



RISK MANAGEMENT STRATEGY

Kristie Arciszewski
Risk Management Consultant



Table of Contents

EXECUTIVE SUMMARY	2
RISK MANAGEMENT PLAN	4
PURPOSE	4
SCOPE	4
STAKEHOLDERS	4
DEFINITIONS	5
COMPLIANCE	5
RISK ROLES AND RESPONSIBILITIES	5
RISK ASSESSMENT TYPE	6
RISK MANAGEMENT PROJECT SCHEDULE	6
RISK ASSESSMENT.....	7
VULNERABILITY IDENTIFICATION	7
THREAT IDENTIFICATION	8
THREAT SOURCE DEFINITIONS	8
RELEVANCE RATING DEFINITIONS	8
THREAT ASSESSMENT	9
PROBABILITY	10
IMPACT	10
PRIORITY LEVEL DETERMINATION	11
CONTROLS	11
RISK REGISTER	12
RISK MITIGATION PLAN	14
BUSINESS IMPACT ANALYSIS	18
BUSINESS CONTINUITY PLAN	23
APPENDIX A – REFERENCES.....	28

EXECUTIVE SUMMARY

A Tier 3 risk assessment was completed on July 12, 2021, to evaluate the internal and external risks associated with the data center located at [REDACTED] (from now on referred to as [REDACTED]). Threats and vulnerabilities were explored and analyzed and the outcomes of this assessment identified viable risks and recommended controls to mitigate them. Since [REDACTED] has not had an IT risk assessment completed before, this assessment shall be considered a baseline from which future assessments will be compared.

The assessment was evaluated using a semi-quantitative approach. Guidelines for this approach are provided in [NIST SP 800-30 Rev. 1, Risk Management Guide for Information Technology Systems](#). This method relies on opinions of internal experts to rank risks according to probability and impact rankings. The risk assessment process was conducted as follows:

1. Completed an inventory of both vulnerabilities and threats.
2. Added risks to risk register.
3. Completed probability ratings for each risk.
4. Completed impact ratings for each risk.
5. Identified vulnerability-threat pairs. These pairs are the risks that will need to be assessed.
6. Completed risk prioritization.
7. Researched and recommended controls.
8. Assessment report submitted for analysis of recommendations.

Upon analysis of vulnerabilities and threats, the following were determined to require priority attention. Detailed data regarding this analysis is available further in this document.

Risk Description	Impact Description	Impact Level	Probability Level	Priority Level
No defense in depth (IDS/IPS) to protect network or servers. If firewall crashes, entire network is exposed.	High	96	5	480
Firewall rules are not regularly updated, leaving an open door for attacker to breach network and access servers.	High	95	4	380
No system configuration documentation for any of the servers, causing excessive time to recover data after an outage, lengthy downtime, loss of productivity and loss of sales.	High	80	4	320

Risk Description	Impact Description	Impact Level	Probability Level	Priority Level
No offsite location for contingency servers in the event that existing building structure or network infrastructure is unusable.	High	95	3	285
Unintentional power outage	High	95	3	285
Fire makes facility inoperable or causes damage to data center assets, permanent data loss, significant down time, and loss of sales.	High	95	2	190
Flooding that makes facility inoperable or causes damage to data center assets, permanent data loss, significant down time, and loss of sales.	High	95	1	95

RISK MANAGEMENT PLAN

Purpose

While [REDACTED] has a risk management plan for its operations side of the business, it does not have one for its IT infrastructure. This plan will document the processes, tools, and procedures that will be used to manage and control situations that could negatively impact [REDACTED] relevant to its IT infrastructure.

This plan will address:

- Risk assessment
- Risk mitigation
- Business impact analysis
- Business continuity planning

Scope

This plan will focus on the servers located within the Data Center only. The servers listed below are significant assets to the proper functioning of the business. Therefore, the main focus of this risk management plan is to analyze the threats and vulnerabilities related to the assets located data center in terms of confidentiality, integrity, and availability of data.

- [REDACTED] -Server-A (Windows): File server
- [REDACTED] -Server B (Windows): ISA 2006, firewall, and VPN
- [REDACTED] -Server-C (Windows): Active Directory, DHCP, DNS, WINS servers
- [REDACTED] -Server D (Windows): Open
- [REDACTED] -Server-CRM (Linux): Customer relationship management database
- [REDACTED] -Server-G (Windows): FTP server
- [REDACTED] -Server-1 (Windows): SQL database
- [REDACTED] -Server-E1: Open

Stakeholders

Stakeholders who have an interest in this risk management project include:

- Customers (current and future)
- Vendors
- Sales and Distribution Division
- Quality Control and Manufacturing Division
- Administration
- Management Review Committee

For clarity and consistency of carrying out the assessment plan, the following terms are understood:

- ## Compliance

█████ has an obligation to comply with all relevant IT laws and regulations. The only IT legal compliance requirement the company currently has is with the State of Wisconsin. As a privately owned company within Wisconsin, █████ is mandated to comply with statute 134.98 - *Notice of unauthorized acquisition of personal information*, otherwise known as Wisconsin's data breach notification law. This law "requires most businesses to notify individuals if an unauthorized person has acquired their personal information" (Wisconsin Department of Agriculture, Trade and Consumer Protection - Bureau of Consumer Protection, 2019).

