Michael Twining

CYB 348, Information Assurance Risk and Compliance

Part 5 Project: Risk Management Plan for [REDACTED] [REDACTED]s

Contents

Purpose

The purpose of the Risk Management Plan (RMP) for [REDACTED] [REDACTED]s, who is a publicly traded organization, who globally manufactures and distributes consumer goods, office supplies and gaming accessories, is to align the organization, business processes, and information systems to the risk to the company. This includes stakeholders, leadership teams, and specialized human assets to assess and evaluate the impact of certain risks to the risk appetite of the organization to recommend and implement proper mitigation activities [REDACTED]rdingly. [REDACTED] [REDACTED]s holds responsibilities to stakeholders and their customers to follow regulatory compliance standards, while maintaining a low to moderate risk appetite, depending on severity of the risk. Low and moderate risks, so long as mitigation strategies are cost-effective with minimal impact to business operations are acceptable. High risks that impact the business functions of the organization, or severity of legal consequences, will require evaluation for transference, avoidance, or mitigation to limit the liability of the organization whenever applicable. To help guide the plan, [REDACTED] [REDACTED]s will utilize the guidance of the National Institute for Standards and Technology (NIST) Special Publication 800-37 revision 2 (NIST SP 800-37 rev. 2) for the overall framework of the management plan, National Institute for Standards and Technology (NIST) Special Publication 800-30 revision 1 (NIST SP 800-30 rev. 1) for assessing risk and vulnerabilities, and National Institute for Standards and Technology (NIST) Special Publication 800-53 revision 5 (NIST SP 800-53 rev. 5) for controls and mitigation recommendations.

Scope

The RMP scope addresses the stages of the risk management framework (RMF) in [REDACTED]rdance with NIST SP 800-37 rev. 2 guidelines. The plan does not go into details on specific risks that do not have an impact on the business objectives of

organization and prioritizes risks that are higher and more likely to occur. Key terms are identified with their definitions in Appendix A.

The **prepare** section will discuss roles and responsibilities for the RMP, reiterate the risk tolerance of [REDACTED] [REDACTED]s, methods for assessing risk, identifying key assets, and methods for monitoring controls and compliance. Most importantly, this section also outlines key regulatory compliance standards, control recommendations around them, how the organization will routinely perform, record, and respond to risk assessments, and the enterprise infrastructure.

The **categorize** section will identify document adverse impacts to [REDACTED] [REDACTED]s operations and assets due to loss of confidentiality, integrity, and availability of the organization's systems and information processed, stored, and transmitted on those systems. The section will categorize characteristics of the system, establish a classification for information managed by those systems, senior management approval of the categorization.

The **select** section deals with establishing controls for the risk. This includes any baseline requirements and allocation of resources, documentation of how those controls is implemented, continuously monitored, and senior management approval. The implement section will cover how the controls are employed in the system.

The **assess** section covers how the threats and that controls are performing and if they are implemented properly.

The **authorize** section covers the acceptance that the system and controls based on the level of risk accepted meets the organization's requirements and commitments to their stakeholders and customers.

The **monitor** section covers how the organization will prioritize controls, responses to mission/business function outages, and changes to the plan, ensure changes are

documented, and that changes are re-evaluated for impact analysis and measurement of the security and privacy posture of the system.

Section 1: Prepare

Compliance and Frameworks for Data Privacy and Protection

[REDACTED] [REDACTED]s' global footprint increases the number of laws and regulations governing the use of private data and the protection of that data from the information systems used by the organization. Some laws include General Data Protection Regulation (GDPR), Brazil General Data Protection Law (LGPD), China Personal Protection Law, Sarbanes-Oxley (SOX), and Payment Card Industry Data Security Standard (PCI DSS). The company's risk tolerance requires that a third-party company, as well as its own internal monitoring to provide audits to ensure and certify compliance with laws and regulations.

The General Data Protection Regulation (GDPR) was created to provide the consumer with more control over their personal data in the EU. [REDACTED] [REDACTED]s sells products globally, including the EU through our retail partners and e-commerce platforms, which means it must abide by the regulations on how consumer information is used, notification rights from a breach, and ability to have that data removed from any company database (Gibson & Igonor, 2022). Similarly, [REDACTED] [REDACTED]s must abide by the regulations outlined in Section 11 of the Brazil General Data Protection Law (LGPD) (Hruby, 2020). This is due to the organization's operations within the Latin American regions, which include Brazil. Because the organization also operates heavily within China due to its manufacturing and distribution supply chain activities, it also sells to Chinese consumers. This requires that [REDACTED] [REDACTED]s also follows all articles under the China Personal Protection Law, which also establishes requirements regarding the handling of personal information (Personal information protection law of the People's Republic of China,2021).

The organization must also adhere to the Payment Card Industry Data Security Standard (PCI DSS) as well given its business operations with payments. This means that the organization must follow the principles outlined by the standards, which as of November 5th, 2024, are to builder and maintain a secure network, protect card holder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy (Gibson & Igonor, 2022).

[REDACTED] [REDACTED]s has a fiduciary responsibility to stakeholders and investors as it is a publicly traded company. It is the responsibility of the leadership to use due diligence to abide by Section 404, which requires the company to use internal controls to protect data (Gibson & Igonor, 2022).

The organization also utilizes information security frameworks to align with regulatory compliance and best practices to maintain a matured security posture. While PCI DSS was previously mentioned, this framework is also crucial to the establishment of the handling or consumer data. To maintain a vulnerability management program as required by other regulations, [REDACTED] [REDACTED]s utilizes the recommendations from NIST SP 800-30. The organization also utilizes best practices for controls as outlined within guidance from the Control Objectives for Information and Related Technology (COBIT) framework. This helps to ensure that proper controls are implemented to address any risks and other vulnerabilities to the organization (Gibson & Igonor, 2022). Lastly, [REDACTED] [REDACTED]s maintains ISO 27002 compliance to establish and maintain security techniques, establishing security policies, asset management, human resources security, physical and environmental security, access controls, incident management, business continuity, and compliance (Gibson & Igonor, 2022). As all these frameworks overlap in recommendations, these ensure a more-complete risk management plan and establishment of controls or processes in place to constantly monitor and maintain a

mature security posture for [REDACTED] [REDACTED]s, customers, stakeholders, investors, and employees.

Key Roles and Responsibilities

The **Chief Executive Officer (CEO)** is responsible for the due diligence of the organization to document and maintain and up to date risk management plan and that the plan sufficiently protects the organization's liability to known risks, and documents how the organization should manage risks as they occur over time.

The **Chief Compliance Officer (CCO)** ensures that the risk management plan reflects the organization's risk appetite and compliance controls. They are also responsible for approving and maintaining up to date risks associated with changes to these laws and regulations, as well as ensuring the business functions of the compliance office are being followed. The Risk Manager works Under the Chief Compliance Officer. They are responsible for the evaluation and monitoring of the risk management plan, including the use of any systems to manage risks throughout the organization and approval of risks outside of the organization's legal responsibilities.

The **Chief General Counsel** is responsible for ensuring that risk management plan reduces the legal liability of the organization and can be properly referenced during inquiry in a court of law. They are also responsible for guidance on incident response as it pertains to notifications under all regulatory compliance requirements. They must work with the Chief Information Systems Officer during such time to ensure that any data breach or incident is reported to the proper channels (i.e. authorities, customers, Security Exchange Committee, etc.).

The **Director of Human Resources** is responsible for the collection and use of personally identifiable information (PII) of employees. This includes the maintenance of current and former employees using the information system. They are also responsible for ensuring that information is properly stored, following retention regulations, maintained in

[REDACTED]rdance with organizational policies and procedures as they pertain to PII, and ensuring information is properly categorized within the department. The Director of Human Resources may share the responsibility a senior manager within the department, but is solely responsible for creation, recommendation, and implementation of organizational policies, including the approval of any revisions.

The **Chief Finance Office (CFO)** is responsible for the execution of business functions of the department. This includes ensuring proper monitoring controls and reporting as they pertain to SOX and PCI DSS regulatory requirements. They may have a senior manager within the department assist in performing any internal auditing procedures to maintain a proactive approach to these regulations and frameworks. They will work with the Chief Information Systems Officer to ensure that any gap analysis identified is properly remediated.

The **Chief Information Systems Officer (CISO)** is responsible for the use of allocated resources to develop, implement, and maintain [REDACTED] [REDACTED]s' information security program. This also includes ensuring documentation of systems configurations, assets, applications, and controls are approved and kept up to date. Furthermore, it is key to the role in the development and implementation of data security and privacy policies for the organization. Lastly, they are responsible for overseeing the recovery and reconstitution progress. They help to ensure resources are available to team members to execute the plan, as well as provide any communication support, and testing of the plan.

The **System Owners** are responsible for validating the restoration of services.

The **IT Support** teams are responsible for performing hardware-related triage efforts before escalating issues to the cybersecurity team. They are also responsible for maintaining all warranty information on system components and ordering replacement

hardware where applicable. They also validate changes and remediations to the physical firewalls and switches.

The **Cybersecurity Analyst** is responsible for testing the restored services to ensure that there are not unintended consequences from hardware or software changes. This includes updates that impact compatibility with other network devices, authorization and authentications services, malware hunting on infected devices and backups, and validating restoration of SIEM Systems components.

Section 2: Categorize

System Description

[REDACTED] [REDACTED]s utilizes several web servers to for North America, Latin America, APAC, and EMEA regions, both for internal and external use. There are also several data servers that are housed in one primary home office within each region. Each internet-facing server contains a firewall. The organizations utilize a Security Incident and Event Management program that aggregates all log data for the whole organizations. Agents are installed on each endpoint device and each device contains an endpoint detection response system. The organization implements micro segmentation techniques to provide quarantine capabilities without disrupting all operations when an incident occurs. With the use of next generation firewalls and endpoint detection, the likelihood of an incident occurrence is somewhat limited.

Figure 1

[REDACTED] [REDACTED]s Network Infrastructure (made with Visio)

Within the infrastructure, assets are maintained and inventoried. This includes the hardware associated with the infrastructure in Figure 1 and classification of data stored within the systems. The organization will classify data as Personal Health Information (PHI), Personally Identifiable Information (PII), Personal Card Information (PCI), Proprietary Information, Sensitive Information, Confidential Information, and Not Confidential Information. This will help in determining the scope of data assets within the organization, as well as provide quick insight in event of a security incident of information that has been impacted.

Section 3: Select

The selection of controls in place are dependent on regulatory compliance and the need to decrease inherent risks to the organization. When selecting controls, they must, in aggregate, provide a residual risk factor of low to moderate. This involves use of the risk management plan and the risk mitigation plan to properly measure the impact of vulnerabilities and controls. Through regular review from internal and external audits, such as vulnerability assessments, penetration testing, and compliance audits, the organization will revise any control deemed ineffective against [REDACTED] [REDACTED]s' risk tolerance with director approval. The selection of controls is derived from the risk mitigation plan, in response to the risk assessment plan that identifies key vulnerabilities above the organization's risk tolerance level.

Section 4: Implement

Implementation of controls after approval from a director follows the process of procurement. Once any licenses, software, hardware, and other prerequisites have been procured, technical teams will be responsible for the installation and implementation of the control. Through regular use of the controls, they will actively monitor them to ensure their functions are performing to expectations required to mitigate risk.

Section 5: Assess

The assessment of the risk management plan incorporates the risk assessment and risk mitigation plans. These plans properly assess and measure the risks, vulnerabilities, and controls based on NIST SP800-53 Rev. 5 and NIST SP800-30 Rev. 1 guidelines.

Risk Assessment Plan Purpose and Scope

The purpose of the Risk Assessment Plan for [REDACTED] [REDACTED]s is to guide the organization in aligning its business processes and information systems. This alignment aims to identify relevant threat sources, threat events, exploitable vulnerabilities, likelihood of threat source identification and successful exploit, adverse impacts, overall

risk score, and potential recommendation for remediation. Through establishing risk assessment standards using the National Institute for Standards and Technology (NIST) Special Publication 800-30 revision 1 (NIST SP 800-30 Rev.1), the business functions can properly assess threats and their potential impacts to the organization.

The risk assessment process evaluates inherent risk based on likelihood and impact. Residual risk, which [REDACTED]unts for the effects of implemented controls, will be measured in subsequent mitigation activities. The results of this risk assessment provide the foundation for the Risk Mitigation Plan, where selected controls will be implemented to address identified risks. Residual risk will be reevaluated post-mitigation to ensure alignment with [REDACTED] [REDACTED]s' risk tolerance.

The Risk Assessment Plan scope addresses the matrix involved in assessing threats that will be used within the organization based on NIST SP 800-30 Rev.1 recommendations. This is key to the categorization of threats and provides a qualitative approach to assessing the impact to the organization.

The plan includes key tasks associated with Tier 3 risk assessment, the assessment of security controls for information systems. The events that must occur is an audit to be performed, results must be recorded in the Governance, Risk, Compliance (GRC) platform, SimpleRisk, a department is assigned a course of action, the department signs off approving the risk and records remediation activities, and the risk is then considered mitigated and continually monitored. Should results lead to discovery of any noncompliance to laws and regulations that require mandatory disclosures, then the scope is expanded to include incident response section not in the Risk Assessment Plan.

Risk Assessment Plan Assets to be Assessed

Assets assessed in this plan include information systems within each business function of [REDACTED] [REDACTED]s, including Human Resources, Finance, Supply Chain, Customer Management, Materials Management, and Facilities.

Risk Assessment Timing

The risk assessment is split into four main sections, preparing for the risk assessment, conducting the risk assessment, communicating and sharing the risk assessment, and maintaining the risk assessment.

- Preparing for the risk assessment: 2-4 weeks depending on internal/external party performing the risk assessment.
- Conducting the risk assessment: Depending on the scope, the risk assessment process could take 1-2 weeks. Larger scope will require more time.
- Sharing and communicating the risk assessment: Once entered to SimpleRisk, each assigned person to the risk must sign off on the identified risk. This could take up to 2 weeks, potentially longer if there are more departments involved in the individual risk assessment.
- Maintaining the Risk Assessment: This would remain ongoing but stored within SimpleRisk. Remediation could take up to a few months for larger infrastructure changes. Otherwise, one month seems appropriate for most remediations.

Risk Assessment Process

Threat Sources

Figure 1 below shows the threat sources [REDACTED]rding to NIST SP 800-30 Rev.1. All threat sources may be within scope of this risk assessment plan.

Figure 1

TAXONOMY OF THREAT SOURCES (National Institute of Standards and Technology, 2012).

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

To measure threat sources relevancy and inclusion into the plan must be based on their adversary capabilities, intent, and targeting, as well as the effects from non-adversarial threat sources. Table 1 and Table 2 below demonstrates the evaluation of a threat source based on NIST SP 800-30 Rev.1 recommendations. Table 1 is for a non-adversarial threat source and d Table 2 is based on an adversarial threat source.

Table 1

Assessment of Fire Threat Source

Identifier	Threat Source	In Scope	Range of Effects
1001	Fire in Facilities	NO	Low/Moderate

The overall range of effects to [REDACTED] [REDACTED]'s IT infrastructure is not impacted greatly due to servers being ran offsite. However, some risk does exist as the threat event of a fire in a server room could occur, which is why it was considered a lower moderate range of effects. Given that [REDACTED] [REDACTED]'s risk tolerance is higher-medium, it is considered out of the scope for the risk assessment plan.

Table 2

Assessment of Outsider Threat

Identifier	Threat Source	In Scope	Capability	Intent	Targeting
3001	Outsider Adversary	YES	Very High	Very High	Very High

Due to the capabilities, intentions, and targeting abilities of an outside adversary affecting the organization, threat events from an outside adversary are considered in scope for the risk assessment plan. Very high ranking overall is over the risk tolerance of [REDACTED] [REDACTED]s.

