SIT Department Risk Assessment Report

Date: 01/14/24
Prepared by: Ferdinand Ngirmekur
Department: SIT/SLDS
Subject: Small-Scale Risk Assessment of the SIT Department for Operational Risk Decisions

---

1. Introduction

This report outlines the findings of a small-scale **risk assessment** conducted within the **State Infrastructure Technology (SIT) Department**. The purpose of this assessment was to identify operational risks and determine if the risk assessment model can be applied to other offices within the **CNMI Public School System (PSS)**. This effort aims to develop a broader plan for PSS that establishes and supports operational risk decisions across departments.

---

2. Purpose and Justification

The purpose of this assessment is to establish a framework that supports **operational risk management** within the PSS. By identifying potential risks in key departments, such as SIT, we aim to minimize operational disruptions, protect critical data and assets, and ensure compliance with internal policies and regulations. This small-scale assessment is intended to serve as a model that can be scaled and applied to other departments within the school system.

---

3. Risk Assessment Overview

Department: State Information Technology (SIT)
Objective: Identify operational risks related to IT systems, data management, and network security to support decision-making and resource allocation.

---

4. Key Steps in the Risk Assessment Process

- **Identify Critical Operations**: Reviewed all critical IT functions within the SIT Department, including network management, data storage, and system security. (Google workspace, Synology, Tyler Munis, Ubiquiti, Meraki Dashboard, Barracuda Firewall, Dell Switches)
- **Assess Potential Risks**: Conducted a detailed analysis of operational risks, including system outages, data breaches, unauthorized access, and hardware failures. (Google Alerts Dashboard for SPAM and unauthorized access and data breaches, Meraki

Dashboard for hardware failures, PRTG for network connectivity issues and failures, Sentinel One for Data breaches and viruses)

- **Evaluate Current Controls**: Assessed the existing safeguards in place to mitigate these risks, such as firewalls, backups, and access control protocols.(Google Admin, Meraki Dashboard, Sentinel One Dashboard, PRTG)
- **Determine Impact and Likelihood**: Measured the potential impact of identified risks on day-to-day operations, ranking them by likelihood and severity. (If these systems were not in place we would not be able to mitigate the issues as quickly as we could with these systems in place. If these systems were not functioning we would be more vulnerable to attacks and privacy risks)
- **Develop Risk Mitigation Recommendations**: Proposed solutions to reduce the likelihood and impact of these risks through updated security measures and resource allocation. (Use current Data breach plan. Use security tools embedded in the systems: Google Admin, PRTG, Meraki Dashboard, Barracuda Firewall interface, Sentinel One dashboard. Awareness trainings to staff, faculty, and students.)

---

5. Findings

Key Risks Identified:

- **System Outages**: Unplanned system downtime due to infrastructure failures or technical issues could significantly disrupt educational operations and communications. (**Potential Causes:**

1. **Hardware Failures:** Server crashes, network malfunctions, or outdated hardware.
2. **Software Issues:** Application bugs or virus, outdated software, or compatibility problems.
3. **Network Failures:** Internet outages, bandwidth limitations, or misconfigured network equipment.
4. **External Factors:** Power outages, natural disasters, or cyberattacks.

- **Data Breaches**: Unauthorized access to sensitive student and staff data is a significant concern, especially in light of increasing cyber threats.(Lack of awareness and training for PII, and privacy measures, and security measures to leadership, staff, students and parents).
- **Hardware Failures**: Aging IT hardware poses a risk of system outages and data loss, especially for mission-critical operations. (Old computers, switches, wifi devices and any machine, etc, and software are potential risk due to unsupported updates and obsolete hardware and software).
- **Insufficient Incident Response Plan**: The existing incident response procedures need further development to address the growing complexity of potential cyber threats. (Aging Data Incident Plan not compatible with the new generation and high technology world).

Existing Controls:

- **Firewalls and Endpoint Protection**: (Barracuda, Sentinel One, Meraki, Google Workspace, and Synology).
- **Data Backups**: Regular data backups are conducted through Synology, but the disaster recovery plan needs to be tested more frequently.
- **Access Control**: Role-based access control is in place, but there are areas where multi-factor authentication (MFA) could enhance security.(Tyler Munis, Infinite Campus, Clever, Blackboard Google Workspace

---

6. Recommendations for SIT Department

1. **Enhance Backup and Recovery Procedures**: Test disaster recovery plans regularly and ensure off-site backups are secure and up to date.
2. **Upgrade IT Infrastructure**: Replace aging hardware and implement proactive maintenance schedules to avoid system downtimes.
3. **Implement Multi-Factor Authentication (MFA)**: Strengthen access controls by implementing MFA for critical systems and sensitive data access.
4. **Incident Response Training**: Develop and conduct incident response drills to prepare staff for potential data breaches and cyberattacks.
5. **Expand Monitoring Capabilities**: Use advanced monitoring tools to detect and address system vulnerabilities in real-time.

---

7. Next Steps

- **Apply the Risk Assessment Model to Other Departments**: Based on the findings from the SIT Department, this model can be adapted and applied to other offices within PSS to identify and mitigate operational risks.
- **Review and Approval by IT Director**: The report will be reviewed by the IT Director to assess the viability of applying the risk assessment model district-wide.
- **Develop Comprehensive Risk Management Plan**: Once the assessment process has been tested in other departments, a **comprehensive risk management plan** will be developed to standardize the approach to operational risk across the district.

---

8. Expected Outcomes

- **Improved Operational Security**: Identifying and addressing risks in the SIT Department will enhance operational security and minimize downtime.

- **Scalable Risk Management Framework**: This model will provide a foundation for a district-wide risk management framework, supporting operational decision-making in all departments.
- **Resource Allocation**: The findings from the risk assessment will help guide resource allocation to address critical risks and improve overall system reliability.

---

9. Conclusion

The small-scale risk assessment of the SIT Department has provided valuable insights into operational risks and control gaps. With the findings and recommendations outlined in this report, we are better positioned to mitigate risks and improve decision-making across the department. The next step is to expand this process to other offices and create a district-wide risk management plan.