**Operational Risk Management Policy**

**Organization: The Xander Protocol**

**Policy Owner: Chief Risk & Compliance Officer (CRCO)**

**Approval Date: 10/22/2025**

**Version: 1.0**

**Review Cycle: Annual**

**Classification: Internal / Confidential**

**Table of Contents**

**1. Executive Summary**

**2. Purpose**

**3. Scope**

**4. Regulatory & Framework Alignment**

**5. Key Definitions**

**6. Governance Principles**

**7. Risk Identification and Assessment**

**8. Risk Ownership and Committee Oversight**

**9. Risk Mitigation and Controls**

**10. Monitoring, Reporting, and Dashboards**

**11. Incident Management and Escalation**

**12. Training and Awareness**

**13. Continuous Improvement and Policy Review**

**14. Enforcement**

**1. Executive Summary**

This policy establishes a comprehensive framework for identifying, assessing, mitigating, monitoring, and reporting operational risks across the entire organization. It ensures that employees, vendors, contractors, and third parties actively participate in risk management. By integrating qualitative and quantitative assessment methods, tiered risk appetite, automation, and continuous monitoring, the organization can minimize operational, human, technological, and supply chain risks, creating a resilient, risk-aware culture.

**2. Purpose**

The purpose of this policy is to provide a structured approach to operational risk management across all business units. It promotes proactive identification, assessment, and mitigation of risks while fostering accountability and a strong risk-aware culture. This policy also ensures alignment with industry-recognized risk frameworks and corporate governance standards, enabling the organization to operate efficiently and securely.

**3. Scope**

This policy applies to all employees, contractors, temporary staff, and third-party service providers. It covers internal operations, technology systems, business processes, and supply chains, addressing operational risks such as process failures, human errors, technology or system failures, and supply chain disruptions. The policy integrates with other corporate policies and governance mechanisms while maintaining an internal focus on effective risk management practices.

**4. Regulatory & Framework Alignment**

This policy is aligned with ISO 31000, which provides guidelines for enterprise risk management, the COSO ERM Framework for comprehensive risk identification and response, and NIST CSF for operational and cybersecurity risk management. It also ensures readiness for audits or regulatory review, maintaining internal compliance and proactive governance.

**5. Key Definitions**

Operational risk refers to the risk of loss resulting from inadequate or failed internal processes, human actions, systems, or external events. Risk appetite defines the organization’s tolerance for various risk categories, structured in a tiered hierarchy to prioritize focus and mitigation. Risk Owners are designated individuals accountable for managing specific risks and implementing controls. Controls include preventive, detective, and corrective measures to mitigate operational risks. An incident is any event or near-miss that exposes the organization to operational risk.

**6. Governance Principles**

Risk management is the responsibility of all personnel and third-party partners. Each operational risk is assigned to a Risk Owner, who is accountable for implementing mitigation strategies, monitoring risk, and reporting incidents. A Risk Committee provides oversight, approves risk appetite tiers, and ensures policy compliance. Employees are expected to report potential risks or near-misses proactively. Mitigation strategies include preventive, detective, and corrective measures, supported by SOPs, process automation, and continuous monitoring.

**7. Risk Identification and Assessment**

Operational risks are identified and assessed using both qualitative and quantitative methods, including risk matrices, scoring, and scenario analysis. Continuous monitoring ensures emerging risks are detected in real time. Risk categories include internal processes, technology systems, human factors, and supply chain vulnerabilities. Risks are categorized into tiers according to likelihood and impact, aligned with the organization’s risk appetite, which guides prioritization and response.

**8. Risk Ownership and Committee Oversight**

Each operational risk has a designated Risk Owner responsible for implementing mitigation strategies and monitoring controls. The Risk Committee oversees enterprise-level risk, approves mitigation strategies, and reviews dashboards and reports. Employees are responsible for immediately reporting any identified risks or procedural gaps to their Risk Owner or supervisor, ensuring accountability across the organization.

**9. Risk Mitigation and Controls**

Mitigation strategies include preventive measures such as training, SOPs, dual-approval workflows, and automation to reduce risk exposure. Detective controls include monitoring dashboards, intrusion detection systems, and periodic audits. Corrective controls respond to incidents through process adjustments, retraining, or system improvements. Technology-driven solutions, including AI-assisted monitoring and automated alerts, are used to enhance risk detection and response. The tiered risk appetite hierarchy ensures high-risk issues are escalated promptly.

**10. Monitoring, Reporting, and Dashboards**

Operational risks are continuously monitored using dashboards, key performance indicators, and automated system alerts. Monthly reports detail operational risks, incidents, and mitigation status, which are reviewed by executives and the Risk Committee. Standardized incident reporting ensures clarity and allows for actionable follow-up. Periodic audits validate the effectiveness of risk controls and mitigation measures.

**11. Incident Management and Escalation**

All operational incidents must be reported immediately to the Risk Owner and Risk Committee. Escalation follows a defined hierarchy based on severity and potential impact. Each incident undergoes a root cause analysis, with corrective actions documented and implemented. Lessons learned from incidents and near-misses are incorporated into continuous improvement initiatives to enhance organizational resilience.

**12. Training and Awareness**

Mandatory operational risk awareness training is provided to all employees, contractors, and third parties. Role-specific modules ensure that critical positions and processes receive focused guidance. Annual refresher courses maintain awareness and reinforce the corporate risk culture. Training includes practical exercises, scenario simulations, and case studies to promote active learning and application.

**13. Continuous Improvement and Policy Review**

The Operational Risk Management Policy is reviewed annually or after significant incidents or regulatory changes. Mitigation strategies, assessment methods, and monitoring tools are updated as needed. Lessons learned from incidents, audits, and employee feedback inform improvements to risk management practices. The policy encourages proactive adaptation and continuous enhancement of operational resilience.

**14. Enforcement**

Non-compliance with operational risk protocols may result in restricted access, disciplinary actions, or other corrective measures. Risk Owners, supervisors, and managers are responsible for enforcing adherence to this policy. All enforcement actions and any exceptions are documented and reported to the Risk Committee for oversight and transparency.