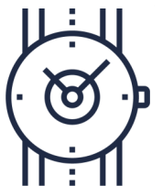
Developing Your IT Recovery Plan

JANUARY 2021| ITSAP.40.004

Unplanned outages, cyber attacks, and natural disasters can happen. If unprepared for these events, your organization may lose information or experience downtime, disrupting or halting critical business functions. **Regardless of the cause, unplanned down time is expensive and could have a lasting impact on your business**. To ensure continued operations with minimal down time, your organization should have an IT recovery plan as part of its overall business continuity approach. In this plan, your organization should identify critical data, applications, and processes and define how it will recover IT services that support business operations, products, and services.



Your recovery response should take many variables into consideration and should clearly identify and document what is to be recovered, by whom, when, and where in a detailed recovery plan. In general, there are two types of plans you should consider developing for your business—disaster recovery and incident response. These two plans take into consideration two major events that could cause an unplanned outage and require you to activate your recovery response.

1. **Disaster Recovery Plan:** The primary goal is to ensure business continuity during an unplanned outage or service disruption.
2. **Incident Response Plan:** The primary goal is to protect sensitive information during a security breach.

KNOW YOUR BUSINESS DISRUPTION TOLERANCE

For an effective recovery plan, you should tailor it to address the impact to your organization if an incident or a disaster occurs and the level of disruption that your organization is willing to accept. There are three key measures to consider in your plan: **maximum tolerable downtime**, **recovery point objective**, and **recovery time objective.**

Maximum tolerable downtime (MTD) The total length of time that a process can be unavailable without causing significant harm to your business.

Recovery point objective (RPO) The measurement of data loss that is tolerable to your organization.

Recovery time objective (RTO) The planned time and level of service needed to meet the system owner's minimum expectations

IDENTIFY YOUR CRITICAL BUSINESS FUNCTIONS, APPLICATIONS, AND DATA

To create an effective plan, you should identify your organization's critical data, applications, and functions. Critical information may include financial records, proprietary assets, and personal data. Critical applications are the systems running your key business functions and are imperative to your business. These are the systems you need to have restored immediately in the event of an unplanned outage, in order to have business continuity. To identify critical business functions, applications, and data, you should conduct a risk assessment to help you identify threats and vulnerabilities. Run through specific scenarios (e.g. cyber attack, significant power outage, or natural disaster) to help you identify key participants and stakeholders, address the significant risks, develop mitigation strategies, and identify the recovery time and effort.

You can conduct a business impact analysis (BIA) to predict how disruptions or incidents will harm your operations, business processes and systems, and finances. During your BIA, you should also assess the data you collect and the applications you use to determine their criticality and choose priorities for immediate recovery.

CREATE YOUR RECOVERY PLAN

1. Identify stakeholders including clients, vendors, business owners, systems owners, and managers.
2. Identify your response team members, as well as their roles and responsibilities.
3. Take inventory of all your hardware and software assets.
4. Identify and prioritize critical business functions, applications, and data.
5. Set clear recovery objectives.
6. Define backup and recovery strategies.
7. Test your plan.
8. Develop a communications plan to inform key stakeholders.
9. Develop a training program for employees to ensure everyone is aware of their roles, responsibilities, and order of operations during an unplanned outage.
10. Optionally, engage with your Managed Service Providers (MSPs) to identify areas in which they can assist you with your recovery efforts.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

CHOOSE YOUR RECOVERY STRATEGY

There are several options to consider when implementing your recovery strategy, but you should choose a recovery strategy that meets your business needs and security requirements.

HOT, WARM, OR COLD SITE

Hot: Back-up site with the same servers and equipment as your primary site. Functions the same as your primary site and is always kept running in case of downtime. Data synchronization occurs within minutes to hours, reducing the risk of data loss.

Warm: Back-up site with network connectivity and some equipment installed. Set up required to get the site to function at the full capacity of your primary site. Data synchronization occurs less frequently, which can result in some data loss.

Cold: Back-up site with little to no equipment. Requires more time and resources to set up and restore business operations. Data synchronization can be a difficult and lengthy process as servers need to be migrated from your primary site, resulting in a higher risk of data loss.

DISK MIRRORING

Disk mirroring replicates data on two or more disk hard drives. Disk mirroring automatically switches your critical data to a standby server or network when your main system experiences unplanned downtime. If you're unable to restore your systems, you can use the mirror copy. It is important the mirrored copy is backed up to a separate server or location that is unaffected by the outage.

STORAGE REPLICATION

Storage replication copies your data in real time from one location to another over a Storage Area Network (SAN), Local Area Network (LAN) or a Wide Area Network (WAN). Since it is done in real time, it is referred to as **synchronous replication.** You can also use **asynchronous replication**, which creates copies of data according to a defined schedule.

CLOUD VS. ON-PREMISES RECOVERY

With a cloud-based recovery platform, you can connect easily, from anywhere, with a variety of devices. You can back up your data frequently, and it can be less expensive than purchasing and maintaining an on-premise platform because you pay for the space you need as you need it. Using the cloud can also reduce or eliminate your need to have a separate offsite recovery site

TEST YOUR PLAN

Testing is critical. You can identify inconsistencies and address areas that need revision. Be sure to use a test environment to avoid business interruptions. Some example test strategies include:

Checklist: Read through and explain the steps of the recovery plan.

Walkthrough: Walk through steps without enacting them.

Simulation: Use a simulated incident or disaster to familiarize the recovery team with their roles and responsibilities.

Parallel test: Set up and test recovery systems to see if they can perform operations to support key processes. You keep your main systems in full production mode.

Cutover test: Your recovery systems are set up to assume all your business operations, and you disconnect primary systems. This type of test causes business interruptions, requiring additional pre-planning.

LEARN MORE

Visit the Cyber Centre website (**cyber.gc.ca**) to learn more about cyber security topics and find our entire collection of publications, including:

- *ITSAP.40.002 Tips for Backing Up Your Information*
- *ITSAP.00.005 Have You Been Hacked?*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*
- *ITSAP.10.116 Cyber Security Tips for Remote Work*
- *ITSAP.00.70 Supply Chain Security for Small and Medium- Sized Organizations*
- *ITSE.50.060 Benefits and Risks of Adopting Cloud-Based Services in Your Organization*
- *ITSAP.00.099 Ransomware: How to Prevent and Recover*
- *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services*

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada