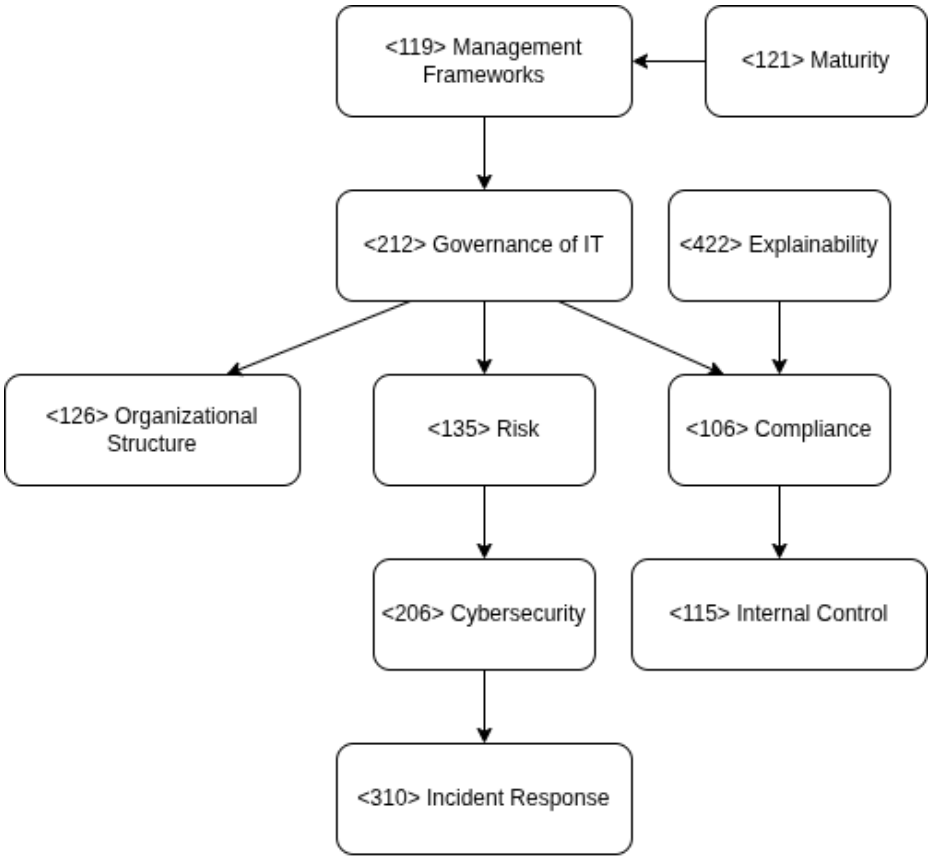
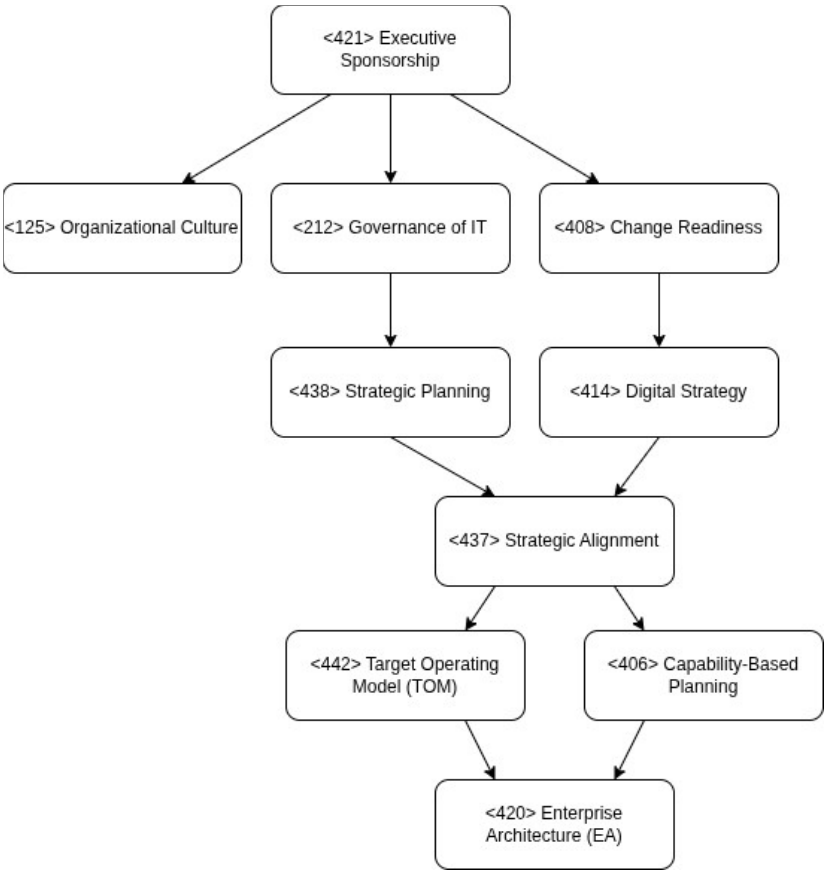
Q2 - 102618 - Ana Almeida

