SGSI Project part 1

Industries:
3: Retail and Digital Commerce
5: Hospitality and Leisure
6: Banking and Financial Services

Authors:
Henrik Niskanen - 115383
Sara Echary- 115340
Laura Staszko - 112985
Natan Gloeh - 112475

Theme 1 – Business Governance & Management

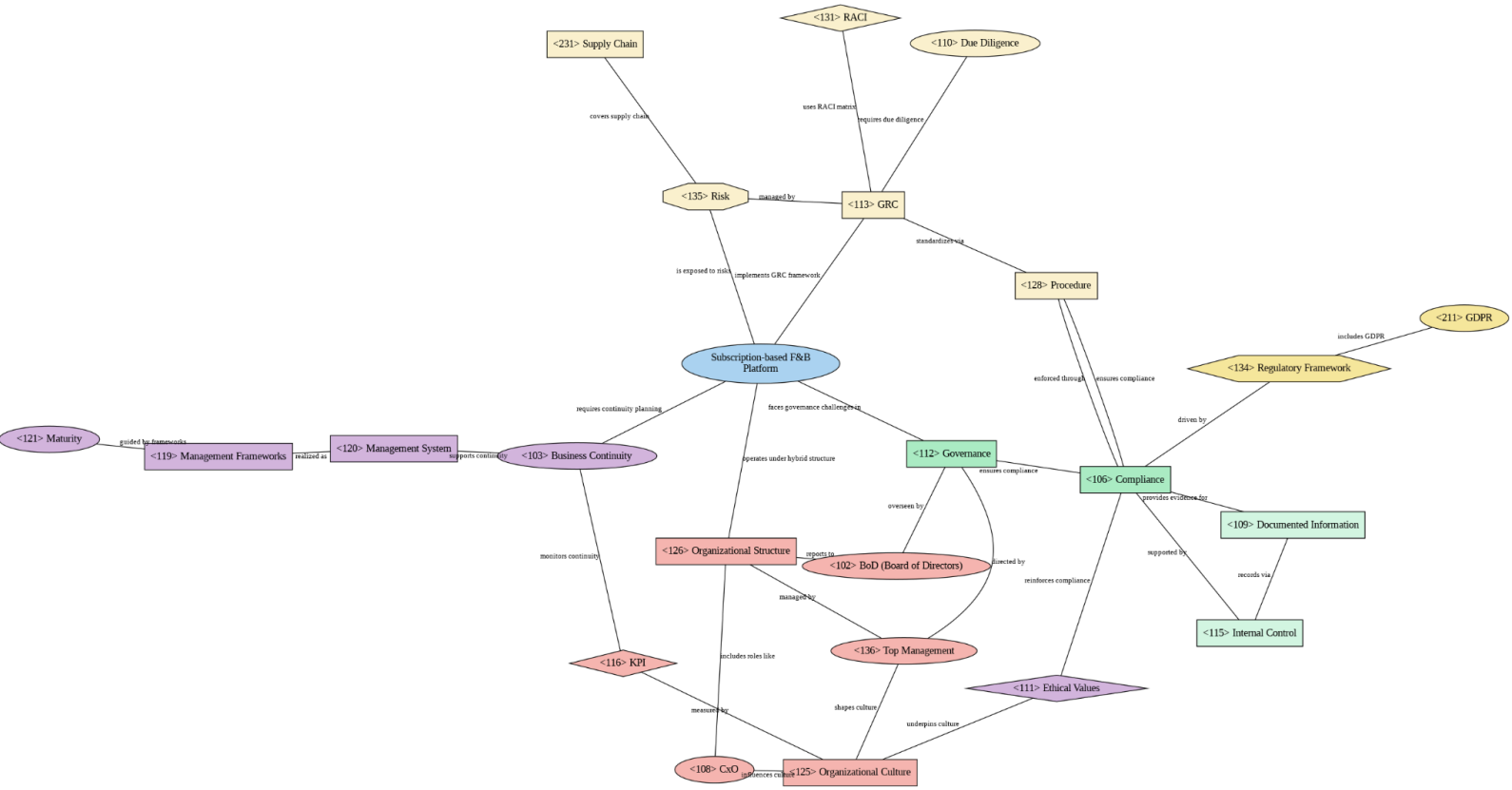
Industry: Retail & Digital Commerce
Niche: Subscription models in the food & beverage segment

Subscription-based F&B platforms exemplify <112> governance challenges arising from managing scalability, customer data, and stringent <134> regulatory frameworks such as <211> GDPR and food safety regulations enforced by <133> regulatory bodies.

1. Governance, compliance, and organizational structure
Effective <112> governance ensures robust adherence to <106> compliance mandates across diverse jurisdictions, particularly in handling sensitive consumer information and food safety standards. Subscription models typically deploy a hybrid <126> organizational structure, blending centralized strategic teams with regional operational units, to balance scalability with localized compliance demands. The <136> top management (<108> CxOs) emphasizes agility, fostering a customer-centric <125> organizational culture crucial for maintaining subscription growth and customer loyalty. This culture is continuously assessed through <116> KPIs like churn rates, customer lifetime value (CLV), and overall satisfaction, ensuring alignment with strategic goals such as <103> business continuity.

2. Risk and policy frameworks
The <135> risk profile for subscription F&B services prominently includes data breaches, regulatory non-compliance, and <231> supply chain disruptions. To mitigate these risks, platforms integrate comprehensive <113> GRC frameworks that emphasize meticulous <110> due diligence processes in vendor management and customer data handling. Clear accountability is structured through <131> RACI matrices, particularly in sensitive operations such as data privacy and dispute resolution. Standardized <128> procedures, notably in customer service and logistics, enhance operational consistency and help maintain high standards of service <130> quality.

3. Organizational maturity and culture
Subscription F&B organizations typically demonstrate moderate to high <121> maturity, characterized by structured and documented processes aligned with established <119> management frameworks. Mature organizations exhibit robust <120> management systems ensuring efficient and consistent service delivery. The platforms emphasize strong <111> ethical values, notably transparency in consumer interactions, data privacy, and sustainability practices, vital for maintaining consumer trust and competitive advantage in the digital marketplace.



Theme 2 – Governance of IT and IT Management

Industry: Retail & Digital Commerce
Niche: Subscription models in the food & beverage segment

Strategic Alignment & Compliance
The core of IT governance (<212> Governance of IT) is ensuring that subscription-F&B initiatives map to business goals - subscriber growth, churn reduction, LTV - and comply with external mandates. An Information Security Management System ([216] ISMS) guided by ISO/IEC underpins this alignment, embedding COBIT processes for strategic planning and performance measurement. Regulatory frameworks like GDPR (<211>) dictate [C-Data Retention] policies (<210>) and breach-reporting obligations to the <133> Regulatory Body, ensuring subscriber PII (<223>) is handled lawfully.

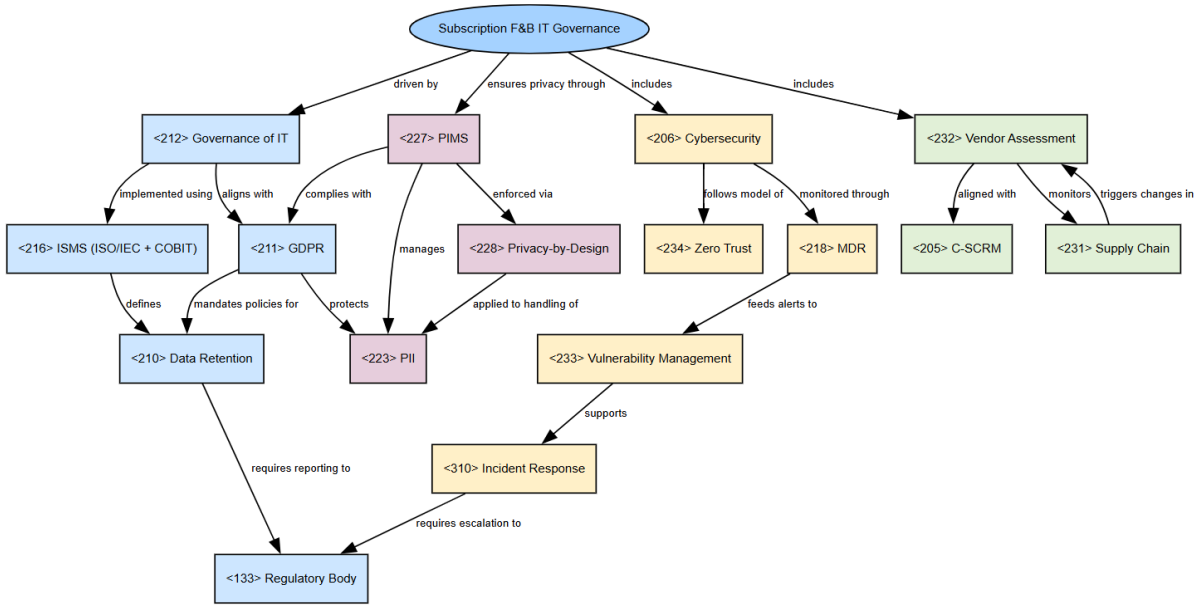
Privacy & Data Protection
Subscription services collect granular consumption and preference data - classified as <223> PII so a robust <227> PIMS (Privacy Information Management System) with <228> Privacy-by-Design principles is mandatory. The PIMS mandates data minimization, purpose-limitation, and automated retention/deletion workflows. It must integrate with billing and CRM systems to enforce consent records and support data-subject requests.