There is no all-inclusive federal law that oversees data security and privacy in the United States. Instead, laws and regulations are specific to particular industries and/or business sectors. At this time, the Cybersecurity Information Sharing Act of 2015 is the one overarching federal data privacy and security law that affects [REDACTED] "This law grants liability protection, privacy protections, and other protections to organizations that share cyber threat indicators and defensive measures" (Cybersecurity & Infrastructure Security Agency, n.d.).

A set of risk management related roles is established to ensure that responsibilities of this plan are consistently carried out. Each risk management role is associated with an organizational role.

Risk Mgmt. Role	Organizational Role	Responsibilities
System Owner	IT Manager	The System Owner is a resource for identifying and determining the various attributes of risk (i.e., likelihood, impact, context, consequence, and prioritization of risk).

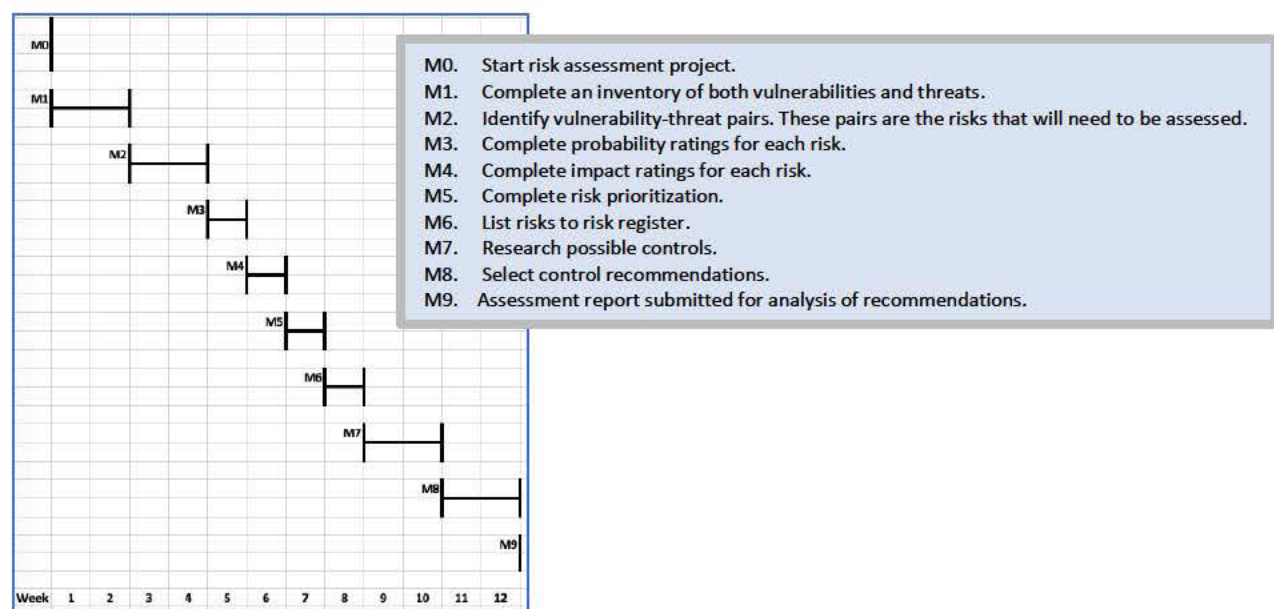
Risk Mgmt. Role	Organizational Role	Responsibilities
Risk Manager	IT Manager	The Risk Manager is a member of the Cross Functional Project Team (CFPT). The Risk Manager monitors and tracks the entire project, ensures that it is moving forward, and continually monitors the project for potential risks.
Cross Functional Project Team	Management Review Committee	The CFPT is responsible for identifying the threats and vulnerabilities, used to assess risk based on the context of the scope. Consultation with experts
Risk Owner(s)	IT Manager	The Risk Owner(s) decides which risks require mitigation and contingency plans and ultimately designs strategies to remedy them. They are also responsible for performing a cost benefit analysis of the proposed strategies. The Risk Owner(s) may also be a member of the CFPT.
Other Key Stakeholders	As required	Other stakeholders assist the CFPT in identifying and determining the context, consequence, impact, timing, and priority of the risk as needed.

Risk Assessment Type

The probability and impact of occurrence for each identified risk will be assessed using the semi-qualitative risk assessment approach. Each identified risk will be assessed and given a rating on its probability of occurrence and potential impact.

Risk Management Project Schedule

The following chart summarizes the timing of the various steps in the process:



RISK ASSESSMENT

A risk occurs when a threat exploits a vulnerability and causes a negative impact to the organization. Therefore, the first step to this risk assessment involves identifying the vulnerabilities that can be exploited by a threat. When a threat coincides with a vulnerability it is categorized as a risk. These vulnerability-threat pairs are then entered into a risk register where mitigation strategies are evaluated using a semi-qualitative approach. Each risk will be evaluated against two key data points: probability and impact to determine their priority.

