DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

Savory Sauce Restaurant - Alberta

Stephen Dornu Dugbartey

Disaster Recovery and Business Continuity Plan Version 1.0	
Prepared By	Sujan Timsina, Incident Response Team Lead
Approved By	Todi Arrowshead, Chair of the Board of Directors
Date Approved	October 18, 2024
Expected Revision Date	October 18, 2025
Document Owner	Stephen Dugbartey, Chief Information Security Officer (CISO)
Review Frequency	Annually
Plan Distribution	All relevant staff, key stakeholders
Confidential Level	Internal Use Only

Table of Contents

RACI Matrix Roles and Responsibilities

This RACI matrix helps clarify roles and responsibilities, ensuring that everyone knows their part in maintaining recovery and business continuity from disasters.

Roles Explained

Responsible: Individuals who perform the task.
Accountable: Person who is ultimately answerable for the correct and thorough completion of the task.
Consulted: Individuals who provide input and advice (two-way communication).
Informed: Individuals who need to be kept informed (one-way communication).

Task/Activity	Responsible	Accountable	Consulted	Informed
Risk Assessment	BC/DR Team	Risk Manager	IT Manager, Security Officer	Senior Management, All Staff
Business Impact Analysis (BIA)	BC/DR Team	BC Coordinator	Department Heads	Senior Management, All Staff
Data Backup	IT Department	IT Manager	Security Officer, DR Team	BC Coordinator, Senior Management
Testing DR/BC Plans	BC/DR Team	DR Coordinator	IT Department, Department Heads	All Staff
Resource Allocation	Procurement Team	BC Coordinator	IT Manager, DR Team	Senior Management, All Staff

Alternative Work Locations	Facilities Management	BC Coordinator	Department Heads, IT Manager	All Staff
Communication Plan	Communications Team	BC Coordinator	PR Manager, Department Heads	All Staff, External Stakeholders
Plan Development and Documentation	BC/DR Team	BC Coordinator	IT Manager, Department Heads	All Staff
Training and Awareness Programs	HR Department	Training Manager	BC Coordinator, DR Coordinator	All Staff
Plan Review and Updates	BC/DR Team	BC Coordinator	IT Manager, Department Heads	All Staff
Incident Response and Management	Incident Response Team	Incident Manager	IT Department, Security Officer	All Staff
System and Data Recovery	IT Department	IT Manager	BC/DR Team, Vendors	Senior Management, All Staff

Document Accountability

Role	R	A	C	I
Chief Information Officer		X		
Chief Technology Officer	X			
IT Project Manager			X	
IT Support Staff			X	
Enterprise Architect			X	
Business Continuity Officer				X

Disaster Recovery and Business Continuity Policy

Executive Summary

Savory Sauce Restaurant operates multiple locations across Alberta, supporting over 4,300 employees. This DRP and BCP ensures business resilience during emergencies, including natural disasters, cyberattacks, and service disruptions.

Key personnel, including the Chief Information Officer (CIO) and Emergency Response Team (ERT), oversee disaster response efforts, including threat mitigation, facility evacuation, and operational continuity. Regional heads are responsible for implementing the plan within their zones, ensuring adherence to defined protocols.

The plan complies with ISO 22301:2019/Amd 1:2024 standards, which incorporate climate action adjustments and global best practices, reinforcing Savory Sauce's commitment to operational resilience and sustainability

Purpose

Savory Sauce Restaurant (Savory Sauce) recognizes the importance of preparing for and responding to disruptions that may affect business operations. The Disaster Recovery and Business Continuity Policy establishes a set of pre-approved response protocols that ensure safety of life, continuation of critical business functions, and compliance with regulatory and ISO 22301:2019 standards during, after and before a disaster. The main objectives of these processes and procedures are intended to minimize financial, reputational, and operational risks, lower costs, decrease downtime resulting from security incidents, and safeguard Savory Sauce assets, and personnel while facilitating a swift return to normal operations in line with creating value for relevant stakeholders.

The objective of this plan focuses on giving priority to the following processes when the region or individual restaurant is hit with a disaster. The objective is to:

- document plans and previous recovery actions taken to serve as restoration guides for future disasters
- provide safety of employees, customers and visitors on the business premises
- contain the spread of threat and damage to life, property, and reducing financial loss
- invoke the plan for maximum use of this plan and available expertise to return critical business functions back to operation soonest
- ensure protection of data and all other information systems assets
- reduce liability claims filed against Savory Sauce, or its directors, or officers

Statement of Management Commitment

The Board of Directors and Management of Savory Sauce is committed to protecting the safety of staff and customers, assets, business functions and any person in a way that allows them to operate within the business premises in a sound mind and working environment. We are committed to ensuring recovery and continuous commitment to resolving disasters that prevent regular business operations in line with creating value for all relevant stakeholders. Savory Sauce is equally committed to supporting information technology handlers through advice, policies, tools, training, resources and governance structures that promote quicker response and recovery in delivering accessible goods, and services at our restaurant.
Savory Sauce Restaurant is committed to:

- sustaining critical business functions during disruptions
- protecting IT infrastructure and data integrity
- providing safe working environments for employees and seamless service for customers
- testing and updating the DRP and BCP to align with evolving risks and regulations
- upholding compliance with ISO 22301:2019 standards

Mandatory Compliance

All employees, contractors, and stakeholders are required to adhere to this policy. Non-compliance will result in corrective actions, which may include training, reprimands, or termination.

Scope of the Plan

The Disaster Recovery (DR) and Business Continuity Plan (BCP) for Savory Sauce Restaurant (Savory Sauce) outlines approved processes, procedures, guidelines, resources and expertise to be relied on by the Disaster Recovery Team (DRT) during a disaster in all business locations within Alberta, Canada. This document does not include in-depth technical instructions, as Savory Sauce information security and information technology engineers are already familiar with the complexities of their roles and the systems they manage. Instead, it offers a clear pathway for action during such chaotic situations. The operations of the business in Alberta is categorized under five zones with a Head responsible for each zone.

