Risk Assessment Report

Business Supplies Inc. (BSI)

Effective Date: August 7, 2024
Version: 1.1

Prepared by: CloudStrategik Consulting
Anderson@cloudstrategik.com

Confidentiality Statement

This document contains proprietary and confidential information of CloudStrategik Consulting. The information contained herein is disclosed to the recipient in confidence for the sole purpose of internal use. No part of this document may be disclosed, reproduced, or distributed without the prior written consent of CloudStrategik Consulting.

Contents

1 Executive Summary

This Risk Management Assessment Report provides a comprehensive analysis of the current risk landscape at Business Supplies Inc. (BSI). The assessment identifies critical information assets, evaluates potential threats, and assesses the risks associated with BSI's business operations. The primary objectives of this report are to:

- Identify and categorize key information assets critical to BSI's operations
- Assess potential threats and their impact on these assets
- Conduct a thorough risk assessment
- Provide recommendations for mitigating identified risks

This report serves as a foundation for BSI to enhance its risk management framework and ensure business continuity in an increasingly complex threat landscape.

2 Introduction

In today's rapidly evolving business environment, effective risk management is crucial for organizational success and resilience. This risk assessment for Business Supplies Inc. (BSI) aims to provide a clear picture of the current risk landscape and offer actionable insights for risk mitigation.

2.1 Background

BSI operates in a highly competitive industry, providing essential business supplies to various clients. The company's operations rely heavily on its IT infrastructure, customer data, and supply chain. Ensuring the security and availability of these assets is crucial for maintaining BSI's competitive edge and customer trust.

2.2 Scope

This assessment covers the following areas:

- Identification and categorization of BSI's key information assets
- Assessment of potential threats to these assets
- Evaluation of existing controls and identification of gaps
- Development of a risk register
- Recommendations for mitigating identified risks

3 Methodology

The risk assessment process involved the following steps:

1. Identifying key information assets critical to BSI's operations
2. Categorizing and ranking these assets based on their importance
3. Assessing potential threats to these assets
4. Evaluating the impact and likelihood of these threats
5. Creating a risk register to document identified risks
6. Analyzing the results and prioritizing risks
7. Recommending mitigation measures to address these risks

This methodology ensures a comprehensive and systematic approach to risk assessment, providing BSI with valuable insights for informed decision-making.

4 Information Asset Inventory and Categorization

The first step in our risk assessment process was to identify and categorize BSI's critical information assets. This inventory forms the foundation for our subsequent risk analysis.

4.1 Information Asset Inventory

The following table provides a detailed list of BSI's key information assets, along with their respective data owners and the types of sensitive data they contain:

Asset	Data Owner	Type of Sensitive Data
AD Service	Manager IT	PII
AD SQL DB	Manager IT	PII
DNS Service	Manager IT	Customer Confidential
DNS SQL DB	Manager IT	Customer Confidential
Exchange Email Server	Manager IT	PII
Email DB	Manager IT	PII
Traverse Accounting Software	CFO	Customer Confidential, PCI, PII
Accounting SQL DB	CFO	Customer Confidential, PCI, PII
Traverse Distribution Software	Manager, Distribution	Customer Confidential
Distribution SQL DB	Manager, Distribution	Customer Confidential
Traverse ERP Software	Manager, Sales	Customer Confidential, PII

Asset	Data Owner	Type of Sensitive Data
ERP SQL DB	Manager, Sales	Customer Confidential, PII
Optimum HRIS	Manager, HR	PII
HRIS DB	Manager, HR	PII
Office 365 Server	Manager IT	Customer Confidential, PII
Office DB	Manager IT	Customer Confidential, PII
IIS for Intranet	Manager IT	Customer Confidential
Intranet DB	Manager IT	Customer Confidential
IIS/Forefront TMG	Manager IT	Customer Confidential
IIS-FTMGDB	Manager IT	Customer Confidential
SupportIT	Manager IT	Customer Confidential
SIT DB	Manager IT	Customer Confidential
NAS 1	Manager IT	Backup, Encrypted Data (Conf, PCI, PII)
NAS 2	Manager IT	Backup, Encrypted Data (Conf, PCI, PII)
Cloud Backup Service	Manager IT	Backup, Encrypted Data (Conf, PCI, PII)

This comprehensive inventory highlights the diverse range of information assets within BSI's ecosystem, each playing a crucial role in the company's operations and data management.