Cybersecurity Operations
Operational resilience against threats depends on layered controls:

- <206> Cybersecurity governed by the ISMS and enforced through <234> Zero Trust (strict identity-and-access controls)
- 24/7 monitoring by <218> MDR (Managed Detection & Response)
- Proactive <233> Vulnerability Management feeding into quarterly penetration tests
- Formal <310> Incident Response (breach plans) executed under the ISMS and reported to regulators.

These processes protect the billing engine, subscription-lifecycle workflows (onboarding - recurring payments - renewal), and subscriber portals.

Supply-Chain & Vendor Risk
Subscription-box fulfilment and digital-platform integrations rely on third-party logistics, payment gateways, and content-recommendation APIs. A <232> Vendor Assessment program, aligned with <205> C-SCRM (Cyber Supply-Chain Risk Management), identifies risks across the supplier ecosystem. Ongoing monitoring under <231> Supply Chain governance ensures that new menu-item rollouts or packaging changes don't introduce vulnerabilities.



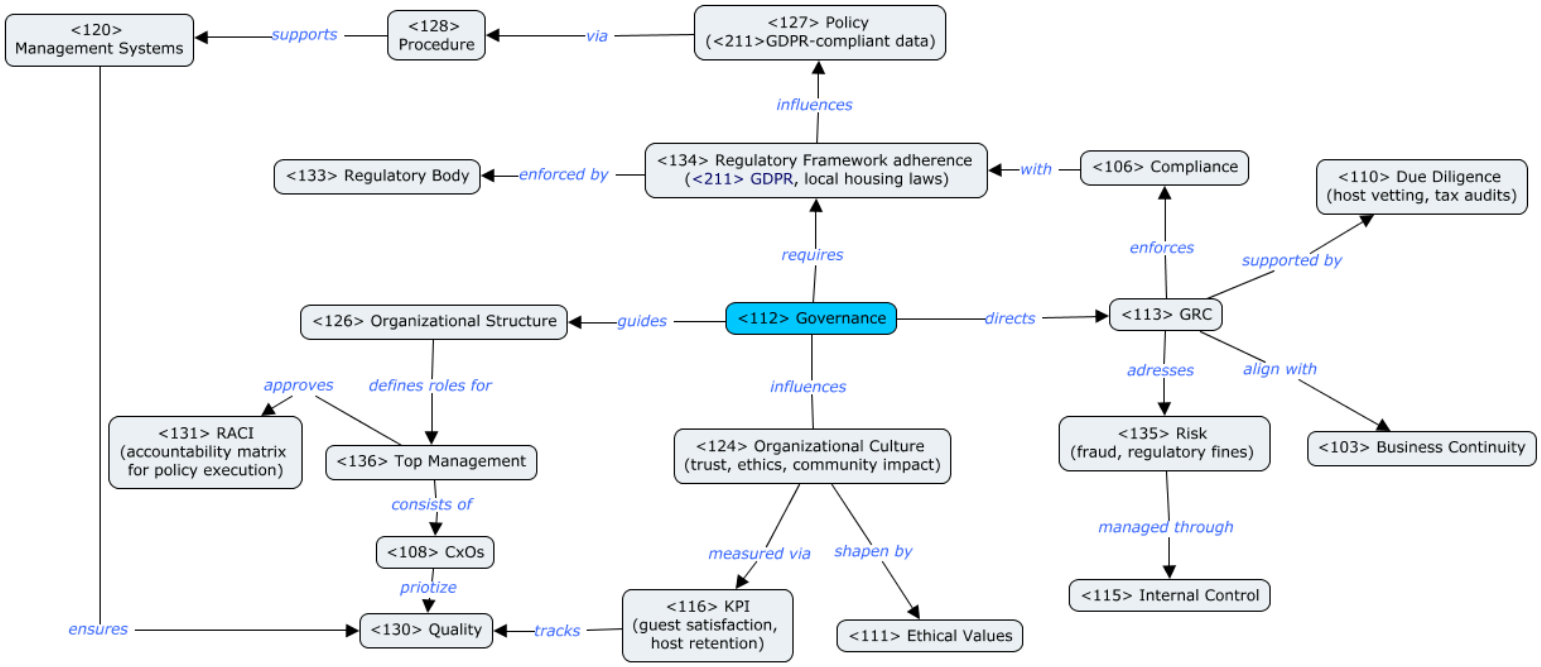
Theme 1 – Business Governance & Management

