RiskIntel™ Business Continuity Planning Guide

echelon®
Insurance

Table of contents

A business continuity plan is a pre-emptive plan to help a business ensure the continuous deliverance of goods and/or services to customers following an unforeseen disaster or event.

In today's highly competitive and ever-changing business environment, businesses large and small face an unprecedented number of exposures that can disrupt business operations. Whether it is a natural disaster such as a wildfire or a man-made event such as a ransomware attack, an unforeseen incident can be devastating for a business. While direct property losses can be overwhelming enough, they often pale in comparison to the loss businesses experience if they are unable to resume operations following an event (e.g., loss of customers, market share, reputation, etc.). While no one can predict the future, damages stemming from business disruption can be mitigated through the establishment of a comprehensive business continuity plan.

What is a Business Continuity Plan?

Considered an integral part of a business's overall risk management strategy, a business continuity plan is a pre-emptive plan to help a business ensure the continuous deliverance of goods and/or services to customers following an unforeseen disaster or event. Such a plan identifies potential threats and vulnerabilities, incorporating specific protocols that target critical aspects of operations to ensure businesses can respond to, and recover from an interruption to operations. This proactive approach builds resilience and helps protect businesses from the impacts of the loss.

Common misconceptions about business continuity planning

1. *"Our business is too small to require a business continuity plan."*

Fact: On the contrary, small businesses, particularly those operating from a single location, are more vulnerable to business interruption losses than large companies (i.e., larger companies may have the capability to diversify their risk across several geographical locations).

2. *"Our staff will know what to do in the event of an emergency, so a business continuity plan is not needed."*

Fact: No one can predict the stress and tension a loss can put on a business and its staff. Leaving staff to their own devices in the event of a loss may only add to the turmoil surrounding the event.

3. *"Our insurance will cover our losses."*

Fact: Relying on insurance alone should never be considered a primary business continuity strategy. While having business interruption coverage is important, several damages may not be covered (e.g., loss of market share, customers, reputation, etc.).

4. *"We don't have the time to create a business continuity plan"*

Fact: The consequences of not taking the time to create a business continuity plan far outweigh any time or cost needed to establish a business continuity plan. Creating a business continuity plan should be top priority for management and time should be allocated to do so appropriately.

5. *"Our current business continuity plan doesn't require continuous review and modification."*

Fact: Market competition and business demands are constantly changing. As such, it is critical to review and modify business continuity plans regularly to ensure their efficacy when there is a need to put them into action.

Developing a Business Continuity Plan

Before a business continuity plan can be developed, there must be a commitment, support, and engagement from senior management within an organization. Forming a business continuity team starts with the assignment of a business continuity manager by senior management, who will oversee the process. From there, the business continuity manager should assemble a team of internal staff representing all departments within the organization, including (but not limited to) facilities, operations, manufacturing, logistics, information technology, finance, communications, human resources, and legal. It is important that the business continuity team has a clear understanding of business goals and objectives from the outset. Roles and responsibilities should be clearly defined for each team member, with each team member being responsible for developing the plan for their respective departmental function, including what their roles will be during emergency response and disaster recovery in the event of a disruption to business operations.

While the components of business continuity plans may differ between organizations, it is common for business continuity plans to have the following elements, which are explained in the preceding sections.

Element one: Overview of business continuity plan

This section should outline the key objectives of the business continuity plan as well as a distribution list.

Objectives play a crucial role in providing clarity to a business continuity plan by defining its purpose and outlining the desired outcome. Typical objectives include:

- Identifying potential risks and threats to the business, and methods to prevent or mitigate them.
- Recognizing and prioritizing critical functions of the business, and the impact a disruption would have on those functions.
- Detailing response protocols in the event a critical incident results in a disruption to business operations.
- Outlining strategies and actions to be taken that will enable the business to recover from a disruption.
- Developing review and maintenance procedures to ensure the business continuity plan is up to date.

A distribution list identifies those individuals who have been provided with a copy of the business continuity plan and the business function they represent.

A sample distribution list can be found in Appendix A.

Element two: Risk management plan

This section outlines potential threats to a business, strategies to prevent threats or mitigate their impact, insurance policy details, and data security and backup protocols.