Threat Event

Threat events associated with their corresponding threat source is the next stage in the risk assessment process. This stage is important as it identifies relevant threat events that may require the selection of controls based on [REDACTED] [REDACTED]'s risk tolerance. Table 3 shows a sample of threat events that can occur from the outsider adversary based on the matrix for assessing threat events in NIST SP 800-30 Rev.1 and the tactics and techniques identified using Common Attack Pattern Enumeration and Classification (CAPEC). Below is a sample of three threat events, recognizing that this is not an exhaustive list of possible threat events.

Table 3

Identification of Outsider Adversary Threat Events

Identifier	Threat Event	Threat Source	Relevance

9001	Overflow Buffers	Outsider Adversary	Expected
9002	Subverting Environment Variable Values	Outsider Adversary	Expected
9003	Redirect Access to Libraries	Outsider Adversary	Expected

[REDACTED] [REDACTED]'s has identified three expected threat events based on these known tactics, techniques, and procedures (TTPs) used against other global manufacturing and distributing supply chains in the industry. It is likely that an adversary will use the same TTPs against the organization's information systems.

Vulnerability and Predisposing Conditions

Utilizing the matrix in NIST SP 800-30 Rev.1, the next stage is to establish if the [REDACTED] [REDACTED]s has vulnerabilities associated with those potential threat events mentioned in Table 3. Vulnerabilities are identified by third-party or internal security assessment and vulnerability reports. This is seen in Table 4.

Table 4

Identification of Vulnerabilities

Identifier	Vulnerability	Vulnerability Severity
12001	Applications and Services – Overflow Buffers	Moderate
12002	Default system configurations – Subverting Environment Variable Values	Low

The two vulnerabilities have been rated based on current [REDACTED] [REDACTED]'s existing security controls. Know that if no controls were already in place, then these would be rated very high in severity.

Directly from the NISTST SP 800-30 Rev.1 recommendations, Figure 2 shows the matrix criteria for measuring the predisposing conditions of the vulnerabilities. Using the ones identified in Table 4, both vulnerabilities apply to all Tier 1, Tier 2, and Tier 3 levels as all levels utilized information systems and software, the measure would be very high for both vulnerabilities.

Figure 2

ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

(National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to **many** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to **some** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to **few** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

Overall Likelihood to Occur

The organization will continue to use the guidance outline in NIST SP 800-30 Rev.1 to measure the likelihood to occur for each threat event. Using the matrix for assessment in the standard, Table 5 shows the measure of likelihood of the threat event occurring at [REDACTED] [REDACTED]s.

Table 5

Likelihood of Occurrence

Identifier	Threat Event	Likely to Initiate	Result in Adverse Impact	Overall Likelihood
13001	Overflow Buffers	High	Very High	Very High

13002	Subverting Environment Variable Values	High	Very High	Very High
13003	Redirect Access to Libraries	High	Very High	Very High

Impact of Threat Events

[REDACTED] [REDACTED]'s will utilize the assessment scale outlined in NIST SP 800-30 Rev.1 guidelines for measuring impact of threat events. For Tier 3 risk assessments, [REDACTED] [REDACTED]s categorizes types of impact as Harm to People, Harm to Assets, Harm to Operations, and Harm to Other Organizations. Figure 3 shows the definitions behind each category.

Figure 3

Adverse Impacts (National Institute of Standards and Technology, 2012)

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Inability, or limited ability, to perform missions/business functions in the future.
	  - Inability to restore missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements (e.g., liability).
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to image or reputation (and hence future or potential trust relationships).

HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life. - Physical or psychological mistreatment. - Identity theft. - Loss of Personally Identifiable Information. - Damage to image or reputation.

HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements.
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to reputation (and hence future or potential trust relationships).

Table 6 uses the assessment scale to measure the maximum impact of the threat event Overflow Buffers from Table 5.

Table 6

Overflow Buffers Adverse Impacts

Type of Impact	Impact	Maximum Impact
Harm to Operations	• Limited ability to perform business functions	High
Harm to Assets	• Damage and potential loss of information systems and networks • Loss of intellectual property	High
Harm to People	• Loss of Personally Identifiable Information • Identity Theft	Moderate
Harm to Other Organizations	• Damage to trust relationships and reputation • Harms due to noncompliance	Very High

Risk Determination

Using NIST SP 800-30 Rev.1 guidance and assessment scale to determine the risk is important to providing an alignment strategy on whether the threat is withing the risk tolerance of the organization or requires more action. Table 7 continues the analysis of the risk determination for the Overflows Buffer.

Table 7

Overflow Buffers Risk Determination

Overall Likelihood of Impact	Adverse Impact	Risk Determination
Very High	High	High

Recall the level of impact of the threat has an overall likelihood of impact rating of very high and an average rating of high adverse impacts, which leads to a high-risk rating. [REDACTED]rding to the guidance, this means, “High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation” (*National Institute of Standards and Technology, 2012*).

Format Sample

The process for writing the Tier 3 risk assessments should follow the standard template as shown in Figure 4.

Figure 4

Risk Assessment

Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and pervasiveness	Overall Likelihood	Level of Impact	Risk
		Capacity	Intent	Targeting							
1001	Electrical Power Outage	N/A	N/A	N/A	Confirmed	High	Power outage due to non-adversarial means like natural disaster or equipment failure.	Moderate	Moderate	Very High	High
1002	Individual - Insider	Very High	Very High	Very High	Predicted	Very High	Employees on strike - Impacting certain business functions and company reputation	Moderate	High	Moderate	Moderate
1003	Organization - Supplier	N/A	N/A	N/A	Expected	Low	Supplier is unavailable due to international sanctions or excessive tariffs	Moderate	Moderate	High	Moderate
1004	Individual - Outsider	Moderate	Low	Moderate	Expected	Moderate	Loss of File Access - Due to denial-of-service event	Moderate	High	Low	Moderate
1005	Individual - Outsider	Very High	Very High	Very High	Predicted	Moderate	Loss of File Access - Due to ransomware event	Very High	High	Very High	Very High
1006	Individual - Outsider	Very High	Low	Very High	Anticipated	Moderate	Systems and files crashing due to buffer overflows - or other hacking tactics that involve exploitation of input fields.	Moderate	Moderate	Moderate	Moderate

Along with the risk assessment, an executive summary section, the purpose and scope of the risk assessment should be identified. Key explanations for each measure in the risk assessment should be in the risk assessment body section. Lastly, [REDACTED] [REDACTED]s requires that a mitigation recommendation is made, and estimated timeline be provided by the assessor. These are covered using the SimpleRisk software, however, should a manual assessment be made, should also include these guidelines for writing the risk assessment plan.

Risk Mitigation Plan Purpose and Scope

The purpose of the Risk Mitigation Plan for [REDACTED] [REDACTED]s is to identify key controls to address vulnerability findings in the Risk Assessment Plan of the organization's assets. The key objective of mitigation efforts it to reduce the inherent risk from known vulnerabilities that have been identified in the Risk Assessment Plan. As those change, so should the Risk Mitigation Plan.

The Risk Mitigation Plan scope addresses the selection of controls as identified in NIST SP 800-53 Rev. 5 recommendations. This is key to the mitigation of threats and provides the organization a means to implement controls to reduce, mitigate, transfer, or avoid risk based on the risk tolerance of the company.

The plan includes a variety of procedural and technical controls. Procedural controls are policy that is driven to minimize risk through defining excepted behaviour of its employees and vendors. Technical controls can include systems configurations, patching, utilization of third-party software, and others to mitigate technical vulnerabilities in systems.