Industry: Hospitality and Leisure
Niche: Short-term rental platforms

Short-term rental platforms (STRPs) like Airbnb face multifaceted <112> Governance challenges due to their global scale, decentralized operations, and <134> Regulatory Frameworks (e.g., housing laws, tax codes, <211> GDPR) across jurisdictions.

1. Governance, compliance and organizational structure
<112> Governance is central to balancing scalability with localized compliance (<106>). STRPs must navigate diverse <134> Regulatory frameworks (EU's <211> GDPR for <223> PII, zoning laws) enforced by <133> Regulatory bodies. <113> GRC (Governance, Risk, and Compliance) frameworks integrate <135> Risk mitigation (as fraudulent listings, safety incidents) and <110> Due Diligence (host verification, tax reporting).
STRPs adopt a hybrid <126> Organizational Structure, combining centralized tech teams with regional compliance units. <136> Top Management (<108> CxOs) ensures <103> Business Continuity during crises like pandemics. <124> Organizational Culture prioritizes trust but faces tensions between profit motives and community impact (housing shortages). This culture is measured via <116> KPIs like guest satisfaction and host retention.

2. Risk and policy frameworks
<135> Risk profiles include regulatory fines (<106> Compliance failures) and reputational damage from unethical practices. <127> Policy frameworks define roles through <131> RACI matrices (e.g., accountability for dispute resolution). <128> Procedure standardization like automated safety checks supports <120> Management Systems, ensuring <130> Quality in service delivery.



Theme 2 – Governance of IT and IT Management

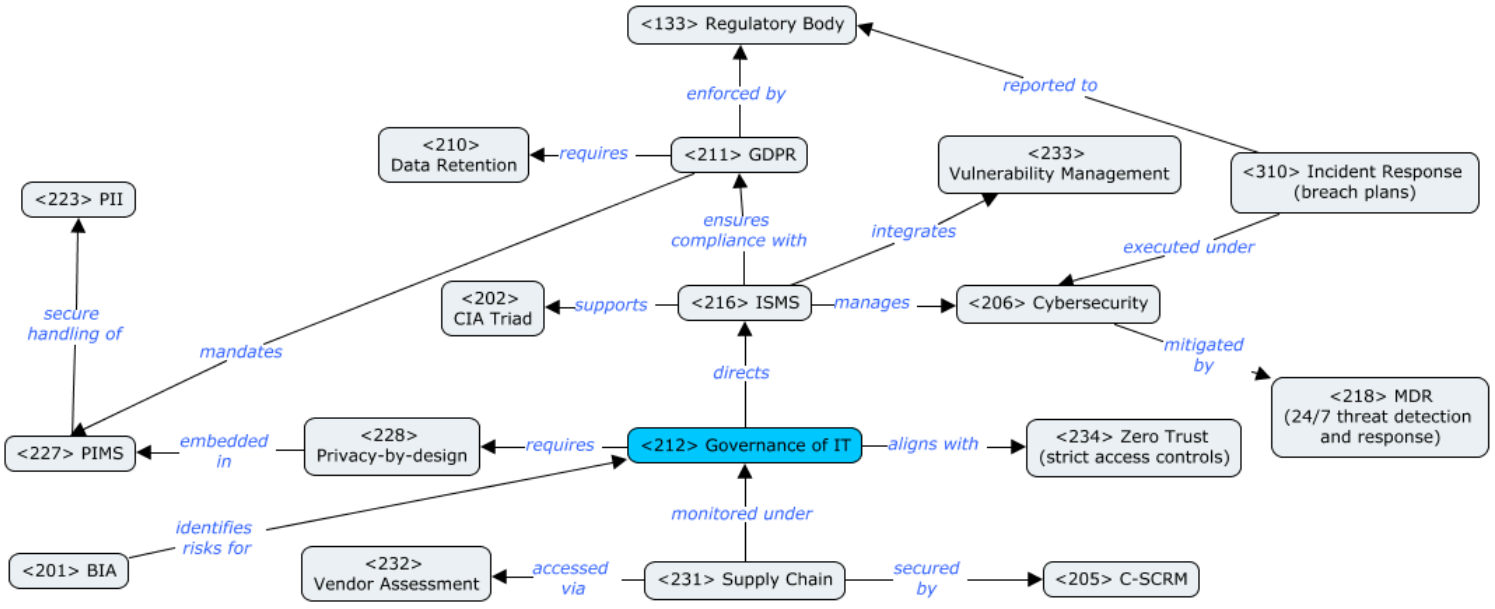
Industry: Hospitality and Leisure
Niche: Short-term rental platforms