Applicability

This plan applies to all Savory Sauce Restaurant locations and personnel in Alberta. It addresses:

- Cybersecurity threats (malware, ransomware)
- Natural disasters (floods, severe weather)
- Operational disruptions (supply chain failures, IT outages)

Any suspicion of exposure to Savory Sauce data or systems? Immediate contact:

Helpdesk – (780) 888-4410 or helpdesk@savorysauce.ca
Information Security Office (ISO) – (780) 888-4414

Business Operations

Savory Sauce Restaurant is an all-cuisine restaurant in Alberta, with over 4300 employees, offering online ordering, delivery, mobile app-ordering, contactless payments, and e-gift cards on the back of POS software, Toast which works on cloud-based platform with constant feature updates and allows the employees to access restaurant data anywhere on their mobile device. The operations of the restaurant in Alberta are categorized under five zones – North Zone, Edmonton Zone, Central Zone, Calgary Zone, and South Zone as represented on the figure 1 below. IT responsibilities within each zone is managed by the head with a supporting hierarchy to operate. The head of the zone is in charge and responsible for providing leadership during planning, declaration and activation of the plan.

Figure 1: Zonal Map of Savory Sauce (AHS, 2024)

Definitions

Savory Sauce Restaurant defines the following terms inline with the organization's information security, disaster recovery and business continuity agenda in line with its value creation objectives of the business.

Event: An event refers to any deviation from the standard functioning of IT infrastructure, systems, or services. Such events can be detected by automated monitoring systems, reported by the information security office or other departments, or uncovered during routine system evaluations, such as when there are signs of system degradation or outages. It's important to recognize that not every event escalates into an incident.

Incident: An incident is defined as minor disruption to the business functions, IT services, IT infrastructure and business operations with manageable impact on the value creation. It poses a minor to average risk impact to the confidentiality, integrity, or availability of Information Systems or Institutional Data.

Disaster: A major disruption to the business functions IT services, IT infrastructure and business operations with severe impact on value creation. It poses an extreme risk impact to the confidentiality, integrity, or availability of Information Systems or Institutional Data, and safety and lives to persons within the catchment area at the time of occurrence.

Recovery: The process of restoring business functions, business processes, data, network, infrastructure, other assets and life back to normal state and operation when a disaster occurs. Data is retrieved from a storage device that was inaccessible through normal methods.

Policy: A set of general expectations outlined by senior management to be followed by the whole or part of the organization expressed in the form of procedure, standards, guidelines and recommendations.

Procedure: A part of policy that outlines the steps to take to achieve a desired expectation in the policy.

Backup: Alternate data storage equal to the capacity, function and use as the main storage that can be relied on in continuation of business operations when a disaster occurs.

Recovery Time Objective (RTO): The goal the organization sets for the maximum length of time it should take to restore systems following a disaster strike.

Recovery Point Objective (RPO): The maximum amount of data the organization can tolerate losing when a disaster strikes. "How far back data can we recover"?

Methodology

This plan describes the fundamental tasks involved in disaster recovery. Given the dynamic nature of disasters and attacks affecting the business, this DR and BCP may be augmented by internal guidelines, standards, and procedures related to the utilization of security tools, technologies, and methods for incident investigation.

Guidelines for Disaster Response Process

Evidence Preservation: The main objectives of disaster recovery are to contain the impact, minimize risks to organization's systems and data, and restore affected systems and data to operational status as swiftly as possible. However, the speed of restoration can sometimes be hindered by the need to collect data for evidence following a data breach.

Operational-Level Agreements: In our technology-driven society, many individuals expect reliable access to systems and data for themselves and those they serve. Service interruptions can lead to significant challenges, and the information systems office will work with impacted groups to reduce downtime. Nonetheless, the restaurant leadership prioritizes investigation activities when there is a considerable risk, which may lead to temporary outages or disruptions.

Training: Ongoing enhancement of DR and BCP processes requires regular reviews, drills, and assessments for improvement. Savory Sauce staff will receive periodic training on reporting and managing disasters to ensure they are well-acquainted with the procedures and the roles of the Disaster Recovery and Business Continuity Team. These training sessions may include both internal and external formats, such as tabletop exercises.

Disaster Recovery and Business Continuity Phases

This DR and BCP processes together consist of seven phases: preparation, response, restoration, resumption, relocation to alternative site, returning to primary site and business continuity after-action review. All the seven phases need not be run during the handing of any disaster.

Preparation: Preparing for a disaster and continuing business involves activities that equip the organization to effectively handle the disaster. This includes developing and reviewing policies, plans, and guidelines that support response, as well as establishing security and technology tools, communication plans, and governance structures. Additionally, it ensures that various branches of the restaurant have put in place the necessary response, recovery, restoration and resumption structures.

Response Phase: Once a source identifies the potential or actual occurrence of a disaster, the organization activates its Disaster Recovery Plan (DRP)and enters the response phase. This phase is focused on safeguarding lives and ensuring safety, minimizing damage to organizational assets, and managing communication with employees and other relevant stakeholders.

Recovery Phase: The organization focuses on recovering any salvageable assets from the affected site. If the damage is not catastrophic, it may be possible to retrieve hardware, office equipment, furniture, and supplies. The response teams assess what can be saved and document any replacement items needed for future recovery efforts. The organization prioritizes rebuilding the most essential business operations first, while less critical functions may be postponed. The primary focus is on restoring production or service operations that directly generate revenue. At the conclusion of the disaster recovery phase, the team evaluates whether it is necessary to activate the Business Continuity Plan (BCP).

Restoration Phase: The organization focuses on the tasks required to restore its primary facilities and prepare them for the resumption of operations. If the disaster results in more extensive damage than can be repaired at any of the primary sites, this phase may involve the decision to relocate to a new permanent location. Additionally, organizations must recognize that this phase could mark the end of the business if the damage is too severe to allow for recovery.

