Guide to Developing a Business Continuity and Disaster Recovery Plan

*intended for Agency Executive Officers*

****

© Organisme d’autoréglementation du courtage immobilier du Québec – All rights reserved.

Table of Contents

[Implementing a Contingency Plan 4](#_Toc153802073)

[Detailed Explanations − Step 1 : Risk Assessment 5](#_Toc153802074)

[**1.** **Identify the Internal and External Risks** 5](#_Toc153802075)

[**2.** **Assess the Potential Impact** 5](#_Toc153802076)

[**3.** **Identify the Critical Assets** 5](#_Toc153802077)

[**4.** **Analyze the Existing Measures** 5](#_Toc153802078)

[**5.** **Update Annually** 5](#_Toc153802079)

[Detailed Explanations − Step 2 : Determining the Priorities 6](#_Toc153802080)

[**1.** **Building an Inventory of Activities** 6](#_Toc153802081)

[**2.** **Impact Assessment** 6](#_Toc153802082)

[**3.** **Ranking by Order of Importance** 6](#_Toc153802083)

[**4.** **Identifying Dependencies** 6](#_Toc153802084)

[**5.** **Validating with Stakeholders** 6](#_Toc153802085)

[Detailed Explanations − Step 3 : Backup and Recovery Plan 7](#_Toc153802086)

[**1.** **Identifying Critical Assets** 7](#_Toc153802087)

[**2.** **Regular Backups** 7](#_Toc153802088)

[**3.** **Recovery of Systems** 7](#_Toc153802089)

[**4.** **Storage of Critical Data** 7](#_Toc153802090)

[**5.** **Assessment of Suppliers and Partners** 7](#_Toc153802091)

[**6.** **Backup and Recovery Tests** 7](#_Toc153802092)

[**7.** **Detailed Documentation** 7](#_Toc153802093)

[Detailed Explanations − Step 4 : Emergency Response Plan 8](#_Toc153802094)

[**1.** **Specific Emergency Scenarios** 8](#_Toc153802095)

[**2.** **Chain of Command and Assigned Roles** 8](#_Toc153802096)

[**3.** **Internal and External Communication** 8](#_Toc153802097)

[**4.** **Training and Awareness Raising** 8](#_Toc153802098)

[Detailed Explanations − Step 5 : Updating the Plan 9](#_Toc153802099)

[**1.** **Revision and Updating** 9](#_Toc153802100)

[**2.** **Ongoing Awareness Raising** 9](#_Toc153802101)

[Appendix 1 – Integrated Risk Management Assessment Process 10](#_Toc153802102)

[Appendix 2 – Identification of Essential Functions and Services by Level of Importance 14](#_Toc153802103)

[Appendix 2.1 – Essential Functions/Services Ranking 15](#_Toc153802104)

[Appendix 3 – Action Plan Template for Maintaining an Essential Service or Activity 16](#_Toc153802105)

[Appendix 3.1 – Decision-Making Diagram – Exercise and Simulation 17](#_Toc153802106)

## **Implementing a Contingency Plan**

A business continuity plan (BCP) is an essential tool for ensuring the resiliency of a business when unforeseen events occur such as natural disasters, technical failures, cyberattacks, pandemics or other emergencies. A team should be clearly assigned the responsibility for preparing for emergencies.

It is advisable to entrust the responsibility for managing the planning process to a single individual and ensure that this “emergency manager” has the power to get the job done.

Here is a simple five-step business continuity plan.

**[Step 1 : Risk Assessment](#_Explication_détaillée_étape_4)**

Identify the potential risks to your business. This may include internal risks such as system outages, equipment failures, human errors, as well as external risks such as natural disasters, social conflicts, etc.

**[Step 2 : Determining the Priorities](#_Explication_détaillée_étape_1)**

Rank your business’s functions and processes by their importance and their impact on operations. Identify the critical activities that must be maintained as a priority to allow the business to survive and continue to function.

**[Step 3 : Backup and Recovery Plan](#_Explication_détaillée_étape)**

Put in place regular backup measures for your critical data and make sure that you have systems that can take over for the essential elements of your work.