4.2 Asset Categorization and Scoring

To prioritize risk management efforts, we categorized and scored the identified assets based on several critical factors. The following table presents the weighted ranking of BSI's information assets:

Asset	Impact on Business Operations (0.3)	Data Sensitivity (0.25)	Regulatory Compliance (0.2)	Availability and Uptime (0.15)	Impact on Profitability (0.1)	Total Score
Traverse Accounting Software	5	5	5	5	5	5
NAS 1	5	5	5	5	5	5
Cloud Backup Service	5	5	5	5	5	5
Accounting SQL DB	5	5	5	5	5	5
NAS 2	5	5	5	5	5	5
Optimum HRIS	5	5	5	4	4	4.75
HRIS DB	5	5	5	4	4	4.75
AD Service	5	5	5	5	3	4.8

Asset	Impact on Business Operations (0.3)	Data Sensitivity (0.25)	Regulatory Compliance (0.2)	Availability and Uptime (0.15)	Impact on Profitability (0.1)	Total Score
Traverse ERP Software	5	4	4	4	5	4.4
ERP SQL DB	5	4	4	4	5	4.4

4.2.1 Scoring Criteria Descriptions

1. **Impact on Business Operations** (Weight: 0.30): Defined as the importance of the asset in maintaining daily business functions. This criterion was selected because business operations are the core of the business. Any disruption to critical operations can significantly impact the business.

2. **Data Sensitivity** (Weight: 0.25): Defined as the level of sensitivity of the data stored or processed by the asset. This criterion was selected because the protection of sensitive data is crucial for maintaining confidentiality, integrity, and availability.

3. **Regulatory Compliance** (Weight: 0.20): Defined as the need to meet legal and regulatory requirements. This criterion was selected because non-compliance can result in legal penalties and loss of trust.

4. **Availability and Uptime** (Weight: 0.15): Defined as the importance of the asset's availability and uptime to the organization. This criterion was selected because downtime can disrupt business operations and result in financial loss.

5. **Impact on Profitability** (Weight: 0.10): Defined as the direct or indirect effect of the asset on the organization's profitability. This criterion was selected because assets that drive revenue or cost savings are crucial.

This categorization and scoring process allows BSI to focus its risk management efforts on the most critical assets, ensuring efficient resource allocation and targeted risk mitigation strategies.

5 Threat Assessment

After identifying and categorizing BSI's critical information assets, the next step in our risk assessment process was to evaluate potential threats to these assets. This section presents our findings on the most significant threats facing BSI's information assets.

5.1 Threat Identification and Ranking

We identified and ranked potential threats based on several key factors. The following table presents the weighted ranking of threats to BSI's information assets:

Threat	Likelihood of Occurrence (0.25)	Impact on Operations (0.25)	Data Sensitivity Impact (0.2)	Recovery Time (0.15)	Financial Impact (0.15)	Total Score
Cyber Attacks	5	4	5	4	4	4.45
Data Breaches	4	5	5	3	5	4.45
Natural Disasters	3	5	4	3	5	4
Human Error	4	4	4	3	3	3.7
Third-Party Risks	3	4	4	3	4	3.6
Insider Threats	4	3	4	4	3	3.6
Legacy system integration	4	4	3	3	3	3.5
Centralized IT Management	3	4	3	3	4	3.4
Hardware Failures	3	4	3	2	4	3.25
Power outages	2	3	2	2	3	2.4

5.1.1 Threat Ranking Criteria Descriptions

1. **Likelihood of Occurrence** (Weight: 0.25): Defined as the probability that a given threat will materialize. This criterion helps prioritize risk management efforts based on the frequency of potential threats.

2. **Impact on Operations** (Weight: 0.25): Defined as the potential disruption to daily business functions caused by a threat. This criterion reflects the critical importance of maintaining smooth operations.

3. **Data Sensitivity Impact** (Weight: 0.20): Defined as the effect of a threat on the confidentiality, integrity, and availability of sensitive data. This criterion emphasizes the high priority of data security.

4. **Recovery Time** (Weight: 0.15): Defined as the time required to restore normal operations after a threat materializes. This criterion highlights the importance of swift recovery to minimize business disruption.

5. **Financial Impact** (Weight: 0.15): Defined as the potential monetary loss resulting from a threat. This criterion quantifies the economic consequences of threats, helping to prioritize risk mitigation efforts based on financial considerations.

This threat assessment provides BSI with a clear picture of the most significant risks facing its information assets, allowing for targeted and effective risk management strategies.