Risk assessment

Assessing the extensive range of potential risks and threats that a business may face can be challenging. Some of these events may be easier to predict than others, particularly those that are weather-related based on historical trends and patterns in a business's geographical area. Others, particularly those that are human caused can be difficult to predict; that being said, it is reasonable to assume these types of events are always possible and could impact a business significantly. These risks and threats can be wide-ranging, including, but not limited to:

- Geological (e.g., earthquake, volcano etc.)
- Meteorological (e.g., hurricane, tornado, flood etc.)
- Biological (e.g., infectious and communicable diseases etc.)
- Building and equipment infrastructure (e.g., fire, structural collapse, mechanical breakdown etc.)
- Human-caused (e.g., terrorism, civil disturbance, ransomware etc.)
- Utility interruption (e.g., communications, electrical, natural gas etc.)
- Computer systems (e.g., hardware failure, telecommunications, interruption etc.)

Evaluating the impact of these risks and threats can help in determining which areas should be prioritized from a time and resource perspective. This can be quantified by completing the following exercise in which the likelihood and impact of a risk or threat are assessed and used to generate a ***level of risk*** score (i.e., likelihood x impact = level of risk). The higher the score, the higher the priority should be to prevent or mitigate their impact.

Likelihood Scale		
Level	**Likelihood**	**Definition**
4	Very High	Occurs more than once a year
3	High	Occurs once a year
2	Moderate	Occurs within 10-year intervals
1	Low	Has only occured once or not at all

X

Impact Scale		
Level	**Likelihood**	**Definition**
4	Severe	Likely to cause closure or significant financial loss
3	High	Major impact on orgnization with large financial loss
2	Moderate	Moderate impact on organizatio with some financial loss
1	Low	Minor impact on organziation with minimal financial loss

=

Risk Level (Likelihood x Impact)		
Score	**Rating**	**Required Action**
12-16	Severe	Needs immediate preventative or corrective action
8-12	High	Needs preventative or corrective action within one (1) month
4-8	Moderate	Needs preventative or corrective action within three (3) months
1-4	Low	Does not currently require preventative or corrective action

Risk prevention and mitigation

After completing the above exercise and pinpointing areas of the concern, the next step is to contemplate strategies to reduce the established risk level. This can be accomplished by taking actions to prevent or mitigate the loss, illustrated through the example below.

Risk/Threat	Likelihood	Impact	Risk Level	Actions Taken
Equipment breakdown	2 (Moderate)	4 (Severe)	8 (High)	• Set up a reciprocal agreement with a third party to limit production losses • Ensure there is a service contract in place with the equipment manufacturer • Retain an inventory of replacement parts and components on-site

A risk management plan template can be found in Appendix B.

Insurance coverage

Having a comprehensive insurance policy (or policies) is vital in ensuring the continuity of business operations. A business could encounter substantial consequences without adequate coverage in place, including having to pay out large sums of money or having to close the business entirely. The types of insurance and level of coverage will vary depending on the business's activities and intricacies. It is important that businesses work with their insurance Broker to ensure all aspects of their operations are covered. Available coverages include (but are not limited to) property, crime, business interruption, and liability (general liability, products liability, etc.).

This section of the business continuity plan should include a summary of current insurance coverages.

A template has been included in Appendix C.

Data security and backup protocols

Information technology (IT) plays a crucial role in modern day organizations by optimizing processes and minimizing the need for physical documentation. Depending on the organization, critical data housed within IT systems could include personnel records, financial data, administration documents, proprietary data, and other intellectual property. IT risks encompass a range of potential threats, including hardware and software malfunctions, human mistakes, spam, viruses, and malicious attacks. Additionally, natural disasters can also pose significant risks to IT systems. As such, measures need to be taken to prevent the loss of critical electronic data in the event of an IT-related incident.

Backing up business data at regular intervals is imperative, including the use of off-site storage locations. This section of the business continuity plan should include a summary of data backup protocols.

A template has been included in Appendix D.

Other measures to prevent the loss of critical electronic data include, but are not limited to, the following:

- Securing computers, servers, wireless networks, and passwords
- Utilizing firewalls, anti-virus protection, and anti-malware protection
- Implementing two-factor authentication for organizational software
- Ensuring the latest versions of software are installed
- Implementing comprehensive IT policies and procedures that are to be adhered to by staff

Element three: Business impact analysis

A business impact analysis (BIA) is arguably the most critical element in the development of a robust business continuity plan. The BIA will use information assembled in the Risk Management Plan section to assess the identified risks and their impact in relation to critical business processes and establish fundamental recovery requirements. Critical business processes are those functions that must continue to support the business.

The BIA should begin by meeting with senior management who understand the direction of the company and the business functions, products, and services that are most important to the financial success of the business and its longevity. Once this information is obtained, business activity questionnaires should be developed and distributed to all department heads within the business for completion.