Vulnerability Identification

The following inputs were used for identifying vulnerabilities:

- Documentation from past security incidents
- Any outage reports
- Past assessment reports, if any
- System logs
- Audit logs
- Vulnerability network scanning
- Personnel interviews
- Controls catalog [NIST 800-53 Rev. 5](#)

The following criteria was used to assess and rate the severity of vulnerabilities:

Qualitative Rating	Numerical Equivalent	Description
Very High	5	The vulnerability is exposed and exploitable, and its exploitation could result in <i>severe</i> impacts. No security measure can be identified to remediate the vulnerability.
High	4	The vulnerability is of <i>high</i> concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation.
Moderate	3	The vulnerability is of <i>moderate</i> concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from exploitation.
Low	2	The vulnerability is of <i>minor</i> concern, but effectiveness of remediation could be improved.
Very Low	1	The vulnerability is not a concern.

Upon reviewing this documentation the following vulnerabilities were identified:

ID	Vulnerability	Vulnerability Severity
V-00001	No offsite location to conduct business in the event that existing building structure or network infrastructure is unusable.	Very High
V-00002	Server configurations are not documented.	High
V-00003	Unnecessary open ports have yet to be identified.	High
V-00004	Security patches are not being regularly implemented on the servers.	High
V-00005	Network events and server faults are difficult to trace back because there is no auditing.	Low
V-00006	Firewall rules are not regularly updated.	Very High
V-00007	No business continuity plan has been developed.	Very High

Threat Identification

Inputs to be used for identifying threats included:

- Table of adversarial threat events in [NIST 800-30 Rev. 1](#) (2012, pp. E-2-6)
- Reviewing incidents that have occurred in organizations similar to [REDACTED]
- Personnel interviews
- Natural and weather events that typically occurs in the area

Threat Source Definitions

- *Adversarial*: Individuals, organizations, or states that want to exploit an organization's dependency on its cyber resources.
- *Accidental*: Unintentional actions of an employee or privileged user.
- *Structural*: Failures of physical equipment or software due to aging, defect, environmental controls.
- *Environmental*: Natural or man-made disasters.

Relevance Rating Definitions

- *Confirmed*: Threat event has been seen by organization.
- *Expected*: Threat event has been seen by organization's peer or partners.
- *Anticipated*: Threat event has been reported by a trusted source.
- *Predicted*: Threat event has been predicted by trusted source.
- *Possible*: Threat event has been described by somewhat credible source.

Threat Assessment

The CFPT identified the following threat events for consideration:

ID	Threat Event	Threat Source	Relevance
T-00001	Attacker performs network reconnaissance or scanning to discover network and computer assets.	Adversarial	Predicted
T-00002	Attacker obtains organizational information via open source research.	Adversarial	Expected
T-00003	Places removable media (e.g. flash drives) containing malware in locations external to the physical perimeter of the premises where employee would likely find it and then use it on internal systems.	Adversarial	Possible
T-00004	Attacker installs sniffing software onto internal information systems and networks.	Adversarial	Predicted
T-00005	Attacker follows employees into secure/controlled buildings or areas to avoid physical security checkpoints and gain access to unauthorized areas and data.	Adversarial	Predicted
T-00006	Zero-day exploitation	Adversarial	Predicted
T-00007	Attacker searches for known exploits in internal information systems and exploits them.	Adversarial	Predicted
T-00008	Attacker conducts attacks using unauthorized ports, protocols, and services.	Adversarial	Predicted
T-00009	Attacker uses direct social engineering techniques on users to cause unintended exposure, disclosure, or mishandling of data.	Adversarial	Predicted
T-00010	Attacker uses indirect social engineering techniques (i.e. email phishing) to acquire sensitive information.	Adversarial	Predicted
T-00011	Authorized privileged user inadvertently exposes critical/sensitive information.	Accidental	Predicted
T-00012	Fire makes facility inoperable.	Environmental	Confirmed
T-00013	Flooding makes facility inoperable.	Environmental	Predicted
T-00014	Natural weather events make facilities inoperable.	Environmental	Predicted
T-00015	Unintentional power outage or brown-outs.	Environmental	Possible

Probability

Probability relates to the likelihood of a risk occurring. For this assessment, each threat event was given a probability rating:

Qualitative Rating	Numerical Equivalent	Description
Very High	5	Threat event is <i>almost certain</i> to occur.
High	4	Threat event is <i>highly likely</i> to occur.
Moderate	3	Threat event is <i>somewhat likely</i> to occur.
Low	2	Threat event is <i>unlikely</i> to occur.
Very Low	1	Threat is <i>highly unlikely</i> to occur.

Adapted from NIST SP 800-30, Rev. 1

Impact

Impact relates to the severity of the threat event when it occurs. Degrees of impact are described as:

Qualitative Rating	Semi-Quantitative Values	Description
Very High	96-100	Threat event could be expected to have <i>multiple severe or catastrophic</i> adverse effects on operations, assets, individuals, or other organizations.
High	80-95	Threat event could be expected to have <i>severe or catastrophic</i> adverse effects on operations, assets, individuals, or other organizations. This includes degradation to the point that primary business functions cannot be performed; damage to assets; major financial loss; and loss of life or serious life-threatening injuries.
Moderate	21-79	Threat event could be expected to have <i>serious</i> adverse effects on operations, assets, individuals, or other organizations. This includes situations where the organization is able to perform its primary functions but the effectiveness of the functions is significantly reduced; damage to assets; financial loss; harm to individuals but with no loss of life or serious injury.
Low	5-20	Threat event could be expected to have <i>limited</i> adverse effects on operations, assets, individuals, or other organizations. This includes situations where the organization is able to perform its primary functions but the effectiveness of the functions is noticeably reduced; minor damage to assets; minor financial loss; minor harm to individuals.
Very Low	0-4	Threat event could be expected to have a <i>negligible</i> adverse effect on operations, assets, individuals, or other organizations.