Sheet 1 – Concept Map:



Sheet 2 – Concept Map:



Theme 2: Governance of IT and IT Management

Introduction of core concepts from the TNO-2023-R11803

1 WHAT IS THE SOC OF THE FUTURE?

In recent years, the Security Operations Center (SOC) has become a central component of institutional cybersecurity efforts. Traditionally viewed as a technical and reactive function focused on incident detection and response, the SOC is now undergoing a redefinition. As described in the TNO report "SOC of the Future" (2023), its role is expanding beyond infrastructure protection, becoming a key governance asset embedded in strategic decision-making and risk management. The SOC of the future must respond not only to cyber threats, but also to the complexities of organisational accountability, cross-sector coordination, and the ethical implications of automated security processes.

2 CURRENT GOVERNANCE REALITIES OF SOCS

Despite their growing importance, many SOCs continue to operate with fragmented governance. Lines of accountability are often unclear, especially in organisations where SOC activities are outsourced or spread across multiple departments. Evaluation tools such as SOC-CMM (Cybersecurity Capability Maturity Model) and SIM3 (Security Incident Management Maturity Model) reveal significant maturity gaps, particularly in areas related to strategic integration, governance structures, and institutional alignment.

Rather than being well-integrated within enterprise governance mechanisms, many SOCs function in silos. They rely heavily on technological instrumentation—such as Security Information and Event Management (SIEM) systems—without corresponding institutional mechanisms for oversight, role definition, or escalation. This isolation undermines both the effectiveness and the legitimacy of the SOC as a pillar of digital governance.

3 EMERGING CHALLENGES BETWEEN 2024 AND 2030

Looking ahead, the TNO report outlines five major developments that are expected to reshape SOC governance by 2030. First is the convergence of IT, OT (operational technology), and IoT (Internet of Things) environments. This convergence broadens the scope of the SOC and introduces new stakeholders, technical dependencies, and governance risks. Second, the increasing use of artificial intelligence in security operations introduces both efficiency gains and new accountability concerns—particularly when AI systems begin to inform or make operational decisions.

A third trend is the growing prominence of European regulatory frameworks, such as the proposed Cyber Solidarity Act, which aims to enhance cross-border cybersecurity cooperation and establish shared obligations. This implies that SOCs will have to operate within multi-level governance structures, subject to both national mandates and supranational coordination. Fourth, the continued outsourcing of SOC functions to managed service providers (e.g., MSSPs and MDRs) creates structural tension between operational responsiveness and institutional control. Finally, there is a growing demand for transparency, explainability, and strategic contribution from the SOC—transforming it from a reactive function to a strategic actor.

4 STRATEGIC IMPLICATIONS FOR IT GOVERNANCE

These changes reinforce the need to treat the SOC not merely as a technical service but as a governance function with strategic relevance. The future SOC must be able to justify its decisions, demonstrate compliance with external regulations, and align its operations with broader enterprise objectives. This requires new approaches to metrics, performance evaluation, and integration into governance frameworks such as COBIT or ISO/IEC 27001.

Moreover, as the report suggests, governance cannot stop at internal controls. Organisations increasingly operate in hybrid ecosystems, relying on third-party providers and engaging with public-sector frameworks. This demands a more distributed model of governance—one that is capable of coordinating across organisational boundaries, managing legal and contractual complexity, and maintaining institutional oversight even in federated or outsourced settings.

