable, and contextually relevant. Common examples include:

- **Uptime / Availability**: Often expressed as a percentage (e.g. 99.9% monthly uptime)
- Mean Time to Restore Service (MTRS)
- Incident response and resolution times
- System throughput or transaction volumes
- User satisfaction ratings

Metrics can also be tiered to reflect different service classes or business priorities. For instance, a core public digital service may require stricter availability guarantees than internal back-office systems.

Effective monitoring depends on tools that offer visibility, traceability, and timely alerts. Dashboards, automated reporting, and trend analysis are common features in mature operational environments. These tools also support compliance reporting, auditing, and continual service improvement.

3.7.3 SLAs in Public vs Private Contexts

In **public sector** settings, SLAs often require alignment with regulatory obligations, transparency requirements, and public service standards. For services impacting citizens or legal obligations, the definition of acceptable performance must reflect public interest concerns, not only commercial feasibility.

In **private sector** environments, SLAs may be shaped more flexibly, responding to competitive dynamics, cost constraints, and contractual negotiation. However, reputational risk, liability, and regulatory compliance (e.g. under GDPR or sectoral laws) remain key considerations.

3.7.4 Governance and Integration

SLAs should not be treated as static documents but as part of broader **service governance frameworks**. Their definition and enforcement must be integrated into risk management, business continuity, and vendor management practices. Tools such as ISO/IEC 20000 (IT service management) and COBIT provide guidance on aligning SLAs with strategic objectives and stakeholder expectations.

A mature SLA process reflects not only technical capability, but also cultural alignment between provider and customer. It is a mechanism for trust, operational clarity, and shared responsibility.

3.8 DevOps and Continuous Delivery Pipelines

DevOps is a **cultural and organisational movement** that promotes closer collaboration between software development and IT operations teams. It emerged in response to the limitations of traditional siloed approaches, where long delivery cycles, handover friction, and reactive operations created bottlenecks and increased risk. DevOps aims to increase the velocity, reliability, and quality of software delivery by integrating processes, automation, and shared accountability across the software lifecycle.

At the core of DevOps lies the principle of **continuous improvement**, supported by practices such as version control, automated testing, infrastructure as code, and real-time monitoring.

3.8.1 ontinuous Integration, Delivery, and Deployment

DevOps practices are typically organised into a **Continuous Delivery Pipeline**, which encompasses several interconnected stages:

- **Continuous Integration (CI)**: Developers merge code changes frequently into a shared repository. Automated builds and tests validate the integrity of the codebase early and often.
- **Continuous Delivery (CD)**: Code changes that pass testing are automatically staged for deployment in production-like environments. This enables rapid feedback and supports business agility.
- **Continuous Deployment**: The final step in automation, where approved changes are automatically deployed into production without manual intervention.

These stages are underpinned by extensive automation and toolchains that reduce manual effort, detect errors early, and shorten recovery times when failures occur.

3.8.2 Tooling and Infrastructure

The DevOps ecosystem includes a wide array of tools, often integrated into delivery pipelines. Common examples include:

- **Source control and CI tools**: Git, GitLab CI, Jenkins, …
- **Configuration management**: Ansible, Puppet, Chef, …
- Containerisation and orchestration: Docker, Kubernetes, …
- **Monitoring and observability**: Prometheus, Grafana, ELK stack, …

Infrastructure is often provisioned through code (Infrastructure as Code), enabling reproducibility and reducing configuration drift. This is essential for managing complex environments and ensuring consistency between development, testing, and production systems.

3.8.3 Governance and Risk Considerations

While DevOps accelerates software delivery, it also introduces new **governance and risk management challenges**. Rapid deployment cycles may increase the potential for undetected flaws, misconfigurations, or compliance breaches. In regulated environments or public service contexts, these risks require structured countermeasures such as:

- Segregation of duties within the pipeline
- Audit trails and change logs
- Automated policy enforcement and security scanning
- **Rollback mechanisms** for failed releases

Frameworks such as **ISO/IEC 20000** and **DevSecOps** principles can help integrating governance and security into the pipeline, aligning operational speed with control and assurance.

3.8.4 Cultural and Organisational Change

DevOps is as much about **culture** as it is about technology!
Successful adoption often requires shifts in mindset, incentives, and leadership. Cross-functional teams must embrace shared responsibility for both the success and the stability of systems. Blame-free incident reviews, continuous learning, and agile workflows become central to organisational maturity.
In both public and private sectors, DevOps adoption is influenced by context: public organisations may face tighter constraints around legacy systems, change control, and external audits, while private entities may prioritise speed and innovation. Nevertheless, the core value remains the same (delivering reliable, high-quality software at pace).

3.9 From DevOps to …xOps

The emergence of **DevOps** in the late 2000s marked a turning point in how digital services could be developed and operated. DevOps challenged the traditional division between software development and IT operations by introducing shared responsibility, continuous delivery, and automation across the lifecycle of software systems. By aligning objectives and workflows, DevOps reduced deployment cycles, improved reliability, and fostered a culture of collaboration and continuous improvement. Its success inspired a broader movement, leading to the extension of DevOps principles to other domains, coining the concept of **"xOps"**, where "x" stands for a specialised operational area.

3.9.1 The "xOps" Proliferation

The term "xOps" now encompasses a family of operational models that apply DevOps-like principles (automation, agility, monitoring, and integration) to specialised areas. Examples are (each of these models adapts the foundational DevOps logic to the unique needs and constraints of its domain):

Term	Stands for	Focus Area
DevOps	Development + Operations	CI/CD, automation, collaboration between dev and ops
SecOps	Security + Operations	Integrating security into operations and incident response
DevSecOps	Development + Security + Operations	Embedding security early into DevOps pipelines ("shift-left")
CloudOps	Cloud + Operations	Managing cloud infrastructure, automation, reliability
AIOps	AI + Operations	Using machine learning to automate and enhance IT operations
MLOps	ML + Operations	Operationalizing machine learning models (deployment, monitoring, retraining)
DataOps	Data + Operations	Agile and automated data management pipelines
GitOps	Git + Operations	Managing infrastructure using Git repositories as the source of truth
FinOps	Finance + Operations	Managing cloud financial operations (cost tracking, forecasting)
BizOps	Business + Operations	Aligning business strategy and operations using data-driven decisions
ChatOps	Chat + Operations	Automating operations through chat platforms (e.g., Slack, Teams)
TestOps	Testing + Operations	Automating and integrating testing into the DevOps lifecycle
ModelOps	Models + Operations	Managing the full lifecycle of AI/ML models, broader than MLOps
NetOps	Network + Operations	Automating and managing network infrastructure
SysOps	Systems + Operations	Traditional system administration tasks, now often in cloud contexts
PlatformOps	Platform + Operations	Managing developer platforms and internal development environments (IDEs, CI/CD, services)
EdgeOps	Edge Computing + Operations	Managing operations at the edge (IoT, remote devices)

3.9.2 Drivers and Enablers

The expansion of xOps is driven by several converging factors:

- **Cloud-native architectures**, which enable rapid provisioning, scalability, and API-driven control
- **Automation tooling**, which reduces human error and increases consistency
- **Compliance demands**, which require traceability, auditability, and secure-by-design practices
- Real-time monitoring and feedback loops, which support adaptive operations

Together, these enablers support high-tempo, high-reliability environments in both private and public sector contexts.

3.9.3 Strategic and Organisational Impact

The rise of xOps represents not merely a change in tooling, but a shift in how organisations think about **operational responsibility, governance, and continuous learning**. Each "xOps" model aims to reduce friction, increase agility, and foster shared ownership across traditionally siloed teams.

However, xOps initiatives also present **organisational challenges**: they may require changes in roles, upskilling, redefinition of KPIs, and alignment of incentives. In public sector contexts, where structures may be more rigid and accountability more formalised, adoption of xOps practices must be carefully adapted to regulatory and cultural conditions.

3.9.4 Governance and Maturity

To avoid superficial or fragmented adoption, organisations increasingly seek to embed xOps practices within a broader governance model. Standards such as **ISO/IEC 20000**, **ISO/IEC 27001**, and **COBIT** can be used to contextualise xOps within strategic alignment, risk management, and control frameworks.

The future trajectory of xOps points toward increased convergence, where digital governance must accommodate rapidly evolving operational models while ensuring traceability, resilience, and public or customer trust.

3.10 Operational Culture and Organisational Maturity

The growing family of "xOps" models extends far beyond tools and automation. At its core, the adoption of these practices signals a transformation in organisational **operational culture**: a shift toward agility, collaboration, transparency, and shared responsibility across the lifecycle of digital services.
This culture emphasises **learning over blaming**, **metrics over opinion**, and **iteration over rigidity**. It requires not only technical capabilities, but also the ability to foster trust, manage complexity, and adapt processes dynamically in response to change.
Organisations that effectively internalise xOps practices tend to operate with a higher level of **maturity**, both in their technology governance and in their strategic alignment.

3.10.1 Dimensions of Maturity

The ability to adopt and sustain xOps practices is a strong indicator of maturity across multiple organisational dimensions:

- **Process maturity**: Consistent, documented, and continually improved processes for change management, monitoring, testing, and incident response.
- **Cultural maturity**: Psychological safety, blameless post-mortems, and a mindset of experimentation and continuous feedback.
- **Technological maturity**: Use of automation, observability, infrastructure-as-code, and secure software supply chains.
- **Governance maturity**: Alignment between operational practices and formal governance frameworks (e.g. ISO/IEC 27001, 20000, COBIT).
- **Strategic maturity**: Ability to align operational practices with organisational goals and regulatory environments.

A high level mature organisation sees "operations" not as a back-office function but as a driver of value, resilience, and innovation.

3.10.2 Barriers to Maturity

Not all organisations are prepared to embrace xOps practices. Common barriers include:

- **Siloed structures** that separate development, operations, security, and compliance.
- **Legacy systems** that are difficult to automate or integrate.
- Fear of change or blame cultures that suppress experimentation.
- **Inadequate metrics** or lack of observability into system performance.
- **Insufficient leadership engagement**, treating xOps as a technical trend rather than a strategic enabler.

Recognising these barriers is an essential step toward meaningful transformation.

3.10.3 Maturity Models and Assessment

Various maturity models have been proposed to assess readiness for xOps practices. These models typically examine capabilities in areas such as deployment frequency, lead time for changes, change failure rates, and recovery time. Frameworks such as **DORA metrics** (used in the State of DevOps reports), **CMMI**, and **ITIL maturity assessments** can be adapted for this purpose.
DORA metrics are a set of four key performance indicators developed by the DevOps Research and Assessment (DORA) team to evaluate the effectiveness of software development and delivery processes:

1. **Deployment Frequency**: How often an organization successfully releases to production.
2. **Lead Time for Changes**: The amount of time it takes a commit to get into production.
3. **Change Failure Rate**: The percentage of deployments causing a failure in production.
4. **Mean Time to Restore (MTTR)**: The average time it takes to recover from a failure in production.

These metrics have become industry standards for assessing DevOps performance and are widely used to identify areas for improvement in software delivery practices.
In the public sector, maturity may also be influenced by procurement constraints, policy cycles, and accountability structures. Even so, gradual adoption of operational culture improvements can yield benefits in service quality, resilience, and public trust.

3.10.4 Toward Continuous Adaptation

Ultimately, the ability to make use of the “ops” cultural paradigm reflects an organisation’s capacity for **continuous adaptation**. It suggests not only technical competence but also leadership maturity, process discipline, and alignment of purpose.
Whether in a hospital adopting DevSecOps for clinical systems or a municipality applying DataOps to urban planning, maturity in operational culture becomes a key enabler of continuous evolution and sustainable service excellence.

3.11 Cloud Operations and Multi-Tenant Governance

The shift from traditional on-premises infrastructure to cloud computing has fundamentally altered how operations are managed. In cloud environments, operational responsibilities are shared between the service provider and the customer, under the **shared responsibility model**. This changes not only the tools used, but also the distribution of risk, accountability, and control.

Cloud operations (often referred to as **CloudOps**) encompass the processes, tools, and practices required to deploy, manage, and monitor workloads across public, private, and hybrid cloud environments. CloudOps must accommodate continuous change, high elasticity, and the use of programmable infrastructure, requiring automation, observability, and dynamic policy enforcement.

3.11.1 Multi-Tenant Contexts

A defining characteristic of many cloud services is **multi-tenancy**: the ability to serve multiple customers (tenants) from a shared pool of infrastructure and services. This introduces unique governance challenges, particularly related to:

- **Data isolation and security**: Ensuring that tenants cannot access or infer each other's data.
- **Resource allocation and performance**: Avoiding contention and ensuring fair usage across tenants.
- **Policy enforcement**: Maintaining tenant-specific configurations, compliance boundaries, and audit trails.

Multi-tenancy exists not only in public cloud platforms but also in internal platforms serving multiple departments, agencies, or customers, such as in **government clouds**, university data centres, or large shared service centres.

3.11.2 Operational Practices in Cloud Environments

Cloud operations integrate with DevOps and xOps practices, but with additional concerns for:

- **Infrastructure as Code (IaC)**: Provisioning and configuration of resources using declarative templates.
- **Auto-scaling and elasticity**: Responding to demand in real time without manual intervention.
- **Cost governance (FinOps)**: Monitoring and controlling usage-based costs.
- **Service level monitoring**: Ensuring uptime, latency, and service availability under dynamic workloads.

Tools such as Kubernetes, Terraform, AWS CloudWatch, Azure Monitor, and GCP Operations Suite are commonly used to support these practices.

3.11.3 Compliance and Governance in Multi-Tenant Settings

In multi-tenant environments, governance must be structured to ensure both central oversight and tenant-level accountability. Key practices include:

- **Identity and access management (IAM)** with tenant-aware roles and policies.
- **Segmentation** through virtual networks, isolated namespaces, and role boundaries.
- **Auditability** of both tenant and provider actions, ensuring traceability across layers.
- **Compliance alignment**, especially with standards such as ISO/IEC 27017 (cloud security), ISO/IEC 27018 (PII protection in cloud), and sectoral regulations.

In public sector contexts, additional oversight may be required to demonstrate adherence to national data protection regulations, procurement rules, and sovereignty constraints. Hybrid or community cloud models are often used to balance control with efficiency.

3.11.4 Strategic Implications

Cloud operations and multi-tenant governance demand a shift from static control models to **dynamic governance**. Policies, roles, and enforcement mechanisms must evolve as workloads scale, users change, or external requirements shift.

Organisations that embrace this model can benefit from increased agility, cost optimisation, and service scalability. However, achieving these benefits requires investment in capability building, risk analysis, and governance tooling.

CloudOps maturity is not measured solely by uptime or automation, but by the ability to deliver scalable, secure, and compliant services in shared and complex environments—without sacrificing control or accountability.

3.12 Zero Trust Architecture and Operational Security Controls

Traditional security models have relied on a **perimeter-based approach**, assuming that systems and users inside the network could be trusted, while those outside could not. This model is increasingly inadequate in the face of cloud services, remote work, mobile access, and increasingly sophisticated cyber threats.

Zero Trust Architecture (ZTA) represents a fundamental shift. It is based on the principle of **"never trust, always verify"**, treating all network traffic (internal or external) as untrusted by default. Access must be explicitly granted, continuously validated, and limited to the minimum necessary.

This approach requires a combination of technical controls, identity management, policy enforcement, and architectural design. It is not a single product or platform, but a security strategy based on a holistic and dynamic posture.

3.12.1 Core Principles of Zero Trust

A Zero Trust Architecture typically includes the following foundational concepts:

- **Identity verification**: Relying on strong, context-aware authentication (e.g. multi-factor authentication, identity federation).
- **Least privilege access**: Granting users and systems only the permissions they need to perform a given task.
- **Micro-segmentation**: Dividing networks and applications into smaller zones to contain breaches and limit lateral movement.
- **Continuous monitoring**: Using real-time telemetry and behavioural analytics to detect anomalies.
- **Policy-based access control**: Decisions are made dynamically based on context such as user role, device health, and location.

The U.S. NIST Special Publication 800-207 offers a widely recognised reference model for implementing Zero Trust concepts.

3.12.2 Operational Security Controls

Operational security in a Zero Trust context depends on several categories of controls:

- **Preventive controls**: Firewalls, endpoint protection, vulnerability management, and encryption.
- **Detective controls**: Security information and event management (SIEM), intrusion detection systems (IDS), and log analytics.
- **Responsive controls**: Automated incident response, containment mechanisms, and rollback capabilities.
- **Administrative controls**: Access reviews, role governance, policy updates, and user awareness training.

These controls must be implemented with high automation and orchestration levels to operate effectively across hybrid and multi-cloud environments.

3.12.3 Integration with Governance Frameworks

Implementing Zero Trust requires integration with broader governance models. ISO/IEC 27001 and its extensions (e.g. ISO/IEC 27017, 27018, and 27701) offer a structural backbone for managing risks and aligning policies. Other relevant frameworks include:

- **NIST CSF** – The Cybersecurity Framework, widely adopted in both public and private sectors.
- **COBIT** – For aligning security with enterprise governance and strategic objectives.
- **ITIL** – Where operational controls intersect with service continuity and incident response.

Zero Trust also affects auditing and compliance, requiring new forms of evidence and real-time assurance mechanisms.

3.12.4 Adoption Challenges and Sectoral Implications

Adopting Zero Trust is not a simple reconfiguration; it involves **organisational change**, **process redesign**, and **technological modernisation**. In the public sector, implementation must align with transparency, accountability, and legal mandates. In private organisations, customer trust, regulatory compliance, and business continuity drive the transformation.
Ultimately, Zero Trust is not an end-state but a journey. Its principles support a resilient, adaptive, and risk-aware posture suitable for modern operational environments, especially those managing sensitive data, distributed teams, and critical infrastructure.

3.13 Operational Resilience and Incident Response

Operational resilience refers to an organisation's ability to continue delivering critical services despite cyberattacks, system failures, supply chain interruptions, or other adverse events. It is not limited to recovery after incidents, but encompasses preparedness, continuity, adaptability, and institutional learning.

Resilience is especially critical in sectors where public trust, safety, or regulatory compliance are central, such as healthcare, financial services, public sector organisations, and critical infrastructure.

In the European Union, the **Digital Operational Resilience Act (DORA)** reinforces the legal and governance obligations for resilience in the financial sector. It mandates that financial entities demonstrate the ability to protect, detect, contain, recover, and repair from ICT-related incidents. Similar expectations are emerging in other domains, reinforcing the need for structured approaches to operational resilience.

3.13.1 Incident Response in the Operational Lifecycle

An effective incident response capability reduces downtime, limits harm, and enhances organisational credibility. Incident response is the set of processes and roles designed to detect, assess, and contain adverse events affecting operations. Typical phases include:

- **Detection and alerting**: Using monitoring tools, telemetry, and logs to identify anomalies in real time.
- **Triage and classification**: Determining impact and urgency, including the need for regulatory reporting.
- **Response coordination**: Activating predefined procedures, roles, and escalation paths.
- **Communication**: Internally and externally, balancing transparency, public trust, and legal obligations.
- **Containment and recovery**: Stabilising systems, restoring services, and verifying remediation.
- **Post-incident review**: Conducting root cause analysis and incorporating lessons into the business.

Depending of the sectors, regulations prompt notification of major ICT incidents to competent authorities, with specific timelines and impact thresholds.

3.13.2 Resilience and Risk Management

Resilience is not a standalone function, it must be embedded in broader governance of risk and compliance. Key components include:

- **Business impact analysis (BIA)**: Identifying critical services and defining tolerance levels for disruption.
- **Scenario-based planning**: Preparing for systemic events, such as ransomware attacks, data loss, or third-party failure.
- **Dependency mapping**: Understanding technological, organisational, and inter-sectoral interdependencies.
- **Continuity and failover strategies**: Including system redundancy, alternative communication channels, and manual fallback procedures.

Standards such as **ISO 22301 (Business Continuity Management)**, **ISO/IEC 27035 (Information Security Incident Management)**, and the **NIST Cybersecurity Framework** offer structured methods for aligning resilience with risk governance and regulatory accountability.

3.13.3 Roles and Coordination

Incident response involves coordination across multiple roles and domains:

- **Technical teams**: Perform diagnostics, implement containment measures, and restore affected systems.
- **Information security and risk officers**: Ensure regulatory compliance and oversee escalation thresholds.
- **Legal and compliance staff**: Advise on breach notification duties and regulatory interaction.
- **Communications and public affairs**: Coordinate messaging and manage reputational risk.
- **Executive leadership**: Provide direction, allocate resources, and approve strategic decisions.
- **Third parties and regulators**: Involve cloud providers, critical suppliers, or supervisory bodies when required.

DORA and other regulations emphasise the need for governance structures with designated senior management oversight.

3.13.4 Public Sector Responsibilities

In public sector settings, operational resilience is intrinsically linked to public interest, service continuity, and trust in institutions. Disruption of digital public services, critical infrastructure, or health systems can have cascading societal effects. Therefore:

- **Resilience planning** must reflect legal mandates, sector-specific obligations, and multi-agency coordination.
- **Incident response** must integrate security, legal, and civic communication strategies, respecting transparency and data protection principles.
- **Interoperability and cross-border coordination** may be required when service platforms or infrastructure are shared or regulated at supranational level.

Where public agencies act as operators of essential services under national cybersecurity laws, they may also be subject to **reporting and audit requirements**, akin to those defined in DORA for financial entities.

3.13.5 Continuous Learning and Maturity

Resilience must be understood as a dynamic capability, one that evolves through experience, reflection, and systematic improvement. Mature organisations embed continuous learning through **metrics (**tracking mean time to detect, respond, and recover (MTTD/MTTR/MTTF)), **audits and exercises** (conducting internal or external simulations, including tabletop exercises and red team assessments), k**nowledge capture** (creating structured incident reports, root cause reviews, and after-action evaluations), **governance integration** (feeding findings into strategy, procurement, training, and system design), etc.

In regulated sectors, this learning process is not optional: **auditability, documentation, and corrective action** are often required to demonstrate compliance and to retain public or investor confidence.

3.13.6 Conclusion

Operational resilience is a convergence of technological, organisational, and regulatory concerns. It requires not only tools and processes, but also leadership, coordination, and an institutional culture of preparedness. Regulatory frameworks such as the EU DORA reflect a broader shift: resilience is no longer a best practice—it is an obligation. By treating resilience as a strategic and auditable capability, organisations can build trust, ensure continuity, and adapt confidently to uncertainty.

3.14 Operations Governance and Reporting to Executives

Operational functions (ranging from infrastructure and service delivery to incident response and vendor management) are not simply support mechanisms. They are strategic assets whose performance, resilience, and alignment with mission objectives directly influence organisational outcomes.
Operations governance refers to the structured oversight of operational practices, ensuring they are efficient, compliant, secure, and responsive to business needs. Governance mechanisms define **roles, policies, standards, escalation paths, and accountability structures**. However, to be effective, they must also support **evidence-based decision-making**, particularly at the executive level.

3.14.1 The Executive View: Focus and Format

Reporting to CxO executives or board members must be **concise, and actionable**. Operational detail is filtered to highlight:

- **Performance**: Are services delivering as expected? (e.g. uptime, SLA compliance)
- **Risk**: Are there emerging threats or compliance gaps?
- **Cost-effectiveness**: Are operations aligned with budget and resource planning?
- **Capability**: Are the right tools, staff, and processes in place to support current and future demands?

Executives are concerned not with isolated technical metrics, but with **trends, deviations, decisions needed, and their implications** for strategic objectives.

3.14.2 Key Governance Inputs

Effective operations governance is supported by structured information from various sources:

- **Operational dashboards**: Summarising SLAs, incidents, changes, capacity, and availability
- **Risk and compliance reports**: Highlighting control effectiveness, audit findings, or regulatory changes
- **Project and portfolio updates**: Indicating alignment between operational capacity and transformation agendas
- **Resilience and continuity metrics**: Readiness to sustain operations under adverse conditions
- **Security reporting**: Summarising incidents, vulnerabilities, and mitigations in a business-impacting format

The challenge is to present **relevant operational data in an executive-friendly narrative**, integrating technical insights with financial, reputational, and strategic considerations.

3.14.3 Governance Models and Escalation Paths

Operational governance typically involves multiple levels:

- **Service management teams** ensure execution and reporting at the technical level
- **Operational management committees** review KPIs, risks, and improvement plans
- **Executive governance bodies** (e.g. digital steering committees or IT boards) receive escalations, approve investments, and align operations with strategy

Well-defined **escalation paths** ensure that critical incidents, compliance issues, or capacity constraints are surfaced to the appropriate level in time to enable response.
Frameworks such as **ITIL**, **ISO/IEC 20000**, and **COBIT** provide structured approaches to organising governance roles, processes, and reporting lines.

3.14.4 Communication and Decision Support

Reporting to executives is not only about information! It is about **framing operational issues as strategic choices**. This includes:

- Highlighting **trade-offs** (e.g. risk vs. speed, cost vs. redundancy)
- Supporting **investment decisions** (e.g. modernisation, cloud migration, automation)
- Triggering **policy reviews** (e.g. access controls, change windows, vendor SLAs)
- Enabling **accountability** (e.g. for regulatory compliance or public service delivery)

This requires alignment between operational, risk, and strategic planning cycles. Reports must support **forward-looking decisions**, not only post-fact accountability.

3.14.5 Maturity and Institutional Learning

In mature organisations, operations governance becomes a platform for **continuous improvement**. Metrics and reports feed into retrospectives, strategic reviews, and capability planning. Executive reporting is no longer reactive but **anticipatory**, identifying trends and preparing responses before they become crises.
This level of maturity depends on reliable data, strong collaboration between operational and strategic roles, and a culture of transparency and shared responsibility.

3.15 CxO Dilemmas

The challenges and recurring dilemmas faced in governing IT operations, are numerous… Following, we list just a few, highlighting the tensions between structure and agility, automation and oversight, and internal control and external dependencies.

3.15.1 How much structure is too much?

Operational governance depends on processes, controls, and metrics, but too much rigidity can reduce responsiveness. Overly formal procedures may hinder adaptation, while informal workarounds introduce inconsistencies and unmanaged risk. CxOs must balance the need for clarity and control with space for autonomy and situational judgement. This balance is especially delicate when operational responsibilities are distributed across teams, units, or vendors, where unclear escalation paths or overlapping roles can undermine coordination and accountability.

3.15.2 Centralise for consistency or decentralise for responsiveness?

Consolidating IT operations under central leadership can reduce duplication, lower costs, and enforce standardisation. Yet, decentralised models often respond faster to contextual needs and empower local decision-making. Hybrid models (common in both public and private sectors) require thoughtful governance that delegates effectively while maintaining alignment. The real challenge lies not in choosing one model over the other, but in ensuring that whichever structure is adopted, responsibilities are clear, and performance remains visible.

3.15.3 Can automation be trusted without losing human oversight?

Automating routine operations increases efficiency and reliability, but overdependence on tools (especially when enhanced by AI) may reduce human vigilance. At the same time, resistance to automation can block much-needed improvements. CxOs must define where human judgement adds value and where automation can take over safely. Key decisions include how to handle edge cases, how to design explainable systems, and how to embed learning loops when automation fails.

3.15.4 How can change be encouraged without risking disruption?

IT operations must evolve continuously, yet every change carry risk. Whether deploying patches or shifting workloads to the cloud, change must be controlled without becoming paralysing. Formal change management processes can appear too slow for dynamic environments, encouraging unofficial workarounds. On the other hand, rushed or undocumented changes undermine system integrity and traceability. Governance must promote change readiness by aligning technical procedures with cultural willingness to follow them.

3.15.5 Who is accountable when services are shared across boundaries?

In ecosystems where multiple providers, departments, and jurisdictions operate together, operational responsibility can become blurred. Incidents involving cloud outages, data breaches, or delayed service responses often reveal that no single actor had full visibility (or authority) to respond effectively. CxOs must define roles and expectations across organisational boundaries and ensure that contracts, SLAs, and escalation paths reflect operational realities. Without this clarity, accountability dissolves when it is needed most.

3.15.6 Conclusion

Operational governance is defined as much by what happens in moments of uncertainty as by what is written in procedures. CxO dilemmas reflect real-world tensions, between efficiency and flexibility, control and trust, autonomy and coordination. Facing these dilemmas with strategic intent and institutional learning allows organisations to build resilience, even in highly dynamic or resource-constrained environments.

3.16 Oops…

3.16.1 The Process That Wasn't There

Carla and Tiago from the Frenetic Team are assigned to support a large logistics company in rolling out a centralised ticketing and issue resolution platform. The goal is to replace fragmented email chains and ad hoc spreadsheets with a consistent IT service management (ITSM) tool, integrated across multiple departments.

The kick-off meeting is optimistic.

Carla, energised by the scale of the initiative, jumps into configuration discussions with the vendor and the client's IT lead. She delegates process mapping to Tiago, assuming the company already has clear workflows in place. After all, everyone keeps referring to "standard procedures."

But as implementation progresses, confusion grows. Different teams define incidents and service requests differently. Escalation rules vary wildly between warehouses. There are undocumented local practices that no one wants to touch. The new tool starts reflecting this confusion, with inconsistent routing and misassigned priorities.

Tiago flags this inconsistency, but too late. The system goes live under pressure to meet a quarterly target. Within days, tickets are bouncing around without resolution, and users begin bypassing the system entirely, returning to direct emails and phone calls.

At the review meeting, the client expresses frustration. "We expected better alignment. Now we're managing chaos, with more screens."

The root cause? Carla assumed technology would standardise practices automatically. The project needed process clarity before tool configuration.
Lesson learned: without well-defined and agreed operational processes, even the best systems amplify confusion. Technology cannot replace the work of mapping, aligning, and validating how things actually get done.

3.16.2 The Hidden Alarm

Bruna, from the Contingent Team, is brought in mid-project to handle system monitoring integration with the new ITSM tool.

Her role is to ensure that automated alerts from core infrastructure feed properly into the centralised platform, helping reduce downtime and streamline incident response.

She quickly realises that not all systems are visible.

A critical legacy logistics subsystem still runs independently, monitored through a separate dashboard in one of the regional offices. It's been flagged for integration "in phase two", a decision made before Bruna's involvement.

Bruna is concerned. The system controls dispatch sequencing, and any failure would ripple across operations. She raises the issue in a team status call, but with the go-live date approaching, it is brushed aside. "Not in scope for now," the project manager says.

Sure enough, two weeks after launch, that exact system suffers a malfunction. No alert was raised through the ITSM tool. The issue was detected late, leading to delivery disruptions and financial penalties for the company.

Bruna is not blamed, but she is left frustrated. She had spotted the gap, but lacked the authority to insist. In hindsight, she realises she could have framed the risk differently, not as a technical flaw, but as an operational exposure with downstream cost implications.

Lesson learned: flagging issues is not enough. The way a concern is framed (especially in terms of impact and accountability) determines whether it is acted upon. In complex operational environments, influence is as important as insight.

These two stories show how operational IT failures often stem from the invisible: undocumented processes, local variations, legacy systems. Even well-intentioned consultants can miss the signs or be ignored if the right questions aren't asked, or the right language isn't used.
Success in IT operations requires not just tools, but coordination, foresight, and the courage to ask: "Are we really ready?"

3.17 …What? …

One Dashboard, Two Realities
Alex, a demanding executive in a high-pressure logistics firm, commissions two consulting teams to support different aspects of a new IT operations dashboard intended to streamline performance reporting across departments. The project includes incident metrics, SLA compliance, and cost visibility—all expected to be available in real-time for executive oversight.

3.17.1 All Metrics, No Meaning

Carla and Tiago from the Frenetic Team are tasked with designing the dashboard's technical interface.

Carla drives the pace hard, instructing Tiago to pull as many system logs and infrastructure KPIs as possible into a unified visual tool.

They focus on data ingestion and visual design (assuming that "more metrics" equals more value).

However, they do not involve the service desk or business units in selecting indicators.

When the dashboard is launched, it impresses visually, but operations staff are confused.

Several KPIs track low-level logs with unclear thresholds. One metric causes a false alarm, triggering an unnecessary escalation.

Alex is unimpressed. "This tells me nothing useful," he says. Worse, the dashboard is now being ignored, and teams revert to informal email updates.

Lesson learned: in operational contexts, dashboards must reflect shared understanding, not just raw data. Without co-creation and operational buy-in, even elegant tools become irrelevant.

3.17.2 Quiet Coordination, Real Results

Sofia and Mateus from the Dream Team are assigned to the same company, but focus on the coordination layer between business units and IT operations.

Rather than jumping into technical tools, they begin with a simple question: "What are the incidents and exceptions you care about most?"

Through one-on-one interviews, they discover that what matters to the customer support team isn't server uptime, but it's resolution time and cross-shift handovers. For finance, it's failed automation in end-of-month reports. For operations, it's network latency in warehouse scanners.

Mateus works with IT to map these indicators against actual system logs, finding a few that can be monitored directly, and others that need manual entry but provide better insight.

When their simplified dashboard goes live, it doesn't have dozens of charts, but it reflects what people actually need to act on.

Alex calls it "surprisingly useful." Department heads start using it to coordinate morning routines. Eventually, the dashboard becomes part of the weekly executive review.

Lesson learned: operational value is built from understanding how people work. Governance of operations is not about monitoring everything, it's about knowing what matters and making it actionable.

These parallel stories show how the same context can produce very different outcomes.
One team overengineered a tool disconnected from the field.
The other co-designed a governance mechanism that, while modest in scope, enabled real alignment and sustained use.
In IT operations, "insight" only exists if someone acts on it (and for that, clarity always beats complexity).

3.18 OK!

3.18.1 The Upgrade That Didn't Break Anything

Ricardo and Bruna from the Contingent Team are engaged by a utilities provider preparing a critical upgrade to its core infrastructure monitoring system.

The company has experienced past disruptions during similar upgrades, leading to a cautious atmosphere.

This time, executive leadership wants assurances that operations will not be disrupted (and that oversight is improved along the way).

Ricardo takes the lead on governance. He starts by mapping all operational dependencies, including third-party systems that aren't covered by internal SLAs.

Bruna, meanwhile, meets directly with operations staff to understand informal workarounds that are not documented anywhere but are used daily.

As the upgrade date approaches, the team proposes a phased rollout, combined with a rollback plan and a dry run over a weekend.

Some executives initially see this as over-cautious, but Ricardo frames it differently: "We're not just upgrading software, we're upgrading trust."

The upgrade proceeds with minor issues, all handled within defined tolerances. No downtime is reported, and for the first time, incident resolution metrics actually improve during the transition period.

Lesson learned: operational resilience isn't just about fixing problems, it's about designing change, so problems don't escalate. Careful attention to hidden dependencies and human practices makes the difference between smooth transitions and operational chaos.

3.18.2 The Escalation That Wasn't Needed

Tomás from the Mature Team joins a municipal IT department struggling with recurring complaints about slow response times from the service desk.

Executives are growing impatient, and there's talk of outsourcing the function. Tomás is asked to assess whether internal improvements are still worth pursuing.

Rather than jumping into analytics, Tomás spends his first days listening (observing ticket triage, sitting in on staff meetings, and reviewing complaint logs).

He discovers that the problem is not technical, but procedural: incidents are being logged with inconsistent priority levels, leading to delays and reassignments.

He proposes a minor intervention: a new triage form with clearer categories and a short training session for frontline staff.

IT managers are sceptical (expecting resistance from users) but Tomás insists on testing it in one unit before expanding.

The results are immediate.

With better ticket descriptions and accurate urgency classification, response time improves without adding staff or new tools.

The executive team scraps the outsourcing plan and commits instead to continuous improvement of internal processes.

Lesson learned: not every operational failure demands a major transformation. Sometimes, strategic patience and small, human-centred changes are enough to restore performance and trust.

These two stories show that when operational governance is approached with curiosity, humility, and a focus on actual workflows, success can follow, even in environments where failure has become the norm.
In both cases, success was earned not by controlling everything, but by engaging with the real dynamics of work, quietly and constructively.

3.19 Wrap-up…

The list below presents key concepts used to understand how organisations manage IT services, monitor performance, respond to disruptions, and support continuity (these concepts help identify the maturity of operational practices, their alignment with governance, and their adaptability in public or private sector contexts):

- **IT Service Management (ITSM)** – The structured approach to designing, delivering, operating, and improving IT services to meet business needs, typically supported by frameworks such as ITIL.
- **Service Level Agreement (SLA)** – A formal agreement between service provider and service consumer that defines expected service quality, performance targets, responsibilities, and penalties or escalation procedures.
- **IT Operations** – The daily activities required to manage and maintain IT infrastructure, applications, and services. This includes monitoring, incident handling, patching, backup, and user support.
- **Resilience** – The ability of an organisation's IT environment to continue delivering essential services during and after disruptions, whether due to failure, cyberattack, or other crisis.
- **Continuity and Recovery** – Plans and procedures to ensure the continuation or rapid restoration of critical IT services in the face of disruption. Includes backup, failover, and disaster recovery planning.
- **Incident Response** – The structured process of detecting, managing, and resolving unexpected events or threats that disrupt normal IT service operations, with clear roles, timelines, and escalation paths.
- **Operational Maturity** – The extent to which IT operations are formalised, measured, continuously improved, and integrated into the broader governance and management system.
- **Technical Debt** – The accumulation of design compromises, outdated systems, or rushed implementations that create long-term maintenance burdens and reduce adaptability.
- **Monitoring and Alerting** – The use of tools and processes to continuously track the health, performance, and security of IT systems, and to generate alerts when anomalies or failures occur.
- **Configuration Management** – The discipline of systematically tracking and managing the technical components (hardware, software, settings) of IT environments to ensure consistency and control.
- **Change Management** – The process used to manage changes in IT systems in a controlled manner to reduce risk, ensure alignment with requirements, and maintain service stability.
- **Continuous Improvement** – The practice of regularly reviewing and enhancing IT operations, typically using metrics, feedback loops, and lessons learned from incidents or audits.
- **DevOps** – A collaborative approach that integrates software development (Dev) and IT operations (Ops), aiming to shorten delivery cycles, increase deployment frequency, and improve reliability.
- **xOps** – An extension of DevOps principles to other operational domains (e.g., DataOps, SecOps, MLOps), emphasising automation, collaboration, and performance in specialised areas.
- **Zero Trust Architecture** – A security model that assumes no implicit trust inside or outside the network perimeter, requiring continuous verification and strong access controls across IT operations.
- **Operational Security Controls** – The tools, procedures, and configurations used to prevent, detect, and respond to threats in real-time IT environments, including firewalls, authentication, and endpoint monitoring.
- **Cloud Operations** – The management of IT services hosted in cloud environments, involving dynamic provisioning, multi-tenant governance, and compliance with provider contracts and regulatory requirements.
- **Multi-Tenant Governance** – The control and coordination of IT environments where multiple clients, departments, or users share the same underlying infrastructure while maintaining logical separation and accountability.
- **Service Desk and Support** – The frontline operational function responsible for handling user incidents, service requests, and communication during outages or updates.
- **Business Process Management (BPM)** – The discipline of modelling, analysing, and optimising business processes, often supported by workflow automation and integration with IT systems.
- **Process Automation** – The use of digital tools to execute repeatable tasks with minimal human intervention, increasing efficiency, consistency, and auditability.
- **Performance Indicators and Metrics** – Quantitative or qualitative measures used to evaluate the health and effectiveness of IT operations, including uptime, response time, incident rates, and user satisfaction.
- **Operational Culture** – The often tacit norms, attitudes, and behaviours that influence how IT operations are conducted, including how teams handle pressure, accountability, and change.
- **Governance of Operations** – The oversight structures, reporting lines, and accountability mechanisms that ensure IT operations align with institutional risk tolerance, service expectations, and compliance duties.

Notes:

- IT operations often reveal the **real level of institutional maturity**—what works under pressure, what fails silently, and how decisions are executed.
- Even the most strategic digital plan will fail if operational processes are fragile or undocumented.
- When advising or assessing operational environments, pay attention to the **interaction between people, processes, and systems**, and always ask: who monitors, who escalates, and who owns the risk?

4 Theme: IT, Strategy, and Change

Strategy refers to the coordinated set of choices that determine how an organisation allocates resources and capabilities to achieve its mission.

IT strategy, in turn, defines how technology supports, enables, or reshapes these choices. In practice, the distinction between "business" and "IT" strategies is increasingly blurred, especially in organisations where digital systems are integral to service delivery, market engagement, or internal processes.

Strategic alignment between IT and organisational goals requires mechanisms for dialogue, prioritisation, and governance. This includes not only formal planning cycles, but also adaptive structures that accommodate experimentation and learning. Portfolio management, architecture frameworks, and performance indicators are among the tools used to maintain coherence and responsiveness. In more mature contexts, the governance of digital initiatives is embedded within broader strategic oversight functions, ensuring that change efforts reflect institutional purpose and stakeholder expectations.

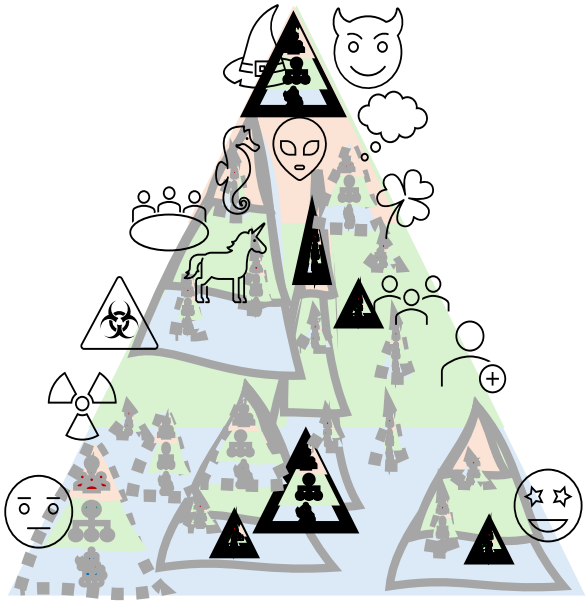
Change is not simply a matter of technical rollout. Organisational transformation involves shifts in roles, capabilities, processes, and often identity. Effective change management requires attention to cultural readiness, risk posture, stakeholder engagement, and institutional resilience. Executive sponsorship plays a crucial role in legitimising transformation efforts and aligning them with long-term goals.

Strategic use of IT also demands continuous evaluation of capability and maturity. Frameworks such as enterprise architecture and capability-based planning help organisations understand their current state and define realistic, value-driven paths to improvement. Tools such as the Target Operating Model (TOM) support the translation of strategy into operational structures and service models. In both public and private settings, such models are increasingly used to justify investments, structure accountability, and guide digital transformation journeys.

Across sectors, strategic IT concerns are shaped by context. In the private sector, competitiveness, customer experience, and innovation often drive digital investment. In the public sector, legitimacy, regulatory constraints, and service equity weigh heavily on strategic decisions. In either case, decision-makers must weigh short-term feasibility against long-term value, balancing efficiency with risk mitigation and innovation with compliance.

The acceleration of digital trends (»cloud migration, platform integration, AI adoption, cybersecurity demands) requires governance structures that support not only implementation but reflection. Strategy is not a one-time document but a process of navigation. Governance of IT, in this context, becomes a discipline of strategic learning: creating the structures through which organisations assess, steer, and adjust their use of technology to respond to external change and internal ambition.

The following sheets explore specific instruments and concerns that support this strategic interplay between IT and organisational transformation. They include conceptual tools such as enterprise architecture and capability models, operational mechanisms such as the Project Management Office (PMO), financial considerations around CapEx and OpEx, and sector-specific challenges such as portfolio governance in public institutions or the ethical implications of AI adoption. Each is treated not only as a management technique but as an expression of strategic intent and institutional evolution.



4.1 Business and Strategy

The term **business** refers not only to commercial enterprise but, more broadly, to the purposeful activities of any organisation, public, private, or non-profit. Business includes the delivery of value to stakeholders, whether in the form of profit, public service, legal enforcement, education, or societal benefit.

A clear understanding of business is essential for aligning digital initiatives with organisational purpose. This requires situating technology within broader structures of mission, vision, goals, and constraints. It also demands awareness of internal dynamics (culture, capabilities, risk appetite) and external factors (markets, regulation, technology trends).

4.1.1 Strategic Thinking and Governance

Strategy is the long-term orientation that guides how an organisation chooses to compete, serve, survive, or evolve.

Strategic thinking involves setting objectives, prioritising investments, managing uncertainty, and ensuring coherence between short-term actions and long-term goals.
In digitally dependent organisations, strategy must increasingly consider:

- **Technological capability** as a source of competitive or mission advantage
- **Risk and resilience**, including cybersecurity and supply chain fragility
- **Stakeholder expectations**, from citizens to shareholders
- **Regulatory frameworks**, particularly in sensitive areas like data, privacy, and AI

Digital initiatives should be embedded in strategy—not added to it. This demands governance models where technology leadership (CIO, CTO, CISO) is part of strategic decision-making.

4.1.2 Public vs Private Sector Strategic Contexts

While strategy is a universal concept, its application varies significantly between sectors:

- In the **private sector**, strategy often focuses on market positioning, innovation, efficiency, and profitability, which may be driven by competition, customer expectations, or scalability goals.
- In the **public sector**, strategy must consider legal mandates, public value, accountability, and fairness. Innovation may be desirable, but legitimacy, trust, and transparency are often primary constraints.

These differences affect how digital investments are framed, how risks are tolerated, and how outcomes are evaluated. Still, both sectors share a need for alignment between mission, capability, and technology governance.

4.1.3 Strategic Alignment and Portfolio Thinking

A key challenge in governance is ensuring that **digital operations, projects, and services** are aligned with strategic intent. This requires:

- A clear articulation of strategic objectives, priorities, and outcomes
- Mechanisms to translate strategy into programmes, projects, and operational goals
- Periodic review of alignment and benefit realisation

This perspective supports **portfolio management**, where initiatives are assessed not only for feasibility but also for strategic contribution, risk, and resource balance.
Frameworks such as **COBIT**, **Balanced Scorecard**, and **Enterprise Architecture** can support the structuring of alignment between business and technology.

4.1.4 Towards Strategy-Aware Governance

Mature governance embeds strategy in daily operations. This means:

- Ensuring strategic traceability in investment and operational decisions
- Enabling adaptability in response to external or internal change
- Supporting continuous learning from outcomes, including unintended effects

Strategic governance is not about rigid plans, but about **coherence, responsiveness, and foresight**. It depends on the capacity of leadership and operational teams to engage with purpose, prioritise across constraints, and manage change in line with institutional values.
In this light, digital governance is not a technical layer—but an enabler of strategic integrity and transformation.

4.2 Business Strategy and IT Strategy

Every organisation, regardless of sector, relies on a layered strategic structure. At the top is the **business strategy**, which defines the mission, long-term goals, competitive positioning, and value creation approach. Supporting this is the **IT strategy**, which determines how technology assets, capabilities, and innovations will contribute to those business objectives.
The relationship between business and IT strategy is not linear. While IT strategy must respond to business priorities, it can also **influence and enable strategic change**.

4.2.1 Aligning Business and IT Strategies

Strategic alignment is the degree to which IT supports and enhances the organisation's mission and strategic goals.
Effective alignment requires:

- **Shared understanding** between executives, technology leaders, and operational teams
- **Common language and priorities** across business and IT domains
- **Joint governance structures**, enabling coordinated decision-making and investment planning

Failure to align may result in duplicated efforts, underused systems, increased risk, or missed opportunities for innovation. Conversely, high alignment enables agility, efficiency, and competitive or mission advantage.

4.2.2 Characteristics of Business Strategy

Business strategy typically includes:

- Mission and vision statements
- Strategic objectives and KPIs
- **External environment analysis** (e.g. market trends, regulation, competition)
- **Internal capability assessment** (e.g. resources, skills, culture)

In the public sector, business strategy is often shaped by **policy priorities, legal mandates, and citizen expectations**. In the private sector, strategy may be more driven by market differentiation, cost optimisation, or innovation.

4.2.3 Characteristics of IT Strategy

IT strategy defines how technology will contribute to strategic goals. It may include:

- Infrastructure and architecture plans
- Digital service portfolios and roadmaps
- Information governance and security policies
- Capability development and sourcing models
- Innovation, research, or emerging technology initiatives

A modern IT strategy must also account for **compliance, sustainability, and resilience**, not just service delivery and cost-efficiency.

4.2.4 Governance and Planning Cycles

To maintain alignment, business and IT strategies should share **governance and planning cycles**. Key mechanisms include:

- Joint strategic planning committees or digital governance boards
- **Enterprise architecture** linking strategic objectives to digital capabilities
- **Portfolio management** processes that prioritise initiatives based on strategic value
- **Performance reporting** that includes both business outcomes and IT contributions

Standards such as **COBIT** and frameworks such as **TOGAF** support the integration of IT strategy into broader business planning.

4.2.5 Evolution and Mutual Influence

IT strategy must not be only responsive, it must be **enabling**.
Technological possibilities can reshape what is strategically feasible. For example:

- Cloud computing enables scalability for international service delivery
- Data analytics informs policy or market decisions
- Automation reduces operational bottlenecks
- Cybersecurity capabilities influence trust and risk postures

In turn, business strategy sets the boundaries and motivations for IT investment, governance, and innovation.
Organisations that treat IT strategy as a **separate technical plan** risk missing the transformative potential of digital capabilities. Those that foster continuous alignment and feedback between business and IT are better positioned to adapt, innovate, and deliver value.

