NOZOMI NETWORKS

WHITE PAPER

Building a Resilient Corporate Control Environment: Lessons from Nozomi's GRC Strategy

Introduction

A Message from Director of GRC

As Director of Governance, Risk and Compliance at Nozomi, I have had the privilege of working alongside a dedicated GRC team committed to advancing our organization's control environment. This article presents my perspective on how the Nozomi GRC team has built a resilient corporate control environment. The following analysis explores how the team's strategy supports governance and risk management, integrates control families across the organization, and maintains a comprehensive policy landscape.

Our approach starts with alignment. Frameworks like SOC 2, ISO 27001, and NIST 800-53 aren't just benchmarks—they're the foundation for how we design and enforce policies. By mapping these frameworks into our GRC program, we ensure that every department—whether HR, Legal, IT, or Engineering—operates under a unified set of expectations. This integration eliminates silos and creates consistency, so compliance isn't a separate function; it's embedded in how we work every day.

Karen Meohas
Director of GRC

Policies as Enablers of Governance and Risk Management

A comprehensive policy framework is the backbone of effective governance and risk management. Policies do more than set expectations—they translate regulatory requirements, industry standards, and organizational values into actionable controls that guide daily operations and strategic decisions. For the Nozomi GRC team, policies are not static documents but dynamic tools that evolve alongside the business and the threat landscape.

Each year, the GRC team undertakes a comprehensive review of all policies. This process is not merely a compliance exercise; it is an opportunity to assess new regulatory requirements, emerging risks, and lessons learned from audits and incidents. The team actively seeks to incorporate enhancements that strengthen security, close gaps, and align with best practices. By continuously refining the policy landscape, the GRC team ensures that Nozomi's controls remain relevant, effective, and resilient—enabling the organization to anticipate and respond to new challenges with confidence.

Take our Information Security Policy, Access Control Policy, Data Handling Policy, and Encryption Policy. They translate technical requirements into practical safeguards, ensuring that sensitive data remains secure across systems and geographies.

Operational resilience is another core area. Policies like Business Continuity and Change Management guarantee that we can adapt to disruptions without compromising service or security. They provide structured processes for responding to incidents, maintaining uptime, and documenting changes—critical for both risk mitigation and audit readiness.

Centralization and Enforcement

What makes this system work is centralization. Our GRC function consolidates regulatory requirements and industry standards into a single governance framework. From there, we cascade these requirements into policies that apply universally—whether you're in product development, finance, or operations. This ensures that every business unit operates under the same compliance lens, reducing gaps and strengthening accountability.

Enforcement isn't about policing—it's about process. Each policy is supported by documented procedures, training, and monitoring mechanisms. For example, access controls are validated through system logs, and security incidents are tracked in centralized platforms. These measures create evidence trails that demonstrate compliance, not just intent.

Independent Assurance Through External Audits

To validate that our controls are not only designed but operating effectively, we undergo rigorous audit cycles performed by independent third parties. These audits—covering SOC 2, ISO 27001, among other standards and regulations—don't rely on declarations; they require evidence and process testing. Auditors review our policies, examine implementation records, and test controls in real-world scenarios. This external validation confirms that our governance framework is more than theory—it's proven in practice.

The result? Confidence for our customers, partners, and regulators that Nozomi meets the highest standards of security, ethics, and operational resilience.

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.