NOZOMI NETWORKS

WHITE PAPER

Managing Digital Supply Chain Risk Through Third-Party Cybersecurity Oversight

1. Executive Summary

In today's hyperconnected environment, managing cybersecurity and privacy risks across a complex network of SaaS and IaaS providers is essential to business resilience. Nozomi Networks' Third-Party Risk Management (TPRM) program is purpose-built to address these challenges, focusing specifically on the digital supply chain and the cybersecurity posture of third-party providers.

2. Our Approach

Our TPRM framework is tightly integrated with enterprise risk management and scales with our vendor ecosystem. We categorize vendors based on criticality using a CIA (Confidentiality, Integrity, Availability) model, which informs the depth of our assessments and the strength of our contractual security requirements.

We leverage technology to continuously monitor live cybersecurity risks for critical SaaS providers, enabling real-time visibility and faster response to emerging threats.

3. Key Capabilities

- **Risk-Informed Vendor Selection and Tiering**: Vendors are segmented based on their impact on our operations and data, using a CIA-based model to guide onboarding and oversight.
- **Security-Focused Due Diligence**: Initial assessments evaluate the vendor's security posture, privacy practices, and compliance with relevant standards.
- **Contractual Safeguards**: We embed information security and privacy requirements into contracts, tailored to the vendor's risk profile.
- **Live Cybersecurity Monitoring**: For critical SaaS providers, we use technology to continuously monitor for vulnerabilities, misconfigurations, and threat indicators.
- **Incident and Issue Management**: We maintain structured processes for responding to vendor-related incidents, ensuring swift containment and remediation.
- **Ongoing Reassessment and Offboarding**: Vendor risk is reassessed periodically, and offboarding includes secure data transition and access revocation protocols.

4. Governance and Accountability

Our TPRM program is supported by a cross-functional governance model that ensures accountability and continuous improvement:

- Procurement leads vendor engagement and contract negotiation.
- Compliance & Risk ensures alignment with regulatory requirements and internal policies.
- Security & IT conducts technical reviews and manages ongoing monitoring.
- Business Owners provide input on vendor performance and risk tolerance.

5. Regulatory Compliance

Without a TPRM program, organizations like ours would face significant consequences, including regulatory non-compliance, data breaches, operational disruptions, and reputational damage. ISO 27001 requires controls for supplier relationships, SOC 2 emphasizes oversight of vendors under its Trust Services Criteria, and GDPR mandates formal contracts and risk-based security measures for data processors. Our TPRM framework ensures that we only meet regulatory and contractual obligations.

At Nozomi Networks, TPRM program plays a critical role in meeting the requirements of ISO/IEC 27001, SOC 2, and the GDPR. These frameworks mandate that organizations assess and manage risks introduced by third-party service providers—particularly those handling sensitive data or supporting critical operations. Our processes ensure compliance by conducting structured due diligence, categorizing vendors, and embedding information security and privacy requirements into contracts. For high-risk SaaS providers, we also implement continuous, real-time cybersecurity monitoring to detect and respond to threats proactively.

6. Conclusion

As digital supply chains grow more complex, so do the risks. Our TPRM program ensures that information security and privacy are embedded into every stage of third-party engagement—protecting our operations, data, and customers.

For further inquiries regarding this white paper on Nozomi Networks' data protection practices, please contact the compliance team at **compliance@nozominetworks.com**

NOZOMI NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.