Short-term rental platforms (STRPs) like Airbnb rely heavily on IT infrastructure to manage decentralized operations, process sensitive data, and deliver seamless user experiences.

1. IT Governance and compliance
<212> Governance of IT ensures alignment between technology investments (like PMS, booking engines) and business goals. STRPs must comply with <211> GDPR for handling <223> PII (guest/host data) and enforce <228> Privacy-by-design principles. <216> ISMS (Information Security Management System) frameworks (ISO 27001) address <206> Cybersecurity risks like data breaches or ransomware attacks. <231> Supply Chain risks (third-party integrations for payments) require <232> Vendor Assessment and <205> C-SCRM.

2. Data privacy and access control
<234> Zero Trust architectures validate every user/device interaction, critical for platforms with decentralized hosts and guests. <227> PIMS (Personal Information Management System) ensures GDPR compliance via <210> Data Retention policies.

3. Cybersecurity, incident management and risk mitigation
<206> Cybersecurity strategies include <233> Vulnerability Management (patching flaws in booking APIs) and <218> MDR (Managed Detection and Response) for threat monitoring. <310> Incident Response plans address breaches (like stolen payment data), requiring coordination with <133> Regulatory Body.
<201> BIA identifies critical IT systems (PMS downtime risks). <202> CIA Triad (Confidentiality, Integrity, Availability) is critical for information security.



Theme 1 – Business Governance & Management

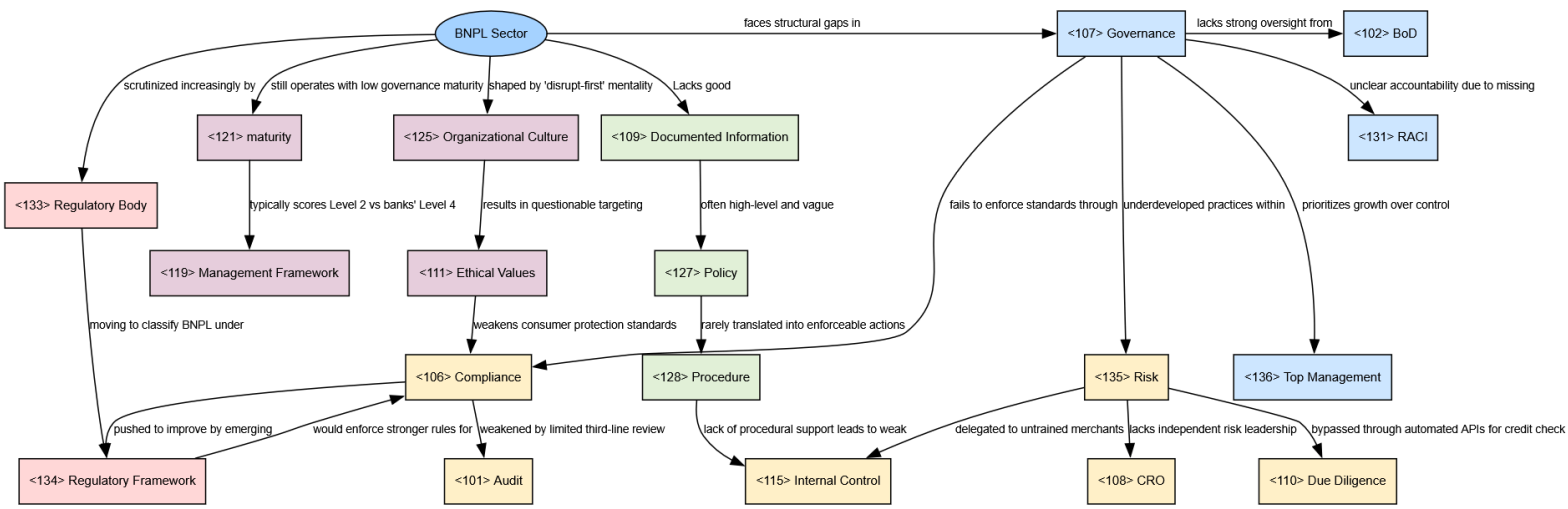
Industry: Banking and financial services
Niche: Buy now, Pay Later (BNPL)