6 Risk Assessment

Building upon our asset inventory and threat assessment, we conducted a comprehensive risk assessment to evaluate the potential impact of identified threats on BSI's critical information assets. This section presents our findings and analysis.

6.1 Risk Assessment Methodology

Our risk assessment methodology combines the criticality of assets with the potential impact of threats. We use a simple formula to calculate risk:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

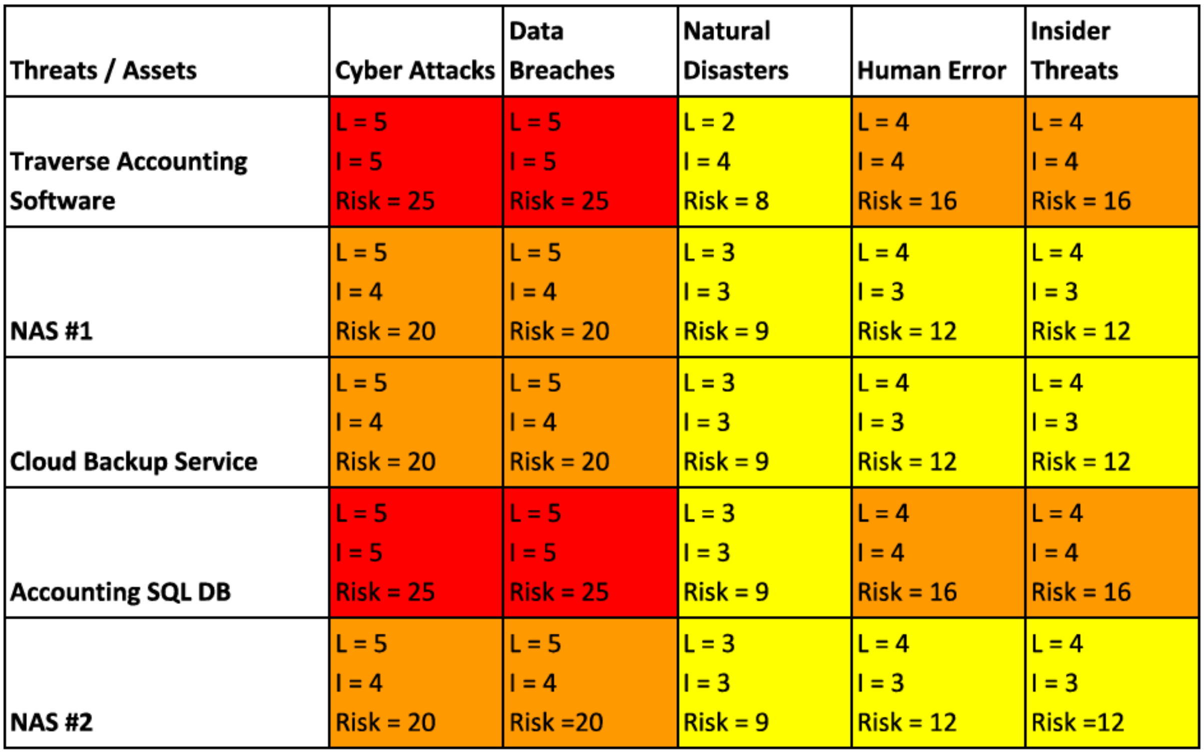
Where:

- Likelihood is scored on a scale of 1 (Very Low) to 5 (Very High)
- Impact is scored on a scale of 1 (Minimal) to 5 (Severe)

This approach allows us to quantify risks and prioritize them for mitigation.

6.2 Risk Assessment Results

The following table presents the results of our risk assessment for BSI's most critical information assets:



Threats / Assets	**Cyber Attacks**	**Data Breaches**	**Natural Disasters**	**Human Error**	**Insider Threats**
Traverse Accounting Software	L = 5 I = 5 Risk = 25	L = 5 I = 5 Risk = 25	L = 2 I = 4 Risk = 8	L = 4 I = 4 Risk = 16	L = 4 I = 4 Risk = 16
NAS #1	L = 5 I = 4 Risk = 20	L = 5 I = 4 Risk = 20	L = 3 I = 3 Risk = 9	L = 4 I = 3 Risk = 12	L = 4 I = 3 Risk = 12
Cloud Backup Service	L = 5 I = 4 Risk = 20	L = 5 I = 4 Risk = 20	L = 3 I = 3 Risk = 9	L = 4 I = 3 Risk = 12	L = 4 I = 3 Risk = 12
Accounting SQL DB	L = 5 I = 5 Risk = 25	L = 5 I = 5 Risk = 25	L = 3 I = 3 Risk = 9	L = 4 I = 4 Risk = 16	L = 4 I = 4 Risk = 16
NAS #2	L = 5 I = 4 Risk = 20	L = 5 I = 4 Risk =20	L = 3 I = 3 Risk = 9	L = 4 I = 3 Risk = 12	L = 4 I = 3 Risk =12