4.3 Stakeholder Engagement and Strategic Communication

Effective governance is not solely an internal function. It also requires meaningful **engagement with stakeholders**, individuals or groups affected by, or capable of influencing, decisions and outcomes.
Stakeholders may include end-users, citizens, regulators, suppliers, public officials, investors, or advocacy groups. In public organisations, this includes democratic institutions, oversight bodies, and the general public.
Strategic communication ensures that stakeholders are informed, consulted, and aligned with the organisation's direction, especially when digital initiatives affect service delivery, privacy, or operational resilience.

4.3.1 The Role of Engagement in Digital Strategy

Stakeholder engagement is particularly important in the context of:

- **"Digital transformation" programmes**: Where process changes impact multiple groups
- **Data governance and privacy**: Where trust and transparency are essential
- **Cybersecurity and risk management**: Where shared responsibility must be understood
- **Service disruption or change**: Where expectations must be managed in advance

Without structured engagement, even technically sound initiatives may face resistance, legal challenges, or reputational damage. Engagement is not simply communication, but a process of dialogue, expectation management, and mutual learning.

4.3.2 Mapping and Segmenting Stakeholders

Organisations must identify and understand their stakeholders using structured methods such as:

- **Stakeholder maps**: Categorising actors by influence, interest, and proximity to the decision process
- **Salience models**: Prioritising stakeholders based on power, legitimacy, and urgency
- **Personas and user journeys**: Particularly for digital services and public-facing platforms

Different stakeholder groups require tailored forms of engagement, ranging from regular reporting and technical briefings to participatory workshops or public consultations.

4.3.3 Communication as a Governance Instrument

Strategic communication refers to the planned use of communication to advance strategic objectives. It supports:

- Transparency and accountability
- Change management and cultural alignment
- Risk communication
- Public trust and legitimacy

In the governance of digital systems, strategic communication must address complexity, uncertainty, and speed. It must convey not only what is changing, but why it matters, what risks are involved, and how feedback will be incorporated.
Key channels include internal communication platforms, formal reporting lines, newsletters, public dashboards, social media, consultation processes, and media relations. These should be coordinated and consistent, but also responsive to evolving contexts.

4.3.4 Public Sector Specificities

Public institutions have a special duty to ensure that digital governance is **visible, inclusive, and legitimate**. This often involves:

- Compliance with open government principles
- Public disclosure of algorithms, data practices, or funding priorities
- Consultation with civil society organisations or expert groups
- **Inter-agency coordination**, particularly in multi-level governance structures

Strategic communication in the public sector is both a governance function and a civic responsibility.

4.3.5 Integration and Maturity

Mature organisations embed stakeholder engagement and communication into programme governance, risk management, and policy cycles. Engagement is planned at the outset, monitored for effectiveness, and adjusted as circumstances change. Metrics may include participation rates, feedback quality, sentiment analysis, trust indicators, or the effectiveness of incident communication. Tools such as ISO 10002 (customer satisfaction and complaint handling) or GRI standards (sustainability reporting[66]) can support structured engagement approaches.
Ultimately, governance that fails to engage its stakeholders is unlikely to be effective. Engagement and communication transform abstract policies into shared understanding (and enable governance that is not only strategic but also socially responsive).

[66] https://www.globalreporting.org/

4.4 The Role of Senior Sponsorship in Change

Successful change initiatives (whether digital, organisational, or regulatory) depend not only on technical design and project management, but also on **visible, active, and accountable leadership from senior figures**. This leadership role is commonly referred to as **sponsorship**.

The **sponsor** acts as the organisational owner of a change initiative, providing strategic direction, ensuring alignment with broader goals, removing obstacles, and maintaining momentum. The absence of effective sponsorship is consistently cited as a leading cause of failure in change programmes.

4.4.1 The Sponsor Is Not Just a Name

While sponsorship may be assigned in formal governance documents, it only has impact when the sponsor engages **actively and visibly** throughout the life of the initiative. The sponsor is not a symbolic figurehead but an **agent of integration** between strategy, operations, and people.
Key functions of a sponsor include:

- **Articulating the case for change** and connecting it to organisational strategy
- **Authorising resources** and defending the investment in decision forums
- **Empowering project leaders** while holding them accountable
- **Intervening when escalation is needed** to resolve conflicts or remove barriers
- **Engaging with stakeholders** and acting as a bridge to executive leadership
- **Championing benefits realisation** and ensuring continued relevance of the initiative

These responsibilities cannot be delegated; they require time, attention, and credibility.

4.4.2 Strategic Positioning of the Sponsor

The sponsor must be **positioned at the right level** in the organisation to influence decisions, allocate resources, and command trust. This is particularly important when:

- The initiative affects multiple departments or jurisdictions
- There is likely to be resistance or disruption to existing practices
- The changes involve legal, financial, or reputational risk
- Outcomes depend on sustained behavioural or cultural change

In such contexts, mid-level sponsorship is insufficient. Executive-level ownership is necessary to provide authority, continuity, and legitimacy.

4.4.3 Sponsorship in Public Sector Settings

In public sector organisations, sponsorship plays an added role in ensuring that:

- Initiatives align with policy priorities and legal mandates
- Public value, not just efficiency, is clearly communicated
- Stakeholders, including citizens and elected bodies, are meaningfully engaged
- Transparency and accountability standards are upheld

Given the complexity of decision-making environments, the sponsor must often navigate **competing priorities, budget constraints, and political sensitivities**, making the clarity of their role even more essential.

4.4.4 Supporting the Sponsor

Sponsors need structured support to fulfil their role effectively. This includes:

- Clear documentation of roles and responsibilities
- Regular access to dashboards, risks, and status summaries
- Access to advisory teams (e.g. PMO, risk, legal, architecture)
- Training or mentoring in change leadership and communication

Supporting the sponsor also means **managing expectations**, ensuring that project teams provide actionable information and surface decisions early.

4.4.5 From Projects to Cultural Signals

The sponsor's behaviour sets the tone. Visible commitment signals that the initiative is not optional or experimental, but essential. Sponsors shape how the organisation perceives the value and seriousness of change, especially in environments where change fatigue or scepticism is high.
Ultimately, strong sponsorship turns projects into organisational priorities, and strategic intent into measurable outcomes.

4.5 The Champion: Symptom or Strategy?

Strategic initiatives in organisations often begin with ambition (digital transformation, cloud-first policies, AI integration, …) endorsed at board level and announced with enthusiasm. Yet many such projects later falter, not due to flawed strategy, but because the organisation lacked the **maturity, readiness, or capacity** to carry the ambition forward. In these situations, success often hinges on the emergence of a **project champion**: an individual who takes on disproportionate responsibility, mobilises support, overcomes resistance, and carries the project beyond what the institution could otherwise deliver.

This raises an important question for boards and advisors:
*is the reliance on a champion a **strategic tactic** or a **warning signal**?*

4.5.1 The Champion as a Symptom of Fragility

When projects are launched without realistic assessments of capability (lacking structured governance, stakeholder alignment, or operational readiness) success becomes contingent on exceptional personal effort. The need for a champion may therefore reflect a deeper institutional weakness: the absence of process maturity, communication channels, or capacity for collective action.

In these cases, the champion may conceal dysfunction rather than resolve it. Organisational learning is limited, and once the champion departs, so does coherence. The project risks becoming an isolated success (or a personal failure).

4.5.2 The Champion as a Tactical Asset

However, the presence of a champion is not inherently negative. If the organisation recognises its limitations early and **deploys a champion intentionally**, this can serve as a transitional scaffold. A credible, energised leader can secure initial momentum, buy-in, and clarity in environments where inertia, ambiguity, or fragmentation would otherwise prevail.

The key lies in treating the champion not as a substitute for systems, but as a **catalyst** for building them: using the champion's legitimacy to surface risk, foster alignment, and prepare the ground for sustainable delivery structures.

4.5.3 The Hidden Risks of Hero Mode

Even when successful, champion-driven initiatives carry hidden costs.
Champions may:

- Over-centralise decision-making, weakening collaboration.
- Suppress dissent or bypass process in the name of urgency.
- Build fragile support networks that depend on charisma rather than accountability.

These dynamics can limit institutional resilience and inhibit future scaling.
Over time, the "hero model" can become culturally entrenched, discouraging structural improvement.

4.5.4 Questions for Discussion

Interesting questions to exercise might be:

- *When should the reliance on a champion be seen as a red flag, and when as a valid tactic?*
- *How can boards or advisors distinguish between a strategic scaffold and a governance gap?*
- *What mechanisms can ensure that a champion's efforts lead to institutional capacity-building?*
- *Is there a point at which a champion should step back to allow systems to take over?*
- *Can the presence of a champion distract from recognising organisational unreadiness?*

4.6 Target Operating Model

Strategic transformation requires not only a clear vision but also a structured articulation of how an organisation will operate to realise that vision.

The Target Operating Model (TOM) plays a central role in this articulation. It describes the "to-be" state of the organisation (how it should function in the future to deliver on its strategy) and serves as a reference for transitioning from the current "as-is" state.

The TOM is typically developed during periods of organisational change, such as digitalisation, mergers, regulatory reform, or service redesign. It links strategic objectives with the operational enablers required to achieve them. It not only clarifies what needs to change but also provides a framework for how change will be executed, monitored, and sustained.

4.6.1 From "As-Is" to "To-Be"

The "as-is" state reflects the current condition of the organisation, including its structures, processes, systems, and cultural practices. It often includes legacy constraints, inefficiencies, or misalignments with emerging goals.

In contrast, the "to-be" model is a purposeful design of the future state. It integrates desired improvements in governance, digital infrastructure, service delivery, competencies, and organisational culture. The TOM enables the organisation to compare these two states, identify gaps, and define a roadmap for transition.

4.6.2 Core Components of a TOM

While the specific configuration varies by context, most TOMs are built around several interrelated components:

- **Organisational structure** – including roles, reporting lines, and decision-making layers.
- **Business processes** – redesigned for efficiency, alignment, or compliance.
- **Capabilities** – functional and cross-cutting capabilities that need to be retained, improved, or developed.
- **Information systems** – the digital and data infrastructure that supports operations.
- **Human resources** – workforce skills, deployment, and cultural alignment.
- **Governance and accountability** – oversight, risk management, and compliance mechanisms.
- **Performance measurement** – key indicators and evaluation frameworks.

These elements must be aligned with the organisation's strategic goals and coordinated across business units and functions.

4.6.3 Support for Change Readiness and Execution

The TOM is more than a design artefact. It is a communication tool for executive sponsors and transformation leaders, helping to explain the rationale behind change initiatives and the benefits expected. It supports change readiness by making the future state concrete and aligning stakeholders around a common understanding.

When linked to transformation roadmaps and phased implementation plans, the TOM becomes a monitoring tool that supports programme governance, allowing leaders to assess progress and adjust course based on real-world developments.

4.6.4 Adaptability and Continuous Learning

Contemporary TOMs are designed for adaptability. The traditional assumption of fixed five-year plans has given way to models that emphasise learning, iteration, and responsiveness. In this view, TOMs are not static blueprints but evolving frameworks that incorporate feedback, respond to policy or market shifts, and accommodate emerging technologies.

This dynamic quality makes the TOM especially suitable for environments where uncertainty, complexity, or cross-sector collaboration are prevalent.

4.6.5 Link to Enterprise Architecture

The TOM and **Enterprise Architecture (EA)** are closely connected. While the TOM defines the desired operational state, EA provides the structured representation of how that state will be realised across business, information, application, and technology layers.

Enterprise Architecture ensures that the elements of the TOM are consistent, integrated, and technically feasible. It provides traceability between strategic objectives and system design, facilitating prioritisation, dependency management, and platform decisions. The synergy between TOM and EA enables strategic alignment at both conceptual and implementation levels.

4.6.6 Capability-Based Planning

A growing trend in TOM development is **capability-based planning**. This approach focuses on what the organisation must be able to do, rather than on specific structures or systems. Capabilities cut across departments and domains, offering a more flexible and strategic lens for identifying investment priorities, sequencing transformation efforts, and measuring maturity.

This is particularly relevant in ecosystems that involve multiple actors or in public sector contexts where legal mandates, funding cycles, and service delivery models may vary.

4.6.7 Conclusion

A Target Operating Model is a foundational instrument for translating strategy into action. It enables organisations to move deliberately from an existing "as-is" condition to a desired "to-be" state. By clarifying priorities, aligning resources, and supporting both planning and execution, the TOM ensures that transformation is not left to chance. When integrated with Enterprise Architecture and capability-based planning, it becomes a powerful enabler of sustainable, strategic change.

4.7 Enterprise Architecture and Alignment

Alignment *is the state in which an organisation's strategies, structures, processes, technologies, and behaviours consistently support and reinforce one another in pursuit of shared objectives.* ***Enterprise Architecture (EA)*** *is a discipline that helps organisations structure and align their business, information, application, and technology domains to achieve strategic objectives.*

EA provides a **holistic view** of the organisation's capabilities, processes, systems, and governance mechanisms, making it possible to identify dependencies, reduce complexity, and guide decision-making.
Unlike technical architecture, which focuses on specific systems, EA connects **strategic intent with operational execution**, acting as a bridge between business strategy and IT strategy.

4.7.1 Components and Domains

Most EA frameworks define four primary architecture layers:

- **Business Architecture**: Describes organisational goals, structures, processes, and value delivery mechanisms.
- **Information/Data Architecture**: Defines how data is stored, governed, and flows across the organisation.
- **Application Architecture**: Maps the applications and systems that support business functions.
- **Technology Architecture**: Details the infrastructure, platforms, and services that underpin operations.

These layers are interconnected and must be governed in coherence with the organisation's strategic direction, risk posture, and regulatory obligations.

4.7.2 Strategic Alignment Through EA

Strategic alignment is achieved when an organisation's **processes, systems, and investments** consistently support its long-term goals. EA supports alignment by:

- Clarifying how capabilities map to strategic objectives
- Identifying redundancies, gaps, or misalignments across systems and services
- **Enabling coordinated decision-making** about investments, sourcing, and design
- **Supporting change management** through structured impact analysis

EA facilitates **traceability**, allowing decision-makers to understand how digital components support mission outcomes and where adjustments are needed.

4.7.3 Frameworks and Methodologies

Several methodologies support the practice of EA. Common examples include:

- **Zachman Framework** – A historical taxonomy for organising architectural artefacts by perspective and abstraction.
- **TOGAF (The Open Group Architecture Framework)** – A widely used reference framework providing a structured approach to architecture development and governance.
- **FEAF and DODAF** – Architecture frameworks developed by entities of the United States government for, respectively, the domains public administration and defence.

ArchiMate is a modelling language specifically created to visually represent models created in the scope of EA.

The choice of framework depends on organisational maturity, sector, regulatory environment, and modelling needs.

4.7.4 EA as a Governance Enabler

Enterprise architecture is a modelling activity in the scope of a **governance function**. It supports:

- **Investment decisions**, by identifying which systems should be maintained, retired, or replaced
- **Standards enforcement**, by defining principles and rules for technology selection and integration
- **Risk management**, by visualising dependencies and vulnerabilities
- **Policy implementation**, by ensuring that strategic policies (e.g. cloud-first, open data, zero trust) are operationalised through coherent system design

In mature organisations, architecture is integrated into **portfolio governance**, **procurement**, and **project design reviews**.

4.7.5 Challenges and Organisational Dynamics

Adopting EA requires addressing several challenges:

- **Cultural resistance**, especially if EA is perceived as bureaucratic or disconnected from delivery
- **Lack of executive sponsorship**, limiting authority and strategic impact
- **Fragmented documentation**, which hinders visibility and coherence
- **Tooling and skills gaps**, particularly in modelling and impact analysis

To overcome these challenges, EA must be **positioned as a facilitator of change**, not merely as a control mechanism. When well integrated, EA helps organisations become more agile, interoperable, and resilient—especially in complex, multi-stakeholder environments.

4.8 Roles in Enterprise Architecture

Enterprise Architecture (EA) is a structured activity that supports the alignment of strategy, operations, data, and technology.

While frameworks and modelling tools provide structure, the practical value of EA emerges from the roles and outputs that guide decision-making across the organisation. These outputs are not purely descriptive; they serve as governance instruments, planning tools, and enablers of coherence across change initiatives.

The contribution of EA depends on the clarity, integration, and authority of the people responsible for creating, validating, and applying architectural artefacts. These individuals operate at the intersection of business and technology, translating strategy into models, constraints, and roadmaps that shape how systems are designed, procured, and evolved.

4.8.1 From Roles to Outputs

The central output of EA is ***architectural guidance*** that informs and constrains organisational design and transformation. This includes:

- **Reference Architectures:** High-level templates describing common structures, standards, and integration principles across domains. These helps reduce redundancy, support interoperability, and simplify solution design.
- **Capability Maps:** Models that identify what the organisation does (or must be able to do), linking strategy to operations and enabling analysis of maturity, gaps, and investment priorities.
- **Target Architectures and Roadmaps:** Descriptions of the desired future state, together with transition plans that guide coordinated change. These outputs are essential for portfolio management and sequencing initiatives over time.
- **Principles and Standards:** Agreed rules and patterns that support governance and design consistency. These include data management rules, integration methods, cloud usage policies, and technology selection criteria.
- **Impact Assessments and Compliance Reviews:** Evaluations of whether proposed initiatives align with architectural direction, helping decision-makers assess trade-offs and risk.

These artefacts are the core deliverables of EA and must be accessible, actionable, and integrated into organisational decision cycles. When used well, they become part of the organisation's "memory" and strategic reflex.

4.8.2 Key Roles and Responsibilities

EA outputs are collectively produced and maintained by a constellation of roles, each with a distinct focus and contribution:

- **Chief Enterprise Architect (CEA):** Provides leadership and coordination across architectural domains. The CEA defines the EA vision, manages the architecture repository, and engages with executive stakeholders to ensure strategic alignment.
- **Business Architect:** Develops models of the organisation's structure, capabilities, and value streams. Business architects link strategic objectives to processes and performance, supporting decisions on investment, outsourcing, and reorganisation.
- **Data Architect:** Designs the conceptual and logical structure of data assets, ensuring consistency, interoperability, and alignment with governance requirements. Outputs include data models, stewardship roles, and quality frameworks.
- **Application Architect:** Creates application landscape maps, integration blueprints, and functional decompositions. These outputs guide development and procurement, ensuring modularity and avoiding redundancy.
- **Technology Architect (or Infrastructure Architect):** Specifies the foundational technologies, including cloud platforms, networks, and security mechanisms. Outputs include technology standards, deployment patterns, and lifecycle plans.

Each role contributes to an evolving set of models, diagrams, principles, and catalogues that shape investment decisions, guide project teams, and support governance bodies in making informed choices.

4.8.3 Integration and Use in Practice

In many organisations, EA roles are distributed across projects, departments, or service units. Outputs may be used in business case evaluations, procurement decisions, strategic portfolio planning, and risk assessments. For this to happen, EA must be embedded in governance processes (such as architecture boards, steering committees, or change advisory groups) where its outputs serve as shared reference points.

Where internal capacity is limited, external consultants may be engaged to deliver specific outputs, such as capability models, maturity assessments, or reference architectures. However, without internal ownership and continuity, these outputs risk becoming shelf artefacts rather than instruments of change.

4.8.4 Conclusion

EA delivers value through its outputs, not only models and diagrams, but the shared understanding, traceability, and design discipline they enable. These outputs help organisations navigate complexity, avoid fragmentation, and invest coherently. The effectiveness of EA depends not only on the quality of its frameworks but also on the credibility of its roles, the integration of its outputs into governance, and the ability to adapt to evolving strategic and operational needs.

4.9 Strategic Portfolio and Investment Governance

Strategic governance of technology investments requires more than managing individual projects—it demands a coordinated view of **portfolios**, where multiple initiatives compete for limited resources, carry interdependencies, and must align with organisational strategy and public value. This approach recognises that not all initiatives are equal in terms of urgency, impact, or risk, and that trade-offs must be managed continuously.

A **portfolio** refers to the full set of initiatives, programmes, projects, and operational investments that an organisation chooses to fund and monitor. Strategic portfolio governance ensures that these investments are not only aligned with organisational objectives but are also coherent, balanced, and adaptable to change.

4.9.1 Principles of Portfolio Governance

Portfolio governance builds on three core functions:

- **Alignment**: Ensuring each initiative supports strategic goals, regulatory duties, or mission-critical services.
- **Prioritisation**: Comparing initiatives based on expected benefits, risks, dependencies, and resource constraints.
- **Monitoring**: Tracking performance, benefit realisation, and continued relevance of investments over time.

This governance should be informed by enterprise architecture, risk assessments, capacity planning, and financial analysis. It must also remain sensitive to external triggers such as regulation, market shifts, or technological innovation.

4.9.2 Investment Lifecycle and Gatekeeping

A mature investment governance model defines clear stages across the investment lifecycle—from ideation to retirement. This often includes:

- **Idea capture and evaluation**: Filtering based on strategic relevance and feasibility.
- **Business case development**: Justifying investment through projected value, costs, and risks.
- **Gate reviews**: Decision points where investments are re-evaluated before progressing.
- **Portfolio balancing**: Ensuring a healthy mix of high-risk/high-reward initiatives and stable, long-term operations.
- **Benefit tracking**: Measuring outcomes beyond delivery, particularly in public value or service improvement.

Gatekeeping mechanisms help organisations prevent scope creep, redirect resources, or discontinue underperforming initiatives.

4.9.3 Governance Structures and Roles

Strategic portfolio governance requires participation from multiple levels:

- **Executive boards or councils**: Provide final decision authority and ensure alignment with mission and policy.
- **Enterprise PMO (Project Management Office)**: Coordinates investment tracking, methodology, and reporting.
- **Architecture boards**: Ensure consistency with technological and information governance standards.
- **Financial controllers**: Validate resource availability, budgeting, and cost-effectiveness.

Governance processes must accommodate both centralised mandates and local innovation, particularly in large or distributed organisations such as ministries, agencies, or multi-entity groups.

4.9.4 Risk, Resilience, and Adaptability

Portfolio governance must address not only return on investment, but also **risk exposure**, **resilience**, and **strategic agility**. Cybersecurity, regulatory change, climate risk, and digital dependency introduce volatility that demands frequent re-evaluation of priorities.

In public sector environments, transparency, fairness, and alignment with policy cycles are additional constraints. Long-term digital investments, such as national infrastructure or health systems, must reconcile continuity with innovation, often over multiple legislative or funding periods.

Governance maturity is reflected not only in documentation, but in the organisation's ability to adapt the portfolio dynamically while preserving strategic coherence.

4.10 Project Management Office

The **Project Management Office (PMO)** is an organisational unit established to standardise and support the governance, planning, execution, and monitoring of projects and programmes.

A PMO acts as a bridge between strategic oversight and operational execution, helping to ensure that change initiatives are aligned with organisational priorities, delivered effectively, and contribute measurable value.

A PMO may serve different purposes depending on the organisational context and level of maturity. In some cases, it provides light-touch support and coordination; in others, it exercises direct control over project delivery.
In both public and private sectors, PMOs play a crucial role in embedding governance practices within the management of change.

4.10.1 Purpose and Functions

The core functions of a PMO typically include:

- **Standardisation**: Developing and maintaining project management methods and tools to ensure consistency across initiatives.
- **Oversight**: Monitoring the status of projects and programmes, tracking performance indicators, and providing consolidated reporting to senior leadership.
- **Support**: Assisting project teams with planning, budgeting, risk identification, and stakeholder communication.
- **Governance**: Enforcing decision-making processes, escalation paths, and compliance with internal or regulatory requirements.
- **Resource coordination**: Supporting portfolio-level decisions about staffing, capacity, and prioritisation across concurrent projects.

These functions help reduce duplication among projects and initiatives, improve transparency, and create conditions for informed executive oversight. In some cases, the PMO may also facilitate knowledge management, benefits realisation tracking, or enterprise-wide learning from project outcomes.

4.10.2 Types of PMOs

PMOs vary in their degree of authority and integration within the organisation.

Common types of PMO include:

- ***Supportive PMO**: Offers guidance, best practices, and documentation, but does not enforce compliance. Suitable for decentralised environments or low-maturity organisations.*
- ***Controlling PMO**: Enforces the use of project management frameworks and reporting standards, while still allowing flexibility. Typically adopted by organisations seeking to balance autonomy and consistency.*
- ***Directive PMO**: Takes direct control of projects, assigning project managers and ensuring strict adherence to processes. Common in high-stakes or regulated environments, especially where project failure would carry significant consequences.*

The choice of PMO model should reflect the organisational culture, maturity, complexity of the portfolio, and strategic ambitions for change.