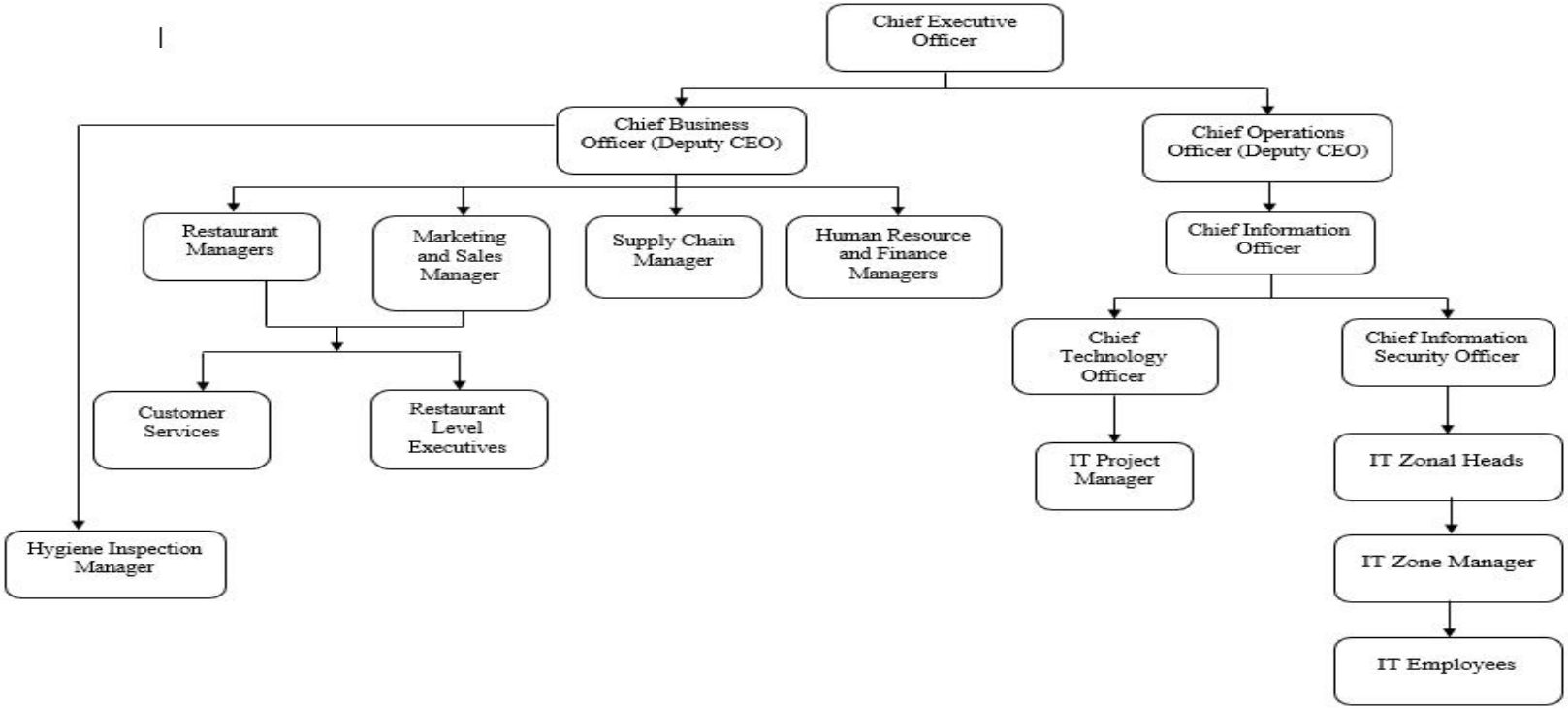
Resumption Phase: While the restoration phase centers on rebuilding the physical facilities, the resumption phase is focused on re-establishing business operations and getting back to work. The Business Impact Analysis (BIA) should serve as the key reference for developing a prioritized list of primary and secondary functions, which will guide the organization in resuming activities at the recovered facilities.

Relocation to Alternative Site: The organization undertakes all activities necessary to relocate the business operations to an alternative site, the resources required and the period necessary to move operations back to its primary site.

Returning to Primary Site: The organization undertakes all activities necessary to relocate the business operations back to its primary site.

Business Continuity After-Action Review: The team will assess what was successful and identify areas for improvement. Before this meeting, each team member should prepare a summary reflecting their experience, noting aspects that worked well and highlighting any areas that could be enhanced. The feedback and insights gathered will then be compiled into a checklist for easy review, be able to incorporate into future disaster recovery plans and monitor progress.

Organizational Structure



Contact List

This section lists the DR and BC response team, list of vendors, list of suppliers, list of emergency services, and list of industry regulators, their contact and role they play in supporting Savory Sauce Restaurant meets its objectives.

Disaster Recovery and Business Continuity Response Team				
Officer	**Name of Officer**	**Role on the Recovery DR and BC Team**	**Phone Number and Email Addresses**	**Responsibilities**
Chief Information Officer (CIO)	Grace Okoro Anyanso	DR and BC Champion	780-888-5001 ganaynso@savorysauce.ca	Overall responsibility for information technology, information security and incident response strategy in integrating and managing various technology platforms used by the retail and online centers system, mobile applications, website, and contactless payment systems. The CIO will also provide strategic vision and linkage to the power structure of the organization.
Chief Technology Officer (CTO)	Eghosa Okpoko	Team Leader	780-888-5002 eokpoko@savorysauce.ca	Develop and execute a thorough operational technology plan that aligns with the business goals. Integrate features and technologies aimed at enhancing the operational and digital customer experience across all areas especially during an incident.
Chief Information Security Officer (CISO)	Stephen Dugbartey	Officer on Duty for all disasters	780-888-5003 sdugbart@savorysauce.ca	Safeguard the confidentiality, integrity, and availability of retail and online information centers. Implement regular security awareness programs to educate staff and perform security audits to identify vulnerabilities and weaknesses in the information systems. The CISO shall also review adverse events, declare for a disaster and activate the DR and BC plan.
IT Project Manager	Jenish Mevada	IT Project Manager	780-888-5004 jmevada@savorysauce.ca	Gathering IT needs and requirements with various zones and recommending. The IT Project Manager shall also lead project planning for efficient and effective use of resources.
IT Zonal Heads	North Zone – Simon Singh	Team Leader	780-888-5005 ssingh@savorysauce.ca 780-888-5006	Implementing and supervising the IT and security strategy designed by the organization at the zonal levels. In the event of a disaster, the IT zonal heads shall provide leadership in making the right decisions for their respective zones.

	Edmonton Zone – Sujan Timsina Central Zone – Samuel Etoo Calgary Zone – Xavi Alonso South Zone – Christiano Ronaldo		stimsina@savorysauce.ca 780-888-5007 setoo@savorysauce.ca 780-888-5008 xalonso@savorysauce.ca 780-888-5009 cronaldo@savorysauce.ca	
IT Zone Managers	North Zone – Ahmed Tinubu Edmonton Zone – Sani Abarcha Central Zone – John Mahama Calgary Zone – Donald Harris South Zone – Clinton Bush	Team Members	780-999-6001 atinubu@savorysauce.ca 780-999-6002 sabarcha@savorysauce.ca 780-999-6003 jmahama@savorysauce.ca 780-999-6004 dharris@savorysauce.ca 780-999-6005 cbush@savorysauce.ca	Directly reports to and aids the IT zonal heads to implement IT and security strategy at the zonal levels.