Adapted from NIST SP 800-30, Rev. 1

Priority Level Determination

Priority Level is determined by multiplying the *Impact* rating by the *Probability* rating:

$$Priority\ Level = Impact \times Probability$$

Controls

Controls are actions used to reduce or eliminate a given risk. The [NIST 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations](#) catalog was a resource used to find the most appropriate controls to mitigate the various risks that were uncovered. [REDACTED] has not completed an IT risk assessment before but that does not mean that controls have not already been implemented in some way. Therefore, the controls catalog was helpful to identify controls that were already in place and see where additional controls may be necessary.

Since this is a Tier 3 risk assessment, technical controls will be the main focus for consideration. Technical controls include, but are not limited to, hardware, software, logon identifiers, session time-outs, system logs, audit trails, input validation, firewalls, and encryption.

RISK REGISTER

A risk register will be created to summarize the analysis of each risk. This register document will reside on the P: (public) drive in the risk management folder. All information in the risk register are required fields that must be completed before submitting for recommendations review. Managers will have access to this folder to add risk entries as necessary which will be reviewed by the CFPT on a monthly basis.

Risks categorized as very high and high will require priority attention for mitigation. Any risks categorized as very low, low, or moderate will be noted and no further action will be required.

Risk Description	Impact Description	Impact Level	Probability Level	Priority Level
External threat actor can scan for network asset information to attempt exploits on.	Low	4	5	20
Threat actor places removable media (e.g. flash drives) containing malware in locations where employees will be tempted to pick up and use on computers that are connected to various servers.	Moderate	79	2	158
Firewall rules are not regularly updated, leaving an open door for attacker to breach network and access servers.	High	95	4	380
No defense in depth (IDS/IPS) to protect network or servers. If firewall crashes, entire network is exposed.	High	96	5	480
Employees click on emails or links that contain malware, compromising the internal network and exposing sensitive data on computers and servers.	Moderate	50	3	150
Authorized privileged user inadvertently exposes critical/sensitive information.	Moderate	50	3	150
Fire makes facility inoperable or causes damage to data center assets, permanent data loss, significant down time, and loss of sales.	High	95	2	190
Flooding that makes facility inoperable or causes damage to data center assets, permanent data loss, significant down time, and loss of sales.	High	95	1	95
No offsite location for contingency servers in the event that existing building	High	95	3	285

Risk Description	Impact Description	Impact Level	Probability Level	Priority Level
structure or network infrastructure is unusable.				
Unintentional power outage	High	95	3	285
No system configuration documentation for any of the servers, causing excessive time to recover data after an outage, lengthy downtime, loss of productivity and loss of sales.	High	80	4	320

RISK MITIGATION PLAN

Below is the list of submitted risks that require mitigation planning:

ID	Status	Subject	Inherent Risk	Submitted	Mitigation Planned
1001	New	Firewall rules are not regularly updated.	Very High	7/23/2021	No
1002	New	No defense in depth: IDS/IPS	Very High	7/23/2021	No
1003	New	No offsite location for contingency servers in the event that existing building structure or network infrastructure is unusable.	Very High	7/23/2021	No
1004	New	No system configuration documentation for any of the servers.	High	7/23/2021	No

The following is a breakdown of the recommended security controls for the risks listed above and an analysis of each.

1001 - Firewall rules are not regularly updated.

Security Control	Reduces	Level (strategic/tactical)
SC-7(5) Boundary Protection – Deny by Default / Allow by Exception	Vulnerability severity	Tactical
SI-4(5) System Monitoring – System-Generated alerts	Threat impact	Tactical

Risk 1001 Mitigation Plan	
Mitigation Submission Date:	7/23/2021
Planned Mitigation date:	8/1/2021
Planning Strategy:	Mitigate
Mitigation Effort:	Exceptional
Mitigation Cost:	\$0 - \$100,000
Mitigation Team:	Branch Management Information Security
Mitigation Owner:	Executive Team
Mitigation Controls	
Current Solution:	Currently, there is no solution.
Security Requirement:	Improve security at the network perimeter.
Security Recommendation:	Review current firewall rules and create or delete rules. Set up regular schedule for review of rules.

Justification:

The servers in the Data Center are connected to the internal network. It is important that the firewall rules are regularly reviewed and adjusted to maintain optimal network security.

The implementation of an IDS/IPS (as noted in risk registry entry #1002) is an important piece of this process. When fully implemented, the IDS/IPS will provide the information necessary about the data going in and out of the network; data that needs to get through the firewall may be blocked by current firewall rules or data getting through to the network that should not be. Review of the IDS/IPS logs will provide the information necessary to make firewall rule adjustments.