Risk Mitigation Process

Vulnerability Sources

Vulnerabilities are identified in the Risk Assessment Plan of the Risk Management Plan for [REDACTED] [REDACTED]s. As new vulnerabilities are identified and approvals to update the Assessment Plan are in place, the Risk Mitigation Plan must be updated as well to address the new vulnerability. New vulnerabilities may be identified from zero-day exploits, use of new hardware and software, third-party vendors, political dynamics, and geographical changes.

Mitigation Determination

Controls and other mitigation efforts are selected based must first be evaluated on their abilities to lower the inherent risk to the risk tolerance of at least medium residual risk for [REDACTED] [REDACTED]s. Some mitigation efforts may be required to maintain

compliance with regulations and local laws regardless of cost. Selected controls based on the above should then undergo a cost-benefit analysis to determine the feasibility of the control. Other controls should be considered should the initial recommendation exceed the cost benefits to the organization.

Risk Mitigation Matrix

Figure 1 shows the risk mitigation plan for the [REDACTED] [REDACTED]s. Vulnerabilities that were identified as Medium to High from the Risk Assessment Plan were added, and controls based on NIST SP 800-53 Rev. 5 were selected and fitted for use within the organization. The vulnerability after the mitigation activity is in place is reevaluated based on the guidelines for measuring risk from NIST SP 800-30 and then the residual risk is recorded. Residual risk levels are evaluated to confirm alignment with [REDACTED] [REDACTED]s' acceptable risk tolerance, ensuring that all risks are reduced to manageable levels.

Figure 1

Risk Mitigation Plan

Vulnerability	Inherent Risk	Control	Responsibility Director Team Member Both	Likelihood of Occurrence	Level of Impact	Residual Risk
Loss of File Access - Due to ransomware event	Very High	NIST CP-9: System Backups - Conduct full backups of system-level information contained in warehouse database semi-annually. Incrimental backups to be performed bi-weekly for a period up to 6 months.	Team Member	Moderate	Moderate	Moderate
Power outage due to non-adversarial means like natural disaster or equipment failure.	High	NIST PE-1 (1):Emergency Power | Alternate Power Supply — Minimal Operational Capability - Provide an uniterruptable power supply system that automatically activates to maintain minimally required operational capactiy.	Both	Moderate	Very Low	Low
Employees on strike - Impacting certain business functions and company reputation	Moderate	Develop policies around regular performance reviews, poll surveys, and implement the use of social media and other OSINT alerting tools.	Director	Low	Very Low	Very Low
Supplier is unavailable due to international sanctions or excessive tariffs	Moderate	Multiple suppliers must be sourced for all raw material goods so that when one supplier is not available, the other supplier may be activated.	Director	Completely Mitigated	Completely Mitigated	Completely Mitigated
Loss of File Access - Due to denial-of-service event	Moderate	NIST SC-5: Denial-of-service Protection - Organization will use third-party provider to detect and monitor, utilize a load balancer and for cloud environments implement quotas, and quarantine any environments where an indicator of compromise from a denial-of-service signature is detected.	Team Member	Very Low	Very Low	Very Low
Systems and files crashing due to buffer overflows - or other hacking tactics that involve exploitation of input fields.	Moderate	NIST SI-10 (5 and 6): Information Input Validation - Organization will adopt safe development practices of all software and databases by prohibiting the use special strings in data input fields and utilize software to test for software vulnerabilities. This includes fuzzy testing of software before being impmlemented in product and manual testing to ensure code or command injection techniques are not able to be used.	Team Member	Completely Mitigated	Completely Mitigated	Completely Mitigated

All mitigation activities must be recorded in the SimpleRisk software, where the director must review and approve the mitigation, and assign the task to the appropriate department and team member for implementation. This will allow [REDACTED] [REDACTED]s to continually monitor any controls or mitigation activities for their continued effectiveness

against the vulnerability. Should the organization discontinue the use of SimpleRisk, this matrix will be continuously updated to reflect newly identified vulnerabilities and to track the effectiveness of implemented controls.

Risk Mitigation Strategy

It is ideal that the controls align with the risk mitigation strategy of [REDACTED] [REDACTED]s. Any updates to the risk mitigation strategy must be approved by a director before controls under that strategy can be implemented. This helps to ensure that controls are aligned with any risk assessment and risk mitigation recommendation that has been measured against the risk tolerance the organization.

1. Recovery from Regular Backups – Information technology team must automate the creation of full backups of system-level information contained in warehouse database semi-annually. Incrimental backups to be performed bi-weekly for a period up to 6 months. This also includes the setup and testing of a hot site in event of a man-made or natural disaster or incident occurs. Operations can be restored and continued at the hot site almost instantaneously at time of impact.
2. Monitor Adversarial Threats to Data – Logging and auditing for all Personal Health Information (PHI), Personally Identifiable Information (PII), Personal Card Information (PCI), Sensitive, Proprietary Information, Sensitive Information, Confidential Information is implemented to ensure confidentiality and integrity of mission-critical information. While this is intended to monitor adversarial insider threats, this may also help prevent unintended changes due to non-adversarial changes, as well as provide monitoring and auditing for critical data from adversarial outsiders.
3. Patch Management – Commonly Vulnerabilities and Exposures (CVEs) are known reported vulnerabilities where an exploit has been identified under the right systems environment. Typically, a software provide will provide an update, or patch, to

remediate the vulnerability. [REDACTED] [REDACTED]s will implement a patch management program to automatically scan for existing programs on all systems and update them if an update is available monthly. Cybersecurity team will see the list of updates before the final push to production environments in event an update has unintended consequences like compatibility issues. If there is a major CVE reported, cybersecurity team may push that update immediately.

4. Protection from Business Email Compromise (BEC) – [REDACTED] [REDACTED]s will use an email gateway provider, Proofpoint, to monitor and detect email threats from known and unknown sources. This is important to protecting company assets, from phishing attacks within the on-site and remote workforce.
5. Network Protection – Multiple layers of security are necessary to maintain a more matured security infrastructure. [REDACTED] [REDACTED]s will utilize on-premises and virtual firewalls and switches to assist in assigning network rules and data flows, while promoting a micro-segmented infrastructure.
6. End-Point Protection – The organization will utilize end-point detection and response systems to respond to heuristic and signature threats from malicious system activity. These systems are intended to trigger the quarantine response to prevent any adversary from lateral movement within the network.
7. Security Information and Event Management (SIEM) – [REDACTED] [REDACTED]s utilizes a SIEM to identify, detect, and respond to threats identified within the alerting system. The team members are responsible for configuring alerts under the director's approval for detecting new threats. The SIEM program contains agents that are installed on end-point devices to aggregate and monitor software, user, and system events.
8. Security Audits – The team members will occasionally perform audits pertaining to vulnerability assessments of systems and the network. This is to ensure the

organization is maintaining a constant state of awareness of existing vulnerabilities. While [REDACTED] [REDACTED]s hires a third-party vendor to perform similar audits, the cadence of the audits may vary. Another key audit from the team members is the active and inactive users and groups. It is the team's responsibility for determining what [REDACTED]unts are required to be deactivated by the IT team.

9. Data Encryption – [REDACTED] [REDACTED]s will ensure that all data at rest and data in transit is encrypted using secured protocols, digital signatures, and certificates. This is to prevent any malicious threat actor from obtaining information through clear text transmissions and by making exfiltrated information illegible and unusable. This will prevent any extortion threats from adversaries from impacting the organization's reputation and fines from a potential breach or leak of data.

Section 6: Authorize

Risk Management Plan Authorization

Under the direction of the CEO, the Risk Management Plan has been created and may be modified with approval from all signatories below. Third-party consulting agencies may also assist in the establishing addendums to the plan with approval from the CCO, CISO, and CTO.

Julie Moore (CEO) Date: 12/3/2024 Julie Moore

Jamal Smith (Chief General Counsel) Date: 12/3/2024 Jamal Smith

James Smith (CCO) Date: 12/3/2024 James Smith

John Smith (CISO) Date: 12/3/2024 Jonathon Smith

John Smith (CTO) Date: 12/3/2024 Jonathan Smith

Risk Assessment Plan Authorization

In coordination with all employees involved with the Risk Assessment Plan, and on behalf of [REDACTED] [REDACTED]s, I approve this Risk Assessment Plan document and authorize the execution of this document.