These questionnaires should cover the following:

- Name and description of the business unit or process
- What the losses would be if the business activity could not be provided
- The maximum amount of time the business activity could be unavailable before losses would incur
- Dependencies on outside services or products that are imperative to the business unit or process

A sample business activity questionnaire can be found in Appendix E.

Once all information is obtained, the business continuity manager should evaluate the criticality of each function and establish a recovery time objective for each, that is, the time frame in which the function must be recovered before serious harm is done to the business. From there, the business continuity manager should then summarize the findings for each function and prioritize (e.g., low, medium, or high) those functions in a business impact analysis spreadsheet (see Appendix F).

Element four: Incident response plan

This section describes how and when a business activates its business continuity plan in response to a critical incident or disaster.

Experiencing an incident or disaster can be an extremely distressing event that can cause significant harm to a business. That said, it is important to have a strategy in place to address these scenarios to reduce the potential harm and damage to the business. This comes in the form of an incident response plan, which is a critical element of a business continuity plan. An incident response plan prepares a business for a timely response to critical incidents, reduces the impact of those incidents on the business, and ensures that essential personnel are well-prepared to respond to an incident promptly and efficiently to mitigate any potential disruptions to business operations.

The following components should be included in an effective incident response plan:

Immediate response checklist

A checklist should be created that outlines the initial actions to be taken following an incident. This checklist should be customized to an organization's needs and could include the following elements:

- Activation of business continuity plan
- Evacuating the site following the incident
- Contacting local emergency response services
- Assessing the severity of the incident
- Accounting for all staff and briefing them accordingly

A sample immediate response checklist can be found in Appendix G.

Evacuation procedures

Evacuation procedures should be in place that clearly details how occupants, including staff and visitors, should be vacated from the premises following an incident. These procedures should be posted in prominent locations throughout the premises.

These procedures could include the following:

- Actions that need to be taken by occupants in the event of an evacuation
- A site plan or map of the facility that includes evacuation routes and the location of the emergency exits
- Establishing strategies for supporting individuals with disabilities
- Selecting and specifying the location of a meeting place, a muster point, away from the building

Staff responsibilities

Businesses should assemble a team of personnel who will be engaged in incident response and outline their respective responsibilities. This starts with the selection of a team leader who, preferably, is a prominent member of the organization (e.g., owner) and has prior incident management experience. This individual should ensure that their team of support staff are qualified for their roles during an incident.

Each member of the incident response team should be provided with a summary of their roles and responsibilities. A template summarizing roles and responsibilities can be found in Appendix H.

Contact documents

Organizations should develop and post a list of staff contacts and external contacts.

Contact list templates can be found in Appendix I and Appendix J.

Element five: Business recovery plan

Business recovery is the return to operations following an incident or disaster. This section describes how an organization can effectively recover from an incident that affects their business operations, with an aim to reduce recovery time and minimize losses.

A business recovery plan consists of a pre-established framework that involves the following:

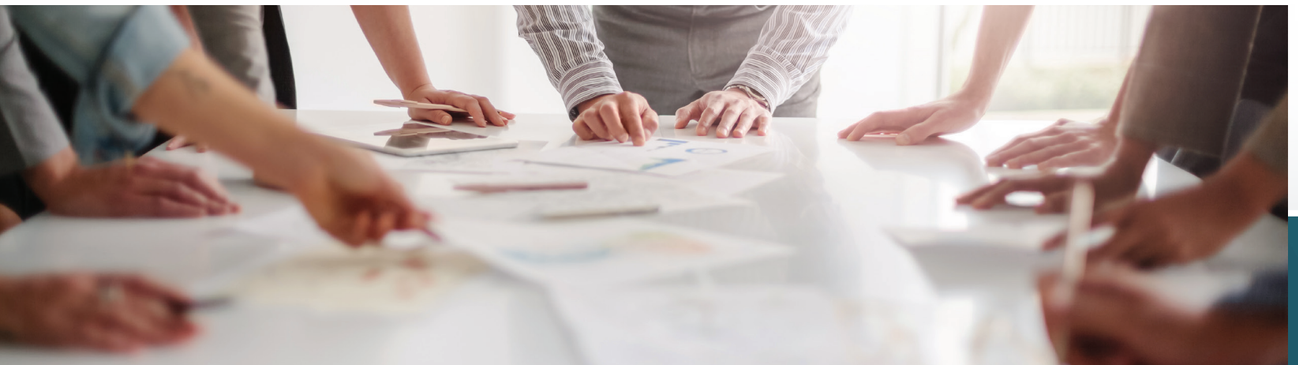
1. Establishing deadlines to reinstate essential business functions
2. Strategies to recover from a range of incidents
3. An outline of essential resources, equipment, and personnel needed
4. Checklist to verify that all necessary actions have been completed

It is recommended that a team be assembled who will be responsible for business recovery activities. The team should consist of internal members, such as a leader who sets clear goals for all essential business operations, external individuals who provide guidance and assistance through professional services, or some combination of both. It is recommended that the team undergo training or seek guidance on incident recovery procedures and their respective responsibilities as part of the planning process.