4.10.3 Public Sector Considerations

In public administrations, PMOs often play a dual role of supportive and directive: managing internal project delivery and ensuring compliance with external mandates such as procurement regulations, transparency requirements, or oversight by funding bodies. In the public sector projects may involve diverse stakeholders, extended time horizons, and evolving political priorities (usually meaning unclear or not stable requirements), all of which increase the need for structured coordination.
PMOs in this context contribute to legitimacy and accountability, while also enabling more reliable planning and delivery of public value.

4.10.4 Strategic Alignment and Executive Interface

A well-functioning PMO acts as a critical interface between strategy formulation and implementation. It provides executives with visibility into project status, risks, and resource use, thereby supporting informed decision-making. The PMO may report to the CIO, the COO (Chief Operation Officer), or to a transformation leader, depending on the structure and focus of the organisation. To be effective, the PMO must also be able to navigate organisational politics, build trust with delivery teams, and adapt to changing priorities. It must avoid becoming a bureaucratic bottleneck while maintaining the integrity of governance processes.

4.10.5 Conclusion

Project Management Offices enable structured, repeatable, and transparent management of change initiatives. By integrating governance, oversight, and delivery support, PMOs provide the scaffolding that allows organisations to translate strategy into outcomes. Their design and operation must be tailored to the organisational context, balancing control with flexibility and enabling both responsiveness and accountability across project portfolios.

4.11 Cybersecurity as Strategic Risk

Cybersecurity has traditionally been viewed as a **technical or operational concern**, often delegated to IT departments or security specialists. However, the growing frequency, scale, and impact of cyber incidents have elevated cybersecurity into the domain of **strategic risk**, affecting reputation, legal compliance, financial sustainability, and even mission continuity.
Treating cybersecurity solely as a technical function underestimates its organisational significance. **In mature governance models, cybersecurity is recognised as a board-level issue, integrated into risk management**, investment planning, and strategic decision-making.

4.11.1 Characteristics of Strategic Risk

A strategic risk is one that:

- Threatens core objectives or value creation
- Imposes significant legal, financial, or reputational impact
- Cannot be mitigated solely through operational controls
- Requires executive engagement and cross-functional response

Cybersecurity meets all these criteria! A major data breach, service outage, or ransomware attack can disrupt critical services, lead to regulatory sanctions, erode stakeholder trust, and result in long-term strategic damage.

4.11.2 Risk Governance and Executive Roles

Recognising cybersecurity as strategic implies a shift in **governance and leadership responsibilities**. Executives and governance bodies must:

- Ensure cybersecurity risk is included in enterprise risk registers
- Review and understand cyber risk reports and threat intelligence
- **Set risk appetite and tolerances** for information assets and digital services
- **Support investment decisions** in preventive and resilience capabilities
- **Hold delivery teams accountable** for implementing policies and controls

The role of the **Chief Information Security Officer (CISO)** becomes central as a technical authority and a strategic advisor.

4.11.3 Integration with Strategic Planning

Strategic planning must account for:

- **Digital dependency**: Increasing reliance on cloud, software, and interconnected platforms raises the potential attack surface.
- **Regulatory exposure**: Laws such as the GDPR, NIS2 Directive, and national cybersecurity acts impose obligations with significant penalties.
- **Reputational vulnerability**: A breach can erode citizen trust, investor confidence, or partner cooperation.
- **Supply chain fragility**: Third-party providers, even when certified, may introduce systemic risks.

Cybersecurity thus becomes a **design consideration**, not just a control layer. It influences architectural choices, procurement criteria, and investment timing.

4.11.4 Public Sector and Critical Infrastructure

In public organisations, cybersecurity has additional layers of significance. It intersects with:

- **Democratic integrity**, when threats target electoral or judicial systems
- **National security**, especially where state actors are involved
- **Service continuity**, in domains such as health, energy, and public safety

Governance must support **whole-of-government coordination**, mandate baseline controls, and ensure reporting mechanisms that reflect the public interest.

4.11.5 Strategic Risk, Resilience, and Communication

Cybersecurity must be aligned with broader **resilience and continuity strategies**. This includes:

- Regular stress testing and incident simulations
- Crisis communication plans, including public disclosures
- Investment in recovery capabilities and fallback systems

Boards and executives should receive **cyber risk briefings** similar to those used for financial, reputational, or compliance risks. These should include threat trends, incident readiness, response effectiveness, and strategic exposures.
Recognising cybersecurity as a strategic risk does not eliminate threats—but it enables organisations to prepare, prioritise, and respond with the full backing of leadership and governance structures.

4.12 Sector-Specific Cybersecurity Standards

While general-purpose standards such as ISO/IEC 27001, NIST CSF, and COBIT provide broad guidance on cybersecurity governance, **sector-specific environments** often demand tailored standards and controls. These reflect unique threat landscapes, operational requirements, regulatory pressures, and safety concerns inherent to specific industries.
Cybersecurity in healthcare, transportation, energy, finance, and manufacturing must consider the criticality of services, life safety implications, and the interconnectedness of systems. Sector-specific standards are developed by international bodies, national regulators, or industry consortia to address these needs with precision.

4.12.1 Healthcare

Healthcare systems process sensitive personal data and operate life-critical technologies, where examples of standards are:

- **ISO 27799** – Information security management in health using ISO/IEC 27002, providing detailed guidance tailored to healthcare environments.
- **Health Insurance Portability and Accountability Act (HIPAA)** – U.S. regulation that sets standards for protecting health information, including administrative, physical, and technical safeguards.
- **HL7 Security and Privacy Ontology** – Frameworks for protecting data exchange between clinical systems.

The integration of health records, telemedicine, and medical devices increases exposure to cyber threats, requiring strict identity, access, and data protection controls.

4.12.2 Automotive

Modern vehicles are complex digital systems with embedded software, connectivity, and increasing autonomy. Key cybersecurity references include:

- **ISO/SAE 21434** – Road vehicles – Cybersecurity engineering, which defines requirements for risk-based cybersecurity throughout the lifecycle of automotive systems.
- **UNECE WP.29 Regulation** – Mandates cybersecurity management systems (CSMS) and software update management systems (SUMS) for vehicle manufacturers operating in applicable markets.
- **AUTOSAR Security Guidelines** – Industry specifications for secure automotive architecture.

These standards address threats to safety, privacy, and intellectual property posed by connected vehicles, over-the-air updates, and V2X communication.

4.12.3 Finance and Banking

Financial institutions are frequent targets of cyberattacks due to the high value of data and transactions.
Sectoral standards include:

- **PCI DSS (Payment Card Industry Data Security Standard)** – A global standard for protecting cardholder data and managing payment-related security.
- **Basel Committee's Principles for Operational Resilience** – Incorporates cyber risk into broader resilience expectations for banks.
- **ISO 20022 Security Guidelines** – For secure messaging in financial services.

Financial regulations also impose reporting obligations and mandate cybersecurity audits and stress testing, especially for critical service providers and infrastructures.

4.12.4 Energy and Utilities

Energy systems involve industrial control systems (ICS) and critical infrastructure, requiring specialised guidance:

- **IEC 62443** – A comprehensive family of standards for securing industrial automation and control systems.
- **ISO/IEC 27019** – Tailored information security controls for the energy utility sector.
- **NERC CIP (Critical Infrastructure Protection)** – North American standards for securing bulk electric systems.

These frameworks integrate cybersecurity with operational safety, availability, and incident response in high-dependency environments.

4.12.5 Cross-Sector Considerations

While each domain has unique risks, there are shared priorities across sectors:

- Identity and access management
- Secure software lifecycle
- Incident detection and coordinated response
- Supply chain security
- Regulatory compliance and audit readiness

Organisations operating across sectors or in regulated ecosystems must often **harmonise** multiple standards. This requires mapping controls across frameworks and aligning them with enterprise governance models.

4.13 Data Protection Impact Analysis

A **Data Protection Impact Analysis (DPIA)** is a structured process for identifying and mitigating risks to the rights and freedoms of individuals arising from the processing of personal data. It is a requirement under the General Data Protection Regulation (GDPR) in situations where data processing is likely to result in a high risk to individuals, such as through the use of new technologies, large-scale profiling, or systematic monitoring of public spaces.

The DPIA is a tool for embedding **privacy-by-design** principles into systems and services. It promotes proactive risk management, transparency, and accountability in how data is collected, processed, stored, and shared.

4.13.1 When a DPIA Is Required

According to the GDPR (Article 35), a DPIA is mandatory when data processing:

- Involves systematic and extensive evaluation or profiling with legal or similarly significant effects
- Includes large-scale processing of special categories of data (e.g. health, biometrics)
- Entails systematic monitoring of publicly accessible areas
- Could otherwise result in significant risks to individuals' rights, such as identity theft, discrimination, or loss of control over personal data

National data protection authorities may provide **lists of high-risk processing activities** for which DPIAs are mandatory or exempted.

4.13.2 Structure and Steps of a DPIA

A typical DPIA process includes the following steps[67]:

1. **Describe the processing**: Define the nature, scope, context, and purposes of the data processing.
2. **Assess necessity and proportionality**: Evaluate whether the data processing is legally justified and whether less intrusive alternatives exist.
3. **Identify and assess risks**: Consider potential harms to individuals' rights and freedoms, including accidental or unlawful access, alteration, or loss.
4. **Define mitigation measures**: Propose technical and organisational safeguards to reduce identified risks.
5. **Consult stakeholders**: In some cases, including with the Data Protection Officer (DPO), affected groups, or supervisory authorities.
6. **Document and monitor**: Record the outcome, revisit as conditions change, and integrate into the broader compliance framework.

Tools such as **ISO/IEC 29134** provide detailed guidance on how to conduct a DPIA, complementing broader privacy management systems such as ISO/IEC 27701.

4.13.3 Organisational Integration and Roles

Conducting a DPIA requires coordinated input from multiple roles:

- The **DPO** ensures methodological integrity and alignment with legal standards.
- The **system owner or process owner** provides insight into the intended data flows and operational context.
- The **security and architecture teams** assess technical safeguards and system design.
- In some cases, **external stakeholders or regulators** may need to be consulted.

A DPIA should not be an isolated exercise but integrated into the lifecycle of projects and services, ideally starting in early design phases. It should also be revisited when systems are significantly changed.

4.13.4 Strategic Relevance

Beyond compliance, DPIAs support a culture of **risk-aware digital governance**. They enhance trust with users, improve alignment between technology and policy, and reduce the likelihood of legal disputes or reputational harm.
In the public sector, DPIAs are particularly significant, as data subjects often have limited choice regarding service providers. In such contexts, transparency, fairness, and ethical considerations must be clearly demonstrated.
When systematically adopted, DPIAs become a key mechanism for operationalising digital rights and embedding privacy into organisational decision-making.

[67] https://gdpr.eu/data-protection-impact-assessment-template/

4.14 Technology Maturity Assessment

Technology maturity assessment is a structured process used to evaluate the readiness, reliability, and suitability of a specific technology for deployment or integration within an organisational context. It provides a systematic method to understand the risks, benefits, and the level of uncertainty associated with technology adoption. Central to technology maturity assessment is the concept of Technology Readiness Level (TRL), a scale developed initially by NASA and subsequently adopted across industries and governments to communicate the maturity status of technologies effectively.

4.14.1 Understanding TRL

TRL offer a standardised scale from 1 (lowest maturity) to 9 (highest maturity), enabling stakeholders to assess, compare, and communicate the developmental stage of technologies clearly. TRLs help to bridge the gap between research, development, and operational use by providing transparent, common reference points. The standard TRL scale includes:

- **TRL 1: Basic principles observed** - Scientific research begins; foundational concepts and observations are established.
- **TRL 2: Technology concept formulated** - Practical application concepts are identified; speculative ideas become structured proposals.
- **TRL 3: Experimental proof of concept** - Analytical and laboratory experiments validate the feasibility of technology concepts.
- **TRL 4: Technology validated in laboratory** - Integration of components verified in controlled environments; basic technology elements successfully demonstrated.
- **TRL 5: Technology validated in relevant environment** - Technology demonstrated within simulated operational environments; reliability and performance assessed.
- **TRL 6: Technology demonstrated in relevant environment** - Functional prototype operated in realistic scenarios; demonstrating integrated system effectiveness.
- **TRL 7: System prototype demonstrated in operational environment** - Near-complete prototypes tested under operational conditions; reliability and robustness demonstrated.
- **TRL 8: System complete and qualified** - Full technology development completed, meeting intended operational requirements; ready for commercial or operational deployment.
- **TRL 9: Technology proven in operational environment** - Technology widely implemented and proven through sustained real-world operation; fully commercialised and reliable.
-

4.14.2 Importance of Assessing Technology Maturity

Several common challenges may arise when assessing technology maturity, including:

- **Subjectivity in assessments**: Different evaluators may interpret criteria differently; thus, structured assessment frameworks and expert consensus are crucial.
- **Complexity of integration**: Technologies rarely operate in isolation; maturity assessments must consider interoperability and integration into existing systems.
- **Dynamic technological environments**: Rapid technological evolution can alter maturity assessments, requiring frequent reassessments and flexibility in management practices.

Accurately assessing technology maturity helps organisations to manage risks associated with technology investment, reducing uncertainty and supporting informed decision-making. Benefits include:

- **Risk mitigation**: Early identification of technological uncertainties prevents costly deployment failures.
- **Resource optimisation**: Efficient allocation of financial (CapEx and OpEx), human, and infrastructure resources towards viable technologies.
- **Strategic planning**: Informed alignment of technological investments with strategic and operational objectives.

4.14.3 Assessment Methods and Tools

Various methodologies are employed to carry out technology maturity assessments, such as:

- **Structured TRL Assessment Tools**: Formal tools and frameworks developed by entities such as NASA, ESA, or defence organisations, providing detailed criteria and evaluation methods for each TRL.
- **Expert Panel Reviews**: Panels comprising multidisciplinary experts assess technological progress against predefined criteria.
- **Gate Review Processes**: Structured project management methodologies incorporating periodic reviews or 'gates', determining if technologies are sufficiently mature to progress to subsequent development stages.

4.14.4 TRL in Public vs. Private Sectors

In the private sector, TRL assessments typically inform investment decisions, manage product development timelines, and ensure competitive advantage through timely innovation. Companies prioritise rapid progression through TRLs to achieve first-mover advantages or quickly adapt to changing market demands.

Public sector applications of TRL often focus on reliability, regulatory compliance, and public safety. Government entities utilise TRLs extensively for procurement processes, risk management, and policy development, emphasising transparency and accountability in decision-making.

4.14.5 Strategic Use of TRL

Organisations strategically use TRL assessments to align innovation pipelines, manage R&D portfolios, and prioritise investments based on clearly defined readiness levels. Clear understanding of TRL supports effective communication among stakeholders, mitigates technological risks, and accelerates technology transition from initial concept to successful operational deployment, significantly enhancing organisational agility and strategic capability.

4.15 Technology Research

Technology research encompasses systematic investigation aimed at discovering, evaluating, and assimilating technological advancements that support strategic business objectives. It involves comprehensive analysis of emerging trends, validation of promising innovations, and proactive assessment of risks and benefits associated with technological adoption.
Effective technology research allows organisations to identify and exploit strategic opportunities, while simultaneously mitigating technological obsolescence and associated risks.

4.15.1 Strategic Alignment and Relevance

The primary goal of technology research within organisations is to support strategic alignment, ensuring that technological investments consistently deliver measurable value in alignment with organisational goals. It requires close collaboration between strategic management, technology leadership, and operational units to understand requirements, define clear technology roadmaps, and prioritise research activities effectively.
CxOs frequently collaborate to establish robust frameworks for evaluating new technologies, driven by criteria such as feasibility, scalability, interoperability, compliance, and strategic impact.

4.15.2 Methods and Approaches

Technology research involves a variety of methodological approaches, ranging from exploratory assessments to structured feasibility studies. Organisations often employ techniques such as:

- **Technology Scanning**: Continuous monitoring of market innovations, competitors, and academic research to spot emerging technologies.
- **Proof-of-Concept (PoC)**: Experimental implementation to validate the practical applicability of new technologies.
- **Benchmarking and Comparative Analysis**: Evaluation of technologies against industry standards, competitors, and best practices.
- **Pilot Projects**: Small-scale deployments intended to assess viability, collect data on performance, and refine the technology's implementation strategy.

These approaches ensure rigorous vetting, effectively balancing innovation and prudent resource allocation.

4.15.3 Technology Research in Public vs. Private Sector

In the private sector, technology research is primarily driven by competitive advantage, efficiency, profitability, and customer engagement considerations.
Private organisations often prioritise rapid adaptation to market conditions and the leveraging of technological advancements to sustain or enhance market positions.
Conversely, the public sector's technology research often prioritises stability, accountability, regulatory compliance, and value to the public. This involves thorough consideration of factors such as transparency, security, accessibility, interoperability, and long-term sustainability. Additionally, public sector CxOs frequently face specific challenges, such as stricter procurement guidelines, higher requirements for public accountability, and intense scrutiny from regulatory bodies.

4.15.4 Technology Research Governance

Governance in technology research involves structured oversight mechanisms and formalised decision-making processes to ensure responsible research practices and prudent resource management. Organisations typically employ governance structures comprising committees or boards that assess research initiatives, evaluate alignment with strategic priorities, and monitor research outcomes. Essential governance considerations include:

- **Transparency and accountability**: Ensuring that technology research aligns clearly with strategic and operational goals.
- **Risk management**: Identifying, assessing, and mitigating risks associated with new technology adoption.
- **Resource optimisation**: Making informed decisions regarding capital expenditure (CapEx) and operational expenditure (OpEx) in technology investments.

4.15.5 Organisational Capabilities and Talent Development

Successful technology research requires not only methodological rigour but also skilled personnel capable of interpreting, evaluating, and managing complex technology landscapes. Consequently, organisations actively invest in talent development programmes, knowledge management systems, and strategic partnerships with universities and research institutions. Such investments ensure ongoing access to essential expertise, knowledge dissemination, and timely identification of crucial technological developments.

4.15.6 Outcomes and Impact of Effective Technology Research

Effective technology research leads to tangible and strategic outcomes including improved organisational agility, enhanced innovation capacity, better risk management, and optimised use of resources. Informed technology selection contributes significantly to competitive advantage, customer satisfaction, regulatory compliance, and operational resilience, clearly demonstrating the essential role of rigorous research practices in sustaining organisational success in increasingly competitive and complex technological environments.

4.16 Technology Research Providers

Leveraging specialised market intelligence significantly enhances an organisation's ability to anticipate market shifts, capitalise on innovation, and align technology investments closely with strategic organisational priorities.
Organisations frequently engage a special kind of **consultant**, external **technology research providers**[68] such as Gartner, IDC, Forrester, EY, Deloitte, etc., to acquire insights into technology landscapes, market dynamics, competition analysis, and strategic forecasting. Those providers leverage extensive industry expertise, comprehensive market data, and proprietary
research methodologies to support executive-level decision-making, strategic planning, and competitive positioning.

4.16.1 Key Research Services Offered

Providers typically deliver a range of structured services tailored to the specific requirements of their clients, including:

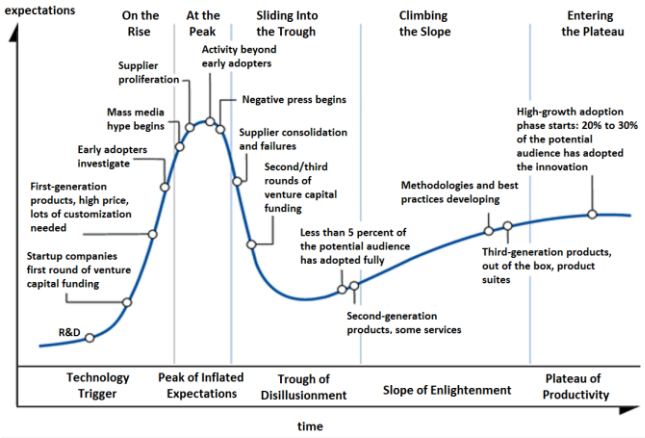
- **Market Analysis and Forecasting**: Identifying growing sectors, assessing market potential, estimating technology adoption rates, and predicting future trends.
- **Competitive Intelligence**: Profiling and benchmarking competitors, evaluating competitor strategies, products, market shares, and positioning.
- **Technology Trend Analysis**: Monitoring and interpreting emerging technological trends and disruptions, providing early insights to inform strategic technology adoption decisions.
- **Product Evaluation and Benchmarking**: Conducting objective evaluations of technology products and services, helping identify strengths, weaknesses, and market positioning relative to competitors.
- **Customer Insights and Demand Analysis**: Analysing consumer behaviour, gauging market demand, and assessing acceptance of new or existing products.
- **Marketing and Messaging Advisory**: Refining product positioning, enhancing marketing messaging effectiveness, and maximising outreach strategies.

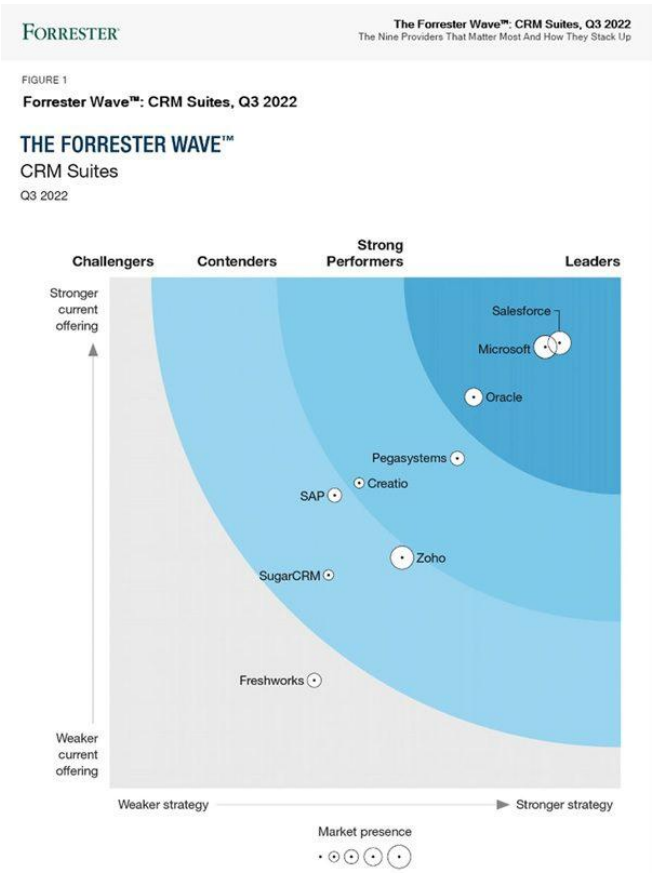
4.16.2 Methodologies and Tools

Technology research providers employ robust methodologies to ensure accurate, credible, and actionable insights. Common methodological frameworks include:

- **Quantitative Research**: Surveys, statistics, and predictive analytics for market trends, customer preferences, and technology adoption patterns.
- **Qualitative Research**: Expert interviews, focus groups, case studies, and comprehensive literature reviews for in-depth market understanding.
- Analytical Frameworks: Strategic models such as Gartner's Magic Quadrant and Hypecycle, Forrester's Wave, IDC's MarketScape, SWOT analysis, and technology maturity assessments to visualise competitive dynamics and vendor capabilities clearly.
- **Big Data Analytics**: Leveraging large datasets and sophisticated analytics tools to uncover hidden patterns, correlations, and predictive insights within the technology market.

The following images are a shape of the hype cycle (image from Wikipedia) and an example of the Forrester Wave:





4.16.3 Selecting and Managing Providers

Selecting suitable technology research providers involves careful consideration of several critical factors:

- **Credibility and Independence**: established reputations for impartiality, rigorous analytical standards, and credible industry insights.
- **Expertise and Specialisation**: experience in relevant technology areas, sector-specific competencies, and proven analytical track records.
- **Alignment with Organisational Objectives**: provider services align with strategic, operational, and competitive objectives of the client organisation.
- **Cost-Benefit Considerations**: research cost implications relative to expected strategic value and actionable outcomes ensure optimal CapEx and OpEx decisions.

[68] See https://comparemaniac.com/gartner-vs-forrester-vs-idc-how-the-major-analyst-firms-compare/

4.17 Strategic Financial Management of Technology

When managing technology investments, organisations primarily classify expenditures as either Capital Expenditure (**CapEx**) or Operational Expenditure (**OpEx**). Clearly distinguishing these categories supports accurate financial planning, strategic decision-making, and alignment of technology initiatives with organisational objectives.

4.17.1 Capital Expenditure (CapEx)

CapEx encompasses funds allocated by an organisation for acquiring, upgrading, or extending the useful life of significant physical or technological assets. CapEx investments result in the acquisition of long-term assets that appear on the balance sheet and are depreciated over their useful lifecycle, reflecting the asset's contribution to business operations across multiple accounting periods. Typical examples of CapEx include:

- Acquisition of data centres, servers, or network infrastructure.
- Purchase or construction of office buildings and facilities.
- Significant upgrades of existing technological systems or infrastructure.
- Investment in software licenses with perpetual ownership.

4.17.2 Operational Expenditure (OpEx)

OpEx refers to the ongoing costs associated with running and maintaining day-to-day organisational operations. OpEx represents short-term expenses fully recorded within the accounting period incurred, directly impacting profit-and-loss statements without depreciation considerations. Common examples of OpEx include:

- Subscription-based software services (Software-as-a-Service – SaaS).
- Utility costs, such as electricity and cloud computing charges.
- Maintenance and repair costs for existing equipment and technology.
- Salaries and wages of operational staff and routine training expenses.

4.17.3 CapEx vs. OpEx: Strategic Implications

Choosing between CapEx and OpEx significantly influences financial strategy, cash-flow management, tax implications, and operational agility:

Criteria	CapEx	OpEx
Financial reporting	Assets, depreciated over useful life	Expenses, fully accounted immediately
Budget predictability	Large, upfront investments	Predictable, recurring payments
Cash-flow management	Significant initial outlay	Lower initial payments, evenly spread
Tax treatment	Depreciation allowances over multiple years	Immediate tax deductions
Flexibility and agility	Lower agility due to sunk costs	Higher agility, scalable

4.17.4 Public vs. Private Sector Considerations

In the private sector, CapEx and OpEx decisions are typically evaluated in terms of financial returns, profitability, strategic alignment, and shareholder value. Organisations prioritise investments that deliver measurable economic benefits, leveraging financial analysis method.

In contrast, the public sector frequently experiences different budgeting dynamics. Often, securing funding for CapEx projects is comparatively easier, as these investments align closely with political priorities. CapEx initiatives are more readily justifiable through structured funding programmes, grants, or special budget allocations intended for infrastructure improvement or public-service innovation. Conversely, obtaining adequate funding for OpEx in the public sector is notoriously challenging. Operational budgets frequently face greater scrutiny, tighter constraints, and more bureaucratic approval processes due to annual budget cycles, strict cost-control measures, and political oversight aimed at limiting recurrent expenditures.

As a result, public organisations often face difficulties in maintaining ongoing services, implementing incremental improvements, or effectively managing day-to-day operations due to limited operational budgets, even when sufficient capital funding is available for investments.

This budgeting dynamic encourages public entities to prioritise CapEx-driven projects, sometimes inadvertently neglecting sustainable operational funding, which can result in challenges maintaining newly acquired or upgraded assets over their lifecycle.

4.17.5 Transition from CapEx to OpEx: Technological Trends

Increasing adoption of cloud computing, managed IT services, and subscription-based technologies has shifted organisational expenditure from traditional CapEx-intensive models to more OpEx-focused approaches. This transition brings notable benefits, including increased financial agility, reduced upfront investment burdens, and improved scalability. However, it requires careful management to avoid hidden costs, vendor lock-in risks, and challenges associated with dependency on external service providers.

4.18 Cloud Assessment Framework

Cloud services have become integral to how organisations operate, innovate, and scale. As cloud adoption increases, so does the need for structured governance mechanisms to ensure alignment with organisational goals, regulatory obligations, and operational resilience. This includes not only evaluating external cloud providers but also establishing internal foundations that enable responsible and effective use of cloud technologies. Cloud governance, therefore, encompasses both assessment frameworks and organisational readiness, moving from isolated procurement decisions to strategic capability.

4.18.1 Assessment Frameworks for Cloud Adoption

To support risk-based cloud adoption, organisations may rely on **Cloud Assessment Frameworks (CAFs).** These frameworks offer a structured methodology to evaluate the suitability, security, compliance, and functionality of cloud services. They are especially relevant in public sector contexts or regulated environments, where accountability, digital sovereignty, and data protection are paramount. Typical assessment domains include:

- **Data Protection and Sovereignty** – Evaluates the handling of personal and sensitive data, including compliance with regulations such as GDPR, data localisation requirements, and cross-border transfer safeguards.
- **Security and Resilience** – Reviews the provider's technical and organisational controls, including threat response, business continuity, and system availability.
- **Compliance and Certification** – Maps service features to standards such as ISO/IEC 27001, ISO/IEC 27017, and to national schemes such as SecNumCloud (France) or C5 (Germany).
- **Governance and Transparency** – Assesses auditability, contractual clarity, reporting mechanisms, and the ability to monitor performance.
- **Service Functionality and Exit Strategy** – Analyses flexibility, interoperability, and migration options to reduce vendor lock-in and support reversibility.

These frameworks often include checklists, scoring models, and qualitative criteria to support consistent evaluation across multiple providers or service types.

4.18.2 Cloud Foundation as an Enabler of Governance

Cloud governance is not limited to external assessment. Internally, organisations increasingly adopt a **Cloud Foundation** approach, a structured set of policies, technical components, and governance practices that enable secure and scalable cloud usage across business units. A Cloud Foundation typically includes:

- **Architecture Blueprints** – Standardised designs for infrastructure, identity, networking, and workload management.
- **Shared Security Services** – Centralised tools for encryption, access control, threat monitoring, and incident response.
- **Automated Controls** – Embedded compliance checks, policy enforcement, and continuous configuration validation.
- **Governance Integration** – Alignment with broader management systems (e.g., risk registers, procurement policies, and oversight bodies).

The maturity of the Cloud Foundation reflects the organisation's ability to adopt cloud services in a coordinated and accountable manner, avoiding fragmented deployments or unmanaged risks.

4.18.3 Public Sector and European Contexts

In public administration and critical sectors, cloud governance frameworks are often mandatory or strongly recommended. Examples include:

- UK Government's Cloud Security Principles, guiding the evaluation of cloud risks.
- **SecNumCloud**, a French certification for high-trust cloud providers.
- **C5**, Germany's compliance framework for cloud services.
- **EUCS**, the forthcoming European Union Cybersecurity Certification Scheme for Cloud Services, aiming to harmonise assurance levels across Member States.

These instruments serve both as procurement references and assurance mechanisms, especially in contexts involving sensitive data or essential services.

4.18.4 Strategic and Implementation Considerations

Successful cloud governance requires integration with strategic, operational, and compliance functions. Key practices include:

- Early articulation of business and regulatory requirements.
- Systematic use of assessment frameworks during procurement and renewal cycles.
- Establishment of a Cloud Foundation to institutionalise good practices.
- Continuous alignment with organisational risk appetite and legal obligations.
- Periodic reassessment of provider services and internal capabilities.

By combining structured assessments with a strong internal foundation, organisations can scale cloud adoption responsibly, supporting innovation while maintaining trust, accountability, and resilience.

4.18.5 Cloud Providers and Compliance

Most of the cloud providers already show their alignment with most of the compliance frameworks:

- https://aws.amazon.com/compliance/
- https://azure.microsoft.com/en-us/explore/trusted-cloud/
- https://cloud.google.com/compliance
- https://www.alibabacloud.com/en/trust-center
- https://www.ovhcloud.com/en/compliance/
- https://www.oracle.com/corporate/cloud-compliance/
- https://www.ibm.com/cloud/compliance

4.19 Robotic Process Automation (RPA)

Robotic Process Automation (RPA) refers to the use of software robots (or "bots") to automate structured, rule-based digital tasks typically performed by humans. These bots mimic user actions within digital systems (such as logging into applications, entering data, performing calculations, and generating reports) without altering underlying the enterprise IT infrastructure. RPA solutions are non-invasive, usually operating at the user interface level, and are often deployed without major software development efforts. This makes RPA attractive for organisations seeking to optimise back-office and operational processes quickly and with relatively low risk.

4.19.1 RPA and Organisational Efficiency

By automating repetitive and time-consuming tasks, RPA enhances productivity, reduces human error, and allows human workers to focus on more strategic or complex responsibilities. The impact is often most visible in departments such as finance, human resources, customer service, and IT support.

In private sector contexts, RPA can be used to streamline supply chain operations, automate invoicing, or handle customer onboarding. In public sector organisations, RPA supports process efficiency in areas like licensing, case management, or benefits processing—where legacy systems are still prevalent and standardised procedures abound.

4.19.2 Connections with Governance, Risk, and Compliance (GRC)

The introduction of RPA affects several dimensions of governance, risk, and compliance. On one hand, automation reduces compliance risks by enforcing uniform execution of procedures and enabling traceable, auditable logs of activity. On the other hand, risks arise when bots interact with systems lacking adequate access controls, or when changes in regulations are not promptly reflected in the automated procedures.

A governance framework is essential to manage RPA initiatives. This includes defining responsibilities for bot development and maintenance, managing changes to automated workflows, and ensuring oversight mechanisms remain effective. Where RPA is integrated into processes handling sensitive or personal data, alignment with regulatory frameworks such as the GDPR becomes critical.

4.19.3 RPA in the Context of Management Systems

RPA implementations should not be seen as isolated technical deployments but rather as components of broader Management Systems, especially those concerned with quality (ISO 9001), information security (ISO/IEC 27001), or IT service management (ISO/IEC 20000). Embedding RPA within such systems ensures that automation contributes to strategic objectives, and that associated risks and controls are properly addressed.

The use of RPA can also support maturity improvement in Management Systems by fostering standardisation and measurability, key indicators of process capability.

4.19.4 Strategic Implications and Ethical Considerations

Strategically, RPA implementation should be carefully planned to avoid reinforcing outdated processes. Poorly selected use cases, or excessive reliance on RPA to bypass deeper organisational change, may lead to fragile and unmaintainable automation layers.

Ethically, RPA raises questions about workforce impact. While often framed as a way to "free employees for higher-value work", the displacement of administrative roles remains a genuine concern. Transparent communication and reskilling initiatives are crucial, particularly in the public sector, where employment practices and social responsibilities differ from the private sector.

4.19.5 Related Concepts in the SGSI 2025 Framework

RPA interacts with several other concepts introduced in this lecture series:

- **Compliance and Regulatory Requirements** (Part 2): RPA can enforce rules and generate audit trails, but requires ongoing compliance monitoring, especially under frameworks such as GDPR and eIDAS.
- **Information Security** (Sheets 2.6, 2.8): Automated processes may access sensitive information; role-based access control and monitoring must extend to bots.
- **Process Optimisation** (Part 4): RPA is often a tactical step, and its effectiveness is tied to the maturity of business process management and digital governance.
- **Systems of Record vs. Systems of Engagement** (Sheet 3.4): RPA frequently interacts with systems of record, automating the flow of data from unstructured inputs (e.g., email) to structured systems.
- **Distinctions between Public and Private Sector Organisations**: Public sector entities may use RPA to address constraints from legacy systems and workforce rules, while private entities often seek ROI through efficiency and scale.

4.20 Hyperautomation

Hyperautomation refers to the disciplined approach by which organisations rapidly identify, vet, and automate as many business and IT processes as possible. It extends beyond traditional automation by combining multiple technologies, tools, and platforms, including **robotic process automation (RPA)**, **process management (BPM), machine learning (ML), artificial intelligence (AI), business** and decision management systems.

The term emerged as a response to the growing need for agility and scalability. Rather than automating isolated tasks, hyperautomation aims to create an interconnected ecosystem of technologies that can adapt, learn, and operate across complex processes. It builds upon the notion that automation is no longer optional; rather, it is a strategic imperative for improving efficiency, compliance, and service delivery.

4.20.1 Automation vs Hyperautomation

Traditional automation typically focuses on well-defined, repetitive tasks. These may include invoice processing, data migration, or basic customer queries. Hyperautomation, by contrast, addresses more dynamic and knowledge-intensive activities, enabling the orchestration of end-to-end processes. It allows for intelligent decision-making and continuous process optimisation by integrating real-time analytics, natural language understanding, and predictive capabilities.

A key distinction lies in scope and adaptability. While traditional automation is rule-based and static, hyperautomation incorporates adaptive algorithms capable of evolving with business needs and environmental changes. This shift also introduces new governance challenges, particularly regarding oversight, accountability, and ethical considerations in decision-making.

4.20.2 Relevance for Public and Private Sector Organisations

In the private sector, hyperautomation is often pursued to reduce operational costs, increase responsiveness to customer needs, and gain competitive advantage. For example, automated onboarding workflows integrated with customer relationship management (CRM) systems can significantly reduce time-to-service while maintaining data integrity.

In the public sector, hyperautomation offers a path toward enhanced service delivery and administrative efficiency, particularly in contexts constrained by budgetary and human resource limitations. Examples include intelligent document processing for benefits administration, predictive analytics in urban planning, and AI-assisted public procurement systems. However, these applications require careful alignment with public values such as transparency, fairness, and legal compliance.

The implementation of hyperautomation in public entities also intersects with broader objectives such as digital government, interoperability, and citizen trust. The challenges are not merely technical, but also institutional, cultural, and ethical.

4.20.3 Governance and Risk Considerations

The adoption of hyperautomation demands a robust governance framework. Key elements include:

- **Process discovery and evaluation**: Systematic identification of candidate processes for automation.
- **Change management**: Communication strategies and capacity-building initiatives to support organisational adaptation.
- **Risk and compliance oversight**: Integration of regulatory requirements and internal controls into automation workflows.
- **Lifecycle management**: Continuous monitoring and improvement of automated processes, including AI retraining where applicable.

Hyperautomation introduces novel forms of risk, including algorithmic opacity, dependency on third-party platforms, and unintended consequences of autonomous decisions. These require a multidisciplinary approach to governance, involving not only CIOs and CTOs but also CISOs, compliance officers, legal advisors, and domain specialists.

4.20.4 Strategic Implications

Hyperautomation aligns closely with strategic initiatives for operational excellence, and innovation-driven growth. It also supports the pursuit of maturity in process governance and digital capabilities. For decision-makers, the challenge lies in balancing ambition with responsibility: selecting the right processes, ensuring interoperability, managing vendor dependencies, and maintaining ethical standards.

Ultimately, hyperautomation is not an endpoint but a capability. It enables organisations to move from fragmented automation efforts toward coherent, intelligent ecosystems, capable of learning, adapting, and delivering value across diverse operational contexts.

4.21 Identity Management

Identity Management refers to the organisational processes, technologies, and policies used to manage digital identities. It encompasses the identification, authentication, and authorisation of individuals, systems, and devices, ensuring that the right entities have access to the right resources at the right times and for the right reasons.
This capability underpins security, privacy, and trust in digital environments. Identity Management is essential not only for operational integrity but also for regulatory compliance, particularly where access to sensitive or personal data is involved. As organisations increase their dependence on digital services, both internally and in interactions with clients and stakeholders, identity-related risks and complexities also rise.

4.21.1 Core Functions and Mechanisms

Traditional **Identity and Access Management (IAM)** systems typically serve internal users, focusing on employee directories, role-based access controls, and lifecycle management. These systems are often tightly integrated with enterprise directories and security policies. Core functions include:

- **Authentication** – Verifying the identity of a user or device (e.g., passwords, biometrics, tokens).
- **Authorisation** – Granting access based on roles, attributes, or contextual rules.
- **Provisioning** – Creating, updating, and revoking identities as part of organisational workflows.
- **Auditing and monitoring** – Tracking access patterns to detect misuse or anomalies.

Federated identity and **Single Sign-On (SSO)** mechanisms enable secure access across organisational boundaries, while **Multi-Factor Authentication (MFA)** increases assurance levels in authentication.

4.21.2 The Emergence of CIAM

Customer Identity and Access Management (CIAM)[69,70,71,72] is a concept that represents a shift in focus from internal control to external engagement. CIAM solutions are designed to manage identities of clients, citizens, or users interacting with digital services. They integrate identity verification, consent management, and user experience features into a single architecture.
Unlike traditional IAM, CIAM must accommodate high scalability, seamless user journeys, and strict privacy and consent requirements. Personalisation, omnichannel access, and social login capabilities are often embedded into CIAM strategies.
CIAM is particularly relevant in contexts where organisations (public or private) must interact with large and diverse populations, such as digital government portals, utility providers, or healthcare platforms. It supports both trust and usability, balancing security with user expectations and legal obligations such as those set by the General Data Protection Regulation (GDPR).

4.21.3 Digital Wallets and Decentralised Identity

Digital Wallets represent a newer paradigm, enabling individuals to store and control digital credentials (e.g., ID cards, licences, qualifications) on their personal devices. This supports the vision of **Self-Sovereign Identity (SSI)**, where individuals have control over their identity data and choose when and how to share it.
In the European context, the **European Digital Identity Wallet (EUDIW)** initiative exemplifies this trend. The purpose it that each Member State must provide to its citizens wallets designed to be interoperable across Member States, usable in both public and private services, and compliant with **eIDAS 2.0** regulation. The EUDIW enables citizens to access services securely while retaining control over their data, thus reinforcing both digital sovereignty and privacy.
For organisations, integrating with digital wallets presents new challenges in terms of trust frameworks, cryptographic verification, and consent capture. At the same time, they reduce the burden of identity proofing and offer improved assurance and fraud resistance.

4.21.4 Governance and Strategic Considerations

Effective IAM (internal or extended to CIAM[73]) is nowadays a complex challenge, requiring alignment between security, privacy, compliance, and user experience objectives. Key governance issues include:

- **Policy definition** – Ensuring that access policies are consistent with business roles, data classification, and regulatory requirements.
- **Lifecycle management** – Coordinating identity data creation and retirement across multiple platforms.
- **Interoperability** – Aligning internal IAM/CIAM systems with external identity providers and digital wallet standards.
- **Incident response** – Preparing for identity breaches or misuse, with appropriate detection and response mechanisms.

Strategically, Identity Management is central to Zero Trust architectures, digital service transformation, and the maturity of information security practices. Its complexity increases in hybrid environments involving cloud services, mobile access, and third-party integrations. Identity is no longer a perimeter function but a fundamental control point in every transaction and interaction.

[69] https://wso2.com/whitepaper/the-five-pillars-of-customer-identity-and-access-management/
[70] https://www.microsoft.com/en-us/security/business/security-101/what-is-ciam
[71] https://www.ibm.com/think/topics/ciam
[72] https://aws.amazon.com/what-is/ciam/
[73] https://www.computerweekly.com/feature/IAM-Enterprises-face-a-long-hard-road-to-improve

4.22 Everything as a Service

XaaS, or *Everything as a Service*, is an umbrella term referring to the delivery of IT services and functionalities by external entities, usually via cloud-based models, where resources are provisioned on-demand and typically consumed through subscription or pay-per-use models.

It generalises more established categories such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), expanding the logic of service abstraction to encompass a wide range of digital capabilities, including databases, development tools, security functions, and even business processes.

The XaaS paradigm emerged with the evolution of cloud computing and the increasing modularisation of IT services. It reflects a shift away from capital expenditure (CapEx) models based on in-house infrastructure and software ownership, towards operational expenditure (OpEx) models that favour agility, scalability, and service-based consumption.

4.22.1 Typologies and Examples

Typical examples of XaaS models include:

- **Software as a Service (SaaS)**: Delivery of software applications over the internet (e.g., CRM, ERP, productivity tools).
- **Platform as a Service (PaaS)**: Environments for application development and deployment without managing the underlying infrastructure.
- **Infrastructure as a Service (IaaS)**: Provisioning of virtualised computing resources such as servers, storage, and networking.
- **Security as a Service (SECaaS)**: Outsourced security services, including threat monitoring, identity management, and incident response.
- **Business Process as a Service (BPaaS)**: Outsourcing of business functions like payroll, customer service, or compliance management through automated platforms.

The landscape is continuously expanding, with emergent models such as AI as a Service, Monitoring as a Service, and even Governance as a Service appearing in various domains.

4.22.2 Strategic Implications

The adoption of XaaS models provides organisations with several strategic benefits:

- **Agility**: Faster deployment of services and solutions, supporting rapid innovation cycles.
- **Scalability**: Ability to adjust resource consumption dynamically in response to demand fluctuations.
- **Cost efficiency**: Reduction in upfront investment and infrastructure management overheads.
- **Focus**: Allows internal teams to focus on core competencies by outsourcing commoditised capabilities.

However, these benefits must be weighed against risks such as vendor lock-in, data sovereignty, service availability, and integration complexity. Decision-makers must assess which services are strategic and which can be externalised without compromising control or compliance.

4.22.3 Governance and Risk Management

A mature approach to XaaS adoption requires careful governance, covering:

- **Service Level Agreements (SLAs)**: Defining expectations for performance, availability, support, and compliance.
- **Risk management**: Evaluating service provider reliability, continuity planning, and regulatory exposure (e.g., GDPR, NIS2).
- **Interoperability and portability**: Ensuring that services can be integrated with existing systems and migrated if needed.
- **Monitoring and auditing**: Maintaining visibility over usage, costs, and security posture across multiple service providers.

XaaS adoption also intersects with broader topics such as enterprise architecture, procurement practices, and innovation roadmaps. Public entities, in particular, must ensure that externalised services remain aligned with legal and ethical obligations related to transparency, accountability, and public value.

4.22.4 Relevance in Public and Private Contexts

In the private sector, XaaS supports leaner operations, faster innovation, and better responsiveness to market changes. In the public sector, it enables modernisation of legacy systems and improved service delivery, particularly where internal IT capacity is limited.

National strategies on digital government often include explicit encouragement of XaaS models, provided that proper safeguards are in place.

The trend toward XaaS is expected to accelerate as more organisations seek resilience, flexibility, and access to cutting-edge technologies without the burden of ownership. Understanding its implications is essential for those involved in strategic governance of IT, procurement, and service design.

4.23 Artificial Intelligence…

Artificial Intelligence (AI) refers to a broad family of technologies that simulate cognitive functions such as learning, reasoning, perception, and decision-making. AI systems can analyse large datasets, detect patterns, and automate tasks that once required human judgement. They are used across sectors to optimise operations, personalise services, support diagnostics, enhance logistics, and enable new forms of interaction. Common forms include:

- **Machine learning**: systems that adjust their outputs based on patterns found in data.
- **Natural language processing (NLP)**: enabling machines to process and generate human language.
- **Computer vision**: interpreting visual information from images or video.
- **Generative AI**: producing content such as text, code, or designs.
- **Autonomous systems**: capable of acting in dynamic environments with limited human input.

As these techniques become embedded in solutions to support strategic decision-making and core operations, they raise new challenges in governance, risk management, and organisational accountability.

4.23.1 Governance of Algorithmic Systems

Algorithmic systems are software-based mechanisms that make or influence decisions using any combination of predefined rules, statistical models, or learning algorithms. What makes them distinctive is not only their speed or scale, but the way in which they translate intent into automated decisions, often without transparent logic or human review, implying its usage always brings risks.

These systems pose significant governance challenges. Their complexity can obscure responsibility, their behaviour may shift over time, and their outcomes may reflect hidden biases in data or design. Without oversight, algorithmic systems can amplify bias, undermine trust, or expose organisations to reputational and regulatory risk. Governing algorithmic systems requires a deliberate effort to clarify:

- What decisions are delegated to automation, and why;
- Who defines objectives and accepts trade-offs;
- How behaviour is monitored, explained, and reviewed;
- What safeguards exist.

A mature governance approach includes explicit documentation, human-in-the-loop oversight, and escalation procedures, integrated into risk management, compliance processes, and information governance. [74]

4.23.2 Explainability and Strategic Risk

Explainability refers to the ability to account for how and why an algorithmic system produces a given output or decision. In many sectors, this is not optional: financial services, healthcare, and public services are subject to laws and expectations that require meaningful explanations for actions that affect individuals.

Lack of explainability introduces multiple risks:

- **Compliance failures**: when decisions cannot be justified under legal or ethical standards.
- **Operational disruption**: when staff do not understand how to interpret or challenge AI recommendations.
- **Strategic misalignment**: when automated decisions contradict organisational values or policy goals.

The pursuit of explainability involves technical, organisational, and cultural dimensions. Some systems can be redesigned to favour interpretability over raw predictive performance. In other cases, governance measures must ensure that decision-making processes remain intelligible and contestable, even if models themselves are complex.

Governance must treat explainability not as a technical feature but as a foundation for trust and legitimacy[75,76].

4.23.3 CxO and Organisational Alignment

AI initiatives typically cut across multiple executive domains. The **CTO** may lead system integration; the **CIO** ensures coherence with existing architectures and services; the **CISO** addresses risks related to data protection, adversarial manipulation, and regulatory compliance. Meanwhile, business executives such as the **COO** or **CMO** are responsible for how AI shapes user experiences and operational outcomes.

Without coordination, these roles may operate in silos, leading to gaps in oversight, conflicting priorities, or unchecked vendor influence. Governance maturity requires clear definition of:

- Strategic ownership and sponsorship of AI initiatives;
- Risk classification and impact assessment procedures;
- Policies for procurement, deployment, and decommissioning;
- Ongoing monitoring and adaptation of AI-enabled processes.

In many organisations, consultants play a vital role in helping leadership understand where governance structures need to be extended or adapted to accommodate algorithmic systems.

4.23.4 Regulatory Context

The EU Artificial Intelligence Act introduces a **risk-based regulatory framework** for AI systems, with obligations that vary according to the level of risk posed to rights, safety, or public interests. It identifies:

- **Prohibited systems** (e.g. social scoring, subliminal manipulation);
- **High-risk systems** (e.g. in employment, education, critical infrastructure);
- **Limited-risk systems** (e.g. chatbots, recommender systems).

Organisations deploying high-risk AI will be required to maintain documentation, ensure human oversight, conduct risk assessments, and register systems in a public database. These rules are likely to influence global standards and sectoral expectations well beyond the EU[77].

Anticipating this landscape, many organisations are adopting internal AI governance frameworks that incorporate principles such as fairness, robustness, transparency, and accountability. International guidance (e.g. OECD AI Principles, ENISA reports) supports the development of voluntary codes of conduct and sector-specific adaptations[78].

Strategically, AI governance is no longer a future issue. Considering its power, it is a present requirement.

[74] https://sloanreview.mit.edu/audio/ethically-sourced-creativity-shutterstocks-alessandra-sala/
[75] https://www.ibm.com/think/topics/chief-ai-officer
[76] https://www.simplyhired.com/search?q=chief+algorithm+officer
[77] https://www.wsj.com/articles/ai-regulation-is-coming-fortune-500-companies-are-bracing-for-impact-94bba201
[78] https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/eu-model-contractual-ai-clauses-pilot-procurements-ai

4.24 Start-ups as Strategic Vehicles

The term "start-up" is often used informally to describe newly founded companies, particularly those working in technological domains. However, in strategic terms, a start-up is better understood not as a type of organisation, but as a **temporary vehicle** created to explore new value propositions under conditions of uncertainty. A start-up precedes the establishment of a repeatable and scalable business model. It exists to **search for product-market fit**, not to operate at scale.
Unlike established organisations, start-ups operate without the stabilising constraints of operational routines, governance structures, or legacy systems. Their purpose is exploratory: to test hypotheses about what value can be created, for whom, and how it can be delivered in a sustainable manner. In this sense, a start-up is more akin to a strategic **experiment** than a company in the traditional sense.

4.24.1 Strategic Role of Start-ups

Start-ups are often situated within broader **strategic transformation efforts**. They can be:

- Independent ventures, later absorbed or scaled;
- Internal initiatives launched within larger organisations (e.g., corporate start-ups or innovation labs);
- Vehicles for public sector transformation, sometimes sponsored through funding programmes or regulatory sandboxes.

In such contexts, start-ups serve as **probes into the future**, allowing an organisation (or ecosystem) to explore possibilities that are too uncertain or too disruptive to be managed through conventional structures.
The start-up approach is particularly relevant in sectors where **regulatory changes** or **emerging technologies** create new opportunity spaces. In public sector innovation, start-up-like models may be used to test policy instruments or new service models before institutionalising them.

4.24.2 Methodologies and Practices

Several strategic and managerial approaches are commonly associated with start-ups:

- **Lean Start-up**: Emphasises iterative development and validated learning through experimentation, using techniques such as Minimum Viable Product (MVP) and Build-Measure-Learn cycles.
- **Innovation Accounting**: Focuses on tracking progress through learning milestones rather than traditional financial metrics.
- **Strategic Pivoting**: Adjusting the core assumptions about the business model based on feedback and evidence, a practice essential in navigating uncertainty.

Start-ups typically prioritise speed, feedback loops, and a high tolerance for failure in order to maximise learning. Their value lies not in immediate success, but in the acceleration of strategic insight.

4.24.3 Lifecycle and Exit

The end of a start-up phase occurs when:

- A viable business model is discovered and the initiative transitions into a conventional enterprise;
- The learning generated is absorbed into another structure[79];
- The initiative is terminated due to failure to validate key assumptions.

*In all cases, the strategic function of the start-up is to **reduce uncertainty** and **inform strategic decisions**. Its success is not defined solely by survival, but by the quality of insight it produces for future decisions.*

[79] "It Was the Worst of Times—and the Best Time to Make $32 Billion - Google just made its biggest deal ever for Wiz, a cybersecurity startup founded only five years ago. It's even unlikelier than it sounds" - https://www.wsj.com/tech/cybersecurity/wiz-google-deal-cybersecurity-cloud-80ec455d?mod

4.25 Technology Due Diligence

Technology Due Diligence (Technology DD) is the structured evaluation of an organisation's technological landscape, including its systems, infrastructure, governance, capabilities, risks, and future-readiness.

Technology DD, or **IT Due Diligence (IT DD)**, is an investigation started by an investor to the IT landscape of a target company (a company that wants an investment). It is typically undertaken in the context of investment, acquisition, outsourcing, or strategic partnerships, and is aimed at reducing uncertainty and informing decision-making. Whether applied in private equity transactions, public-sector outsourcing, or innovation-driven collaborations, technology due diligence provides a factual foundation for assessing technological maturity, integration potential, and operational risk.

While financial due diligence focuses on past performance and compliance, and legal due diligence examines contractual and regulatory exposure, technology due diligence focuses on understanding how the organisation's digital assets and practices enable or constrain its mission and strategic goals. It combines technical analysis with broader insights into organisational structure, resource allocation, governance posture, and capability development.

4.25.1 Dimensions of Technology DD

A due diligence process typically includes several dimensions:

- **Architecture and Infrastructure -** The evaluation considers whether core systems are fit for purpose, scalable, and maintainable. This includes examining the design, complexity, and integration of legacy and modern systems; hosting arrangements (on-premise, cloud, hybrid); dependency on proprietary components; and potential for future adaptability. Inadequate or outdated infrastructure can represent a hidden cost, especially if major refactoring or migration would be required to meet the buyer's or partner's standards.
- **Applications and Data -** Applications are assessed in terms of business alignment, lifecycle maturity, vendor support, and customisation. The treatment of data (its quality, ownership, portability, and compliance with protection and localisation rules) is a critical element, especially in regulated sectors. The ability to generate timely, actionable insights from data is also an indicator of strategic readiness.
- **Security and Risk Exposure -** A core area of concern in any technology assessment is cybersecurity. The review considers current security controls, policies, and incident history, as well as exposure to vulnerabilities through third-party providers, shadow IT, or poor user practices. It also examines alignment with security standards (e.g. ISO/IEC 27001), incident response capacity, and the independence of the security function.
- **Governance and Documentation -** Effective governance is essential to sustained performance and resilience. Due diligence examines the clarity of decision-making structures, documentation of processes, auditability of actions, and maturity of management systems. Where governance is informal, reactive, or opaque, risks may be underestimated or poorly managed.
- **People and Capability -** The knowledge, experience, and retention of internal teams, along with dependency on key individuals or external contractors, are reviewed as part of assessing continuity and scalability. Organisational culture, internal communication, and the alignment of IT with business functions also play a role in determining how well technology serves the broader enterprise.
- **Alignment with Strategy and Compliance -** Technology is not neutral (it either supports or obstructs strategic intent). Due diligence evaluates how well the technology stack aligns with stated business goals, regulatory requirements, ESG commitments, and the organisation's operational model. This includes consideration of technical debt, roadmap feasibility, and change readiness.
- **Public vs Private Sector Contexts -** In the private sector, technology due diligence often informs pricing, negotiation, or integration strategy. In the public sector, it may serve as a basis for investment justification, risk assurance, or vendor selection. Public entities also face additional layers of scrutiny regarding transparency, procurement rules, and long-term accountability.

4.25.2 Conclusion

Technology DD transforms assumptions into evidence. It helps uncover hidden costs, unacknowledged risks, and overlooked strengths. Whether performed internally or by external specialists, it must be framed not as a mere checklist, but as a strategic inquiry into the fitness of technology to serve institutional goals, respond to risk, and support future growth or transformation.

4.26 CxO Dilemmas

The path from IT strategy to organisational change is rarely smooth. Even well-resourced initiatives encounter tensions, blind spots, and competing priorities that must be addressed with care and maturity[80],[81].

4.26.1 Tension Between Stability and Change

Organisations must uphold operational continuity and compliance while responding to technological shifts, evolving stakeholder expectations, and competitive pressures. Balancing the demand for innovation with the need for predictability poses a recurring challenge. Legacy systems may constrain progress, while newer solutions often introduce operational and governance risk. The difficulty lies not in choosing change over stability, but in pacing and structuring change without compromising reliability.

4.26.2 Fragmentation of Responsibility

Many organisations operate within distributed ecosystems involving internal departments, outsourced services, regulatory bodies, and platform providers. When digital initiatives cross organisational or contractual boundaries, it becomes difficult to attribute responsibility for outcomes. Even well-defined frameworks may be insufficient when deeper issues such as power imbalances or unclear incentives are present. Failures often stem from fragmented governance rather than poor technology.

4.26.3 Competing Rationalities

Strategic decisions are shaped by legal, political, economic, cultural, and ethical concerns. These dimensions do not always align neatly. For instance, deploying AI to optimise workflows may conflict with transparency or fairness concerns. Increasing surveillance for security may infringe on privacy or civil liberties. These are not purely technical dilemmas but require institutional judgement and capacity for deliberation.

4.26.4 Strategic Ambition Versus Organisational Capacity

Digital strategies must be calibrated to the actual maturity, culture, and capabilities of the organisation. Overambitious programmes may overwhelm internal teams, erode trust, or fail to deliver value. Conversely, underinvestment in capacity building may limit transformation and expose the organisation to unmanaged risk. Strategic realism (understanding the organisation's limits and enabling gradual learning) is key to sustainable change.

4.26.5 Timing, Sequencing, and Pacing

Deciding when to act, and in what order, is a strategic concern. Acting too early may incur costs before readiness; acting too late may mean missing critical opportunities. Incrementalism may lead to slow progress; disruption may cause institutional resistance[82]. Poor timing can derail otherwise sound plans. Effective sequencing supports organisational learning, maintains alignment, and preserves momentum.

4.26.6 Navigating Ambiguity and Noise

Strategic environments are full of ambiguity. Terms like "digital transformation," "agility," or "smart governance" often lack shared definitions. They may obscure more than they reveal. Governance maturity involves not only using frameworks but critically engaging with concepts, questioning assumptions, and clarifying what is actually at stake. This includes resisting buzzwords and anchoring discussions in real organisational concerns.

4.26.7 Conclusion

Strategic change is not linear.
It is shaped by dilemmas that require more than technical solutions, they demand institutional reflection, leadership maturity, and a capacity to hold competing values in view.
The role of governance is not to resolve all tensions, but to provide clarity, structure, and accountability in navigating them.

[80] Risks in "too much" innovation: https://www.nytimes.com/2024/08/23/business/economy/realpage-doj-antitrust-suit-rent.html
[81] Risks of "too much" success: https://www.nytimes.com/2024/08/13/technology/google-monopoly-antitrust-justice-department.html
[82] …or even worst: https://www.wsj.com/tech/sonos-speakers-app-ceo-24250f2c

4.27 Oops…

4.27.1 The Wrong Cloud at the Right Time

Tomás, the junior consultant from the Mature Team, joins a strategic initiative in a large public sector agency aiming to migrate core services to the cloud.

The migration is framed as a move toward agility, cost-efficiency, and long-term resilience.

Tomás is tasked with mapping the existing application landscape and supporting the selection of services for early migration.

The agency's leadership is enthusiastic, citing political priorities and alignment with European digital goals.

However, as Tomás works through the inventories, he notices several systems are deeply entangled with legacy data stores and vendor-specific dependencies. Integration costs are likely to be much higher than anticipated.

Tomás raises the concern cautiously during a strategy session, but the project sponsor insists the migration proceed as scheduled. "The cloud provider will handle those issues," is the response. Eager not to block progress, Tomás moves on.

Months later, the early-migrated applications suffer performance issues. Latency increases. Internal teams struggle with integration across cloud and on-prem environments. Procurement contracts are revisited under pressure, and what was meant to be a showcase of cloud readiness becomes a cautionary tale.
Lesson learned: strategic timing is not enough. Cloud transitions demand rigorous application assessment—not just by infrastructure type, but by business entanglement, dependency chains, and interoperability. If ignored, those roots trip even the best-intentioned leaps.

4.27.2 Oversight in the Shadows

In the same project, Fábio from the Wildcard Team is brought in to support stakeholder engagement and change communication.

He's energised by the potential of cloud to transform service delivery and user experience.

His idea: run a series of interactive sessions to build momentum and showcase what's coming. The focus is on visual narratives and bold messaging: "Public Services, Anywhere. Anytime."

Fábio quickly becomes the face of the change effort. His sessions attract attention and even press coverage.

But behind the scenes, several departments are growing concerned.

Privacy risks haven't been fully mapped. The national data protection officer has not yet been formally involved. A data residency clause in the cloud agreement is still under legal review.

One of Fábio's slide decks, widely shared, promises "cross-border data access and real-time analytics." When legal teams see this, alarms go off. The project is halted for reassessment. Trust with stakeholders is strained.

Fábio reflects on what went wrong. He had asked about legal review early on, but received vague reassurance that "it's being handled." He hadn't pushed or paused his messaging to verify alignment.

Lesson learned: communication is powerful, but risky when misaligned with legal and governance realities. In strategic change, visibility must be earned not through ambition, but through coherence across functions. If the groundwork isn't finished, no amount of storytelling can fix the fallout.

These two failures were not caused by technology or bad intent. They were born from assumptions (about what could be migrated, what had been reviewed, and who was paying attention). Strategic initiatives need vision, but also structure. In cloud transformation especially, timing, legal preparedness, and honest mapping of readiness are not secondary, they are the strategy.

4.28 …Oops … again…

The Rush to Shine

The Ministry of Education and Innovation (MEI) in a mid-sized EU country announced its boldest initiative yet: a nationwide platform to unify student records, teacher dashboards, funding data, and AI-driven insights across all public schools.
The project, branded **EDU.ONE**, was launched under pressure (European recovery funds required visible results within 18 months).

Two consulting firms were hired under separate contracts:

- **BrightWave Digital**, to lead platform design, tech stack selection, and user experience.
- **PraxisCore**, to support strategy, risk governance, and compliance.

From BrightWave came:

- **Carla**, tasked with making the country "look like Estonia in a year." Known for flair and tight deadlines.
- **Tiago**, her trusted developer, enthusiastic about cloud-native architectures and open-source reuse.

From PraxisCore:

- **Laura**, a cautious strategist with experience in large-scale education reform projects.
- **Tomás**, specialised in due diligence and regulatory alignment.

Tension was immediate…
BrightWave pushed for a high-visibility launch. Carla called meetings "obstacles."
PraxisCore requested a formal **due diligence phase**, to assess data classification, vendor dependencies, and system readiness. Tiago, impatient, told a colleague, "Due diligence is for banks, not builders."

The MEI Director, politically ambitious, backed BrightWave. "We'll fix governance once the beta is live," he said.

PraxisCore was sidelined.

BrightWave went fast. The team selected a mix of commercial and open-source tools, many of which required **third-party plugins** with unclear licensing. Tiago imported "AI models for student performance prediction" from a public repo without review. A major cloud provider was engaged, **without a procurement competition or formal data residency guarantees**.

Laura issued a written warning: without clarity on roles, risk ownership, and integration governance, MEI was exposed to massive reputational and legal risk. Her warning was ignored.

EDU.ONE launched six months early, with the Prime Minister attending.
It lasted five days.

- Teachers couldn't access historical records.
- Parents received wrong eligibility notices for benefits.
- A data leak revealed sensitive data of 200 minors due to misconfigured API permissions.

Journalists revealed the AI model was trained on foreign data, violating EU data sovereignty rules.
The Data Protection Authority opened an investigation. Parliament froze the second funding tranche.
The MEI Director resigned.

An external audit (now led by Laura and Tomás) revealed what had been missing from day one:

- **No Target Operating Model**.
- **No Strategic Portfolio Governance**.
- **No Enterprise Architecture integration**.
- **No vendor due diligence**, not even a DPIA.

Carla left BrightWave.
Tiago disappeared from LinkedIn.

PraxisCore's final report concluded that *had a proper due diligence process been respected and the two consultancies integrated into a shared governance structure*, most failures could have been prevented.
The platform was decommissioned. Public trust in "AI for education" collapsed.

As one school principal later told a journalist:
"They came to make us smarter. They left us cleaning up their homework."

4.29 …What? …

4.29.1 All the Right Words, None of the Right Anchors

Inês and Fábio from the Wildcard Team are brought in to support a fast-track digital strategy initiative in a national healthcare organisation.

The objective is ambitious: define a "cloud-first, AI-enabled, user-centred" transformation roadmap to be presented to government stakeholders within six weeks.

Inês, known for her creative brilliance, proposes a bold reimagining of the organisation's operating model. She sketches conceptual maps, uses cutting-edge terminology, and captures executive attention with visionary ideas.

Fábio supports by creating sleek visual materials and injecting provocative metaphors into every workshop.

But behind the scenes, operational staff grow uneasy.

Critical infrastructure is still bound to legacy platforms. No assessment of organisational maturity or procurement constraints has been completed. Privacy implications of the proposed analytics tools remain unaddressed.

When the roadmap is presented, internal leaders nod politely, but implementation stalls. Legal and IT teams push back. The political sponsor, embarrassed, scales back the project.

Inês later reflects that their work had style, but not enough structure. Fábio, too, admits: "We made a strategy for an organisation we imagined, not the one that was actually there."

Lesson learned: vision without grounding becomes noise. In strategic transformation, clarity requires not just aspiration, but traction with reality (technical, legal, and institutional).

4.29.2 Same Ambition, Different Groundwork

Meanwhile, in a neighbouring directorate, Sofia and Mateus from the Dream Team are engaged in a parallel transformation effort.

Their brief is less glamorous: support the early-phase design of a governance model for digital change. It's not expected to be "inspiring," but it's strategically critical.

Sofia begins by listening. She meets with IT operations, legal, programme management, and clinical leaders. She maps their actual pressures (procurement bottlenecks, staffing shortfalls, cybersecurity gaps).

Mateus builds a maturity model reflecting their current capabilities and projected effort required for key changes. They propose a phased roadmap (not flashy, but operationally credible).

When they present their findings, the response is different. Instead of silence, they hear: "That's exactly what we've been trying to explain." The proposal is adopted as the internal reference for the next funding cycle. It forms the spine of the wider change programme, and is later incorporated into a national digital health strategy.

Lesson learned: success in strategic transformation is not always about being visionary, it's about creating clarity others can act on. When ideas resonate with the real constraints and rhythms of the organisation, transformation becomes not just possible, but durable.

These two stories highlight that strategy is not only a product, but also a process!
One pair of consultants built narratives detached from the ground.
Another built alignment by honouring the lived complexity of the system.
Both had talent. Only one built trust.
The difference lay in how they listened (and what they chose to ignore).

4.30 OK!

4.30.1 Strategic Calm in a Political Storm

Laura and Tomás from the Mature Team are supporting a national regulator during a tense period of organisational transition.

A new strategic plan is being finalised under political pressure, with high expectations for digital innovation, but also a legacy of stalled initiatives and compliance anxieties.

Laura is asked to facilitate the articulation of strategic digital goals. She quickly senses unease: different directors express contradictory visions, and the board expects consensus within weeks.

Tomás, helping with preparatory interviews, realises that unresolved past frictions still shape current positions.

Rather than rush to synthesis, Laura slows the process. She proposes a working session focused not on solutions, but on surfacing strategic tensions safely.

With Tomás facilitating side conversations, they co-develop a shared map of constraints, dependencies, and reform fatigue.

When the final plan is submitted, it is modest in language, but clear in priorities, phases, and governance.

Instead of promising a digital revolution, it commits to enabling one through stability, funding alignment, and internal capability-building.

Lesson learned: in politically exposed strategies, what goes unsaid matters as much as what is declared. Strategic clarity often emerges not from big declarations, but from helping institutions breathe, reflect, and reset expectations.

4.30.2 From Vendor-Led to Value-Led

Bruna and Ricardo from the Contingent Team are assigned to a regional healthcare network undergoing a major system renewal.

A platform vendor had initially taken the lead in framing the digital architecture and implementation schedule, and things were moving fast, but leadership began to feel disempowered, unsure if their specific needs were being translated into actual configurations.

Bruna picks up on this hesitation during early meetings. She notices that executives are deferring to the vendor on core strategic choices, including interoperability and data-sharing frameworks.

Ricardo suggests holding a “pause and clarify” retreat, not as a reset, but as a way to formally reconnect strategy with implementation.

During the retreat, Bruna facilitates a walkthrough of key architectural choices from the organisation’s point of view.

Ricardo translates those choices into governance implications.

The tone shifts: leadership begins to assert their authority over design decisions and to reframe the vendor relationship from technical supplier to strategic partner.

The project continues, but now with stronger alignment, better documentation, and a new steering committee that includes legal and operational leads (not just IT and vendor reps).

Lesson learned: strategic control doesn’t require confrontation; it requires structure and space to think. In complex change environments, even small interventions can restore ownership and reshape trajectories.

These stories show that when strategy is shaped with humility, clarity, and respect for institutional pace, progress follows.
The absence of visible failure does not mean success is easy, only that it was quietly and carefully earned.
Strategic consultants thrive not just by proposing ideas, but by cultivating the conditions under which good decisions can emerge.

4.31 Wrap-up…

The list below presents the key ideas for understanding how organisations use information systems and technology not only to support current operations but also to drive strategic transformation, adapt to change, and innovate responsibly:

- **Business Strategy** – The coordinated set of actions and priorities through which an organisation seeks to achieve its long-term goals and fulfil its mission.
- **IT Strategy** – The plan that defines how information technology will support, enable, or shape the business strategy, ensuring coherence between technological capabilities and organisational ambitions.
- **Strategic Alignment** – The process of ensuring that IT initiatives, resources, and governance structures are directly connected to strategic business objectives and can adapt as goals evolve.
- **Digital Transformation** – The deliberate integration of digital technologies into all areas of an organisation, fundamentally changing how it operates and delivers value.
- **Stakeholder Engagement** – The structured identification, involvement, and management of individuals or groups who are affected by or can influence strategy, ensuring support, communication, and shared understanding.
- **Strategic Communication** – The purposeful use of communication practices to align internal and external stakeholders around strategic goals, manage expectations, and support change initiatives.
- **Senior Sponsorship** – The active role of a senior executive in championing and steering a strategic initiative, providing authority, resources, and legitimacy.
- **Target Operating Model (TOM)** – A blueprint of the desired future state of an organisation's capabilities.
- **Enterprise Architecture (EA)** – The practice of designing and governing the relationships between business processes, information flows, applications, and technological infrastructure to achieve the objectives.
- **Capability-Based Planning** – An approach to strategy that focuses on building and evolving the organisational capabilities needed to achieve future goals, rather than only projects or technologies.
- **Portfolio Governance** – The oversight and coordination of an organisation's entire set of strategic initiatives and investments, ensuring that resources are prioritised, risks managed, and outcomes aligned with strategic goals.
- **Investment Governance** – The frameworks and processes used to evaluate, prioritise, approve, and monitor strategic investments, particularly in IT and innovation initiatives.
- **Change Management** – The structured approach to preparing, supporting, and guiding individuals, teams, and organisations through transitions or transformations.
- **Strategic Risk Management** – The identification, assessment, and mitigation of risks that could significantly impact an organisation's ability to achieve its objectives.
- **Cybersecurity as a Strategic Risk** – The recognition that failures in cybersecurity can have consequences for reputation, trust, continuity, and regulatory compliance, requiring board-level visibility and proactive governance.
- **Sector-Specific Standards for Cybersecurity** – Industry or sector-specific frameworks (e.g., in healthcare, energy, finance) that shape how cybersecurity is managed in support of strategic objectives and regulatory compliance.
- **Data Protection Impact Assessment (DPIA)** – A systematic process to evaluate the risks to privacy and fundamental rights arising from new initiatives, particularly those involving personal data, ensuring that privacy risks are addressed from the design phase.
- **Technology Maturity Assessment** – The evaluation of the maturity and readiness level of a technology (e.g., using Technology Readiness Levels - TRL), informing strategic decisions about adoption, investment, or integration.
- **Technology Research** – The systematic exploration and evaluation of emerging technologies and their potential strategic value, including scouting, piloting, and collaboration with research providers.
- **Technology Research Providers** – External organisations (such as specialised firms, universities, or think tanks) that support strategy by offering insights, assessments, and projections about emerging technologies.
- **Capital Expenditure (CapEx)** – Investment in assets such as hardware, infrastructure, or major systems that are expected to provide value over several years, often with strategic implications for budgets and governance.
- **Operational Expenditure (OpEx)** – The ongoing costs for running systems and services (e.g., cloud subscriptions, maintenance, support), increasingly relevant in modern IT strategies where flexibility and scaling are valued.
- **Cloud Adoption Assessment** – The structured evaluation of an organisation's readiness and strategic needs related to migrating to or expanding cloud services, balancing benefits with governance, risk, and compliance concerns.
- **Everything as a Service (XaaS)** – A model in which services traditionally delivered internally (such as infrastructure, platforms, or software) are provided on demand by external vendors, shifting strategic considerations about control, cost, and agility.
- **Governance of Algorithmic Systems** – The application of governance principles (accountability, fairness, transparency) to systems that use algorithms, especially AI, recognising their influence on decisions and operations.
- **Explainability in AI and Strategic Risk** – The capacity to understand, interpret, and justify decisions made by AI systems, recognised as critical for strategic risk management, especially in regulated sectors.
- **Start-ups as Strategic Vehicles** – The use of start-up structures to explore innovation, manage uncertainty, or develop transformative capabilities that may not be achievable through existing organisational forms.
- **Technology Due Diligence** – The structured assessment of technology assets, capabilities, and risks during mergers, acquisitions, partnerships, or investment decisions, ensuring strategic alignment and risk visibility.
- **Strategic Ambition versus Organisational Capacity** – The critical evaluation of whether an organisation's culture, processes, and resources are sufficient to achieve its strategic ambitions, as overreach can cause failure.

Notes:

- Strategic thinking must be tightly connected to **governance, risk awareness, and institutional maturity**.
- Digital transformations are not simply about adopting new tools; even if that is a vague concept, it always should be understood as about **aligning technology, people, and processes** to real strategic goals.
- In consulting and advisory roles, understanding strategic misalignments, capability gaps, or portfolio governance weaknesses will be essential for giving credible advice.

Real-World Cases

Following is a list of real-world cases related to the concepts addressed in these notes. Each case includes a short description, references to relevant lecture note items, and a classification by cause, consequence, and result. These examples serve as learning tools to illustrate how decisions, failures, and successes influence the governance and evolution of digital systems in both public and private organisations.

<1> Maersk and the Quiet Catastrophe

Description: A.P. Møller–Maersk, the world's largest shipping and logistics company, suffered a massive operational shutdown in 2017 due to the NotPetya malware. Originating from a tax software update in Ukraine, the attack spread rapidly across global systems, disabling terminals, bookings, and communications. Maersk's recovery relied on salvaging a domain controller from a remote office that had been offline during the attack. The incident exposed deep architectural coupling, limited segmentation, and dependency on informal recovery practices.

Relevant Lecture Note Items:

- 3.5 Technical Debt and System Evolution
- 3.13 Operational Resilience and Incident Response
- 2.25 IT Supply Chain
- 2.15 The Ecosystem of Cybersecurity

Classification:

- **Cause:** Architectural fragility and lack of segmentation
- **Consequence:** Global service disruption across business units
- **Result:** Operational loss (~$300M), reputational questions, improved cyber architecture

Sources:

- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- https://softwarelab.org/blog/notpetya/
- https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

<2> Colonial Pipeline and the Long Weekend (2021)

Description: In May 2021, Colonial Pipeline shut down fuel distribution after a ransomware attack on its IT systems, even though OT systems were not directly compromised. The lack of visibility into the breach's full impact, along with poor coordination between IT and OT, led to a service halt affecting the U.S. East Coast. The company paid a $4.4 million ransom, partially recovered by authorities. The event demonstrated how digital risks can cascade into critical physical infrastructure.

Relevant Lecture Note Items:

- 3.13 Operational Resilience and Incident Response
- 2.6 Operational Technology and the IT/OT Interface
- 2.25 IT Supply Chain
- 2.15.2 National Authorities and Coordination
- 2.29.4 Strategic Relevance and Governance Maturity

Classification:

- **Cause:** Ransomware attack + poor IT/OT integration
- **Consequence:** Pre-emptive operational shutdown and fuel shortages
- **Result:** Economic disruption, federal policy reaction, cyber regulation update

Sources:

- https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
- https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
- https://www.bbc.com/news/business-57050690
- https://ransomware.org/blog/one-year-later-lessons-from-colonial-pipeline/

<3> ING agile transformation (2015)

Description: ING restructured its organisational model to adopt agile practices across banking functions, dismantling traditional hierarchies in favour of autonomous squads and tribes. While initially disruptive, it became a benchmark for digital transformation, despite early concerns from regulators.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 4.1 Business and Strategy

Classification: Intended cause, Good consequence, Positive results

Sources:

- https://www.mckinsey.com/industries/financial-services/our-insights/ings-agile-transformation
- https://www.ing.com/Newsroom/News/Squads-sprints-and-stand-ups.htm

<4> OpenAI and the Boardroom Shockwave (2023)

Description: In November 2023, OpenAI's board suddenly fired CEO Sam Altman without consulting key stakeholders. The lack of transparency and stakeholder alignment provoked near-unanimous staff backlash, a public offer from Microsoft to hire the entire team, and the board's subsequent reversal. The event revealed governance fragility in hybrid non-profit/commercial structures and the strategic risk of board isolation from operational realities.

Relevant Lecture Note Items:

- 1.21 Board Dynamics and Governance Structures
- 1.25 CxO Roles in Governance and Strategic Engagement
- 4.26 CxO Dilemmas
- 4.3 Stakeholder Engagement and Strategic Communication

Classification:

- **Cause:** Governance misalignment and opaque board decision-making
- **Consequence:** Organisational crisis and mass resignation threats
- **Result:** Board restructuring, Altman reinstated, stakeholder trust questioned

Sources:

- https://en.wikipedia.org/wiki/Removal_of_Sam_Altman_from_OpenAI
- https://medium.com/aicorporateedge/openais-boardroom-bombshell-unveiling-the-radical-shake-up-and-the-secret-players-behind-it-1e4a133fed5e
- https://boardshape.com/blog/when-boards-clash-with-visionaries-sam-altman-saga

<5> NHS email storm (2016)

Description: An accidental mass email sent to NHS staff caused disruption across the UK health service. Despite initial confusion, the event prompted improved controls and digital hygiene measures.

Relevant Concepts:

- 1.2 Management and Maturity
- 2.1 Governance of IT

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://www.bbc.com/news/technology-37979456
- https://arstechnica.com/information-technology/2016/11/nhs-email-storm-distribution-list-blunder/

<6> SEF migration debacle (2023)

Description: The poorly planned restructuring of Portugal's border agency SEF led to service failures, system outages, and a public backlash. Unclear role distribution and weak stakeholder coordination contributed to the disruption.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 1.2 Management and Maturity

Classification: Intended cause, Bad consequence, Negative results

Sources (Portuguese):

- https://cnnportugal.iol.pt/sef/problemas/problemas-informaticos-deixam-sef-lento-e-ate-parado-numero-de-processos-pendentes-nao-para-de-aumentar/20231003/65142e31d34e65afa2f5c77a
- https://observador.pt/2024/02/05/falta-de-acesso-as-bases-de-dados-do-sef-nao-compromete-investigacao-da-pj-diz-seguranca-interna/
- https://www.rtp.pt/noticias/pais/falta-de-acesso-as-bases-de-dados-do-sef-nao-compromete-investigacao-da-pj-garante-seguranca-interna_a1548639

<7> Germany's E-ID project

Description: Germany's digital ID initiative faced low adoption and public criticism due to inter-agency misalignment, low trust, and limited usability, despite its ambitious goals.

Relevant Concepts:

- 1.2 Management and Maturity
- 2.1 Governance of IT

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.signicat.com/blog/digital-identity-in-germany-market-status-trends-and-regulations-that-you-need-to-consider
- https://link.springer.com/chapter/10.1007/978-3-031-45648-0_29

<8> France health data hub realignment (2018…)

Description: Facing backlash over storing health data on US cloud infrastructure, France restructured its Health Data Hub to use a European provider, rebuilding trust and compliance posture.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 2.1 Governance of IT
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- https://implicity.com/everything-you-need-to-know-about-health-data-hub/
- https://openfuture.eu/note/the-french-data-protection-authority-reluctantly-greenlights-the-health-data-hubs-hosting-by-microsoft
- https://gdprhub.eu/index.php?title=CE_-_N%C2%B0_444937
- https://www.euractiv.com/section/health-consumers/news/french-decision-to-have-microsoft-host-health-data-hub-still-attracts-criticism/
- https://azure.microsoft.com/es-es/blog/microsoft-azure-is-now-certified-to-host-sensitive-health-data-in-france/
- https://learn.microsoft.com/en-us/compliance/regulatory/offering-hds-france

---

<9> Sonos App Overhaul Fallout (2024…)

Description: In 2024, Sonos released a major redesign of its mobile app that removed features, broke support for older devices, and degraded user experience. Loyal customers voiced frustration through negative reviews and social media backlash. Sonos was slow to respond, undermining trust. The case illustrates the risk of digital product changes without sufficient transition strategy or user engagement.

- **Relevant Lecture Note Items:**
  - 4.3 Stakeholder Engagement and Strategic Communication
  - 4.6 Enterprise Architecture and Alignment
  - 4.5 Target Operating Model
  - 3.5 Technical Debt and System Evolution
- **Classification:**
  - **Cause:** Abrupt digital product redesign without stakeholder alignment
  - **Consequence:** Feature loss, brand damage, and customer backlash
  - **Result:** Negative publicity, user trust erosion, delayed roadmap revisions
- **Sources:**
  - https://www.theverge.com/2025/1/13/24342282/sonos-app-redesign-controversy-full-story
  - https://edition.cnn.com/2025/02/08/tech/sonos-app-update-redemption-2025/index.html
    https://www.wsj.com/articles/sonos-marketing-chief-exits-as-fallout-from-app-calamity-continues-422ff362

<10> Harley-Davidson boardroom eruption (2025)

Description: Governance weaknesses led to a leadership crisis during CEO succession at Harley-Davidson, exposing gaps in board oversight and strategic alignment, and resulting in reputational and strategic setbacks.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 1.3 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.wsj.com/business/inside-the-boardroom-eruption-harley-davidson-future-ceo-search-proxy-battle-e740b646?mod=wknd_pos1
- https://eu.jsonline.com/story/money/business/2025/04/17/harley-davidson-corporate-drama-the-players-impact-on-customers/83127406007/

<11> Amazon Web Services (AWS) outages (2021)

Description: Several high-profile outages of Amazon Web Services disrupted global digital services, affecting major platforms across finance, media, logistics, and healthcare. These incidents raised awareness of over-reliance on single-cloud vendors and prompted widespread adoption of multi-cloud and hybrid strategies to improve resilience.

Relevant Concepts:

- 3.1 IT Services and Operations
- 3.2 Resilience and Incident Response
- 4.3 Strategic Portfolio and Investment Governance

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://devdosvid.blog/2024/06/03/unpacking-aws-outages-system-design-lessons-from-post-event-summaries/
- https://aws.amazon.com/message/12721/
- https://aws.amazon.com/premiumsupport/technology/pes/
- https://health.aws.amazon.com/health/status

<12> Boeing and the 737 MAX crisis (2018…)

Description: Two fatal crashes involving Boeing 737 MAX aircraft revealed failures in software design, risk disclosure, and regulatory coordination. Investigations uncovered governance breakdowns, prioritisation of financial goals over safety, and suppression of internal warnings, leading to massive reputational damage and executive accountability reforms.

Relevant Concepts:

- 1.5 Governance, Risk and Compliance
- 1.10 Control: The Three Lines of Defence
- 1.25 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/Boeing_737_MAX_groundings
- https://corpgov.law.harvard.edu/2024/06/06/boeing-737-max/
- https://apnews.com/article/boeing-plea-737-max-crashes-b34daa014406657e720bec4a990dccf6
- https://www.aviacionline.com/boeing-the-737-max-and-the-avoided-screw-crisis
- https://www.politico.eu/article/boeing-crisis-everybody-freaking-out-faa-easa-alaska-door-plug-737-max9/

<13> Estonia's digital government ecosystem (2001…)

Description: Estonia developed a comprehensive digital government ecosystem with strong interoperability and user-centric services. Based on X-Road architecture and digital identity infrastructure, the country became a global reference for secure, integrated public services supported by proactive legal and governance frameworks.

Relevant Concepts:

- 4.1 Business and Strategy
- 4.2 Enterprise Architecture and Alignment
- 4.21 Identity Management

Classification: Intended cause, Good consequence, Positive results

Sources:

- https://e-estonia.com/solutions/interoperability-services/x-road/
- https://complexdiscovery.com/estonias-digital-strategy-shines-in-the-2024-un-e-government-report/
  https://thedocs.worldbank.org/en/doc/165711456838073531-0050022016/original/WDR16BPEstonianeGovecosystemVassil.pdf

---

<14> Facebook / Cambridge Analytica scandal (2018)

Description: Facebook allowed personal data of millions of users to be harvested without consent and exploited by Cambridge Analytica for political profiling. The case triggered global scrutiny of digital platform governance, data protection compliance, and algorithmic accountability.

Relevant Concepts:

- 2.11 Information Privacy
- 2.13 Consent Mechanisms
- 4.22 Governance of Algorithmic Systems

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
- https://www.bbc.com/news/technology-54722362

<15> GitLab backup deletion and live recovery (2017)

Description: A GitLab administrator accidentally deleted a production database, and all backup mechanisms failed — except a snapshot saved on a developer laptop. The recovery was livestreamed and transparently documented, earning praise for crisis communication and triggering long-term infrastructure improvements.

Relevant Concepts:

- 3.2 Resilience and Incident Response
- 3.10 Operational Culture and Organisational Maturity
- 3.12 Service Management Frameworks

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://about.gitlab.com/blog/2017/02/01/gitlab-dot-com-database-incident/
- https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8970730&fileOId=8970734

<16> Hawaii emergency alert: UI mistake, systemic failure (2018)

Description: A false missile alert was sent to Hawaii residents due to a poorly designed user interface and lack of process checks. The alert took 38 minutes to be retracted. The incident illustrated how human error, combined with UI flaws and inadequate governance, can cause mass panic.

Relevant Concepts:

- 3.2 IT Services and Operations
- 3.13 Operational Resilience and Incident Response
- 1.5 Governance, Risk and Compliance

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert
- https://www.nngroup.com/articles/error-prevention/

<17> IKEA and the shift to unified digital platforms (2018…)

Description: IKEA consolidated fragmented systems into a unified global digital platform to support ecommerce and supply chain visibility. The transformation was grounded in strong enterprise architecture and gradual rollout. It enabled agility during the pandemic and positioned the company for omnichannel growth.

Relevant Concepts:

- 4.1 Business and Strategy
- 4.6 Enterprise Architecture and Alignment
- 4.8 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- https://www.theagilityeffect.com/en/case/how-ikea-is-stepping-up-its-digital-transformation/
- https://www.thehrdigest.com/ikeas-digital-transformation-how-the-swedish-furniture-giant-is-adapting-to-the-new-retail-landscape/

<18> Knight Capital: a $440 million error in 45 minutes (2012)

Description: A faulty software deployment at Knight Capital caused unintended high-frequency trading activity, resulting in a $440 million loss in under an hour. The case exposed the absence of change control, rollback procedures, and operational safeguards in mission-critical systems.

Relevant Concepts:

- 3.3 IT Operations
- 3.5 Resilience
- 3.12 Service Management Frameworks

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- https://www.henricodolfing.com/2019/06/project-failure-case-study-knight-capital.html (**great stuff this site!!!**)
- https://www.cio.com/article/286790/software-testing-lessons-learned-from-knight-capital-fiasco.html

<19> Lidl and the SAP retail project failure

Description: Lidl invested heavily in a custom SAP-based retail management system to standardise operations across countries. After seven years and over €500 million, the project was cancelled due to poor architectural alignment, weak change management, and incompatibility with Lidl's existing decentralised processes.

Relevant Concepts:

- 4.6 Enterprise Architecture and Alignment
- 4.8 Strategic Portfolio and Investment Governance
- 4.25.4 Strategic Ambition Versus Organisational Capacity

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.panorama-consulting.com/lidl-erp-failure/
- https://www.henricodolfing.com/2020/05/case-study-lidl-sap-debacle.html (**great stuff this site!!!**)
- https://www.humology.com/lidl-case-study

<20> Log4Shell vulnerability (2021)

Description: A critical zero-day vulnerability in the widely used Log4j library allowed remote code execution, affecting systems worldwide. The incident revealed widespread dependency risks and prompted urgent patching efforts, stronger software bill-of-materials practices, and vendor accountability reforms.

Relevant Concepts:

- 2.16 Frameworks for Information Security and Risk Management
- 2.25 IT Supply-Chain
- 3.2 Resilience and Incident Response

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://en.wikipedia.org/wiki/Log4Shell
- https://www.nytimes.com/2021/12/20/technology/log4j-cybersecurity-vulnerability.html

---

<21> OVH cloud data centre fire (2021)

Description: A fire in an OVHcloud data centre in Strasbourg caused service outages for thousands of European clients. The incident exposed weaknesses in disaster recovery and prompted new norms for data centre resilience, off-site backup practices, and transparency obligations in cloud infrastructure.

Relevant Concepts:

- 3.2 Resilience and Incident Response
- 3.10 Operational Culture and Organisational Maturity
- 2.1 Governance of IT

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://www.theregister.com/2021/03/10/ovh_strasbourg_fire/
- https://www.datacenterdynamics.com/en/analysis/ovhcloud-fire-france-data-center/
- https://www.datacenterdynamics.com/en/opinions/ovhclouds-data-center-fire-one-year-on-what-do-we-know/

<22> SolarWinds supply chain attack (2020)

Description: Attackers compromised the software update system of SolarWinds, injecting malicious code that reached thousands of public and private sector clients. The case underscored the strategic risks of digital supply chains and the need for stronger detection, supplier vetting, and policy coordination.

Relevant Concepts:

- 2.25 IT Supply-Chain
- 2.17 Frameworks for InfoSec and Risk Management
- 2.29 International and National Governance of Cybersecurity

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://www.gao.gov/products/gao-22-104746
- https://www.csoonline.com/article/570191/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

---

<23> Spotify and the strategic use of cloud infrastructure

Description: Spotify transitioned from in-house data centres to Google Cloud, enabling rapid scaling, data analytics, and improved user experience. This strategic shift supported business agility but required careful management of vendor lock-in, data governance, and technical integration challenges.

Relevant Concepts:

- 4.1 Business and Strategy
- 4.2 Enterprise Architecture and Alignment
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- https://cloud.google.com/customers/spotify
- https://engineering.atspotify.com/2019/12/views-from-the-cloud-a-history-of-spotifys-journey-to-the-cloud-part-1-2/
- https://www.computerworld.com/article/1655983/how-spotify-migrated-everything-from-on-premise-to-google-cloud-platform.html

---

<24> TSB Bank IT migration failure (UK)

Description: TSB's attempted migration to a new IT platform in 2018 led to major service outages, affecting millions of customers. The failure was linked to inadequate testing, overconfidence in vendor capabilities, and governance flaws. The case triggered fines, CEO resignation, and scrutiny of IT change management.

Relevant Concepts:

- 1.7 Governance, Management and Operations
- 3.3 Change Management
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.bankofengland.co.uk/news/2022/december/tsb-fined-for-operational-resilience-failings
- https://www.computerweekly.com/news/252528519/TSB-hit-with-huge-fine-after-IT-migration-disaster
- https://www.bbc.com/news/business-64036529

<25> UK Post Office Horizon IT scandal

Description: The UK Post Office prosecuted hundreds of sub-postmasters based on faulty data from the Horizon IT system. The case exposed institutional failures in IT governance, accountability, and legal safeguards, leading to widespread public outcry, compensation claims, and a national inquiry.

Relevant Concepts:

- 2.1 Governance of IT
- 2.9 Information Security
- 4.22 Governance of Algorithmic Systems

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/British_Post_Office_scandal
- https://www.bbc.com/news/business-56718036
- https://en.wikipedia.org/wiki/Mr_Bates_vs_The_Post_Office (the TV series)
- https://www.postofficescandal.uk/ (the book)

<26> Uber and its toxic culture

Description: Uber's early leadership fostered a high-growth environment marked by toxic work culture, regulatory evasion, and poor internal controls. Whistleblower revelations led to reputational damage, executive turnover, and organisational reforms focusing on ethics, compliance, and governance.

Relevant Concepts:

- 1.19 Governance and Organisational Culture
- 1.25 CxO Roles in Governance and Strategic Engagement
- 4.1 Business and Strategy

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.hrmagazine.co.uk/content/features/uber-s-toxic-corporate-culture-much-more-than-a-pr-problem
- https://observer.com/2017/06/fixing-a-toxic-culture-like-ubers-requires-more-than-just-a-new-ceo-business-ethics-sexism-harassment-leadership/

<27> Volkswagen Dieselgate scandal

Description: Volkswagen installed software in diesel cars to cheat emissions tests, misleading regulators and customers. The scandal revealed a systemic failure of ethics, compliance, and internal control. It led to executive resignations, criminal charges, multibillion-dollar fines, and a global reputational crisis.

Relevant Concepts:

- 1.5 Governance, Risk and Compliance
- 1.18 Governance and Ethics
- 1.25 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal
- https://www.bbc.com/news/business-34324772

<28> Wirecard financial fraud

Description: Wirecard, a German fintech firm, admitted that €1.9 billion in assets were missing. The scandal exposed regulatory failures, weak audit oversight, and governance gaps. It led to the company's collapse, arrests of senior executives, and a reckoning for EU financial supervision.

Relevant Concepts:

- 1.5 Governance, Risk and Compliance
- 1.16 Management Assurance: Auditing
- 1.25 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.ft.com/wirecard
- https://en.wikipedia.org/wiki/Wirecard_scandal

<29> The Netherlands' Common Ground initiative (2024…)

Description: The Dutch government launched the Common Ground initiative to standardise municipal data handling and improve service interoperability. By separating data from applications and adopting modular architecture, it enhanced local autonomy and digital maturity across municipalities.

Relevant Concepts:

- 4.2 Enterprise Architecture and Alignment
- 4.1 Business and Strategy
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- https://en.shift2.nl/visie-op-common-ground
- https://interoperable-europe.ec.europa.eu/collection/elise-european-location-interoperability-solutions-e-government/solution/eulf-blueprint/best-practice-79
- https://commonground.nl/ (in Dutch)

<30> Travelex ransomware and prolonged shutdown (2020)

Description: A ransomware attack forced Travelex to shut down global currency exchange operations for weeks. The incident exposed weak IT hygiene and lack of resilience. The company suffered reputational damage and financial losses, prompting stronger crisis management practices sector-wide.

Relevant Concepts:

- 3.2 Resilience and Incident Response
- 2.9 Information Security
- 2.17 Frameworks for InfoSec and Risk Management

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://www.bbc.com/news/business-51017852
- https://www.itgovernance.co.uk/blog/ransomware-victim-travelex-forced-into-administration
- https://www.onsecurity.io/blog/cyber-nightmares-what-went-wrong-with-travelex/

<31> $463M telemedicine fraud (2022)

Description: A large-scale fraud in the US involved telemedicine companies billing Medicare for unnecessary genetic tests. The case revealed oversight gaps in digital healthcare and regulatory frameworks. It undermined public trust and led to stricter controls on telehealth billing.

Relevant Concepts:

- 4.1 Business and Strategy
- 1.5 Governance, Risk and Compliance

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.justice.gov/archives/opa/pr/lab-owner-convicted-463-million-genetic-testing-scheme-defraud-medicare
- https://healthexec.com/topics/healthcare-management/healthcare-policy/labsolutions-minal-patel-sentenced-medicare-fraud
- https://healthcarechief.com/genetic-testing-labs-in-463m-fraud-case/

<32> Vastaamo and the Therapy Data Blackmail (2018)

Description: Between 2018 and 2019, Finnish psychotherapy provider Vastaamo suffered multiple data breaches due to serious failures in its IT and security governance. The attackers stole highly sensitive patient records, including therapy notes, and began blackmailing both the company and individual patients in 2020. It was later revealed that the breached database had been left exposed online for more than a year without password protection. Vastaamo's executive leadership failed to report the breach in a timely manner and neglected to implement even basic information security controls. The organisation ultimately went bankrupt, and its CEO faced criminal charges. The incident led to widespread public trauma, loss of trust in digital healthcare, and a national conversation on the governance of health data.