5 A CASE FOR RETHINKING GOVERNANCE STRUCTURES

The transformation of the SOC exemplifies broader challenges in the governance of IT and information security. It reflects the tensions between control and agility, between central oversight and distributed execution, and between compliance and innovation. For students engaging with the governance of IT, the SOC offers a rich, practical context to examine how strategic integration is negotiated, how risk is managed across technological and institutional layers, and how governance frameworks must evolve to remain effective.

Ultimately, the SOC of the future becomes a lens through which one can understand the shifting boundaries of responsibility in digital governance. It invites a reconceptualisation of what it means to "govern" IT in a world where threats are continuous, responsibilities are shared, and accountability must be both operational and ethical.

Theme 4: IT, Strategy, and Change

Strategic Framing based on the content of TNO-2023-R11803

1 RETHINKING THE SOC AS A STRATEGIC ASSET

Historically, Security Operations Centers (SOCs) have been positioned as tactical response units within IT departments, focused on incident detection, alert triage, and operational resilience. This framing, while still relevant, is no longer sufficient. As highlighted in TNO-2023-R11803, the SOC is undergoing a paradigmatic change. It is increasingly seen not only as a protective function, but as a key enabler of institutional strategy, digital transformation, and public trust.

This repositioning has profound implications for governance, leadership, and investment. Rather than being treated as a cost center or a reactive buffer, the SOC must be integrated into the strategic planning processes of organizations. Its decisions, what to monitor, how to respond, and which risks to prioritize, now shape not just technical outcomes but institutional direction, legal exposure, and reputational resilience.

2 STRATEGIC PRESSURES AND THE EXTERNAL LANDSCAPE

Several external forces are converging to raise the strategic importance of the SOC. Regulatory pressure is growing: initiatives like the EU's Cyber Solidarity Act are pushing national and sectoral infrastructures toward cross-border coordination, minimum capability thresholds, and federated response models. At the same time, strategic risk is being reframed. Cybersecurity is no longer just about defending perimeters: it is about protecting trust in digital services, safeguarding continuity in the face of systemic threats, and enabling innovation in a secure and resilient way.

In this environment, SOCs are expected to provide more than visibility; they are expected to inform board-level decision-making, align with enterprise risk frameworks, and support adaptive governance models. Their metrics must evolve from raw event counts to value-oriented indicators: impact on service availability, alignment with risk appetite, and contribution to strategic resilience goals.

3 GOVERNANCE TRANSFORMATION AND CAPABILITY PLANNING

Embedding the SOC in strategic governance requires significant internal change. Traditional IT governance models often treat security as a "necessary constraint" rather than a dynamic capability. In contrast, the SOC of the future must be woven into governance mechanisms such as strategic portfolio management, risk-based investment planning, and enterprise architecture.

This transition also affects capability planning. The future SOC is not a standalone entity; it operates in a network of actors, including cloud providers, national authorities, and sector-specific coordination structures. Strategic leaders must therefore plan not only for internal staffing and tooling, but also for inter-organizational alignment, legal interoperability, and cross-sector scenario readiness. This aligns closely with concepts such as the Target Operating Model (TOM), where SOC capabilities must be viewed as part of the institutional "to-be" architecture for resilience.

4 CHANGE MANAGEMENT AND LEADERSHIP IMPLICATIONS

Strategic change rarely occurs without resistance. Transforming the SOC into a strategic actor involves cultural shifts: security teams must engage with business objectives; senior leaders must assume accountability for digital risk; and governance boards must integrate cyber metrics into performance reviews. This requires strong executive sponsorship, as well as a clear articulation of value that goes beyond compliance.

Leadership must also manage a delicate balance: promoting agility and innovation in IT operations, while ensuring that the SOC maintains sufficient independence and oversight. This echoes the broader tension, well explored in Theme 4, between stability and change, risk and opportunity, central control and distributed responsibility.

5 FRAMING THE SOC WITHIN DIGITAL STRATEGY

Ultimately, the SOC of the future is not just an instrument of defense, it is an institution-building function. Its governance reflects how seriously an organization takes its digital responsibilities, how mature its risk thinking is, and how aligned its technology operations are with its mission. From a strategic perspective, the SOC becomes a litmus test for digital governance maturity.

Students examining this case through the lens of IT, Strategy, and Change are invited to consider not only how SOCs respond to threats, but how they shape organizational readiness, stakeholder confidence, and institutional agility. In other words, the SOC is both a mirror and a mechanism of strategic capability.