Acceptable Risk Documentation for System Outages

This document provides a comprehensive overview of acceptable risks associated with potential system outages due to non-security vendor defects. It outlines the inherent risks, applied controls, and the remaining residual risk level for each identified risk. This analysis aims to ensure that these risks are documented, managed, and reviewed periodically.

Risk ID: RISK-001

Risk Description: Potential system outage due to vendor software defect in data processing
Inherent Risk Level: High
Applied Controls: Vendor SLA for timely patches and support; Internal monitoring
Residual Risk Level: Medium
Risk Owner: IT Operations Manager
Review Dates: Last reviewed on 2024-01-15, next review scheduled for 2024-07-15.

Risk ID: RISK-002

Risk Description: Potential system downtime due to vendor software defect in reporting module
Inherent Risk Level: Medium
Applied Controls: Backup processes; Vendor support agreement
Residual Risk Level: Low
Risk Owner: Data Processing Lead
Review Dates: Last reviewed on 2024-01-15, next review scheduled for 2024-07-15.

Risk ID: RISK-003

Risk Description: Potential system disruption due to vendor hardware issue impacting performance
Inherent Risk Level: Medium
Applied Controls: Hardware redundancy; Vendor maintenance support
Residual Risk Level: Low
Risk Owner: IT Infrastructure Lead
Review Dates: Last reviewed on 2024-01-15, next review scheduled for 2024-07-15.

How to Use This Documentation

This documentation package provides a structured approach to managing and assessing the acceptable risk of system outages due to non-security vendor defects. To effectively leverage these documents in your organization's risk management process, follow these steps:

1. **Review Each Risk**: Start by examining each risk in the spreadsheet. For each risk, evaluate the 'Inherent Risk Level' and consider the impact and likelihood of the risk if controls were not applied.
2. **Evaluate Applied Controls**: Review the 'Applied Controls' column to understand the measures already in place. These controls are designed to mitigate the inherent risk.
3. **Assess Residual Risk Level**: After evaluating the controls, review the 'Residual Risk Level'. This represents the risk that remains after the mitigation measures are applied.
4. **Follow the Scheduled Reviews**: The 'Next Review Date' helps ensure ongoing risk monitoring. Establish a process to reassess each residual risk on or before the indicated review date.
5. **Considerations for Sales**: For potential clients, these documents demonstrate a proactive approach to managing vendor risks, emphasizing commitment to operational resilience and adherence to industry standards. Use this documentation as a talking point to showcase a structured risk management process.

Standards and Best Practices Considered

The design of these documents aligns with several industry standards and best practices to ensure comprehensive and compliant risk management. The following standards were considered in creating this documentation:

- **ISO 31000: Risk Management**: Provides principles and guidelines for managing risks effectively, especially in identifying, assessing, and documenting both inherent and residual risks.
- **ISO 27001: Information Security Management**: Emphasizes documentation of risk assessment and treatment, highlighting the need for tracking both controls and residual risks in information systems.
- **NIST SP 800-53 and SP 800-37**: Guides the management and documentation of residual risks in federal information systems and includes a framework for periodic risk reevaluation.
- **ISO 22301: Business Continuity Management**: Outlines practices for assessing risks that could impact business continuity, including potential disruptions from vendor defects and establishing regular review cycles.
- **COSO ERM Framework**: Focuses on enterprise risk management, particularly the integration of residual risk tracking and the evaluation of risk levels against an organization's overall risk appetite.
- **FFIEC IT Examination Handbook**: Used in the financial sector, this handbook includes specific guidance on documenting and managing residual risks, particularly in IT and

operational resilience.

These standards were referenced to ensure that the residual risk documentation process meets industry benchmarks for robustness, compliance, and operational resilience. By aligning with these standards, your organization can be confident in the effectiveness of the applied controls and the management of vendor-related risks.

Call to Action

We encourage stakeholders and potential clients to integrate these risk management practices into their existing frameworks. By doing so, you can enhance your resilience against system outages and vendor-related disruptions.

For additional guidance, training, or to learn how these practices can be customized to your organization's unique needs, please contact BugZero.