1002 – No defense in depth: IDS/IPS

Security Control	Reduces	Level (strategic/tactical)
CM-7 Least Functionality	Vulnerability severity	Tactical
SI-4(5) System Monitoring – System-Generated alerts	Threat impact	Tactical

Risk 1002 Mitigation Plan	
Mitigation Submission Date:	7/23/2021
Planned Mitigation date:	8/16/2021
Planning Strategy:	Mitigate
Mitigation Effort:	Exceptional
Mitigation Cost:	\$0 - \$100,000
Mitigation Team:	Branch Management Information Security
Mitigation Owner:	IT Manager
Mitigation Controls	
Current Solution:	Currently, there is no solution.
Security Requirement:	Enhance confidentiality, integrity, and availability of data
Security Recommendation:	Research, purchase, install and configure IDS/IPS system

Justification:

An intrusion detection (IDS) and prevention system (IPS) monitors all network activity and will also analyze the data for patterns that indicate an imminent attack. The IDS can alert when those patterns materialize. The IPS can be placed after the firewall to catch anything that the firewall may not block, providing defense in depth. The logs generated by these systems will provide the information needed to adjust firewalls which will, in turn, improve security of the network overall.

1003 - No offsite location for contingency servers in the event that existing building structure or network infrastructure is unusable.

Security Control	Reduces	Level (strategic/tactical)
CP-2 Contingency Plan	Vulnerability severity	Tactical

Risk 1003 Mitigation Plan	
Mitigation Submission Date:	7/23/2021
Planned Mitigation date:	8/23/2021
Planning Strategy:	Mitigate
Mitigation Effort:	Considerable
Mitigation Cost:	\$0 - \$100,000
Mitigation Team:	Information SecurityData Center
Mitigation Owner:	IT Manager
Mitigation Controls	
Current Solution:	Currently, there is no solution.
Security Requirement:	Recovery of data during natural disaster.
Security Recommendation:	Develop and test contingency plan for loss of Data Center

Justification:

Laptops and desktop computers backup daily to OneDrive. The servers are backed up minimally and if the site were to experience a natural disaster, there is currently no plan on what to do in the event the servers are physically destroyed. At this time, the company is at risk of losing significant amounts of data for all department areas and at all levels. This loss of data could, in effect, put [REDACTED] out of business.

1004 - No documented configuration of servers.

Security Control	Reduces	Level (strategic/tactical)
CP-2 Contingency Plan	Vulnerability severity	Tactical

Risk 1004 Mitigation Plan	
Mitigation Submission Date:	7/23/2021
Planned Mitigation date:	9/1/2021
Planning Strategy:	Mitigate
Mitigation Effort:	Exceptional
Mitigation Cost:	\$0 - \$100,000
Mitigation Team:	IT System ManagementData Center
Mitigation Owner:	IT Manager
Mitigation Controls	
Current Solution:	Currently, there is no solution.
Security Requirement:	Contingency planning

Risk 1004 Mitigation Plan	
Security Recommendation:	Inventory servers. Use virtual machines to model configuration of each server and document steps in the process.

Justification:

Currently, the chief operations officer (C.O.O.) and IT manager have general awareness of what is on each server but not the specific configurations of them. In addition, if neither of those individuals are available to re-establish a failed server, it will be nearly impossible for other IT staff to do this task in their absence, causing significant down time. Data is backed up to OneDrive but configuration information for each of the servers is not and no instructions exist for reconstruction purposes.

As an inventory is being done of each of the servers, it would be a timesaving measure to also document the configuration settings and installation steps for each. This can be achieved by recreating servers as virtual machines. The steps required for successful installation and configuration can be interpreted into written instructions and tested.

Regularly reviewing this system information also allows IT staff to remain knowledgeable of sunsetting operating systems and applications and becoming proactive with solutions to deal with those situations.

BUSINESS IMPACT ANALYSIS

Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the Data Center. It was prepared on August 2, 2021.

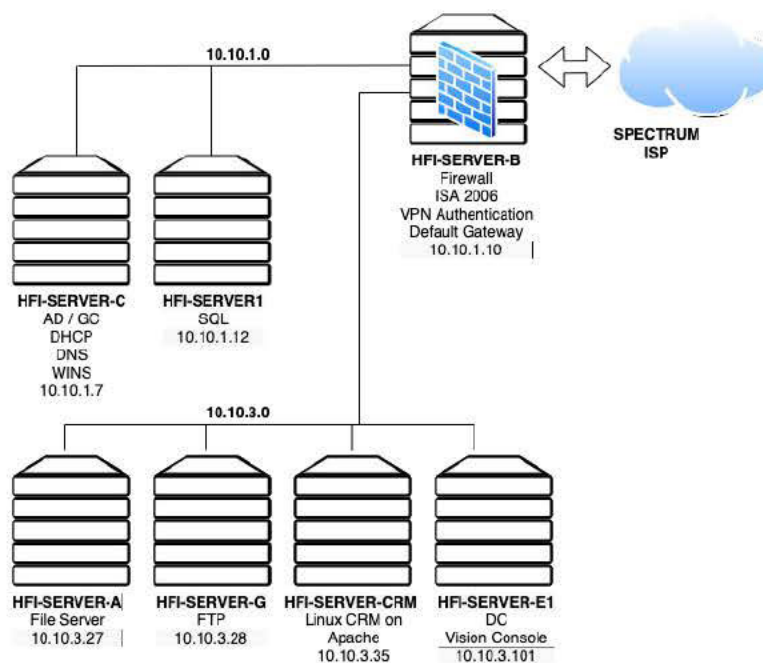
Purpose

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.