Helpdesk and IT Support Personnel	Availability varies based on officer on duty	Team Members	780-111-1111 780-111-2222 780-111-3333 780-111-4444	To be the first point of contact for employees' technology, incident and security reporting and support. The desk will assist with timely support and resolution incidents in areas of physical, operating systems, and network security.
Marketing and Sales Manager	Joe Doe	Team Member	780-999-6006 jdoe@savorysauce.ca	Promoting positive business image, advertising and effectively implementing strategies that increase business revenue and profit.
Supply Chain Manager	Marvin Jason	Team Member	780-999-6007 mjason@savorysauce.ca	Coordinating the movement of goods between suppliers and the business while optimizing transportation routes, select logistics providers, manage warehousing and distribution centers, and track shipments to ensure on-time delivery and to reduce costs
Finance Manager	Nina Trevor	Team Member	780-999-6008 ntrevor@savorysauce.ca	Responsible for the financial health of the organization in creating financial reports, direct investment activities, and developing plans for the long-term financial goals of the organization. The finance manager will support the recovery team budget and emergency ancillary expenses during a disaster
Human Resource Manager	Olivia Khan	Team Member	780-999-6009 okhan@savorysauce.ca	Attracting the best skills to fill roles, develop training programs, design and implement compensation while ensuring compliance and safety at the workplace. Before a disaster occurs, the HR shall support the recovery team with training and awareness programs. During a disaster The HR shall support the redefinition of working schedules and redistribution of expertise.
Customer Service Manager	Lucia Gustavo	Team Member	780-777-3001 lgustavo@savorysauce.ca	Managing the needs of customers, ensuring they are retained and satisfied. During. The manager shall also manage media interaction during the management of a disaster.

Vendor List				
Vendors	**Names**	**Phone Number**	**Email**	**Responsibilities**
Software and IT Support Vendor	Agility IT Services	416-587-4478	service@agility.ca	Providing, hardware, network maintenance and application support services to IT infrastructure
Internet Services	MTN Globacom	613-628-0903 450-666-6748	service@mtn.ca service@glo.ca	Provides internet and communication services
Electricity Services	Power to the People Inc Asogli Power	905-494-9749 418-497-6323	service@ppi.ca service@asogli.ca	Provides electricity services
Water Service	Alberta Water Services	613-674-6601	service@aws.ca	Provides water services
Engineering Support	Sparta Engineering Services	819-359-4454	service@sparta.ca	Provides technical and maintenance services to machines and equipment
Private Security	Eagle Eye Security	414- 149-5574	watch@eagleeye.ca	Providing private security services

Supplier List					
Categories of Suppliers	**Name of Supplier**	**Contact Person**	**Phone Number**	**Email**	**Supplier Location within Alberta**
Vegetable Farmers	Freshco Farms Nature Farms	Anita Hammond Beatrice Arthur	705-341-6129 416-515-6049	supply@freshco.ca supply@nature.ca	Grande Praire, Wabasca River Hylo, Red Deer, Arrow Wood
Fruit Farmers	No.1 Farms AgroFoods	Diamond Jason Shana Stuwart	705-312-7692 416-412-1823	supply@number1.ca supply@agrofoods.ca	Edmonton, Calgary, Valley View Hanna, Jasper NP, Edson

Bakery	Comfort Flour Meals Diana Bakery	Amanda Nelson Diana Hamilton	306-939-0263 416-343-8948	supply@comfort.ca supply@dianabakery.ca	St. Albert, Edmonton Wagner, Calgary
Breweries	Spirito Brewery Cloud 9 Brewery	Peter Bruce Evan Hunter	514-266-5534 250-447-8881	supply@spirito.ca	Edmonton, Calgary, Lethbridge Calgary, Lethbridge
Meat	Protanica Meat Living Meat	Mayfair Barnes Manuel Walters	306-931-8909 306-268-4597	supply@protanica.ca supply@living.ca	Edmonton Calgary
Sea Food	Shells Sea Foods Ocean Drive Foods	Kite Shadow Princes Scott	709-456-5716 416-375-6105	supply@shells.ca supply@oceandrive.ca	Clear Water River, Edmonton Lesser Slave Lake, Lethbridge

List of Emergency Services and Industry Regulators			
Agency	**Details**	**Contact Details**	**Availability**
Fire, Police and Ambulance Services	All Zones	911	24 hours a day
Insurers	Protect Insurance Worry-No-More Insurers	551-478-7896 888-921-3654	Daytime Daytime
Building Inspectors	North Zone Office Edmonton Zone Office Central Zone Office	419-111-1111 419-111-2222 419-111-3333	Daytime Daytime Daytime

	Calgary Zone Office South Zone Office	419-111-4444 419-111-5555	Daytime Daytime
Canadian Food Inspection Agency	North Zone Office Edmonton Zone Office Central Zone Office Calgary Zone Office South Zone Office	703-701-9964 703-710-8261 587-582-9648 306-424-5900 306-368-5363	Daytime Daytime Daytime Daytime Daytime

Disaster Recovery and Business Continuity Strategies

The DR and BCP update process must be organized and carefully managed. Any modifications to the plan should undergo thorough testing, and corresponding updates must be made to the training materials. This will require the implementation of formal change control procedures, overseen by the Chief Information Officer (CIO). Important to the contingency plan is life. Additionally, the assets and reputation needed to be protected when possible. The Central theme to the DR and BCP is to “protect and forget”.

Plan Documentation Storage

The Plan will be stored in both digital and physical formats in secure locations designated by the company. Senior management will receive both a CD and a printed copy of the plan to be kept at their residences. Members of the Disaster Recovery and Business Recovery Teams will also be provided with both a CD and a hard copy. Additionally, a master copy of the plan, with protection measures in place, will be maintained on dedicated resources set up for this purpose. The softcopy should be created with easy links on the table of content to easily navigate the document is times of urgency. Alternatively, colours should be used to differentiate the portions of the hard copies of this plan. The reason is to also be able to easily navigate the document under emergency.

Backup Strategy

The key business processes and their corresponding backup involves establishing a fully mirrored recovery site at the company’s Alberta restaurants. This strategy ensures that a complete duplicate of the primary site is maintained, allowing for seamless, real-time switching between the main site in Edmonton and the backup location. Geographically, the management of business in Alberta will establish two extra designated data backup solutions in addition to the primary site in Edmonton. The secondary site in Calgary and another with a cloud service provider that meets the internal vendor selection criteria of Savory Sauce Restaurant.