The Buy Now, Pay Later (BNPL) sector exemplifies the governance (<112>) tensions that arise when financial innovation outpaces existing regulatory frameworks (<134>). As a nascent industry, BNPL firms often lack the robust corporate governance (<107>) structures typical of traditional banks—particularly in Board of Directors (BoD) (<102>) oversight and top management (<136>) accountability. Many fintechs prioritize rapid growth over risk control, often bypassing formal certification (<105>) standards such as ISO 27001. This leads to notable compliance (<106>) deficiencies; for instance, recent FCA data reports that 40% of BNPL users miss payments, highlighting weak affordability checks and consumer protections.

BNPL providers' GRC (<113>) capabilities remain underdeveloped relative to industry norms. Risk (<135>) management is fragmented across the Three Lines of Defense: first-line internal controls (<115>) are often delegated to under-trained merchants; second-line reliance on external scoring APIs limits effective due diligence (<110>); and third-line audit (<101>) mechanisms are minimal. Compounding these gaps are weaknesses in documented information (<109>), with generic policies (<127>) and poorly defined procedures (<128>), especially in areas like dispute resolution and fraud handling.

A lack of stakeholder alignment further complicates governance. Fintech firms like Afterpay prioritize scale over formal Chief Risk Officer (CRO) (<108>) oversight, while traditional banks lobby for regulatory parity in capital requirements. Meanwhile, regulatory bodies (<133>) like the CFPB face pressure to balance innovation with oversight, increasingly moving to classify BNPL under traditional credit regimes. Accountability is blurred, especially in cases of merchant fraud, where the absence of a clear RACI (<131>) structure obscures responsibility.

These structural issues reflect deeper cultural misalignments. BNPL's "move fast" ethos clashes with the risk-averse norms of finance, eroding shared organizational culture (<125>) and fostering questionable ethical values (<111>), e.g., targeting younger consumers with low financial literacy. In terms of maturity (<121>), most BNPL providers operate at Level 2 (ad-hoc) when benchmarked against established management frameworks (<119>) like ISO 31000, seen in traditional banks.



Theme 2 – Governance of IT and IT Management

Industry: Banking and financial services
Niche: Buy now, Pay Later (BNPL)

1. Strategic Alignment & Compliance

BNPL IT governance (<212> Governance of IT) is enforced by an ISMS (<216> ISO/IEC 27001 + COBIT) that aligns approval-rate and default-rate initiatives with business KPIs. Controls tie each project to PSD2 (<211> Open Banking) and GDPR (<211>), ensuring data-subject rights, breach notification, and automated compliance. Major incidents and exceptions are reported to the <133> Regulatory Body (e.g., FCA, SEC) for full auditability.