6.3 Risk Analysis

Based on our risk assessment, we can draw the following key insights:

1. **High-Risk Areas**: The highest risks for BSI are cyber attacks and data breaches targeting the Traverse Accounting Software and Accounting SQL DB, with risk scores of 25 for both threats on both assets. These areas require immediate attention and robust mitigation strategies.
2. **Critical Assets at Risk**: NAS 1, NAS 2, and the Cloud Backup Service also face significant risks from cyber attacks and data breaches, with risk scores of 20. As these assets contain backup and encrypted data, their protection is crucial for business continuity and data recovery.
3. **Human Factors**: Human error and insider threats present moderate risks across all assessed assets, with risk scores ranging from 12 to 16. This highlights the importance of employee training and internal security measures.
4. **Natural Disasters**: While less likely than cyber threats, natural disasters still pose a significant risk, particularly to the Traverse Accounting Software, with a risk score of 8. This underscores the need for robust disaster recovery and business continuity planning.

7 Risk Mitigation Recommendations

Based on our risk assessment findings, we recommend the following mitigation strategies for BSI:

1. **Enhance Cybersecurity Measures**:
   - Implement advanced intrusion detection and prevention systems
   - Conduct regular penetration testing and vulnerability assessments
   - Encrypt sensitive data at rest and in transit
   - Implement multi-factor authentication for all critical systems
2. **Improve Data Protection**:
   - Implement a comprehensive data classification policy
   - Enhance access controls and implement the principle of least privilege
   - Regularly backup critical data and test restoration procedures
   - Implement data loss prevention (DLP) solutions
3. **Strengthen Backup and Disaster Recovery**:
   - Implement a 3-2-1 backup strategy
   - Develop and regularly test a comprehensive disaster recovery plan
   - Consider implementing redundant systems for critical assets
   - Conduct regular disaster recovery drills

4. **Address Human Factors**:
   - Implement a comprehensive security awareness training program
   - Develop and enforce clear security policies and procedures
   - Implement robust monitoring and auditing of user activities
   - Establish an insider threat program
5. **Enhance Third-Party Risk Management**:
   - Develop a vendor risk assessment process
   - Regularly audit third-party access and permissions
   - Include security requirements in vendor contracts
   - Monitor third-party compliance with security policies

8 Conclusion

This risk assessment has identified critical information assets, evaluated potential threats, and assessed the risks associated with BSI's business operations. By implementing the recommended mitigation strategies, BSI can significantly enhance its risk management posture and ensure the security and resilience of its operations.

It is important to note that risk management is an ongoing process. Regular reassessments and updates to this risk management plan are crucial to address new threats and changes in the business environment.

9 Appendices

9.1 Appendix A: Glossary of Terms

- **PII**: Personally Identifiable Information
- **PCI**: Payment Card Industry
- **NAS**: Network Attached Storage
- **ERP**: Enterprise Resource Planning
- **HRIS**: Human Resource Information System
- **IIS**: Internet Information Services
- **TMG**: Threat Management Gateway

9.2 Appendix B: Risk Assessment Matrix

[Include a visual representation of the risk assessment matrix]

10 Document Revision History

Version	Date	Description of Changes	Author
1.0	08/07/2024	Initial document creation	A. Anthony
1.1	08/15/2024	Incorporated additional risk analysis and mitigation recommendations	A. Anthony

11 Approval

This document has been reviewed and approved by:

Name: **Signature:**

Title: **Date:**

Name: **Signature:**

Title: **Date:**

12 Disclaimer

This risk assessment report is based on information available at the time of the assessment and may not reflect all potential vulnerabilities or risks. It is recommended to regularly review and update security measures as new threats emerge and technology evolves.

13 Contact Information

For any questions or clarifications regarding this report, please contact:

Name:	Anderson Anthony
Title:	Chief Compliance Officer
Email:	Anderson@cloudstrategik.com
Phone:	+1 (555) 123-4567