Cross Training

In the event of an emergency, such as an epidemic or severe weather preventing some employees from arriving at the restaurant on time, it is crucial for other staff members to be able to fill in for the absent employees. To ensure this, monthly cross-training are key components of the restaurant's continuity strategy. By cross-training staff, employees can acquire a range of skills from their colleagues, enabling them to step in for one another and maintain smooth operations at Savoury Sauce Restaurant. The Human Resources Department, along with other teams, has been and will continue to provide cross-training across various roles to prepare for situations where employees may be absent for extended periods. Due to that, each activity under the emergency responses has a primary and an alternative officer.

Alternative Vendors, and Suppliers

Alternative inventory suppliers and vendors have been identified to mitigate the impact of supply chain disruptions. Power outages can lead to food spoilage, data loss, and disruptions to various systems and equipment. Break on the internet and communication can lead to inability to process customer requests and receive payment. To address problems, each input supply has two readily available suppliers, and each service provider has two readily available vendors. Both supply the organization needs to prevent heavy reliance on a single person.

Insurance

The organization shall undertake two types of insurance for each business operating facility: life insurance and asset insurance. Each type of insurance should have two vendors as listed in the vendor list in the previous section.

Plan Triggering Events

The following events should trigger the activation of the Disaster Recovery Plan.

- Possible indicators (presence of unfamiliar files, presence of unknown programs, unusual consumption of commuting resources, unusual crashes)
- Probable indicators (activities at unexpected times, presence of unexpected new accounts, reported attacks, alerts from IDPS)
- Definite indicators (use of dormant accounts, changes in logs, presence of hacker tools, notification by peers, notification by hacker)
- Total loss of all communications
- Total loss of power
- Loss of internet connection
- Flooding of the premises
- Loss of portions of the restaurant building
- Report by meteorological agencies regarding potential disasters
- Announcing by selected media outlets regarding potential disasters

Emergency Alert

This policy and procedure have been put in place to ensure that, in the event of a disaster, personnel are clearly informed about who to contact. The procedures are designed to enable rapid communication during the activation of the disaster recovery process. The DR plan will primarily depend on key management and staff members, who will bring the necessary technical and managerial expertise to facilitate a seamless recovery

of both technology and business operations. Critical suppliers will also continue to play a role in supporting the restoration of business activities as the company returns to normal operations.

Assembly and Accountability

In the event of an evacuation, the DRP activation plan designates three assembly points for each restaurant:

- *Primary*: The far end of the main parking lot
- *Secondary:* The parking lot of the company located across the street. Primary and secondary evacuation routes are marked with a RED Exit Sign. Emergency lighting will illuminate exits if power fails. Employees are required to exit the building through designated evacuation routes when at all possible.
- *Tertiary:* When the primary and secondary are not possible, the CIO will activate rescue mission with state emergency services to aid. The Disaster Response Team will establish five designated locations to serve as central hubs for emergency response for the province. The primary center will be in the head office in Edmonton, with a secondary center located in Calgary, Lethbridge, Red Deer, and Grand Prairie as represented by the five geographical zones of operations by the business. If the primary and secondary centers are unavailable due to a disaster, the emergency services team will relocate the team to any close and safe tertiary center. All centers will be equipped with blueprint, of the building, alarm activation and deactivation codes, first aid kits, copy of the emergency plan, chain of command list and contact information, three flashlights fully charged with spare batteries fully charged, 20 litres of clean water, and map of the surrounding areas.

Once an evacuation of the facility has been declared, employees should gather at the designated assembly point to ensure all personnel are accounted for. Each employee must check in upon arrival at the evacuation location, either by signing a paper log or emailing the emergency services and the DR and BC teams. For any individuals not accounted for, their names and last-known locations should be reported to the Emergency Response Team, who will then attempt to reach those employees. If any personnel remain unaccounted for after two hours, the Emergency Response Team will notify local authorities. In the event the situation escalates, Fire Fighters will conduct further evacuation efforts. Customers, vendors, or other visitors who were evacuated along with employees will also be required to sign in and out before leaving the assembly area.

Risk Assessment

Savory Sauce Restaurant faces a variety of business risks that could impact its profitability, reputation, health and safety and internal operations, including natural, human-caused, and technological risks. For easy assessment and contaminants of the various risks the business faces, each has been grouped under four categories.

Types of Business Risks

***Security Risks*:** Includes threats such as theft, vandalism, and fraudulent activities. Examples of fraud include billing schemes, check tampering, skimming operations, and payroll fraud. Cybersecurity threats, such as cyberattacks and online fraud, also fall under this category.

***Personnel Risks*:** Risks involving staff shortages due to resignations, pandemics, or labor disputes. These disruptions can significantly affect day-to-day operations.

Natural Disasters: Hazards caused by severe weather conditions, including flooding, snowstorms, and other climate-related events, which can impact facility access and service continuity.

***Operational Risks*:** Disruptions to the supply chain, transportation networks, IT infrastructure, and telecommunications systems, which are essential for smooth business operations.

***Infrastructure Risks*:** Threats related to physical assets, such as fires, hazardous material incidents, power outages, and utility failures, which can severely impact operational capabilities and safety.

Classification of Disasters

All together, Savory Foods classifies the identified business risks under four disaster categories. Some disasters overlap between being classified as man-made or natural disaster but to create simplicity of using this plan, they are clearly underlisted classified under any of the following four categories below:

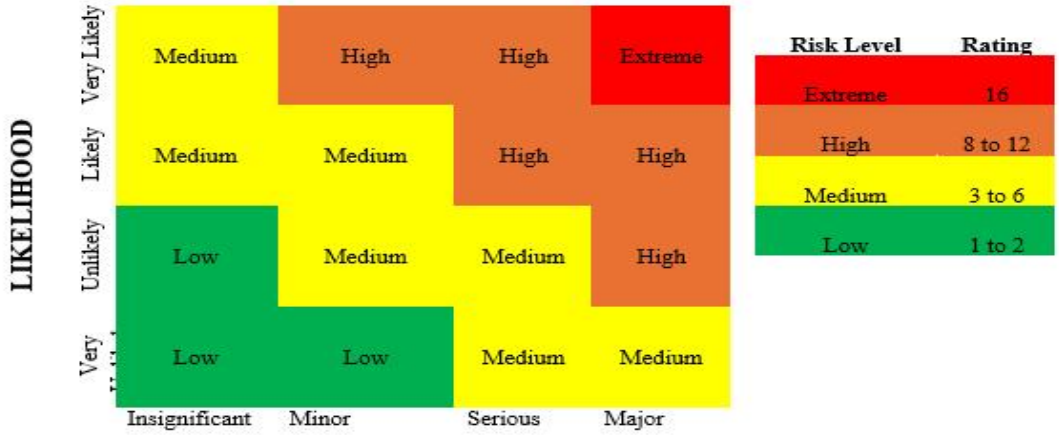
- Category 1 - A threat to public safety or life
- Category 2 - A threat to sensitive data
- Category 3 - A threat to computer systems
- Category 4 - A disruption of services

