

**Business Impact Analysis Procedure**

*A policy for resuming business operations after an adverse event*



Table of Contents

[Scope 3](#_Toc39670001)

[Responsibilities 3](#_Toc39670002)

[Procedure 3](#_Toc39670003)

[Recovery Point and Time Objectives 3](#_Toc39670004)

[Document Control 4](#_Toc39670005)

[About Prevalent 4](#_Toc39670006)

# Scope

This procedure defines how an organization identifies and assesses the critical assets required to resume business operations following an adverse event.

# Responsibilities

[Business Continuity Manager] is responsible for carrying out the business impact analysis (BIA), using the BIA toolset.

All [Business Functional Managers] are responsible for identifying services/activities/processes that fall within the scope of the business resilience program and providing the input for them to be analyzed in line with the requirements of this procedure.

# Procedure

[Organization Name] conducts a business impact analysis [annually] or whenever significant changes in the business continuity landscape occur, as determined by the [Business Continuity Manager].

A BIA tool will be used to capture the impact assessment. The process for completing an impact assessment is as follows:

1. Identify the location(s) of all offices/workspaces under scope of your resilience plan.
2. Identify all critical assets, including information systems, personnel and supporting services. These can be listed by department (where appropriate), type and specific resource.
3. Once all assets have been selected, identify the impact types and criteria relevant to the organization’s context. *(e.g., Pandemic threats will typically include threats including loss of staff, disruption due to reduction in supplier services or availability.)*
4. Finally, identify the critical owner or owners responsible for each identified asset. This will also be used in the resilience plan RACI matrix, which details core responsibilities for managing the assets and functions during an event.

# Recovery Point and Time Objectives

Recovery point objectives (RPO) and Recovery time objectives (RTO) should be identified as a means to determine clear parameters to help the organization recover from the threats and scenarios defined through the business impact assessment.

* **Recovery point objectives (RPOs)** are used to determine how much data or information can be lost before impacting business operations.
* **Recovery time objectives (RTOs)** are used to determine timelines required to ensure applications or systems must be restored following a disaster.

Determining the recovery point and time objectives will be dependent on the criticality of the assets identified, and timeliness required in getting them back to operational levels. *(For example, a mission critical system or asset may require an RTO of 1 hour if it holds client sensitive data and is under a service level agreement*, *versus a system or asset not under an SLA but still important as a supporting platform or application which may require an RTO of 24 hours.)*

One method of determining the RTO and RPO levels is to classify each identified asset based on a tiered approach.

[Organization Name] has created its RTO and RPO timescales against each of the identified assets, using a tiering process as follows:

* Tier 1: Mission critical assets – requiring an [RTO of xx and RPO of xx]
* Tier 2: Business-critical assets – requiring an [RTO of xx and RPO of xx]
* Tier 3: Non-critical assets – requiring an [RTO of xx and RPO of xx]

Review the rest of the impact criteria as stated in the worksheet and establish whether all or any of them within each of the high-level categories is relevant to how [Organization Name] uses the identified critical assets and recovery objectives in the testing of its resilience plan to ensure objectives defined are sufficient and achievable.

# Document Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Action** | **Comment** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors and suppliers throughout the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit [www.prevalent.net](http://www.prevalent.net).

© Prevalent, Inc. All rights reserved. The Prevalent name and logo are trademarks or registered trademarks of Prevalent, Inc. All other trademarks are the property of their respective owners. 06/23