2. Privacy & Data Protection

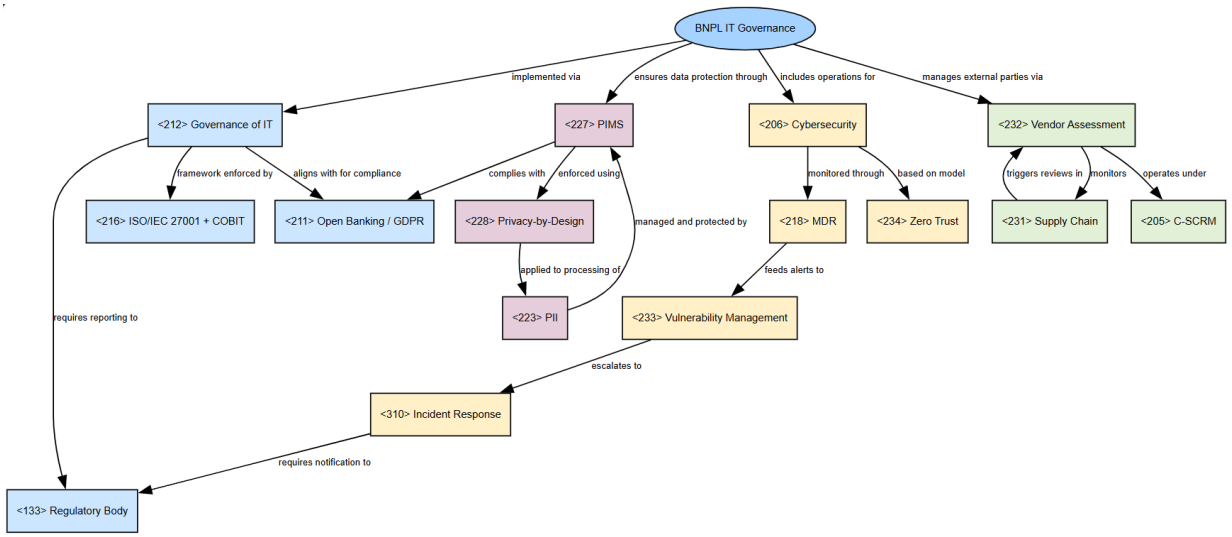
Consumer credit-score and PII data (<223>) power BNPL underwriting and personalized reminders—so a robust Privacy Information Management System (<227> PIMS) is mandatory. Leveraging <228> Privacy-by-Design, it enforces consent capture, strict minimization, and automated retention/deletion. Tight integration with CRM and underwriting platforms logs all subject-access and rectification requests.

3. Cybersecurity Operations

Under the ISMS, <206> Cybersecurity employs a Zero Trust model (<234>) requiring continuous authentication and least-privilege access. A 24/7 Managed Detection & Response service (<218> MDR) feeds into <233> Vulnerability Management for CVE scanning and patching. On detecting a breach or fraud event, a formal <310> Incident Response plan triggers escalation, forensic logging, and post-mortem audit.

4. Third-Party & Payment-Network Risk

BNPL relies on merchant integrations, card-network tokenization, and credit-bureau APIs. A structured <232> Vendor Assessment program under <205> C-SCRM rates each provider on security posture and SLA compliance. Ongoing monitoring via the <231> Supply Chain layer triggers contract reviews or technical mitigations whenever a vendor's risk profile shifts.



Comparing theme Business Governance & Management

in BNPL (Banking) and Short-term Rentals (Hospitality)

BNPL and short-term rental platforms both disrupt traditional industries but face distinct governance challenges.

Structural Governance: BNPL lacks mature corporate governance (107), with weak BoD (102) oversight and top management (136) accountability. Short-term rentals employ hybrid organizational structures (126), balancing centralized tech with local compliance teams.

Regulation & Compliance: BNPL struggles with regulatory frameworks (134), avoiding credit classification, leading to compliance (106) gaps (e.g. missed payments). Short-term rentals actively navigate zoning laws and GDPR (211), implementing automated due diligence (110) for hosts.

Risk Management: BNPL's risk (135) controls are fragmented, relying on unvetted APIs and lacking internal controls (115). Short-term rentals use standardized procedures (128) for safety checks and fraud prevention.

Culture & Ethics: BNPL's organizational culture (125) prioritizes growth over consumer protection, raising ethical (111) concerns (e.g., targeting vulnerable users). Short-term rentals focus on trust, measured via KPIs (116) like guest satisfaction, though face criticism over housing shortages.

Accountability: BNPL lacks clear RACI (131) accountability, especially for fraud. Short-term rentals define roles in policy frameworks (127) for disputes.

Maturity: BNPL operates at Level 2 (ad-hoc), while short-term rentals reach Level 3 (defined processes), showing better adaptation to regulatory demands.

in subscription models in the F&B (Retail) and Short-term Rentals (Hospitality)

Governance Structures: Subscription F&B platforms leverage their organizational culture (125) to embed compliance within operations, using KPIs (116) like customer lifetime value as governance tools. Their hybrid organizational structure (126) tightly couples centralized strategy with regional food safety teams. Short-term rentals employ a different hybrid model, balancing tech scalability with hyperlocal compliance units for zoning laws, reflecting more complex regulatory frameworks (134).