**[Step 4 : Emergency Action Plan](#_Explication_détaillée_étape_2)**

Develop a detailed action plan to deal with various emergency scenarios. Make sure that your personnel are well acquainted with this plan and train regularly on dealing with them. Also include guidelines on communication in the event of an incident, internally and with external stakeholders.

**[Step 5 : Updating](#_Explication_détaillée_étape_3)**

Keep in mind that the business continuity plan should be easily accessible to all employees concerned and should be updated and improved to reflect the changes in your business and its environment.

## **Detailed Explanations − Step 1 : Risk Assessment**

The risk assessment step is crucial, as it allows you to identify the potential threats to your business. It helps you understand your business’s specific vulnerabilities and take preventive measures to mitigate them. Here is how to proceed.

### **Identify the Internal and External Risks**

* + The internal risks come from your business. They may include system outages, human errors, management issues, equipment failures, etc.
	+ The external risks come from factors external to your business. These may include natural disasters (hurricanes, earthquakes, floods), social conflicts, cyberattacks, supply problems, pandemics, etc.

### **Assess the Potential Impact**

* + For each risk identified, assess the probability of its occurrence and its potential impact on your business’s activities. What are the possible consequences in terms of financial losses, property damage, downtime, reputation, etc.? Rank the risks in terms of their severity and their probability of occurring.

### **Identify the Critical Assets**

* + Identify the assets, processes or services that are essential to the operation of your business. These may include customer data, vital computer applications, key personnel skills, special installations, etc. Focus on the elements the loss or unavailability of which would have a significant impact on the continuity of your operations.

### **Analyze the Existing Measures**

* + Examine the security and prevention measures already in place in your business to deal with certain risks. These include the backup systems, emergency plans, security policies, etc. Assess the effectiveness of these measures and identify the potential gaps.

### **Update Annually**

* + Update your plan annually to ensure that it is properly tailored to your operations and current risks. Based on the identified risks and their potential impact, create realistic emergency scenarios.

([See Appendix 1](#_Annexe_2_–))

## **Detailed Explanations − Step 2 : Determining the Priorities**

The priority determination step consists of identifying and ranking your business’s functions, processes and activities by their importance and their impact on the continuity of your operations. This will allow you to focus your resources on the critical elements in the event of a crisis, which will help you to maintain your essential activities regardless of the disruptions.

Here is how to proceed.

### **Building an Inventory of Activities**

* + Start by building a complete inventory of your business’s activities. This includes the operational processes, client services, support functions, etc. Be thorough so no important elements are overlooked.

### **Impact Assessment**

* + For every activity identified, assess its impact on the business as a whole in the event it is disrupted. Ask yourself the following questions: What are the consequences if this activity cannot be carried out for a certain period of time? What are the domino effects on other activities?

### **Ranking by Order of Importance**

* + Next, rank the activities according to their importance for business continuity. Identify the activities that are essential for keeping the business operational and those that are less critical. You can use a priority scale to facilitate this ranking (for example, high, medium, low).

### **Identifying Dependencies**

* + Identify the dependencies between the various activities. Some processes may be interdependent, which means that the disrupting of one process may have repercussions on others. By understanding these links, you will be better able to anticipate the domino effects during a crisis.

### **Validating with Stakeholders**

* + Involve the business’s key stakeholders in this ranking process. These may include the officers, department managers and other individuals with thorough knowledge of the operations. Their participation will help you get different perspectives and ensure better adherence to the business continuity plan.

Once this step is done, you will have an overview of your business’s critical activities and their interdependence. This will allow you to focus your efforts and your resources on the backing up and protecting of the essential elements in the event of a crisis. The ranking by order of priority will guide you throughout the development of the business continuity plan by helping you define specific response strategies for each category of priorities.

([See Appendix 2](#_Annexe_3_–) and [Appendix 2.1](#_Annexe_3.1_–))

## **Detailed Explanations − Step 3 : Backup and Recovery Plan**

The backup and recovery plan consists of implementing measures for protecting your business’s critical assets and ensuring they are continuously accessible and available, even in the event of a crisis. These measures are aimed at reducing downtime, minimizing losses and allowing your business to continue to function as normally as possible in spite of the disruptions.

Here is how to proceed.

### **Identifying Critical Assets**

* + Use the information gathered in step 2 to identify the assets, processes and services that were ranked as essential for business continuity. These are the elements that you must prioritize in your backup and recovery plan.

### **Regular Backups**

* + Set up a regular backup system for the critical systems and data. Make sure that the backups are done frequently, and that the data is stored in a secure location away from the main workplace.

### **Recovery of Systems**

* + Consider having redundant systems in place for the essential systems. This means having disaster recovery equipment ready to take over in the event a main system fails. For example, disaster recovery servers or disaster recovery data centres.

### **Storage of Critical Data**

* + Ensure that the critical data is stored in a secure manner and accessible when needed. This may include using secure cloud storage or external hard disks kept off site.

### **Assessment of Suppliers and Partners**

* + If your business depends on suppliers or partners for certain critical products or services, assess their own business continuity plan. Make sure they have measures in place to deal with potential disruptions to reduce the risks for your business.

### **Backup and Recovery Tests**

* + Regularly test your backup and recovery systems to make sure they are working properly. This will allow you to detect and correct potential problems before they turn into critical situations.

### **Detailed Documentation**

* + Make sure that all backup and recovery measures are carefully documented in your business continuity plan. This will facilitate implementing actions during a crisis and will help your team members to know what to do.

By implementing an effective backup and recovery plan, you can mitigate the risks related to service interruptions and ensure operations resume quickly in the event of a crisis. Remember to keep your plan up to date and reassess it regularly to reflect the changes in your business, in technology and in the external environment.

## **Detailed Explanations − Step 4 : Emergency Response Plan**

The aim of the emergency action plan step is to develop a set of specific measures to be taken in the event of an incident or crisis. These measures are designed to enable your business to react rapidly, effectively and in a coordinated manner when a disruptive event occurs.

Here is how to proceed.

### **Specific Emergency Scenarios**

* + Using the information gathered during the risk assessment step, identify the specific emergency scenarios that your business might face. The scenarios should be realistic and take into consideration the most likely and most serious threats.

### **Chain of Command and Assigned Roles**

* + Clearly define the chain of command for emergencies. Appoint individuals in charge of each key role and clarify each person’s responsibilities. Ensure that all team members know who to contact when a crisis occurs.

### **Internal and External Communication**

* + Set up an emergency communication plan. This includes guidelines on how to communicate rapidly and effectively with employees, internal and external stakeholders (clients, suppliers, partners, etc.). Transparent and regular communication are essential for managing a crisis effectively.

### **Training and Awareness Raising**

* + Ensure that all personnel concerned are trained on the specific emergency measures and procedures of the business continuity plan. Regularly increase your team’s awareness of the emergency protocols to ensure that they are properly prepared to act when needed.

The emergency action plan is essential for ensuring that your business is ready to deal with specific emergency scenarios. By having clear and well-defined procedures, you will be able to reduce downtime, minimize losses and protect the continuity of your operations when crises occur. Don’t forget to keep your plan up to date and review it regularly based on organizational changes and new identified risks.

(See [Appendix 3](#_Annexe_4_–) and [Appendix 3.1](#_Annexe_4.1_–))

## **Detailed Explanations − Step 5 : Updating the Plan**

The plan updating step is essential for ensuring that your business continuity plan is operational, effective and adapted to the changes in your business and its environment. This step consists of checking the appropriateness and feasibility of the measures in the plan, identifying the weaknesses and making the necessary adjustments.

Here is how to proceed.

### **Revision and Updating**

* + Update your business continuity plan to improve the aspects that have not worked as expected and strengthen the prevention and response measures. Make sure that the changes made are clearly communicated to all team members concerned.