James Smith (CCO) Date: 12/3/2024 James Smith

Joe Smith (CTO) Date: 12/3/2024 Joseph Smith

John Smith (CISO) Date: 12/3/2024 Jonathan Smith

Risk Mitigation Plan Authorization

In coordination with all employees involved with the Risk Mitigation Plan, and on behalf of [REDACTED] [REDACTED]s, I approve this Risk Mitigation Plan document and authorize the execution of this document.

James Smith (CCO) Date: 12/3/2024 James Smith

Joe Smith (CTO) Date: 12/3/2024 Joseph Smith

John Smith (CISO) Date: 12/3/2024 Jonathan Smith

Business Continuity Plan Authorization

In coordination with all employees involved with the Information System Contingency Plan (ISCP), and on behalf of [REDACTED] [REDACTED]s, I approve this BCP document and authorize the execution of this document.

Joe Smith (CTO) Date: 12/3/2024 Joseph Smith

John Smith (CISO) Date: 12/3/2024 Jonathan Smith

Section 7: Monitor | Business Continuity Plan and Business Impact Analysis

1. Overview

Information systems are vital to [REDACTED] [REDACTED]s' mission/business processes; therefore, it is critical that services provided by multiple technological components of the IT infrastructure can operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover these systems quickly and effectively following a service disruption.

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the [REDACTED] [REDACTED]s. It was prepared on December 3rd, 2024.

All sections and activities are based on guidance from the National Institute of Standards and Technology (NIST), NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.

2. Purpose

This business continuity plan (BCP) includes actionable steps to recover systems from disruptions. These sections are covered after the BIA sections, which have been measured with Federal Information Processing Standards (FIPS) 199 – *Standards for Security Categorization of Federal Information and Information Systems*. Within the ISCP sections, the categories below will be included for each system component. The following recovery plan objectives have been established:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Activation and Notification phase*** to trigger a response to continency operations;

- ***Recovery phase*** to restore system component operations; and
- ***Reconstitution phase*** to ensure that each component is validated through testing and that normal operations are resumed.

- Identify the activities, resources, and procedures to carry out system components processing requirements during outages to normal operations.
- Assign responsibilities to designated [REDACTED] [REDACTED]s personnel and provide guidance for recovering each system component during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for [REDACTED] [REDACTED]s contingency planning strategies. Ensure coordination with external points of contact and vendors associated with Fortinet, Cisco, Netgear, Internet Service Providers, Splunk Support, and Local Law Enforcement and execution of this plan.

This plan assumes that all backups are usable and not compromised, as well as the enterprise policy for new hardware or software shipped through expedited shipping should a replacement be required. It is the general rule that the organization must have backup hardware available for mission/business functions that are rated high impact in the BIA for the organization to expedite the recovery process.

The purpose of the BIA is to identify and prioritize system components that support [REDACTED] [REDACTED]s' mission/business processes and use this information to characterize the impact on the processes if the system were unavailable.

This BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.**
   Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts

and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.

2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the [REDACTED] [REDACTED] Critical Business Processes Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system, including, but not limited to, the Disaster Recovery Plan (DRP) or Cyber Incident Response Plan.

3. System Description

[REDACTED] [REDACTED]s network infrastructure is illustrated by Figure 1.

Figure 1

[REDACTED] [REDACTED]s Network Infrastructure (made with Visio)

[REDACTED] Mainframe: The main server contains databases that hold information on the customer, vendor, supplier, material, financial, and certificates. The server databases are backed up daily.

SIEM System: The Security Information Event Management (SIEM) system reads, in parallel, all network traffic in the whole infrastructure, as well as cloud-hosted log aggregation is analyzed by [REDACTED] [REDACTED]s' third-party provider. This system also acts as the primary sever for cybersecurity teams to be able to access systems within the infrastructure remotely and manage enterprise-managed devices.

Read Only Backup Server: This server only allows users to remotely read information that is stored. This server requires a manual connection to allow write and copy access onto an

external device. Hot site has a mirror service on the cloud to enable hot site activation from the most recent backup. Backups are updated when each server has posted their updates to the server.

Firewalls: Each segment hosts several physical and virtual firewall appliances. These are to lock down the system to allow only legitimate traffic onto the internal network, as well as block traffic appropriately to limit impacts to the organization of a security breach.

Virtual Server/Switch: The organization utilizes a virtual switch to flow from the company internal server to the regional operations servers.

Regional Servers: Regional servers support applications, production and testing server resources, authorization, and authentication services. Regional servers also host telecommunication systems. Regional servers are backed up monthly

Within each office or plant, there is a standard IT infrastructure each will follow. Note that plants will differ using supervisory control and data acquisition (SCADA) systems.

DMZ Virtual Web Server: This server hosts the web page content to the corresponding [REDACTED]s within the facility. This is important as it helps to segment web resources in the event of the website becoming inoperable. Web servers are backed up daily.

Perimeter Firewall: This is a cloud-hosted virtual next generation firewall that is used to monitor and block any malicious web traffic.

Router: Each facility has a router that allows incoming and outgoing internet traffic from internal and external networks.

Enterprise Managed Firewalls: The company utilizes a network of enterprise firewalls where access controls are set from the SIEM System.

Individual Department Server: Each department has their own servers with their corresponding department users, printers, and access points. This server allows business

users to access other internal network resources, as well as internet resources. Department servers are backed up weekly.

Switch: Manufacturing and distribution facilities contain a switch that is not connected to the internet. These connect the internal network resources to the SCADA systems.

SCADA for Plant Operations: This is the main control for all operational technology (OT) in the facility. This system provides machine controls inputs from internal databases like bill of material recipes, as well as automated distribution and inventory sorting machines.

4. BIA Data Collection

After interviewing and meeting with executives, directors, business functional groups, and team members for an understanding of mission/business processes, the following has been evaluated.

Customers rely on access to the web server to shop and purchase goods online. Should the router, perimeter firewall, or web server become unavailable, customers will not be able to shop online.

Within the internal network, the human resources department performs payroll functions weekly and stores personally identifiable information (PII) of all employees within their facility. If the enterprise firewall, switch, or the regional server is unavailable, then the process will be impacted.

IT business function of backing up systems, troubleshooting business user issues, and updating applications relies on all technological components operating except the SCADA Systems, internet and router.

Customer service provides ordering support services for non-online shoppers, mainly business to business sales. This requires manual computer entry for orders and

phone systems. Regional servers, department servers, firewalls, switches, and the mainframe must be available to fully operate this service.

The [REDACTED]unting department must be able to collect payments from customers, as well as submit payments to suppliers and vendors. These systems rely on the mainframe, regional server, firewalls, switch, internal department server, router, and internet to be operating to allow payments online.

Manufacturing and distribution operations require the use of automated systems for pulling materials to make finished goods, as well as to automate packing and sorting for shipping out of the facility. They also rely on automated systems for inventory monitoring, reporting available assets to the executive team and shareholders. These processes rely on the full functionality of the SCADA system, firewalls, switches, and regional servers, and the mainframe.

Marketing teams require the use of the internet to establish and maintain marketing campaigns. This is not only to support ecommerce activities, but also to share digital assets to retailers reselling goods. This requires the department server, enterprise firewall, switch, router, regional server, and mainframe to be working properly.

4.1 Determine Process and System Criticality

Step one of the BIA process - Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

Mission/Business Process	Description
E-commerce Functions	Customers rely on access to the web server to shop and purchase goods online. Should the regional server, mainframe, router, perimeter firewall, or web server become unavailable, customers will not be able to shop online. Web servers and the mainframe are backed up daily.
Payroll Functions	Payroll functions are performed weekly and stores personally identifiable information (PII) of all employees within their facility. If the enterprise firewall, switch, or the regional server is unavailable, then the process will be impacted. Department servers are backed up weekly.