Risk Analysis

The risk analysis process involves mapping the likelihood of occurrence against the impact of the disaster category to determine the overall risk level rating which gives the DR and BC team reason to commit time and resources to the risk management process. The table below summarizes the mapping and possible outcomes. The likelihood and impact of the four categories of disasters have been determined to determine their priority with the following steps:

- All categories of disasters have been listed with their respected affected functions
- The likelihood of occurrence of the disaster have been determined
- The impact of the disaster has been determined
- The likelihood of occurrence value is multiplied against the impact value to determine the overall value rating
- The overall value rating determines the importance to be placed on the disaster type with resources and time allocation
- From the table it is determined that the most impactful disaster to the operations of Savory Sauce Restaurant within the Alberta province is Category 1: Flood, Extreme Weather Conditions and Natural Fire.

Risk Assessment Diagram



Explanation

Value	Likelihood	Description
4	Very Likely	Very likely to occur in the foreseeable future
3	Likely	Likely to occur in the foreseeable future
2	Unlikely	Not likely to occur in the foreseeable future
1	Very Unlikely	Will only occur in exceptional circumstances

Value	Severity	Description	Impact on Profitability, Reputation, Health and Safety and Internal Operations	Recovery Time
4	Major	Loss of key business functions and severe damage to business assets	Major	1 month or more
3	Serious	Significant impact on of key business functions and damage to business assets	Significant	1 week to 1 month
2	Minor	Minimal impact on key business functions and no damage to business assets	Minimal	1 to 7 days
1	Insignificant	Negligible impact on key business functions and no damage to business assets	None	Immediate

Category of Contingency	Type	Business Functions Impacted	Likelihood of Occurrence	Impact on Business Processes	Overall Disaster Risk Rating
Category 1	Flood, Extreme Weather Condition, and Natural Fire	Food Storage Table Services Sales Food Delivery Receiving Supplies Receiving Payments Security Services Customer Services Advertising and Promotions	Very Likely (4)	Major (4)	Extreme (16)
Category 1	Hurricane, Tornados, Volcano Eruption, Earthquake, Tsunami, Pandemic and Other and Disease Outbreaks	Food Storage Table Services Sales Food Delivery Receiving Supplies Receiving Payments Security Services Customer Services Advertising and Promotions	Unlikely (2)	Major (4)	High (8)
Category 2	Data Loss, Device Loss, and Man-made Fire	Sales Receiving Supplies Customer Services Advertising and Promotions	Very Likely (4)	Serious (3)	High (12)
Category 3	Malware Attack, DoS, and DDoS	Sales Food Delivery Receiving Payments Customer Services	Very Likely (4)	Serious (3)	High (12)
Category 4	Power, Internet and Communication Outages, and Supply Chain Disruption	Food Storage Table Services Sales Food Delivery Receiving Payments Receiving Supplies Security Services Customer Services	Likely (3)	Serious (3)	High (9)

Business Impact Analysis (BIA)

The Business Impact Analysis (BIA) examines the critical business processes relevant to continuous delivery of service to customers in achieving the value creation objective of Savory Sauce Restaurant. This section analyses and arranges the various business functions in order of criticality, and the impact of possible disasters on business processes.

Business Functions	Personnel Required	Resources Required	Contribution to Profitability (0.4)	Contribution to Health and Safety (0.3)	Contribution to Reputation (0.2)	Contribution to Internal Operations (0.1)	Process Criticality (1.0)
Food Storage	Supply chain manager, Hygiene inspectors, restaurant manager	Cold storages, Electricity, internet, telecommunications	5	5	5	4	4.9
Table Services	Floor Manager, Chef, Customer service manager, Waiter	POS, electricity, internet, kitchen, Toast software	5	5	3	4	4.5
Sales	Restaurant manager, Chef, Customer service manager	Kitchen, POS, Toast software, internet, Data backup	5	5	3	4	4.5
Food Delivery	Delivery driver, chef, Bus boys, Customer service manager, IT support staff	Cold storage van, kitchen, mobile app, GPS, internet	5	4	3	2	4.0
Receiving Supplies	Supply chain manager,	Delivery truck, inventory software,	4	4	2	2	3.4

	Restaurant manager	electricity					
Receiving Payments	Customer service manager, Finance manager, IT support staff	POS, internet	5	2	2	3	3.3
Security Services	Security personnel, IT support staff	Telecommunication, CCTV, monitor	1	5	5	2	3.1
Customer Services	Customer service manager, Restaurant manager	Computerized workstation, data backup, customer software	4	1	3	4	2.9
Advertisement and Promotions	Advertising manager, Finance manager	LED displays, Billboards	4	1	3	1	2.6

Explanation to BIA on Key Processes

- The contribution of the various business processes has been weighted against profitability (0.4), health and safety (0.3), reputation (0.2) and internal operations (0.1). The total weights sum up to 1.0.
- The assigned numbers to each process ranges between 1 to 5 with 5 being the highest contribution.
- Profitability is the most weighted impact as it heavily contributes to the value creation objective of Savory Sauce Restaurant.
- Food storage is the most critical business process whiles advertisement is the least critical process, therefor resources like electricity, internet, telecommunications and cold storages are similarly critical resources

Disaster Responses

Each of the identified disaster category have been treated in this chapter, recommending the necessary actions to be taken under the disaster recovery and business continuity phases while assigning responsibility, reporting and resources needed to bring business back to normal operations as soon as possible.

