

BEST PRACTICES

Business Continuity Program Best Practices Checklist

A business continuity program is an important component of an organization's risk management strategy. Creating a business continuity program involves:

1. Identifying risks that can affect and disrupt the company's operations.
2. Planning alternative measures to ensure personnel and assets are protected and are able to function if a disaster occurs.

The checklist below outlines the core components of every business continuity program. Use this checklist to start defining your program and/or self-evaluate your program against best practices.

CHECKLIST

IDENTIFY AND CATALOG PROCESSES CRITICAL TO BUSINESS OPERATIONS

Identify the processes that are critical to keeping your business running and the key components of those processes. Use the following when evaluating key components:

- » Who is involved in these processes? List departments and individuals.
- » What resources are critical to these processes? List these resources and what parts of the process they support.
- » What vendors and/or external services are involved in these processes?
- » What IT assets support these processes?
- » Are any of the people, resources, vendors or assets dependent upon another? Identify and catalog any dependencies.

CONDUCT RISK ASSESSMENTS

Assess your critical processes, resources, vendors and IT assets for risk to better understand the potential impacts of a disruption. When conducting assessments, ensure the following risks are accounted for:

- » Impact on customer service
- » Non-compliance with government regulations or contractual obligations
- » Increased operating costs
- » Penalties
- » Loss of shareholder confidence
- » Loss of competitive edge and/or reputation

IDENTIFY RECOVERY OBJECTIVES

Determine how quickly your processes must be back up and running and how much data you can afford to lose.

Calculate Recovery Time Objectives (RTO)

Recovery time objective (RTO) is the targeted duration of time and service level a business process, service or information is restored after a disruption. Below are the RTO best practices categories and timeframes:

- » Life & Safety - within 24 hours
- » Production and Client Support – 24 to 48 hours
- » Client Relations and Account Management – within 48 hours
- » Internal Support, Sales, Marketing, Finance – within one week
- » Business Enhancement, Audit – within one month

Calculate Recovery Point Objectives (RPO)

Recovery point objective is the maximum amount of data you can afford to lose since your last backup. Determine how frequently your backups take place and measure data loss in hours. Below are the RPO best practice categories and time frames:

- » Criticality Level 1 – 0-30 minutes
- » Criticality Level 2 – 1 hour
- » Criticality Level 3 – 4 hours
- » Criticality Level 4 – 24 hours
- » Criticality Level 5 – 48 hours

CONDUCT A BUSINESS IMPACT ANALYSIS (BIA)

A business impact analysis quantifies the potential financial impacts of an interruption to critical business operations. Use the below table to extrapolate how much revenue per hour is lost during a disruption.

Hour	Revenue Lost	Non-Revenue Losses	Other Impact Measure
1 Hour			
2 Hours			
4 Hours			
8 Hours			
2 Days			
3 Days			
5 Days			

Your BIA plans will help create the plan priorities. However, that is not the sole determination. Use the information collected to set your RTO priorities listed in the above section.

CREATE BUSINESS CONTINUITY PLANS

Design plans to address risks in critical processes before, during and after a disruption. Leverage the BIA to prioritize what plans to create first (the bigger the impact, the higher the priority). Create the below plans for each process.

- » **Response plan** – a plan that ensures critical processes are running during the disruption.
- » **Recovery plan** – a plan that outlines steps to recover critical processes from the disruption.
- » **Restoration plan** – a plan that details how the business can resume normal operations following recovery of critical processes.

In addition to the BIA, use RTO and RPO to establish plan priorities.

TEST PLANS THROUGH SIMULATIONS

Once plans are developed, run them through simulations to test their effectiveness.

Tabletop Exercises

Simulate the plan's scenario and review actions with key participants in a low-stress environment to identify ineffective, outdated or missing processes, personnel and assets. It also helps to align all parties involved on what should happen if this disruption occurred. Discuss the following when reviewing the plan:

- » Who owns the exercise?
- » What is the situation for the exercise?
- » What items do you need to take with you in case of an evacuation?
- » What documents are vital to continuing your operation that you should consider taking with you?
Can they be accessed remotely?
- » How do you account for employees not present?
- » Where do employees meet for roll call?
- » Where is your business continuity plan?
- » What is the time frame for resuming operations to avoid impact with customers?

'What if?' Scenario Testing

Similar to tabletop exercises, 'What if?' scenario testing alters one or two factors in the scenario. Leverage this test to identify plan gaps and dependencies to better gauge plan effectiveness.

COMMUNICATE PLANS

When program planning is complete, communicate business continuity plans and procedures to all parties involved. Having everyone aligned on what to do during a specific scenario will expedite continuity activities and make the process run smoother.

- » Share plans with plan participants
- » Share plans with key stakeholders and executives
- » Collaborate with third parties on business continuity plans
- » Save plans in a place that is accessible during a disturbance

This checklist is a starting point to building a best practices business continuity program. It is one part of a NAVEX Global toolkit that includes additional guidance and templates for a best practice business continuity program. To download the full toolkit, visit NAVEXGlobal.com/bctoolkit.

For more information on how NAVEX Global can assist with your business continuity program, contact us at info@Lockpath.com.

ABOUT NAVEX GLOBAL

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services. Trusted by more than 14,500 customers, our solutions help organizations manage risk, address complex regulatory compliance requirements and foster an ethical, highly productive workplace culture. For more information, visit www.navexglobal.com.