The business recovery team should establish communication with all staff and key external stakeholders (i.e., major clients, suppliers, etc.) following an incident, preferably within 24 hours. In addition, it is crucial to maintain regular communication with these parties for the duration of the recovery process, updating them on the recovery status or progress and any actions implemented to restore operations.

Templates establishing this framework can be found in the Appendix of this report, including:

- Recovery checklist (Appendix K)
- Recovery plan template (Appendix L)
- Supplier information (Appendix M)
- Customer information (Appendix N)
- Equipment and machinery list (Appendix O)



Element six: Evaluation and maintenance

Business continuity plans require ongoing evaluation and maintenance to keep pace with changes to facilities, operations, hazards, regulations, personnel, funding, and resources. Practical examples of why this is necessary include the following:

- When a building is renovated or replaced entirely, travel paths to exits or evacuation assembly areas may change.
- When processes are added or there are modifications to existing processes, new hazards may be introduced.
- Changes to codes and regulations, as our understanding of hazards and effective mitigation strategies can evolve over time.
- Staff turnover within the organization. Numerous individuals are required to contribute to the program and, if they were to depart, new individuals must be appointed and trained to ensure the program's continued existence.
- Changes in funding or management's commitment to the program will also require changes to the program.
- Changes in the availability and capacity of external resources must be assessed and the plan updated, as required.

Business continuity plans should be reviewed every six to twelve months. In the event of any major changes to the business such as those described above, more frequent reviews may be necessary. Reviews should be documented accordingly, including the review date, why the review took place, and a description of any changes made to the plan.

A review schedule template has been included in Appendix P.

Conclusion

A well-prepared and maintained business continuity plan is crucial for safeguarding the continuity of business operations. Business continuity planning is not a universal process and should be customized to the organization and its unique characteristics. A successful program begins with management commitment, direction, and support. From there, a series of sequential tasks should be conducted, including:

- Assessing possible risks and threats to the organization, along with strategies to avoid or minimize their impact.
- Identifying and ranking essential functions within the business, as well as understanding the consequences of any interruptions to those functions.
- Outlining response procedures to a critical incident that results in a disruption to business operations.
- Developing plans and implementing measures to facilitate the business's recovery from a disruption.
- Implementing procedures for reviewing and maintaining the business continuity plan to ensure it remains current.

By following this process, businesses can better prepare for, respond to, and recover from incidents, thus reducing the likelihood of prolonged disruptions to business operations.

References

NFPA Fire Protection Handbook, Section 1.8. – Emergency Management and Business Continuity

NFPA 1600 – Standard on Continuity, Emergency, and Crisis Management

Business Development Bank of Canada – Business continuity plan in 8 steps
https://www.bdc.ca/en/articles-tools/business-strategy-planning/manage-business/business-continuity-8-steps-building-plan

City of Toronto – Guide to Business Continuity Planning
https://www.toronto.ca/wp-content/uploads/2018/01/94bf-Guide-to-Business-Continuity-Planning.compressed.pdf

FEMA/Ready.gov – Business Continuity Planning
https://www.ready.gov/business/emergency-plans/continuity-planning

Queensland Government – Business Continuity Planning
https://www.business.qld.gov.au/running-business/risk/continuity-plan

Insurance Institute for Business & Home Safety, Open for Business-EZ Toolkit
https://ibhs1.wpenginepowered.com/wp-content/uploads/OFB-EZ-Toolkit-IBHS.pdf

Appendix A: Distribution List

Distribution List				
Copy no.	**Name**	**Position**	**Phone no.**	**Email Address**

Appendix B: Risk Management Plan

Risk Management Plan				
Risk description	**Likelihood**	**Impact**	**Risk level**	**Preventive actions**

Appendix C: Summary of Insurance Coverage

Summary of Insurance Coverage				
Insurance type	**Coverage**	**Insurance company**	**Policy no.**	**Policy period**

Appendix D: Data Backup Protocols

Data Backup Protocols				
Data to be backed up	**Backup frequency**	**Backup mechanism**	**Person responsible**	**Backup procedures**

Click here or visit **echeloninsurance.ca/riskintel** to download a Business Continuity Toolkit containing printable business continuity documents listed in this appendix.