The 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
2. **Identify resource requirements.** Thoroughly evaluate resources (e.g. facilities, personnel, equipment, software, data) needed to resume mission/business processes and determine interdependencies as quickly as possible.
3. **Identify recovery priorities for system resources.** When system resources are correlated to critical mission/business activities, recovery activities can be properly prioritized.

System Description



BIA Data Collection

Critical Functions

The following outlines specific mission/business processes that depend on the various servers located in the Data Center.

Mission/Business Process	Description
Customer emailing salesperson with order	Customer emails salesperson with items to order.
Entering orders into database.	Salesperson enters parts into ordering application.
Order fulfillment, including shipping and receiving	Warehouse personnel pull and print orders, prepare parts for shipping and ship to customer.
Invoicing customer	Invoice is printed and sent to customer.
Collecting payment from customer.	Customer sends payment with check or credit card. Credit card is processed by accounting department.
Inventory	Entering materials and parts into inventory database.

Impact Analysis

Those same critical processes and analysis values are consolidated into the business impact analysis chart below. Descriptions which explain the values follow.

Critical Business Function Description	Impact Level	Operational Impact	Financial Impact	Critical Resources	Max. Tolerable Downtime	RTO	RPO
Customer accessing website	1	Lost sales and income Negative cash flow resulting from delayed sales or income Customer dissatisfaction or defection	> \$300K	Web server SQL Database Authentication server Internet access	2 hours	2 hours or less	1 hour or less
Customer emailing salesperson with order	2	Lost sales and income Negative cash flow resulting from delayed sales or income Customer dissatisfaction or defection	> \$300K	Email server	24 hours or less	24 hours or less	24 hours or less
Entering orders into database.	2	Lost sales and income Negative cash flow resulting from delayed sales or income Customer dissatisfaction or defection	> \$300K	SQL Database File server	24 hours or less	24 hours or less	24 hours or less
Order fulfillment, including shipping and receiving	2	Lost sales and income Negative cash flow resulting from delayed sales or income Customer dissatisfaction or defection	> \$300K	SQL Database File Server Internet access	24 hours or less	24 hours or less	24 hours or less

Critical Business Function Description	Impact Level	Operational Impact	Financial Impact	Critical Resources	Max. Tolerable Downtime	RTO	RPO
Invoicing customer	3	Lost sales and income Negative cash flow resulting from delayed sales or income	> \$300K	SQL Database Email Server Finance Database File Server Printers Internet access	3 days or less	72 hours or less	72 hours or less
Collecting payment from customer.	1	Lost sales and income Negative cash flow resulting from delayed sales or income	> \$300K	Finance Database Internet Access	2 hours or less	2 hours or less	1 hour or less
Inventory	4	Lost sales and income	< \$10K	SQL Database	1 week	7 days	7 days

Impact Levels

	MAO	Description
Level 1	2 hours or less	Business functions must be available during all business hours. Online systems must be available 24 hours a day, seven days a week.
Level 2	24 hours or less	Business processes can survive without the business function for a short amount of time.
Level 3	3 days or less	Business processes can survive without the business functions for one or more days.
Level 4	1 week or less	Business processes can survive without the business functions for extended periods.

Estimated Downtime

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

- Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
- Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

- **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.

Identify Resource Requirements

The following table identifies the resources that compose the Data Center including hardware, software, and other resources such as data files.

System Resource/Component	Platform/OS/Version (as applicable)	Description
■-Server-A	Windows	File server RAID Configuration: 2 disks
■-Server-B		ISA 2006 Default gateway Firewall VPN Authorization
■-Server-C	Windows	Active Directory Server / GC DHCP Server DNS Server WINS Server 1 Volume Windows RAID: 2 disks
■-Server-D	Windows	Windows RAID 2 Volumes
■-Server-G		FTP server SCSI RAID
■-Server-CRM	Linux	CRM database
■-Server-1	Windows	SQL Windows RAID 5 volumes
■-Server-E1		SCSI RAID

It is assumed that all identified resources support the mission/business processes identified in the Critical Functions section unless otherwise stated.

Identify Recovery Priorities for System Resources

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

- **Recovery Time Objective (RTO)** - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

Priority		Recovery Time Objective
	-Server-B	8 hours or less
	-Server-C	12 hours or less
	-Server-1	24 hours or less
	-Server-CRM	24 hours or less
	-Server-D	24 hours or less
	-Server-A	2 days or less
	-Server-E1	24 hours or less
	-Server-G	24 hours or less

BUSINESS CONTINUITY PLAN

Purpose

The purpose of this plan is to define the recovery process developed to restore [REDACTED] critical business functions. The plan components detail [REDACTED] procedures for responding to an emergency situation, which affects [REDACTED] ability to deliver core services to our customers or our ability to meet legal or regulatory requirements.

