# Literature Review on Third-Party Risk Management Frameworks

## NIST SP 800-161 and ISO/IEC 27001

Third-party risk management (TPRM) has become a top priority in cybersecurity strategy, especially as organizations increasingly depend on external vendors, cloud providers, and service partners. High-profile breaches often trace back to vulnerabilities within the extended supply chain. To address these risks systematically, several standards and frameworks have been developed, including NIST SP 800-161 (Rev.1) and ISO/IEC 27001:2013 Annex A.15 (also known as Supplier Relationships). This review critically explores academic and professional literature surrounding these frameworks, comparing their scope, application, and effectiveness in managing third-party cybersecurity risks.

### NIST SP 800-161: Supply Chain Risk Management for Systems and Services

NIST SP 800-161 provides a U.S. government-backed framework focused on Cybersecurity Supply Chain Risk Management (C-SCRM). It is tailored to organizations operating critical infrastructure or government systems but has been increasingly referenced by private sector entities seeking rigorous TPRM strategies.

#### Key Themes Identified

**Systemic Risk Awareness**: NIST emphasizes not just individual vendor risks, but systemic vulnerabilities introduced through interconnected systems, products, and services (O’Reilly & Rigopoulos 2021).

**Tailored Control Implementation**: Research from organizations such as MITRE underscores the value of tiered control sets that allow tailoring based on system criticality and risk tolerance.

**Lifecycle View of Risk**: Literature consistently emphasizes the importance of managing third-party risk across the entire system lifecycle from design and acquisition to retirement. This is a distinctive strength of the NIST model compared to ISO standards.

However, NIST 800-161 requires significant internal expertise and institutional capacity to implement effectively, posing a challenge for SMEs (Sabidi & Zolkipli 2024).

### ISO/IEC 27001

In an increasingly digital world, organizations face complex risks not only from internal vulnerabilities but also through their interactions with external suppliers and service providers. **ISO/IEC 27001**, a globally recognized standard for information security management systems (ISMS), has emerged as a cornerstone framework for securing organizational assets, especially when dealing with third parties. The standard provides a structured approach to identifying, assessing, treating, and monitoring information security risks, including those introduced by suppliers and partners.

The ISO/IEC 27001 standard is widely adopted across industries due to its risk-based and process-oriented structure. The standard's flexibility allows it to be customized to different organizational contexts, which makes it especially valuable for both SMEs and large enterprises (Kenyon 2024).

ISO/IEC 27001 places strong emphasis on top management commitment, a principle that sets it apart from many purely technical frameworks. This emphasis facilitates a security-aware culture, ensuring that third-party risks are not only addressed by IT teams but also embedded in organizational decision-making processes (Malatji 2023).

Annex A.15 of the 2013 edition of ISO/IEC 27001 addresses information security within supplier relationships, specifically focusing on the protection of assets accessible by third parties (Nasser 2017). It introduces controls under A.15.1 (Information security in supplier relationships) and A.15.2 (Supplier service delivery management).

#### Key Findings:

**Contractual Controls**: A major strength identified in the literature (Culot et al. 2021) is ISO's focus on embedding security clauses in supplier contracts, which helps define clear accountability and reduce legal ambiguity.

**Ongoing Monitoring Emphasis**: A.15.2 encourages continuous review of supplier performance and security compliance, though enforcement varies widely by organization (Rozi et al. 2024).

**Risk-Based Application**: The ISO standard promotes a risk-based approach, allowing organizations to scale security measures based on the nature of services provided and the sensitivity of information involved (Rozi et al. 2024).

Despite these strengths, ISO 27001 A.15 has been critiqued for being too high-level, lacking the technical detail found in NIST frameworks, and providing limited guidance on how to conduct real-time supplier risk assessments (Suorsa & Helo 2023).

## NIST SP 800-161 vs ISO 27001 Annex A.15

|  |  |  |
| --- | --- | --- |
| Feature | NIST SP 800-161 | ISO/IEC 27001 Annex A.15 |
| Focus | Cybersecurity supply chain (C-SCRM) | Supplier relationships |
| Depth of Technical Guidance | High technical, lifecycle-based | Moderate – policy and contract based |
| Primary Audience | U.S. federal agencies, critical sectors | Broad, international business |
| Lifecycle Risk Management | Strong emphasis | Limited, more transactional |
| Ease of Implementation | Complex and resource-intensive | More accessible, certification-ready |

Generally, NIST SP 800-161 provides stronger technical rigor, particularly for organizations managing national infrastructure or sensitive data systems. In contrast, ISO 27001 A.15 is more practical and globally accepted, especially in industries where formal compliance and certification are key drivers of vendor trust.

The 2022 revision of ISO/IEC 27001 replaced Annex A.15 with Annex A.5.19 (Information Security in Supplier Relationships), aligning it more closely with modern digital supply chains. This update incorporates better alignment with digital service models and improves guidance on cloud-based vendor risks (Rakan et al. 2024).

Meantime, researchers are exploring automation tools, AI-driven vendor scoring systems, and continuous monitoring technologies as essential extensions to these frameworks. However, most TPRM frameworks still lack robust guidance for fourth-party risk, which arises when a vendor's subcontractors introduce vulnerabilities.

Moreover, with increased regulatory focus globally such as the Digital Operational Resilience Act (DORA) in Europe and CISA’s recommendations in the U.S. There is growing pressure to enhance the real-time monitoring capabilities of both frameworks.

# References

O’Reilly, P. & Rigopoulos, K. 2021, ‘2020 cybersecurity and privacy annual report’, *NIST Special Publication*, no. 800, p. 214.

Sabidi, M.L. & Zolkipli, M.F. 2024, ‘The role of risk management in cybersecurity protocols’, *Borneo International Journal*, vol. 7, no. 2, pp. 77-81.

Nasser, A. 2017, ‘Information security gap analysis based on ISO 27001:2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen’, *International Journal of Scientific Research in Multidisciplinary Studies*, vol. 3, no. 11, pp. 4-13.

Culot, G., Nassimbeni, G., Podrecca, M. & Sartor, M. 2021, ‘The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda’, *The TQM Journal*, vol. 33, no. 7, pp. 76-105.

Rozi, N.R.F., Wirabudi, A.A. & Rozano, S.A. 2024, ‘Chance evaluation and improvement of get to control data security administration based on ISO/IEC 27001 at Telkom University Jakarta Campus’, *International Journal of Science Education and Cultural Studies,* vol. 3, no. 2, pp. 1-2.

Suorsa, M. & Helo, P. 2023, ‘Information security failures measured and ISO/IEC 27001:2022 controls ranked by General Data Protection Regulation penalty analysis’, *2023 11th International Conference on Cyber and IT Service Management (CITSM)*, IEEE, pp. 1-5.

Rakan, R., Mulyana, R. & Lubis, M. 2024, ‘Utilizing ISO 27001: 2022 to design information security for BPRACo SME digital transformation’, *Jurnal Teknologi dan Sistem Informasi Bisnis*, vol. 6, no. 4, pp. 820–83.

Kenyon, B. 2024, ISO 27001 controls: A guide to implementing and auditing.

Malatji, M. 2023, ‘Management of enterprise cyber security: A review of ISO/IEC 27001:2022’, *International Conference on Cyber Management and Engineering (CyMaEn)*, IEEE, pp. 117–122.