Appendix E: Business Activity Questionnaire

Business Activity Questionnaire			
Function/department name			
Description of activities			
Provide details on the internal dependencies of function			
Staffing		IT applications	
Machinery/equipment		Support services	
Facilities		Other internal dependencies	
Provide details on the external dependencies of function			
Suppliers (i.e., raw materials, etc.)			
Third-party subcontractors			
Clients (particularly if operations are contingent on relatively few clients)			
Other external dependencies			
Describe the financial ramifications if this function could not be performed for a prolonged period (e.g., loss of revenue, increased costs, fines/penalties, etc.).			
Describe the non-financial ramifications if this function could not be performed for a prolonged period (e.g., staff resignations, damage to reputation, etc.).			
For what maximum amount of time could this business activity be unavailable before the losses would occur?			
Are there seasonal impacts or other factors that might affect operations at different points during the year?			
What expenses (beyond normal budgets) might need to be incurred by continuing operations during and after a disruption?			
Additional comments:			

Appendix F: Business Impact Analysis

Business Impact Analysis				
Critical business activity	**Description**	**Priority**	**Impact of loss**	**Recovery time objective**

Appendix G: Immediate Response Checklist

Immediate Response Checklist		
	Actions taken	**Details**
	Business continuity plan activated	
	Assessed severity of incident	
	Premises evacuated (if necessary)	
	Staff located and accounted for	
	Personnel briefed on incident	
	Contacted emergency services	
	Initiated event log	
	Activated incident response team, roles, and responsibilities	
	Assessed damage	
	Identified critical activities that have been disrupted	
	Contacted key internal and external stakeholders	
	Appointed organization spokesperson	
	Initiated media/public relations response	

Appendix H: Roles and Responsibilities

Roles and Responsibilities				
Role	**Designated individual**		**Alternate / backup**	
	Name		Name	
	Phone no.		Phone no.	
Responsibilities:				
Role	**Designated individual**		**Alternate / backup**	
	Name		Name	
	Phone no.		Phone no.	
Responsibilities:				

Appendix I: Staff Contact List

Staff Contact List					
Name	**Position**	**Phone no.**		**Email address**	
		Business	Personal	Business	Personal

Appendix J: External Contact List

External Contact List	
Contact Type	**Phone no.**
Police department	
Fire department	
Emergency medical services	
Hospital	
Security monitoring company	
Insurance company	
Electricity provider	
Natural gas provider	
Water supply provider	
Sewer company	
Telecommunications provider	

Appendix K: Recovery Checklist

Recovery Checklist	
Incident details	
	Record details of any injured people, including staff, customers, and other members of the public
	Photograph or record damage to buildings, equipment, company vehicles, and stock
	Record impact on your business functions
	Record any anticipated damage to your business's reputation
Communication to staff	
	Conduct a critical incident debrief within 24 hours following an incident
	Hold a meeting with your staff to ask them about their reactions to the crisis
	Inform staff about the recovery process and schedule regular updates
	Keep staff informed about what is expected of them
	Advise staff whether they should return to work the next day
Contact insurer	
	Contact your insurance company to initiate the claim filing process, if necessary
	Photograph or record damage to your premises, fixtures, vehicles, stock, customer records, and equipment to support claims
Review of recovery process	
	Record what you have learned from this crisis, including what went well and what did not
	Consider and record key lessons learned
	Review and update your recovery plan

Appendix L: Recovery Plan

Recovery Plan					
Critical business activity	Recovery actions	Resource requirements	Recovery time objective	Responsible personnel	Date completed

Appendix M: Supplier Information

Supplier Information						
Name	Status		Address	Phone no.	Email address	Main contact
	Current	Backup				

Appendix N: Customer Information

Customer Information				
Name	Address	Phone no.	Email address	Main contact

Appendix O: Critical Equipment and Machinery

Critical Equipment and Machinery					
Make	Model	Function	Primary supplier	Alternate supplier	Order time for replacement

Appendix P: Review Schedule

Review Schedule		
Review date	Reason for review	Modifications made

echeloninsurance.ca

AM BEST A- EXCELLENT Financial Strength Rating

echelon® Insurance