Category 1: Pandemic and Other Disease Outbreaks, Flood, Hurricane, Tornados, Volcano Eruption, Earthquake, Tsunami, Snowstorms, Extreme Weather Conditions, and Fire				
Disaster Recovery and Business Continuity Phases	**Required Actions**	**Required Resources**	**Primary Responsibility**	**Secondary Responsibility**
Preparation	Develop a pandemic response plan. Conduct staff training on health protocols and remote work procedures. Stockpile essentials supplies (sanitizers, masks, non-perishable food). Establish communication channels for emergency updates.	Health supplies, remote communication tools (e.g., video conferencing software), emergency contacts.	Human Resource Manager	Restaurant Manager
Response	Activate emergency communication plan Enforce health protocols (mask-wearing, sanitization). Modify operations for health safety (e.g., takeaway-only service).	PPE (personal protective equipment), communication systems.	Operations Manager	Health and Safety Officer
Recovery	Assess impact on operations and staff. Sanitize facility post-crisis.	Sanitization supplies, phased reopening	Health and Safety Officer	Restaurant Manager

	Plan for phased reopening of full operational resumption.	guidelines		
Restoration	Restore full operations based on assessment. Replenish stock and supplies	Inventory list, supply chain contacts	Restaurant Manager	Operations Manager
Resumption	Determine priority for backlog services Resume regular customer service. Update customers on operational status.	Communication tools, customer contact database.	Marketing and Communications Manager	Restaurant Manager
Relocation to Alternative Site	Identify alternate sites and assess readiness. Transport essential staff and supplies	Transportation, alternate site contacts	Operations Manager	Human Resource Manager
Returning to Primary Site	Inspect and prepare primary site for safe reopening Notify staff and customers.	Inspection team, communication tools.	Restaurant Manager	Facilities Manager

Category 2: Data Loss, Device Loss, and Fire				
Disaster Recovery and Business Continuity Phases	**Required Actions**	**Required Resources**	**Primary Responsibility**	**Secondary Responsibility in absence of primary responsibility**
Preparation	Induction and refresher training to staff on appropriate use of devices Exercise plan testing	Classroom setup, portable device, internet Portable device, internet	Human Resource Manager Zonal IT Head	CISO Restaurant Manager

	Annual review of data and device loss recovery plan	Previous plan document, experienced disruptions	CISO	CTO
	Test data backup alternatives	Tapes, backup servers	CISO	CTO
	Test electricity alternatives	UPS, generators, fuel	IT operations manager	CTO
	Secure and track device, encrypt data	Password managers, trackers, encryption software	IT operations manager	CTO CIO
Response	Declare disaster	SMS, email	CISO	Direct supervisor
	Knowing of data loss, device loss from staff involved	Phone	IT helpdesk	-
	Notification of relevant stakeholders	SMS, email	IT helpdesk	-
	Isolate, block user access or lockdown premise	password server, network server, CCTV, keys and locks	Security Analyst, Network Analyst, Database Administrator	CIO
	Ascertain amount of data loss or type of device lost	Database software SMS, email	IT helpdesk	
	Declare switch into recovery phase		CISO	

Recovery	Salvage of data tapes, device profile	Tapes, privilege access	Security analyst	-
	Salvage backup software functions	Backup software	Operating systems analyst	Application analyst
	Salvage of database server	Database server	Database administrator	-
	Disable missing device dispose from asset list	Database server	CISO	CIO
	Declare switch into restoration phase	SMS, email	CISO	CIO
Restoration	Assess amount of data loss	Database software	Database analyst	-
	Analyse the integrity of lost data or missing device	Database software, device tag identity	Database analyst	-
	Patch database software	Operating system	Operating systems analyst	Application analyst
	Improve firewall, antivirus protection	Firewall, antivirus	Security analyst	-
	Inform affected department or persons	SMS, email	CISO	CIO
	Report to the police of necessary	Report	CISO	CIO
	Declare switch into resumption phase	SMS, email	CISO	CIO
Resumption	Compare lost data integrity to master data	Database server	Database analyst	-
	Install backup if necessary	Backup storage	CISO	CTO

	Communicate closure of disaster to stakeholders and document key lessons	SMS, email	CISO	CIO

Category 3: Malware Attack, DoS, and DDoS				
Disaster Recovery and Business Continuity Phases	**Required Actions**	**Required Resources**	**Primary Responsibility**	**Secondary Responsibility**
Preparation	Implement cybersecurity protocols. Periodic internal scanning and audits System configuration Backup resilience testing Conduct regular training on identifying phishing, strong passwords, and malware.	Antivirus software, firewall, Strengthened IDPS, Data backups, employee training materials.	Network Administrator, Security Analyst	IT Manager
Response	Block intrusion and isolate affected systems. Seek internet service provider support where needed Notify relevant stakeholders but mitigation strategy is to “protect and forget”. Remove breach components Engaging the media and public	Incident response software, backup communication. Phone, emails	IT Helpdesk Customer Service Manager	CISO -
Recovery	Restore from clean backups.	Backup systems,	IT Support	Security Analyst

	Run a system scan to ensure no residual malware.	antivirus software.	Specialist	
Restoration	Reinstate affected services. Implement additional security measures.	Firewall, updated antivirus protocols	CISO	IT Manager
Resumption	Monitor system for anomalies. Report incident closure	Monitoring software, incident report forms	Security Analyst	IT Manager

Category 4: Power Outages, Internet Outages, Communication Outages, and Supply Chain Disruptions				
Disaster Recovery and Business Continuity Phases	**Required Actions**	**Required Resources**	**Primary Responsibility**	**Secondary Responsibility**
Preparation	Training to staff on power, internet and communication systems Exercise plan testing Annual review of power, internet and communication outages recovery plan Test secondary alternative power, internet and communications	Classroom setup, portable device, internet Portable device, internet Previous plan document, experienced disruptions UPS, internet service provider, generators, fuel	Human Resource Manager Zonal IT Head CISO IT operations manager	CISO Restaurant Manager CTO CTO
Response	Knowing of the outage Declare disaster	Phone SMS, email	IT helpdesk CISO	Direct supervisor CIO

	Notification of relevant stakeholders Ascertain quick reason for the outage Declare switch into recovery phase	SMS, email Phone, resource dashboard SMS, email	IT helpdesk IT helpdesk CISO	- Engineering vendor CIO
Recovery	Restore power and communication. Confirm supply chain stability	Utility contacts, internet service provider contacts	Facilities Manager	Operations Manager
Restoration	Verify systems are functioning. Conduct inventory check.	Power and internet systems, inventory lists	Restaurant Manager	Chain Manager
Resumption	Resume normal service operations	Customer communication channels	Communications Manager	Restaurant Manager
Relocation to Alternative Site	Move to a backup facility if the primary location has prolonged power or supply issues.	Transport, backup facility setup	Facilities Manager	Operations Manager
Returning to Primary Site	Inspect and prepare primary site, communicate return to normal operations.	Inspections tools, communication channels	Restaurant Manager	Facilities Manager

Disaster Recovery and Business Continuity After-Action Review

The After-Action Review (AAR) is a vital process for Savory Sauce Restaurant to evaluate its response to disruptions and enhance resilience for future challenges. As part of the organization's commitment to maintaining operational excellence and safety, the AAR serves as a structured evaluation tool to identify successes, gaps, and areas for improvement in the DR and BC processes. Once the business continuity activities are concluded and the organization has either returned to its primary facility or relocated to a new permanent alternate site, the business continuity team should convene to review the outcomes. The team should assess what was successful and identify areas for improvement. Before this meeting, each team member should prepare a summary reflecting their experience, noting aspects that worked well and highlighting any areas that could be enhanced.

