

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.