Mission/Business Process	Description
IT Functions	Perform back up of systems, troubleshoot business user issues, and update applications. These rely on all technological components operating except the internet and router. All servers have a backup schedule. SCADA systems and OT will require maintenance or replacement of equipment.
Customer Service Functions	Provides ordering support services for non-online shoppers, mainly business to business sales. This requires manual computer-entry for orders and phone systems. Regional servers, department servers, firewalls, switches, and the mainframe must be available to fully operate this service. Regional and department servers are backed up weekly and mainframe is backed up daily. Other hardware components will require maintenance or replacement of equipment.
[REDACTED]unting Functions	Collect payments from customers, as well as submit payments to suppliers and vendors. These rely on the mainframe, regional server, firewalls, switch, internal department server,

Mission/Business Process	Description
	router, and internet to be operating to allow payments online. Regional and department servers are backed up weekly and mainframe is backed up daily. Other hardware components will require maintenance or replacement of equipment.
Marketing Functions	Must be able to use of the internet to establish and maintain marketing campaigns. This is not only to support ecommerce activities, but also to share digital assets to retailers reselling goods. This requires the department server, enterprise firewall, switch, router, regional server, and mainframe to be working properly. Regional and department servers are backed up weekly and mainframe is backed up daily. Other hardware components will require maintenance or replacement of equipment.
Warehouse Functions	Manufacturing and distribution operations require the use of automated systems for pulling materials to make finished goods, as well as to

Mission/Business Process	Description
	automate packing and sorting for shipping out of the facility. They also rely on automated systems for inventory monitoring, reporting available assets to the executive team and shareholders. These processes rely on the full functionality of the SCADA system, firewalls, switches, and regional servers, and the mainframe. Regional servers are backed up weekly and mainframe is backed up daily. SCADA systems and OT will require maintenance or replacement of equipment.

4.1.1 Identify Outage Impacts and Estimated Downtime

Outage Impacts

The following impact categories represent important areas for consideration in the event of disruption or impact.

Impact category: **Cost**

Impact values for assessing category impact:

- High = Cost impact will exceed $30,000.
- Medium = Cost impact is greater than $10,000 but less than $30,000.
- Low = Cost impact is $0 but less than $10,000.

Impact category: **Reputation**

Impact values for assessing category impact:

- High = Issue results in loss of reputation due to non-compliance or cyber incident.

- Medium = Significant, but not total, loss of reputation to customers, suppliers, or vendors.
- Low = No significant impact to reputation to customers, suppliers, or vendors.

Impact category: **Morale**

Impact values for assessing category impact:

- High = Additional workload/disruption exceeds current workforce resources.
- Medium = Additional workload/disruption requires 95% of current workforce resources.
- Low = Additional workload/disruption has no impact on current workforce resources.

The table below summarizes the impact on each mission/business process a technological resource was unavailable, based on the following criteria:

Mission/Business Process	Cost	Reputation	Morale	Impact
E-commerce Functions	Low	Medium	Low	Low
Payroll Functions	Low	Low	High	Medium
IT Functions	High	Low	Medium	Medium
Customer Service Functions	Medium	Medium	High	High
[REDACTED]unting Functions	Medium	High	Low	High
Marketing Functions	Low	High	Low	Medium
Warehouse Functions	High	High	High	High

Considerations of cost are related to equipment replacement for SCADA systems and OT, servers and firewalls. Aggregate equipment costs can increase dramatically if equipment failure occurs. This is due to the potential that replacing equipment may result in unintended consequences like compatibility issues between other hardware and applications.

Considerations of reputation are primarily based on issues from non-compliance issues, negative impacts on customers or suppliers, and overall view of the organization.

Considerations of morale are related to the strain on human resources needed to compensate for any outages or impacts to the business processes.

Estimated Downtime

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration because of a disruptive event.

- **Maximum Tolerable Downtime (MTD).** MTD is the amount of time that the organization can allow an outage of a mission/business critical service. This is intended to aid in the guidance of a recovery plan and a baseline for any contingency plan trigger where applicable.
- **Recovery Time Objective (RTO).** RTO defines the amount of time before the disruption has an impact on the mission/business critical service. This is key to implementing a remediation activity for the disruption of service.
- **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MTD, RTO, and RPO for the [REDACTED] [REDACTED]s' mission/business processes that rely on technological components of the IT infrastructure.

Mission/Business Process	MTD	RTO	RPO
E-commerce Functions	48 hours	24 hours	1 hour
Payroll Functions	96 hours	24 hours	2 hours
IT Functions	24 hours	8 hours	6 hours

Mission/Business Process	MTD	RTO	RPO
Customer Service Functions	56 hours	18 hours	2 hours
[REDACTED]unting Functions	48 hours	24 hours	3 hours
Marketing Functions	32 hours	12 hours	6 hours
Warehouse Functions	24 hours	6 hours	2 hours

E-commerce functions must be restored by 48 hours to not exceed lost sales tolerance. After 48 hours, [REDACTED] [REDACTED]s loses more than $30,000. Customers will simply log in on the same day to place an order if they are unable to arrive earlier in the day, however after a day has passed, they may choose a different provider. Recovery is expected to require the restoration of a backup and patching of the webserver. Customer Service may alternatively place orders on behalf of customers when calling the customer service center.

Payroll functions have become strained past 4 days in past, as it requires a lot of bandwidth to catch up reporting of all employees within any particular facility. Labor unions also require proper time keeping ensuring compliance with bargaining unit agreements. After 24 hours, we must report an outage to the union leaders per our agreement. Once the server and firewalls are restored, loading the latest backup and patches could take up to 2 hours.

IT functions are critical within the organization. Because of this, the maximum time allowed to be out is 24 hours. After 8 hours of no IT functions, impacts cascade into other business areas from non-resolved IT issues. Depending on the issue, it may take up to 6 hours to identify the issues, fix equipment, test network, and implement the fix into production.

Customer service functions are essential for all levels of customers. After 56 hours, the organization’s damage to relationships with customers becomes irreversible. The

organization should resolve the issues no later than 18 hours to ensure that customers' concerns and orders are resolved. Once the server is available, it may take up to 2 hours to restore the backups to the servers. Customer service may place orders on behalf of customers in offline mode, and when the system is back up, the orders will be placed to production in the appropriate facility.

[REDACTED]unting functions cannot exceed an outage of over 48 hours. This is because of payment terms to suppliers and vendors of the organization. Failure to make on-time payments may impact on the company's credit rating. After 24 hours the company begins to lose large orders due to their inability to provide net terms to customers. Because any resolution will require testing to ensure all databases and backups are working with the department server this may take up to 3 hours.

Marketing functions provide the ability to provide digital assets and manage campaigns. Any outage reduces the organization's ability to leverage resources to improve sales performance on products sold by the organization. After 32 hours, the organization misses on customer promotional activities. Any issues after 12 hours may impact the ability for customers to build their own marketing activities that promote [REDACTED] [REDACTED]s' products. Because the backup of the server contains images and videos, the recovery time is long, for a total of 6 hours.

The ability to ship goods from our facilities is one of the most important priorities. The organization does not tolerate delays longer than 24 hours, as for some customers, the organization may be liable for fines. On-time shipping also helps build reputation as a reliable supplier of consumer goods. After 6 hours of an outage, work becomes backlogged, and plant operations begin to halt. Once the issue with equipment has been resolved, it should take no longer than 2 hours to restore any backups, test solution, and implement the solution in production.

4.2 Identify Resource Requirements

The following table identifies the resources that compose the technological components of the IT infrastructure of [REDACTED] [REDACTED]s, including hardware, software, and other resources such as data files.