Relevant Lecture Notes Sections:

- **2.1** Governance of IT
- **2.2** Leadership Roles and Governance Posture
- **2.7** Stakeholder Management and Information Systems
- **2.8** Information Governance and Management
- **2.9** Information Security
- **2.11.2** Privacy by Design and Risk Orientation
- **2.12** General Data Protection Regulation
- **2.13.3** Consent Mechanisms
- **2.14** Personal Data
- **3.13** Operational Resilience and Incident Response

Classification:

- **Cause:** Inadequate IT governance and failure to apply basic information security practices.
- **Consequence:** Massive privacy violation, criminal extortion, psychological harm to patients.
- **Results:** Organisational collapse, legal prosecution, national policy scrutiny on health data governance.

Online Sources:

- https://en.wikipedia.org/wiki/Vastaamo_data_breach
- https://www.edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en
- https://www.bbc.com/news/articles/c97znd00q7mo

<33> Portugal’s Justice System Offline: The CITIUS Crash (2014)

Short: In September 2014, Portugal’s Ministry of Justice deployed an updated version of CITIUS (the national platform used by judges and legal professionals for court case management) without adequate testing or fallback planning. The rollout coincided with the launch of a major judicial reorganisation that altered court structures and processes across the country. Within days, critical failures emerged: court staff could not access files, submit case updates, or process legal actions. The system remained unstable for weeks, causing thousands of delays and triggering nationwide protests from judges and court clerks. An internal investigation exposed poor coordination between the IT provider, the Directorate-General for Justice Policy, and frontline users. There had been no comprehensive system test, insufficient training, and no rollback strategy. Political fallout forced the resignation of the Justice Secretary, and the case became a symbol of digital misgovernance in public sector transformation.

Relevant Lecture Notes Sections:

- **2.1** Governance of IT
- **2.2** Leadership Roles and Governance Posture
- **2.5** Strategic Alignment
- **2.7** Stakeholder Management and Information Systems
- **2.9** Vendor and Contract Management
- **3.3** IT Operations
- **3.5** Resilience

- **3.10** Continuity and Recovery
- **4.6** Target Operating Model (TOM)
- **4.8** Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Lack of IT governance, absence of integrated planning for simultaneous legal reform and system upgrade.
- **Consequence:** Nationwide system outage in the judiciary, operational paralysis, reputational damage to the Ministry of Justice.
- **Results:** Delays in court cases, national protest by justice workers, political accountability and resignation, overhaul of governance processes in digital justice programmes.

Online Sources (Portuguese):

- https://www.publico.pt/2014/09/01/sociedade/noticia/site-citius-continua-indisponivel-no-arranque-do-mapa-judiciario-1668298
- https://tvi.iol.pt/noticias/sociedade/sindicato-funcionarios-judiciais-sobre-as-falhas-na-plataforma-informatica/citius-instituto-considera-abusivas-criticas
- https://expresso.pt/economia/2019-09-30-Auditoria-ao-colapso-do-Citius-classificada-como-confidencial-pela-IGF
- https://www.publico.pt/2018/03/30/sociedade/noticia/tres-anos-e-meio-apos-colapso-do-citius-nao-se-sabe-o-que-parou-os-tribunais-1808572
- https://www.jornaldenegocios.pt/economia/justica/detalhe/igfej_diz_que_citius_esta_em_pleno_a_partir_desta_segunda_feira

---

<34> The "Offshores Apagão": A Failure in Finantial Data Processing

Description: Between 2011 and 2014, the Portuguese Tax Authority (Autoridade Tributária e Aduaneira – AT) failed to process in a first moment all the declarations from financial institutions reporting offshore money transfers, amounting to around €10 billion. The underlying issue stemmed from a data import failure in the PowerCenter ETL system used by AT. The error was not flagged by any automated control until it was discovered in 2016 when a manual processing found inconsistencies in the data. Even if no data was lost, public outcry and media scrutiny followed, particularly after it emerged that the incident had been kept out of the political spotlight during an election year. Although criminal sabotage was ruled out, the case exposed failures in information management, internal controls, and accountability mechanisms.

Relevant Lecture Notes Sections:

- **2.1** Governance of IT
- **2.2** Leadership Roles and Governance Posture
- **2.5** Strategic Alignment
- **2.7** Stakeholder Management and Information Systems
- **2.8** Information Governance and Management
- **3.3** IT Operations
- **3.5** Resilience
- **3.10** Continuity and Recovery
- **3.13** Operational Resilience and Incident Response

Classification:

- **Cause:** *Systemic failure in information governance* — Lack of auditability, absence of alerts for unprocessed data, poor design of error handling in critical tax processing systems. No formal mechanisms ensured completeness or cross-verification of ETL imports.
- **Consequence:** *Institutional invisibility of €10 billion in offshore transfers* — Failure to detect undeclared transactions hindered compliance monitoring and undermined public trust in the justice and fiscal system.
- **Results:** *Political scandal, loss of institutional credibility, and reinforcement of demands for digital transparency and auditability in public sector systems* — The Ministry of Finance faced reputational damage, and Parliament initiated inquiries. Though the judiciary later closed the case without finding criminal intent, structural issues in public sector digital governance, management and operational assurance were questioned.

Online Sources (Portuguese):

- https://www.publico.pt/2023/03/14/economia/noticia/ministerio-publico-arquiva-apagao-offshores-afasta-sabotagem-informatica-2042221
- https://pplware.sapo.pt/informacao/autoridade-tributaria-apagao-fez-desaparecer-10-mil-milhoes-de-euros/
- https://sicnoticias.pt/pais/2023-03-14-Arquivado-caso-do-apagao-que-deixou-fugir-10-mil-milhoes-ao-Fisco-5b753024
- https://jornaleconomico.sapo.pt/noticias/dez-mil-milhoes-para-offshores-ministerio-publico-arquiva-caso-do-apagao-na-autoridade-tributaria/

<35> Amazon's HR Tech Backlash (2021)

Description: Amazon faced significant employee dissatisfaction following the rollout of new internal HR technologies designed to manage performance evaluations, promotions, and employee support services. Instead of improving the employee experience, the new systems were often seen as opaque, rigid, and dehumanising. Reports highlighted that

automated workflows led to delays in resolving HR issues, errors in leave management, and communication breakdowns, damaging trust and morale. The case illustrates the risks of deploying internal digital systems without adequate governance of change management, stakeholder engagement, and employee-centric design.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.19 Governance and Organisational Culture
- 2.5 Governance and Information Technology
- 2.7 Stakeholder Management and Information Systems
- 4.3 Stakeholder Engagement and Strategic Communication
- 4.5 Target Operating Model
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Poor stakeholder engagement; weak operational governance of internal digital initiatives.
- **Consequence:** Employee dissatisfaction; reputational damage; operational inefficiencies.
- **Results:** Ongoing adjustments to HR tech platforms; increased scrutiny on internal digital transformation governance.

Online Sources:

- https://www.nytimes.com/2021/10/24/technology/amazon-employee-leave-errors.html
- https://www.shrm.org/topics-tools/news/technology/amazons-troubles-hold-lessons-hr-tech-employee-experience
- https://www.forbes.com/sites/jackkelly/2021/10/25/a-hard-hitting-investigative-report-into-amazon-shows-that-workers-needs-were-neglected-in-favor-of-getting-goods-delivered-quickly/

<36> Delta's Digital Cascade Failure (2024)

Description: In July 2024, Delta Air Lines suffered a massive operational breakdown following a critical software failure triggered by a faulty update from cybersecurity vendor CrowdStrike. While many organisations recovered quickly, Delta's dependence on fragile internal systems (especially for crew-tracking and scheduling) amplified the disruption. Over 7,000 flights were cancelled, affecting more than 1.3 million passengers. Investigations revealed that Delta's internal resilience plans had not adequately addressed external vendor risks or critical system dependencies. Moreover, communication with stranded passengers was slow and confusing, eroding trust. The incident exposed systemic weaknesses in vendor governance, operational resilience, and stakeholder crisis management, prompting regulatory investigations, reputational fallout, and renewed calls for integrated risk oversight in critical infrastructure sectors like aviation.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.7 Governance, Management, and Operations
- 2.5 Governance and Information Technology
- 2.23 Vendor and Contract Management
- 2.25 IT Supply-Chain
- 3.5 Resilience
- 3.13 Operational Resilience and Incident Response
- 4.3 Stakeholder Engagement and Strategic Communication
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Over-reliance on third-party software; insufficient operational resilience testing; weak vendor dependency governance.
- **Consequence:** Service paralysis; massive customer dissatisfaction; reputational harm; financial claims.
- **Results:** Federal investigations launched; Delta initiated strategic reviews of IT governance, vendor risk management, and resilience frameworks.

Links for Further Reading:

- https://en.wikipedia.org/wiki/2024_Delta_Air_Lines_disruption

---

<37> Via Verde: Seamless Mobility, Strategic Risks (1991…)

Description: Via Verde, launched in 1991 in Portugal, pioneered automatic electronic toll collection, allowing vehicles to pass through highway tolls without stopping. Over time, the system expanded to other services such as car parks, fuel stations, and drive-thru payments. Its success is attributed to strong stakeholder alignment (infrastructure operators, banks, government) and user-centric design. However, the strategic dependence on a single identity-token (the Via Verde transponder) raised concerns about privacy, service resilience, and vendor lock-in. The system's evolution illustrates both the benefits of digital integration and the governance challenges of managing multi-service platforms at national scale.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.7 Governance, Management, and Operations
- 2.5 Governance and Information Technology

- 2.7 Stakeholder Management and Information Systems
- 2.8 Information Governance and Management
- 2.11 Information Privacy
- 4.1 Business and Strategy
- 4.5 Target Operating Model
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Strategic drive for frictionless mobility and national-scale digital integration.
- **Consequence:** Outstanding service convenience; growing dependency on a single platform; privacy and competition concerns.
- **Results:** Expansion into multiple service domains; reinforcement of governance structures; emerging public debates on data protection and future interoperability with European frameworks.

Links for Further Reading:

- https://novaresearch.unl.pt/en/publications/a-collaborative-network-case-study-the-extended-viaverde-toll-pay
- https://recil.ulusofona.pt/server/api/core/bitstreams/54eb0b03-6272-49cb-b34a-430e14d284a3/content
- https://en.wikipedia.org/wiki/Via_Verde
- https://executivedigest.sapo.pt/cadernos-especiais/via-verde-mais-do-que-uma-marca-um-conceito/

<38> Southwest's Meltdown: The Real Cost of Technical Debt (2022)

Description: In December 2022, Southwest Airlines faced a catastrophic operational collapse, cancelling thousands of flights and stranding millions of passengers. Investigations revealed that the disaster was rooted in years of accumulated **technical debt,** particularly the failure to modernise its crew-scheduling system, SkySolver. While other airlines recovered quickly after a major winter storm, Southwest's outdated system could not handle the scale of disruptions, forcing employees to manually reestablish crew assignments by phone. The incident highlighted systemic weaknesses in IT governance, operational resilience, and strategic risk management, demonstrating how deferred investment in core systems can magnify external shocks into full-blown organisational crises.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.7 Governance, Management, and Operations
- 2.5 Governance and Information Technology
- 2.23 Vendor and Contract Management
- 2.25 IT Supply-Chain
- 3.5 Resilience
- 3.10 Operational Culture and Organisational Maturity
- 3.13 Operational Resilience and Incident Response
- 4.1 Business and Strategy
- 4.3 Stakeholder Engagement and Strategic Communication
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Accumulated technical debt; delayed IT modernisation; operational culture tolerating fragile legacy systems.
- **Consequence:** Widespread flight cancellations; reputational damage; financial losses; regulatory scrutiny.
- **Results:** Forced strategic review of IT and operational processes; accelerated (belated) investment in cloud migration and resilience initiatives; stronger industry focus on technical debt governance.

Links for Further Reading:

- https://devops.com/southwest-technical-debt-richixbw/
- https://www.nytimes.com/2023/01/10/podcasts/the-daily/the-southwest-airlines-meltdown.html
- https://www.nytimes.com/2023/01/06/business/southwest-airlines-meltdown-costs-reimbursement.html
- https://www.nytimes.com/2022/12/29/opinion/southwest-airlines.html?searchResultPosition=4 (**by Paul Krugman!!!**)
- Popular Science Report

Acronyms

The following list provides a reference of acronyms used throughout the lecture notes.
Each acronym is expanded using UK English spelling, where applicable, and reflects terminology relevant to the management, governance, risk, security, and strategic engagement with information systems.
Where multiple interpretations exist, the meaning adopted aligns with the primary context of this course.
This list is provided as a support tool and does not replace the need for critical interpretation of terms within specific organisational, sectoral, or regulatory contexts.

- **ACM** – Association for Computing Machinery
- **AG** – Aktiengesellschaft (German term for a public limited company)
- **AI** – Artificial Intelligence
- **AMA** – Agência para a Modernização Administrativa
- **AML** – Anti-Money Laundering
- **AP** – Access Point
- **APCER** – Associação Portuguesa de Certificação
- **API** – Application Programming Interface
- **AT** – Acceptance Testing
- **AUTOSAR** – Automotive Open System Architecture
- **AWS** – Amazon Web Services
- **BAI** – Business Analysis Institute
- **BCBS** – Basel Committee on Banking Supervision
- **BCMS** – Business Continuity Management System
- **BIA** – Business Impact Analysis
- **BIS** – Bank for International Settlements
- **BPM** – Business Process Management
- **BPMN** – Business Process Model and Notation
- **BPMS** – Business Process Management Suite
- **BPR** – Business Process Reengineering
- **BYOD** – Bring Your Own Device
- **CA** – Certification Authority
- **CAB** – Change Advisory Board
- **CAF** – Cloud Adoption Framework
- **CAIRO** – Consulted, Accountable, Informed, Responsible, Out of the Loop (variant of RACI)
- **CAO** – Chief Administrative Officer
- **CAP** – Capability Assessment Plan
- **CCO** – Chief Compliance Officer
- **CCPA** – California Consumer Privacy Act
- **CD** – Continuous Delivery
- **CDO** – Chief Data Officer
- **CEA** – Comissão de Ética para a Investigação Clínica
- **CECO** – Chief Ethics and Compliance Officer
- **CEO** – Chief Executive Officer
- **CER** – Council of European Regulators
- **CFO** – Chief Financial Officer
- **CIAM** – Customer Identity and Access Management
- **CIO** – Chief Information Officer
- **CISO** – Chief Information Security Officer
- **COBIT** – Control Objectives for Information and Related Technologies
- **COO** – Chief Operating Officer
- **CRM** – Customer Relationship Management
- **CSIRT** – Computer Security Incident Response Team
- **CSO** – Chief Security Officer
- **CTO** – Chief Technology Officer
- **DLP** – Data Loss Prevention
- **DPIA** – Data Protection Impact Assessment
- **DPO** – Data Protection Officer
- **DORA** – Digital Operational Resilience Act
- **EA** – Enterprise Architecture
- **EDPB** – European Data Protection Board
- **EDPS** – European Data Protection Supervisor
- **eIDAS** – electronic Identification, Authentication and Trust Services
- **ENISA** – European Union Agency for Cybersecurity
- **ERP** – Enterprise Resource Planning
- **EU** – European Union
- **EUDI** – European Digital Identity
- **EUDIW** – European Digital Identity Wallet
- **EV** – Electric Vehicle
- **GDPR** – General Data Protection Regulation
- **GRC** – Governance, Risk, and Compliance
- **IAM** – Identity and Access Management
- **ICS** – Industrial Control Systems
- **ICT** – Information and Communication Technology
- **IEC** – International Electrotechnical Commission
- **IIoT** – Industrial Internet of Things
- **IM** – Information Management
- **IoT** – Internet of Things
- **IP** – Intellectual Property
- **IPaaS** – Integration Platform as a Service
- **ISO** – International Organization for Standardization
- **ISP** – Internet Service Provider
- **ISMS** – Information Security Management System
- **IT** – Information Technology
- **ITAM** – IT Asset Management
- **ITIL** – Information Technology Infrastructure Library
- **ITS** – Intelligent Transport Systems
- **KPI** – Key Performance Indicator
- **KYC** – Know Your Customer
- **LMS** – Learning Management System
- **M&A** – Mergers and Acquisitions
- **MFA** – Multi-Factor Authentication
- **MSP** – Managed Service Provider
- **MSS** – Managed Security Service
- **MSS** – Management System Standard
- **MSSP** – Managed Security Service Provider
- **NIS** – Network and Information Security (Directive)
- **NIS2** – Second Network and Information Security Directive
- **NIST** – National Institute of Standards and Technology
- **OpEx** – Operational Expenditure
- **OT** – Operational Technology
- **PaaS** – Platform as a Service
- **PBX** – Private Branch Exchange
- **PCI DSS** – Payment Card Industry Data Security Standard
- **PDCA** – Plan–Do–Check–Act
- **PDF** – Portable Document Format
- **PII** – Personally Identifiable Information
- **PIMS** – Privacy Information Management System
- **PKI** – Public Key Infrastructure

- **PMBOK** – Project Management Body of Knowledge
- **PMO** – Project Management Office
- **PoC** – Proof of Concept
- **PRM** – Partner Relationship Management
- **PSD2** – Second Payment Services Directive
- **PSI** – Public Sector Information
- **PSTI** – Product Security and Telecommunications Infrastructure
- **QA** – Quality Assurance
- **QoS** – Quality of Service
- **RA** – Registration Authority
- **RACI** – Responsible, Accountable, Consulted, Informed
- **RAM** – Random Access Memory
- **RBAC** – Role-Based Access Control
- **RDP** – Remote Desktop Protocol
- **REMS** – Risk Evaluation and Mitigation Strategy
- **RGPD** – Regulamento Geral sobre a Proteção de Dados
- **RMM** – Risk Maturity Model
- **ROSI** – Return on Security Investment
- **SaaS** – Software as a Service
- **SBOM** – Software Bill of Materials
- **SCADA** – Supervisory Control and Data Acquisition
- **SDLC** – Software Development Life Cycle
- **SDN** – Software-Defined Networking
- **SIEM** – Security Information and Event Management
- **SIM** – Subscriber Identity Module
- **SLA** – Service Level Agreement
- **SME** – Small and Medium-sized Enterprises
- **SMS** – Short Message Service
- **SOC** – Security Operations Centre
- **SoD** – Segregation of Duties
- **SOP** – Standard Operating Procedure
- **SPI** – Service Provider Interface
- **SQL** – Structured Query Language
- **SSI** – Self-Sovereign Identity
- **SSO** – Single Sign-On
- **SWOT** – Strengths, Weaknesses, Opportunities, and Threats
- **TCO** – Total Cost of Ownership
- **TDP** – Technology Development Plan
- **TI** – Tecnologia da Informação
- **TLD** – Top-Level Domain
- **TLP** – Traffic Light Protocol
- **TOM** – Target Operating Model
- **TRL** – Technology Readiness Level
- **UI** – User Interface
- **UK** – United Kingdom
- **URL** – Uniform Resource Locator
- **USB** – Universal Serial Bus
- **US-CERT** – United States Computer Emergency Readiness Team
- **UX** – User Experience
- **VA** – Vulnerability Assessment
- **VPN** – Virtual Private Network
- **VPS** – Virtual Private Server
- **VSM** – Value Stream Mapping
- **VUCA** – Volatility, Uncertainty, Complexity, and Ambiguity
- **WAF** – Web Application Firewall
- **WAN** – Wide Area Network
- **WHOIS** – Internet Domain Registration Lookup Protocol
- **WLAN** – Wireless Local Area Network
- **WORM** – Write Once, Read Many
- **XaaS** – Everything as a Service
- **XML** – eXtensible Markup Language
- **xOps** – Collective term for operational practices (e.g., DevOps, SecOps)
- **Zero Trust** – Security Model "never trust, always verify"
- **ZTA** – Zero Trust Architecture

…BTW…

Some time has passed. Projects were delivered. Decisions were made. Some roles changed; some stayed the same. Across sectors and contexts, the people who once shaped those stories continued on, each in their own direction.

The Costumers

- **Verónica** *(public sector executive – methodical, respected, cautious with change)* - She remains in office, having quietly transformed her agency's approach to digital oversight. What began as a small dashboard project matured into a full performance governance model. Staff now speak of "clarity" as a working principle. She still reviews every brief herself—but no longer alone.
- **Lucas** *(public sector executive – visionary, energetic, vague in execution)* - His innovation programme ran over budget but left behind real institutional learning. A second round is now underway—this time with a defined scope and a team empowered to challenge his slides. He still dreams aloud but now listens when others help land the ideas.
- **Alex** *(private sector executive – sharp, strategic, demanding)* - His business expanded. So did his expectations. After several successful deliveries, he created a formal governance office with portfolio dashboards. He no longer attends every planning meeting—but when he does, his questions are sharper, and his thanks more sincere.
- **Trish** *(private sector executive – overwhelmed, informal, scattered)* - Trish still rushes from meeting to meeting, but her engagements run more smoothly. A new operations director now filters and scopes digital projects, allowing her to focus on strategic positioning. She's still overloaded, but no longer flying blind.

The Consultants

- **Sofia** *(Dream Team senior: diplomatic, trusted, structured)* - She now leads public sector strategy for a major consultancy. Her calm authority has become institutional memory. Clients who once relied on her now refer others to her team. She hasn't changed her style—just the scale at which she works.
- **Mateus** *(Dream Team junior: responsible, observant, quietly effective)* - After a series of steady contributions, Mateus was promoted. He leads discovery phases with new clients, especially in complex or ambiguous contexts. His work is still thoughtful, still precise. Some call him quiet, others, indispensable.
- **Carla** *(Frenetic Team senior: fast, improvisational, high energy)* - Carla has become more selective. After a difficult stretch involving overcommitment and rework, she rebalanced. She still thrives in intensity, but now insists on at least one planning session before launching into action.
- **Tiago** *(Frenetic Team junior: creative, immature, erratic)* - Tiago burned out, paused, and returned. He now runs a tech-adjacent blog on digital transformation clichés (half satire, half analysis). He consults occasionally, but only when given time to think. He still uses too many slides, but now also asks better questions.
- **Laura** *(Mature Team senior: disciplined, principled, methodical)* - Laura transitioned to a public advisory body. She contributes to national frameworks on IT governance, with a focus on certification and audit coherence. Her documents are referenced across ministries. Her margin notes are quoted verbatim.
- **Tomás** *(Mature Team junior: analytical, thoughtful, rigorous)* - Still working alongside Laura, Tomás has become a core part of policy drafting. His internal models and quiet persistence helped structure an entire GRC guidance framework. His name rarely appears publicly, but his influence is everywhere.
- **Inês** *(Wildcard Team senior: brilliant, disruptive, challenging)* - After a sabbatical and two false starts, she returned to academia, public speaking, and selected provocations. She runs a think tank on governance innovation. Some ignore her. Others build careers interpreting her metaphors.
- **Fábio** *(Wildcard Team junior: visionary, erratic, hard to manage)* - Fábio left consulting and now builds small, exquisite software tools for community organisations. He speaks at events on ethical design, rarely using slides, often leaving questions unanswered. Some say he's a dropout. Others say he's ten years early.
- **Ricardo** *(Contingent Team senior: pragmatic, experienced, resilient)* - He accepted a national-level role in operational resilience. When systems go down or crises escalate, his phone rings. His working hours remain irregular, his instincts precise. He no longer leads projects (but makes others possible).
- **Bruna** *(Contingent Team junior: structured, systems-oriented, composed)* - Bruna now manages resilience assessments for critical infrastructure. She still defers to Ricardo for judgment calls, but increasingly leads complex engagements on her own. Her briefings are clear, her confidence steady. She mentors junior hires (not by telling, but by listening).

…and, BTW… the Academia 😉

- **José** (the prof., architect of the course, observant, quietly amused) - He designed the course[83] not to deliver answers, but to sharpen questions. He watched as others met Verónica, puzzled over Trish, argued about Inês, and tried to map out what exactly Alex wanted. He adjusted scenarios just enough to be real, but not too real. He believes in clarity, but not in certainty. He thinks governance is about people, not procedures (and he's still refining that thought). He doesn't like to use slides but write on the board…
- **The Teaching Assistants** (collective, attentive, curious, occasionally sceptical) - They came from different backgrounds. Some have other jobs; some are still studying. They read drafts, tested dilemmas, and sometimes challenged José with harder questions than he had prepared for. They fixed typos, built bridges, and translated confusion into insight. They will go on to lead projects, shape systems, and maybe one day teach (with or without a board).

The stories are fictional. The patterns are not. Governance, risk, and strategy may depend on frameworks and policies, but their success depends on people. On how they listen, adapt, and grow. What happens after the project ends is just as important as what happened during. Everyone continues uncertain, changing, learning. Just like the organisations they serve

[83] …with tremendous help from ChatGPT, which provided a major boost in efficiency, helping to organise ideas and, above all, saving a great deal of typing time… 😉