Compliance Challenges: Where F&B contends with dual GDPR (211) and food safety regimes, rentals navigate a triple burden adding property/tax rules. Both deploy GRC frameworks (113), but F&B's due diligence (110) focuses on supply chain (231) risks, while rentals prioritize host verification and tax reporting through automated controls (115).

Risk & Operational Maturity: F&B demonstrates higher maturity (121) in standardizing procedures (128) for perishable logistics, while rentals excel in scaling management systems (120). Their risk profiles (135) diverge: F&B worries about ingredient sourcing, rentals about fraudulent listings. Both use RACI matrices (131) but apply them differently—F&B for recall protocols, rentals for dispute resolution.

Cultural Alignment: The sectors manifest ethical values (111) differently: F&B through sustainability pledges measured by product quality (130) metrics, rentals via trust-building KPIs like host retention. This reflects their core challenges, F&B's subscription model demands consistent experience, while rentals' peer-to-peer nature requires community balance.

Business Resilience: Both maintain robust business continuity (103) plans, though F&B's center on supply chain redundancy and rentals on crisis response (e.g., pandemic refund policies). Their top management (136) prioritizes different resilience aspects, F&B on delivery reliability, rentals on platform stability.

Comparing theme IT Governance and Management

in BNPL (Banking) and Short-term Rentals (Hospitality)

Strategic Alignment & Compliance: In BNPL sector, <212> Governance of IT ensures compliance with financial regulations like <211> PSD2 (Open Banking) and <211> GDPR, using frameworks such as <216> ISMS to automate risk assessments and fraud detection. STRPs, by contrast, focus on <211> GDPR to protect guest data, relying on <216> ISMS to secure booking systems against cyber threats like ransomware.

Privacy & Data Protection: BNPL services implement <227> PIMS to manage sensitive credit scores with <228> Privacy-by-Design to enforce strict consent mechanisms (<221> Opt-in). STRPs, use <227> PIMS to safeguard guest identities and payment details, via <234> Zero Trust to validate host-guest interactions.BNPL emphasizes financial vetting, when STRPs enforce decentralized access controls.

Cybersecurity Operations: BNPL platforms combat financial fraud through <218> MDR services and the <202> CIA Triad. STRPs prioritize PMS uptime, using <233> Vulnerability Management to patch API flaws and prevent downtime. Both sectors face cyber risks, but BNPL targets transaction integrity, whereas STRPs mitigate disruptions to guest experiences.

Third-Party & Supply Chain Risk: BNPL relies on <205> C-SCRM to secure credit bureaus, requiring <230> SBOM for payment software transparency. STRPs employ <205> C-SCRM to assess property services, conducting <201> BIA to prioritize PMS recovery.

Incident Response: BNPL's <310> Incident Response ensures transaction logging and regulatory reporting. STRPs focus on notifying GDPR authorities and restoring bookings. Both sectors emphasize accountability, but BNPL safeguards financial workflows, while STRPs protect user-facing platforms

in subscription models in the F&B (Retail) and BNPL (Banking)

Strategic Alignment & Compliance: Subscription F&B platforms use an ISMS (<216> ISO/IEC 27001 + COBIT) to link fulfillment SLAs and churn KPIs to GDPR (<211>) and food-safety rules, with exceptions reported to the <133> Regulatory Body, while BNPL embeds approval-rate and default-rate metrics into PSD2 (<211>) and GDPR workflows, routing all breaches to financial regulators (e.g., FCA, SEC).

Privacy & Data Protection: Subscription F&B leverages a PIMS (<227>) with Privacy-by-Design (<228>) to govern PII (<223>) in CRM and billing, logging every data-subject request, whereas BNPL secures credit scores and transaction histories via its PIMS plus explicit Opt-in (<221>) flows and encrypted vaults in underwriting systems.

Cybersecurity Operations: Both sectors apply Zero Trust (<234>) under their ISMS with 24/7 MDR (<218>) and Vulnerability Management (<233>), but Subscription F&B focuses on supply-chain API resilience and order-management services, while BNPL prioritizes payment-gateway telemetry and fraud-response drills in its Incident Response (<310>) playbook.

Third-Party & Supply-Chain Risk: Subscription F&B rates kitchens, couriers, and suppliers via Vendor Assessment (<232>) under C-SCRM (<205>) with Supply Chain (<231>) triggering contract reviews, and BNPL similarly evaluates merchants, card networks, and bureaus—adding SBOM (<230>) transparency and API-gateway isolation for high-risk partners.