System Resource/Component	**Platform/OS/Version (as applicable)**	Description
[REDACTED] Mainframe		The main server contains databases that house information on the customer, vendor, supplier, material, financial, and certificates.
Physical Firewalls	Fortinet	Provides access controls for inbound and outbound rules. Also provides virtual private network (VPN) capabilities.
SIEM System	Cisco and Splunk Tools	Network and log audit monitoring. Server used to

		remotely access and investigate any cyber events and incidents within the organization.
Backup Server		Stores all backups for all servers and applications.
Virtual Switch		Provides access to internal network resources without the need for equipment.
Regional Servers		Supports applications, production and testing server resources, authorization, and authentication services. Also host telecommunication systems.
Router	Internet Service Provider (ISP) provided router.	Provides internet access, routes to

		DMZ and internal network
Switch	Netgear	Provides access to internal and external network resources
DMZ Virtual Web Server	Apache	Hosts ecommerce website
Department Servers		Provides access to internal network resources within the department
SCADA Systems	Controller for OT	Controller for OT or Industrial Control Systems (ICS)
Department Endpoint Devices	Printers/Laptops/Monitors/Docking Stations/Telephones	Physical equipment business users are using.

4.3 Identify Recovery Priorities for System Resources

The table below lists the order of recovery for technological component resources. The table also identifies the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption.

Priority	System Resource/Component	Recovery Time Objective
[REDACTED] *Mainframe*		1 hour as most business functions require it.
Physical Firewalls	Fortinet	1 hour as most business functions require it.
SIEM System	Cisco and Splunk Tools	24 hours as the organization becomes vulnerable for any service disruptions to security.
Backup Server		24 hours as the organization loses the ability to backup servers that are on a daily schedule
Virtual Switch		1 hour as most business functions require it.
Regional Servers		1 hour as most business functions require it.
Router	Internet Service Provider (ISP) provided router.	12 hours as it provides access to the webserver for customers. Employees can operate up to a workday without internet access for most departments.

Priority	System Resource/Component	Recovery Time Objective
Switch	Netgear	1 hour as most business functions require it.
DMZ Virtual Web Server	Apache	12 hours as customers may give up afterwards waiting for the server to come back online.
Department Servers		1 hour as most business functions require it.
SCADA Systems	Controller for OT	1 hour as warehouse functions require it.
Department Endpoint Devices	Printers/Laptops/Monitors/ Docking Stations/Telephones	6 hours as most business functions require use of these to complete their tasks.

5. Roles and Responsibilities

The ISC establishes several roles for the individual components' recovery and reconstitution. The people below have been trained to respond to a contingency event affecting these systems. While their responsibilities have been mentioned earlier in this plan, the system component responsibilities are provided in the chart below.

System Resource/Component	Vendor	Roles and Responsibility
[REDACTED] *Mainframe*		**System Owner** – Maintains databases, including backup of them.

		IT Support – Addresses troubleshooting issues, including remediation activities. Includes restoring backups.
Physical Firewalls	Fortinet	**IT Support** – Addresses troubleshooting issues, including remediation activities. Includes working with the Fortinet partner on any hardware-related root causes. They are considered the system owners. **Cybersecurity Analyst** – Ensures all updates and patches for the firewalls have been in place and new firewall rules have been applied within the network. Also tests restoration of authorization and authentication on restored systems.
SIEM System	Cisco and Splunk Tools	**IT Support** – Addresses troubleshooting issues, including remediation activities. Includes working with the Cisco partner on any hardware-related root causes. **Cybersecurity Analyst** – Works with Splunk and Cisco partners to address any non-hardware issues.

		Ensure all updates and patches for the system have been in place and new firewall rules have been applied to the router. In this case, the analyst also acts as the system owner, maintaining backups of configurations for software and routing of logs.
Backup Server		**System Owner** – Maintains backups, including communication to hot site and ensure hardware/software compatibility with IT infrastructure. **IT Support** – Addresses troubleshooting issues, including remediation activities. Includes restoring communication to hot site and replacement hardware. **Cybersecurity Analyst** – Tests all backups before restoration for indicators of compromise (IoCs) to ensure network is not infected or reinfected with malware.
Virtual Switch		**IT Support** – Ensures proper addressing and mapping to regional servers are configured. Includes

		documentation of configuration settings and patching.
Regional Servers		**System Owner** – Maintains backups. **IT Support** – Addresses troubleshooting issues, including remediation activities. Includes restoring backups and replacement hardware. **Cybersecurity Analyst** – Tests restoration of authorization and authentication on restored systems, including patches.
Router	Internet Service Provider (ISP) provided router.	**IT Support** – Addresses troubleshooting issues, including remediation activities. Includes working with the ISP on root cause, potentially replacing hardware. Ensure proper addressing as well. **Cybersecurity Analyst** – Ensures all updates and patches for the router have been in place and new firewall rules have been applied to the router.
Switch	Netgear	**IT Support** – Addresses troubleshooting issues, including

		remediation activities. Includes working with the Netgear representative on root cause, potentially replacing hardware. Ensures proper addressing in IP tables as well. **Cybersecurity Analyst** – Ensures all updates and patches for the switch have been in place and new firewall rules have been applied to the router. Also tests restoration of authorization and authentication on restored systems.
DMZ Virtual Web Server	Apache	**IT Support** – Addresses troubleshooting issues, including remediation activities. Includes restoring backups. **Cybersecurity Analyst** – Tests restoration of restored systems, including any patches or code changes.
Department Servers		**System Owner** – Maintains databases, including backup of them. **IT Support** – Addresses troubleshooting issues, including

		remediation activities. Includes restoring backups. **Cybersecurity Analyst** – Tests restoration of authorization and authentication on restored systems, including patches.
SCADA Systems	Controller for OT	**Plant Supervisors** – Configures all ICS and OT technology. **IT Support** – Addresses troubleshooting issues, including remediation activities.
Department Endpoint Devices	Printers Laptops Monitors Docking Stations Telephones	**Business Users** – Operates endpoint devices, including restoration of user files. **IT Support** – Addresses troubleshooting issues, including remediation activities. Includes restoring backups. **Cybersecurity Analyst** – Tests restoration of authorization and authentication on restored systems, including updates and patches.

6. Activation Criteria and Procedure

The ISCP is activated if the RTO exceeds the allotted time for the system component called out in the BIA. The ISCP is immediately activated for any mission/business processes that have a high impact on [REDACTED] [REDACTED]s.

7. Notification and Outage Assessment

The IT Support Ticketing system provides an automated workflow, including email notifications to the ISCP team members for issues outside of the RTO for the impacted system component. While this does not prioritize them, the impact value is provided for the impacted mission/business function. There are escalation procedures that will notify executive leadership if an issue arises that requires longer times or high costs to recover than outlined in the BIA.

Once a system disruption has been reported through the IT Support Ticketing system, a member of the IT Support team will work with the user to triage and identify the root cause of an issue. If the issue involves working with a vendor partner, they will coordinate with the vendor to resolve the issue. If the outage involves a cyber incident, the ticket is immediately escalated to the Cybersecurity Analyst. Any changes in hardware that requires testing from both IT Support and Cybersecurity Analysts will be open actions in the ticketing system awaiting approval that testing has been performed. The final step is to confirm or validate with the system owner that the service has been restored. Once this is confirmed, the ticket may be closed.

8. Recovery

It is required that all IT support tickets document activities towards resolutions that were used during the incident. Without this, the organization cannot track potential revisions needed to the BIA or BCP. This should include a sequence of recovery activities on the impacted system component, as well as recovery procedures taking place.

8.1 Reconstitution

This is the process once recovery activities have been completed and normal operations can resume. If there has been no ability to recover the system component, then this phase can be used to apply a system processing requirements document towards a

solution. Any major changes to IT infrastructure will require validation of function and data, as well as reauthorization.

8.2 Recovery Declaration

Once the systems have been tested and validated, IT Support will declare the recovery efforts completed and that the system or business functions have returned to normal operations. Points of contact (POCs) and users will be emailed the outage has been restored at the closing of the ticket.

9. Offsite Data Storage

All backups are stored on the Backup Server; however, they are also mirrored via a cloud-hosted service. Cloud backups are used to provide backup data to the hot site located in the EU. Backup schedules are identified within the BIA section of the BCP.