Objectives

- Facilitate timely recovery of core business functions
- Protect the wellbeing of our employees, their families, and customers
- Minimize loss of revenue/customers
- Maintain public image and reputation
- Minimize loss of data
- Minimize the critical decisions to be made in a time of crisis

The following Business Contingency Plan and all related procedures are approved by the president and chief operating officer of [REDACTED] effective the date signed below.

_____	_____
[REDACTED], President	Date

_____	_____
[REDACTED], Chief Operating Officer	Date

Recovery Strategies

Recovery strategies identified for [REDACTED] equipment and services:

- Business functions will be recovered in priority sequence based upon the classification of the function as agreed with business senior management and implemented jointly.
- Communications concerning the recovery status will be coordinated through the Business Contingency Planning Team so that those executing the recovery will not be interrupted repeatedly for status.
- Purchase and acquisition of equipment and supplies needed for the recovery effort will be coordinated through company Department Heads.
- The contingency planning infrastructure will provide for coordination of travel arrangements, food, and accommodations for individuals supporting the recovery effort.
- Non-critical [REDACTED] functions will be cleared without backup as necessary to support the recovery efforts.
- [REDACTED] personnel from other sites may be called in to support the recovery efforts.

Business Contingency Planning Team

The following individuals are designated plan coordinators for their respective departments and are responsible for the execution of this plan in a qualified disaster.

Name	Title	Phone	Email
[REDACTED]	Chief Operating Officer	[REDACTED]	[REDACTED]
	Human Resources		
	Community Relations		
	Sales/Marketing		
	Finance		
	Legal		
[REDACTED]	Vice President of Distribution		
	Insurance		
[REDACTED]	Vice President of Quality & Manufacturing		
[REDACTED]	Warehouse Manager		

Offsite Data Storage

All documentation of importance to the operations of [REDACTED] will be stored on the OneDrive cloud service:

- Weekly backups of ALL files, including servers and PCs
- System, program product, and in-house developed software manuals and guides
- Legal: Copies of contracts, leases, legal and critical correspondences
- Insurance: Policies, riders, and addendums
- Financial: General and private ledgers, year-end financial statements, tax returns, bank records
- Recovery plans: A complete set
- Assets: Complete fixed asset listings
- Referenced Items: Copies of any item referenced within recovery team plans
- Floor plans
- Architectural drawings that should include mechanical plans
- Photos of facility and various work areas
- Other critical documents or data critical to the operation of the business

Property Protection

Protecting facilities, equipment and vital records is essential to restoring [REDACTED] operations once an emergency has occurred.

Only members of the Business Contingency Planning team will authorize, supervise and perform a facility shutdown.

Facility Shutdown Procedures

Facility shutdown is generally a last resort but always a possibility. Improper or disorganized shutdown can result in confusion, injury, and property damage. Department heads are to establish shutdown procedures, including information about when and how to shut off utilities. In this effort, they will need to identify:

- The conditions that could necessitate a shutdown
- Who can order a shutdown
- Who will carry out shutdown procedures
- How a partial shutdown would affect other facility operations
- The length of time required for shutdown and restarting

Site Map Documentation

All appropriate information pertaining to building and site maps are to be included in the Appendices. This will include, utility shutoffs, water hydrants, water main valves, water lines, gas main valves, gas lines, electrical cutoffs, electrical substations, storm drains, sewer lines, location of each building (include name of building, street name and

number), floor plans, alarm and enunciators, fire extinguishers, fire suppression systems, exits, stairways, designated escape routes, restricted areas, hazardous materials (including cleaning supplies and chemicals) high-value items.

Plan Activation

Emergency Alert

In the event that a situation or disaster occurs at [REDACTED], the Business Contingency Planning Team is responsible for contacting the Management Team and assessing the emergency situation.

An alert will be sent to all Department Heads. Status updates will be provided by the Business Contingency Planning Team to the Department Heads for dissemination of pertinent information.

Damage Assessment

During the damage assessment phase, the Business Contingency Planning Team will identify specifically who and what has been affected by the disaster. The Business Contingency Planning Team will evaluate the event that has occurred and determine what Department Heads will be required to respond to the situation. The decision to activate the disaster recovery plan for the affected areas may be made at this point or after notification and review with the Business Contingency Planning Team.

As part of the damage assessment process, the risk assessment to the business will be evaluated.

Considerations of engaging temporary facilities, equipment and vendors will be reviewed and a determination to enact recovery procedures will be determined by the Business Contingency Planning Team and Department Heads.

If after assessment it is determined that activation of the recovery plan is required, notification to the Executive Team will be made. An authorized individual will immediately notify the affected site that the disaster has been DECLARED.

Resuming Operations

The previously identified Department Heads will act as the Recovery Teams with the utmost attention of ensuring the safety of personnel and property. The Recovery Team for the affected operations will assess any remaining hazards and maintain security at the incident scene.

The Recovery Team will conduct an employee briefing relaying pertinent details of what happened, what business operations were affected and the plan for recovery.