### **Ongoing Awareness Raising**

* + Regularly increase the awareness of all employees of the importance of the business continuity plan and testing. Make sure that every staff member understands their role in implementing the BCP and knows how to act when an emergency occurs.

The updating process is iterative, which means that it should be repeated regularly to ensure that your business continuity plan remains relevant and effective with respect to the changing needs and risks of your business. By keeping your plan up to date, you increase the chances of your business succeeding in overcoming crises and maintaining the continuity of its essential operations.

## **Appendix 1 – Integrated Risk Management Assessment Process**

**Step 1**

Assess the **probability of occurrence** of each risk using a scale. Bear in mind that the probability of occurrence is related to the frequency of the risk.

To assist you, see the probability of occurrence of risk reference table (scale):

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident occurs​** | **Assessment guide​** | **Likelihood of realization of the risk​** | **Rating​** |
| Regularly​ | Currently materializing, or will materialize more than once in the next year​ | Very high​ | 5​ |
| Occasionally​ | Will likely materialize in the short term (within one or two years)​ | High​ | 4​ |
| More than once​ | Moderate likelihood of materialization estimated at once every two years​ | Moderate​ | 3​ |
| Once ​ | Limited likelihood of materialization estimated at once every three to five years​ | Low​ | 2​ |
| Rarely or never​ | Will materialize exceptionally only​ | Unlikely​ | 1​ |

**Step 2**

Assess the **impact of the risk** using a scale. You must estimate what would be the magnitude of the potential negative effects of the occurrence of this risk were it to occur.

To assist you, here is a reference table (scale) for assessing the potential impact to allow you to make a fair and objective assessment of each of the risks or events analysed:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Impact​** | **Financial​****(Adverse ​variation of)​** | **Clients ​****(decreased satisfaction)​** | **Notoriety, image, reputation​** | **Achieving business goals​** | **Rating​** |
| Very high​ | more than **20%** of your income ​ | of **more than 10%**​ | Negative, repetitive and widespread media coverage​ | Affects the achievement of your **overall** goals​ | 5​ |
| High​ | **10%** of your income​ | from **7 to 9.9%**​ | Widespread negative media coverage, but not recurring​ | Affects the achievement of **many** of your goals ​ | 4​ |
| Moderate​ | **5%** of your income​ | from **4 to 6.9%**​ | Significant criticism from members, citizens, or partners, but little media coverage​ | Affects the achievement of **one** goal ​ | 3​ |
| Low​ | **3%** of your income​ | from **2 to 3.9%**​ | Significant isolated criticism to one or a limited number of members, citizens, or partners.​ | Affects the achievement of **sub-goals**​ | 2​ |
| Very low​ | less than **1%** of your income​ | less than **2%**​ | No significant criticism​ | May **slightly** affect the achievement of sub-goals​ | 1​ |

**Step 3**

**Assess the mitigation measures (controls).** The nature of these mitigation or control measures may include, in particular, insurance coverage, monitoring reports, documented processes, guidelines, policies and other control mechanisms.

To assess the mitigation measures as well as the quality control, a grading scale is used and considers the following two criteria: the **effectiveness of the control** and its **degree of application**.

This scale makes it possible to determine whether the existing controls allow maintaining the risk at an acceptable level for the organization and identify opportunities where the controls could be improved. The following scale allows you to **assess the mitigation measures and the quality of the control**.

|  |  |  |  |
| --- | --- | --- | --- |
| **Measure assessment​** | **Quality of control ​** | **Mitigation factor​** | **Need for improvement​** |
| Appropriate and well implemented measures. ​Reduce risk to an acceptable level.​ | Excellent​ | 80%​ | No​ |
| Sufficient mitigation measures.​Could be improved.​ | Good ​ | 60%​ | Low​ |
| Mitigation measures implemented. ​Reduce risk partially.​ | Fair ​ | 30%​ | Moderate​ |
| Mitigation measures implemented. ​Insufficient to reduce risk.​ | Low​ | 10%​ | High​ |
| Measures in place do not mitigate risk or do not exist.​ | None​ | 0%​ | Urgent​ |

**Mitigation Measures**

Now, let’s take out our calculators!

First, the **inherent risk** must be calculated. The inherent risk represents the risk incurred without taking the existing controls into consideration.

So, the **probability rating** is multiplied by the **impact rating** = inherent risk.

Ex.: You estimate the probability of occurrence of the situation to be **high** (rating 4) and its impact to be **moderate** (rating 3).

The inherent risk will therefore be 12 (4 X 3).

If you implement mitigation or control measures, how do you manage your risk? This is called calculating the residual risk. The residual risk is “what impact remains” once you have implemented mitigation measures. An example of **residual risk**: the seatbelt in cars.

Before people were obliged to wear seatbelts, many died on the roads every year. The legally mandated wearing of a seatbelt has resulted in a significant reduction in the number of deaths and injuries. However, injuries and deaths in accidents are still occurring, even with the wearing of seatbelts. It can therefore be concluded that seatbelts succeeded in **mitigating** the risk, but some risk still remains and this is the **residual** risk. This is the portion of the risk that cannot be eliminated. It is this residual risk therefore that is your true risk.

Now, let’s get back to our calculation. We had estimated that the probability of occurrence of a situation is high (rating 4) and that its impact would be moderate (rating 3). Therefore, 4 X 3 = 12, this is when the third scale comes into play. If you believe that your measures are **fair (partial), that is 30 %.**

Here is the method for calculating the residual risk :

* [Inherent risk] - [ [Inherent risk] X [Mitigation factor %] ] = [Residual risk]
* [4 X 3 = 12] – [12 X 30 % = 3.6] = [8.4 residual risk]
* Note : 3.6 is obtained by multiplying 12 (inherent risk) by 30 % (attenuation measure).
* Therefore the residual risk = 8.4.

The residual risk level rating is **moderate** according to the following scale: 

## **Appendix 2 –** **Identification of Essential Functions and Services by Level of Importance**

##### **Service/Business Unit: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Essential Functions and Services and Level of Importance**  | **Current Number of Employees Who Provide Services**  | **Number of Remaining Employees If Absenteeism Rate of 35% Is Applied**  | **Degree of Risk (High, Medium, Low)**  | **Possibility of Working from Home****(Yes or No?)** | **Action Plan Implemented for Essential Service (Yes or No?)**  |
|  |  |  |  |  |  |
| **A.** |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **B.** |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **C.** |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

***Level of importance:***

1. *Crucial service. Cannot be interrupted or suspended.*
2. *Functions/services that can be suspended for a short period of time (for a month, for example).*
3. *Functions/services that can be suspended for a long period of time.*

## **Appendix 2.1 – Essential Functions/Services Ranking**

##### Service/Business Unit : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Areas Affected and Degree of Influence***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Level of Importance of the Essential Service**  | **Finance** | **Employees** | **Clients** | **Supplier/****Business Partners**  | **Legal/****Regulatory** | **Public/****Community** | **Other** | **Total Score (Prioritize and Draw up the Services in** **Appendix 2)** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

***1 = Weak negative influence 10 = Strong negative influence***

## **Appendix** **3 – Action Plan Template for Maintaining an Essential Service or Activity**

|  |  |
| --- | --- |
| **Service/Business Unit:** |  |
| **Essential service:**(Identify and provide a brief description) |  |
| **Individual/position responsible** for implementing a specific action plan:  | (Name) | (Phone numbers) | (Email addresses) |
| **Backup individual/position responsible** for implementing a specific action plan:  | (Name) | (Phone numbers) | (Email addresses) |
| **Agency impact issues:**(if any) |  |
| **Action plan:**(including the notification methods, communication strategy, employee reassignment plans, use of other service sectors, any change in scope of service delivery process, monitoring and report production requirements, etc.)  |  |
| **Human resource needs:**(List the needs and provide the contact details of the resource persons – staffing, equipment, subcontracting services, etc.)  |  |  |  |

## **Appendix 3.1 – Decision-Making Diagram – Exercise and Simulation**

 