For Savory Sauce Restaurant, the AAR is conducted to achieve the following objectives and benefits:

- To assess the effectiveness of the response to the disruption
- To highlight operational or procedural shortcomings that hindered an effective response
- To capture and document insights to refine the DR and BCP that ensures that the organization is better prepared for future disasters
- To reassure employees, customers, regulators, and partners of Savory Sauce commitment to continuous improvement and safety

Lessons Learned

The lessons learned process is an integral part and a key component of the After-Action Review (AAR). It involves identifying important issues that came up before, during and after the disaster and how the organization could leverage on the opportunities or gaps to improve future preparedness and response. An effective lesson learned process must include activities around post-disruption data collection, reviewing objectives and outcomes, facilitating feedback, analysing root causes, monitoring and evidence gathering, notification of stakeholders and regulators, cost and damage assessment, plan review and updates, and testing and maintenance.

Post-Disruption Data Collection*:* Comprehensive documentation is essential for a meaningful review in the areas of:

- Recording details of events, including the onset, escalation, and resolution of the disruption.
- Highlighting successes, challenges, and observations from those involved in the response
- Documenting data on downtime, recovery timelines, and impacts on key processes
- Receiving feedback input from employees, customers, and suppliers on how the incident affected them

Reviewing Objectives and Outcomes: The AAR compares the outcomes of the disaster to the intended objectives outlined in Savory Sauce's DR and BCP. This involves answering important questions.

- Were key business functions restored within the specified Recovery Time Objectives?
- Did data recovery align with the Recovery Point Objectives?
- Were safety protocols effective in protecting employees and customers?

Facilitating Team Feedback*:* A collaborative review meeting allows the DR and BC response and emergency response teams to discuss:

- Which processes and actions worked well and delivered positive outcomes?
- Which bottlenecks or failures hindered the response?
- What enhancements or changes could improve future responses?

Analyzing Root Causes*:* For identified challenges or failures, a root cause analysis helps pinpoint the underlying issues. Common areas of focus include:

- Training and preparedness before the occurrence of the disaster
- Resource availability and sufficiency
- Timely, clear and effective communication

Monitoring and Evidence Gathering: Collect evidence of the disruption, such as photos, videos, and operational data, to support analysis and insurance claims

Notification of Stakeholders and Regulators: Ensure that emergency services, regulatory bodies, and key stakeholders are informed of the incident and response measures taken.

Cost and Damage Assessment**:** Evaluate the financial, operational, and infrastructural impacts of the incident, including costs for recovery and any lost revenue.

Plan Review and Updates**:** Use findings from the AAR to revise the BCP-DRP, addressing identified gaps and incorporating new scenarios or strategies.

Testing and Maintenance: Schedule follow-up testing of the updated plan and provide targeted training for employees to address weaknesses.

Disaster Recovery and Business Continuity Plan Checklist

The checklist below can be adapted to aid the DR and BC team to collect and analyze the aftermath of the disaster. The checklist in summary will assist to reveal the needed lessons that to be learnt in areas that are relevant before, during and after the disaster.

Disaster Recovery and Business Continuity Plan Checklist		
Type of Disaster:	**Location of Disaster:**	**Date of Occurrence:**
DR and BCP Phases	**Required Actions**	**Answer As Applicable**
Preparation	Are all members aware of the security policies of the organization?	
	Do all members of the Disaster Recovery Team know whom to contact?	
	Do all disaster responders have access to journals and access to responses toolkits to perform the actual incident response process?	
	Have all members participated in disaster response drills to practice the response process and to improve overall proficiency on a regularly established basis?	
Response	Where did the disaster occur?	
	Who reported or discovered the incident?	
	Are there any other areas that have been compromised by the incident? If so, what are they and when were they discovered?	
	What is the scope of the impact?	
	Have the source(s) of the incident been located? If so, where, when, and what are they?	
	Can the problem and affected system be Isolated from non-affected systems?	
	Have forensic copies of affected systems been created and stored in a secure location for further analysis?	
	Have all malware and other artifacts left behind by attackers been removed?	
	Has the affected systems been patched and hardened against recent attacks?	

	What day and time would be feasible to restore affected systems back into production?	
	What tools will be needed to test, monitor and verify that systems restored are further compromised by the same cause of the original disaster?	
Restoration	What critical assets are damaged beyond repairs?	
	Have totally damaged critical assets been disposed properly without a trace of vital data left?	
	Can repairable damaged assets be fixed within the required SLA?	
	Can the non-repairable assets be replaced within a reasonable time?	
Resumption	Can all critical business functions be returned to operation within the required after restoring critical assets	
	What resources are required to return critical business functions back to operations?	
	Has any meeting been held to discuss lessons learnt?	
	Did the meeting discuss any error where the response could have been handled better?	
	Will the primary business site be safe for operation for life and assets? Will an alternative location be needed?	
	Has the process for insurance claim started?	
Relocation to Alternative Site	Which alternative site will serve alternative purpose within the soonest time?	
	What resources are needed to quickly prepare the alternative site for use	
	Which business functions can operate from the alternative site? Where will other business functions operate from?	
	How long will it take to start operations on the alternative site?	
Returning to Primary Site	Is the primary site safe for life and assets required for regular operations?	

References

Mattord, M. E. (2022). *Principles of Incident Response & Disaster Recovery.* Boston: Cengage Learning Inc.

NIST. (2012). *SP 800-61r2: Computer Security Incident Handling Guide.*

NIST. (2016). *SP 800-184: Guide for Cybersecurity Event Recovery.*