Additional notifications will be made to:

- Employee's families about the status of personnel on the property

- Off-duty personnel about work status
- Insurance carriers about incident details
- Appropriate government agencies

An investigation will be conducted by the Recovery Team notating details of the incident scene via video recording and digital photography. Damage related costs will be recorded to include charges for purchases and repair work.

Training

All employees will review disaster preparation and emergency action plan procedures with their Department Heads. New employees will be introduced to our emergency action plans via employee orientation.

Mock disaster training will be conducted annually and will involve local police and fire authorities. Quarterly training will approach a walk through to functional drills to an evacuation drill leading to full-scale mock disaster training.

Walk-Through Drill -- The Business Contingency Planning Team, Department Heads and Recovery Teams will perform their emergency response functions.

Functional Drills -- These drills will test specific functions such as medical response, emergency notifications, warning and communications procedures and equipment, though not necessarily at the same time. Facility shutdown procedures will be tested, reviewed and modified as needed. Personnel are asked to evaluate the systems and identify problem areas.

Evacuation Drill -- Personnel walk the evacuation route to a designated area where procedures for accounting for all personnel are tested. Participants are asked to make notes as they go along of what might become a hazard during an emergency, e.g., stairways cluttered with debris, smoke in the hallways. Plans are to be modified accordingly.

Full-Scale Exercise -- A real-life emergency situation is simulated as closely as possible. This exercise involves company emergency response personnel, employees and management, and community response organizations.

Appendix A – References

- Anderson, S. (2015, July 22). Fire at Imperial Laundry. *The Journal Times*.
https://journaltimes.com/news/local/fire-at-imperial-laundry/article_d043c572-bdee-53c0-a27d-25603bfc4f33.html
- Carson, A. (2021, June 25). Data privacy laws: What you need to know in 2021.
<https://www.osano.com/articles/data-privacy-laws>
- Cybersecurity & Infrastructure Security Agency. (n.d.). *Automated Indicator Sharing*. Retrieved August 10, 2021, from <https://www.cisa.gov/ais>
- Cybersecurity & Infrastructure Security Agency. (n.d.). *Cybersecurity Information Sharing Act of 2015 Procedures and Guidance*. Retrieved July 9, 2021, from <https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance>
- Department of Homeland Security & Department of Justice. (2020, October). *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* (Department of Homeland Security & Department of Justice, Authors).
https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf
- Department of Homeland Security & Department of Justice. (2021, January 4). *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (Department of Homeland Security & Department of Justice, Authors).
<https://wilawlibrary.gov/topics/records/privacy.php>

Federal Trade Commission. (n.d.). *Privacy and Security*. Retrieved July 9, 2021, from <https://www.ftc.gov/tips-advice/business-center/privacy-and-security>

Gibson, D., & Igonor, A. (2022). *Managing Risk in Information Systems* (3rd ed.). Jones & Bartlett Learning.

HFI Fluid Power Products. (n.d.). *Custom Hydraulic Assemblies*. Retrieved August 10, 2021, from <https://www.hfi.us.com/>

International Organization for Standardization. (n.d.). *ISO/IEC 27001 Information security management*. Retrieved August 9, 2021, from <https://www.iso.org/isoiec-27001-information-security.html>

Joint Task Force Transformation Initiative. (2012). Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>.

Joint Task Force Transformation Initiative Interagency Working Group (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>.

Journal Times staff. (2017, February 14). Crews respond to Uptown fire. *The Journal Times*. https://journaltimes.com/news/local/crews-respond-to-uptown-fire/article_874c47c1-326b-5647-a77a-447a6032dd87.html

Latham & Watkins. (2016, February 18). What You Need to Know About the Cybersecurity Act of 2015. *Client Alert Commentary*, (1927).

<https://www.lw.com/thoughtLeadership/lw-Cybersecurity-Act-of-2015>

Ready. (n.d.). *Business Impact Analysis Worksheet* [Table].

<https://www.ready.gov/sites/default/files/2020-07/business-impact-analysis-worksheet.pdf>

Template for business impact analysis.

Ready. (2021, May 26). *Business Continuity Plan*. Ready.gov. Retrieved August 9, 2021, from <https://www.ready.gov/business-continuity-plan>

Ready. (2021, June 17). *Business Impact Analysis*. Ready.gov. Retrieved August 9, 2021, from <https://www.ready.gov/business-impact-analysis>

Templateral.com. (n.d.). *Sample Business Continuity Plan*.

<https://www.checklist.templateral.com/wp-content/uploads/Business-Continuity-Plan-Checklist-Template.pdf>

Top database security threats and how to mitigate them. (2015, July 30). *SHRM*.

<https://www.shrm.org/ResourcesAndTools/hr-topics/risk-management/Pages/Top-Database-Security-Threats.aspx>

USA.com. (n.d.). *Racine, WI Natural Disasters and Weather Extremes*. Retrieved August 5, 2021, from <http://www.usa.com/racine-wi-natural-disasters-extremes.htm>

Wisconsin Department of Agriculture, Trade and Consumer Protection - Bureau of Consumer Protection. (2019, December). *Wisconsin's Data Breach Notification Law*. <https://datcp.wi.gov/Documents/IDTheftDataBreach607.pdf>