10. Deactivation

Once all activities have been completed and documentation has been updated, the IT Support team will formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

11. Changes to the BCP

All changes to the BCP must be approved by both the CTO and CISO, documenting the sections and specific changes made to the plan, date of change, and signature.

References

Gibson, D., & Igonor, A. (2022). Understanding and Maintaining Compliance. In *Managing Risk in Information Systems* (pp. 55–67). essay, Jones and Barlett Learning.

Hruby, M. (2020, October). Brazilian General Data Protection Law (LGPD, English translation). https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

National Institute of Standards and Technology (2010) Continency Planning Guide for Federal Information Systems. (Department of Commerce, Washington, D.C.), Special Publication 800-34. Rev. 1. https://doi.org/10.6028/NIST.SP.800-34r1.

National Institute of Standards and Technology (2012) Guide for Conducting Risk Assessments. (Department of Commerce, Washington, D.C.), Special Publication 800-30. https://doi.org/10.6028/NIST.SP.800-30r1.

National Institute of Standards and Technology (2020) Security and Privacy Controls for Information Systems. (Department of Commerce, Washington, D.C.), Special Publication 800-53 Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5.

Personal information protection law of the People's Republic of China. (2021, December 29). http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

APPENDIX A. Key Terms and Definitions

Business Email Compromise (BEC) – A tactic used by adversaries that exploit the user into believe an email has come from a legitimate user, convincing them to download a file or click on a link for malicious purposes.

Confidential Information – Category of data that contains information that is not publicly available and not under other classification of data that would otherwise be confidential or sensitive.

Common Attack Pattern Enumeration and Classification (CAPEC) - Established by the Department of Homeland Security, provides a catalog of common attack patterns that to help people understand how adversaries exploit weaknesses.

Commonly Vulnerabilities and Exposures (CVEs) – Similar to CAPEC, established to identify known vulnerabilities with steps to remediate them.

Federal Information Processing Standards (FIPS) 199 – These standards from the National Institute for Standards and Technology establishes guidelines for the categorizing of federal information and information systems, which can also be used for private industries.

Inherent Risk – Risk measured from a vulnerability based on the likelihood of occurrence and level of impact from the Risk Assessment Plan.

Maximum Tolerable Downtime (MTD) – MTD is the amount of time that the organization can allow an outage of a mission/business critical service.

NIST SP800-30 - Framework from the National Institute of Standards and Technology that provides guidance on conducting risk assessments.

NIST SP 800-53 Rev. 5 – Framework from the National Institute of Standards and Technology that provides a series of controls within over 20 category families.

Not Confidential Information – Category of data that contains information that would not damage the company or individuals should information because public knowledge.

Payment Card Information (PCI) – Category of data that contains information about individual's payment card information.

Personally Identifiable Information (PII) - Category of data that contains information about individual's identify information.

Personal Health Information (PHI) - Category of data that contains information about individual's health information.

Procedural Controls - Policies that is intended to minimize risk by defining excepted behaviour of the organization's employees and vendors.

Proprietary Information - Category of data that contains information that would damage the company should information because public knowledge. This information is specific to the company and would provide competitors an advantage if it was lost, leaked, or altered.

Recovery Point Objective (RPO) - RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

Recovery Time Objective (RTO) – RTO defines the amount of time before the disruption has an impact on the mission/business critical service.

Residual Risk – Risk measured from a vulnerability after the mitigation effort is in place based on the likelihood of occurrence and level of impact from the Risk Mitigation Plan.

Risk Tolerance – The level of risk that helps the organization determine what risks require further assessment for vulnerabilities and mitigation versus risks that are simply accepted.

Security Information and Event Management (SIEM) – A sysytem that aggregates log and audit information from various sources and provides dashboarding and alert capabilities to identify indicators of compromise on the network or on an endpoint.

Sensitive Information – Category of data that contains information that is sensitive in nature, like confidential information. While confidential information may be among two parties, internal and external, sensitive information is private among internal parties.

Tactics, Techniques, and Procedures (TTPs) – Information from Lockheed Martin on threat actor's adversarial behavior to exploit vulnerabilities.

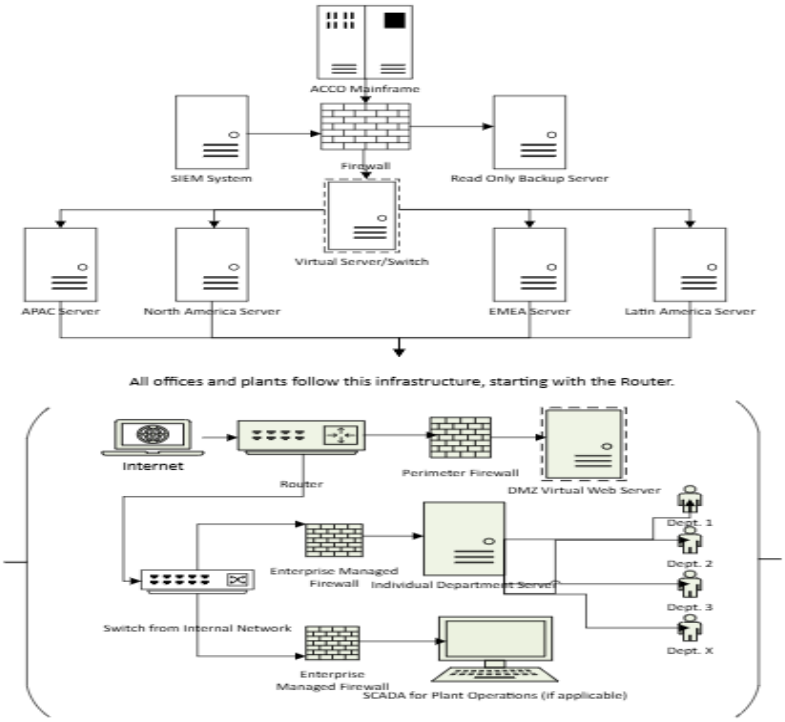
Technical Controls - Include systems configurations, patching, utilization of third-party software, and others to mitigate technical vulnerabilities in systems.

Threat – Anything that may exploit a vulnerability, like natural disasters or an adversary for example.

Vulnerability – A weakness in a system or network that can potentially be exploited.

Zero-day Exploits – Exploitation of commonly unknown vulnerabilities, where not patch currently exists.

APPENDIX B. [REDACTED] [REDACTED]s Network Infrastructure



APPENDIX C. PERSONNEL CONTACT LIST

[REDACTED] [REDACTED]s ISCP Key Personnel		
Key Personnel	**Contact Information**	
ISCP Director	Work	*1-800-123-4567 ext. 1234*
Joe Smith	Home	*555-123-4567*

Chief Technology Officer	Cellular	*515-369-1476*
	Email	*cto@[REDACTED][REDACTED]s.com*
ISCP Coordinator	Work	*1-800-123-4567 ext. 1235*
John Smith	Home	*555-123-4568*
Chief Information Security Officer	Cellular	*515-369-1479*
	Email	*ciso@[REDACTED][REDACTED]s.com*
ISCP Team – Team Members	Work	*1-800-123-4567 ext. 1245*
IT Support Team	Home	
Cody - Bill	Cellular	
	Email	itsupport@[REDACTED][REDACTED]s.com
	Work	*1-800-123-4567 ext. 1246*
Cybersecurity Analyst Team	Home	
Sam - Mike	Cellular	
	Email	cyber@[REDACTED][REDACTED]s.com
System Owners		
Jerry H. – Backup Servers	Email	jerry.h@[REDACTED][REDACTED]s.com
Suzie Q. – Regional Servers	Email	suzie.q@[REDACTED][REDACTED]s.com
Vijay S. – [REDACTED] Mainframe	Email	vijay.s@[REDACTED][REDACTED]s.com
John R. – Department Servers	Email	john.r@[REDACTED][REDACTED]s.com