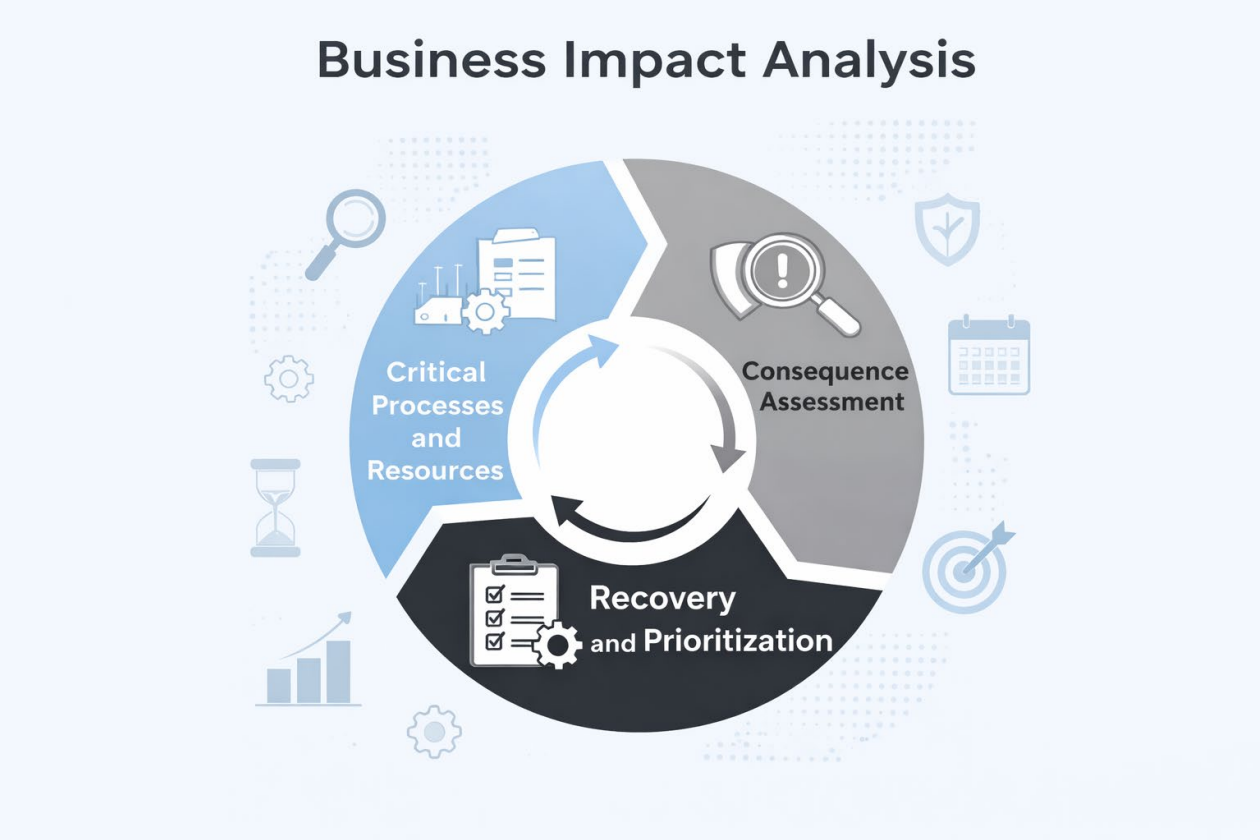
Business Impact Analysis (BIA)



The tool have been provided in connection with the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), funded by the Danish Industry Foundation. Publication date: 29.12.2025

The Business Impact Analysis

→A Business Impact Analysis (BIA) is a structured tool that can be used to assess and understand the potential consequences of disruptions to an organization's business-critical processes.

→The purpose is to identify which processes and functions are most vital to the organization's survival and continued operations, as well as how quickly they must be restored after an incident (e.g., system outages, cyberattacks, natural disasters, or other business interruptions).

→A BIA is often carried out using a **matrix**, where processes are systematically evaluated across several dimensions

Elements in a Business Impact Analysis

1. Identification of business-critical processes and activities:
   → Which processes are essential to maintaining the business?
   → Which supporting resources (personnel, IT systems, locations, suppliers) are necessary?
2. Assessment of impacts:
   → What would the consequences be if the process does not function for a shorter or longer period?
   → This can be measured financially (loss of revenue), operationally (production delays), or legally/regulatorily (fines, sanctions).
3. Prioritization and criticality:
   → How quickly must each process be restored to minimize damage?
   → Determination of the Maximum Tolerable Downtime (MTD), i.e. how long a process can be unavailable before the impact becomes unacceptable.
4. Identification of dependencies:
   → Which internal or external resources depend on each other?
   → For example, IT systems, supply chains, or key personnel.
5. Input to contingency planning:
   → The results from the BIA are used to develop Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP).

Procedure

1. Identify processes: List all business-critical and non-business-critical processes.
2. Collect data: Conduct interviews with process owners.
3. Assess impacts: What financial, legal, operational, or reputational losses arise from downtime?
4. Define Recovery Time Objective (RTO) / Recovery Point Objective (RPO): How quickly must the process be restored (RTO), and how much data loss can be tolerated (RPO)?
5. Prioritize processes: Establish a recovery priority.
6. Document and report: Summarize in a matrix or a BIA tool.

BIA template

Process	Responsible	Criticality (H, M, L)	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Impact of downtime	Dependent resources	Recovery priority

Notes: H = High, M = Medium and L = Low.
RTO = Recovery Time Objective (a measure of how quickly critical systems and processes must be up and running again after an incident).
RPO = Recovery Point Objective (the amount of data that a company can tolerate losing in the event of an unforeseen incident, without causing excessive harm to the company).

BIA template (example)

Process	Respon-sible	Criticality (H, M, L)	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Impact of downtime	Dependent resources	Recovery priority
Purchasing	Purchasing Manager	H	24 hours	6 hours	Production stoppage Loss of raw materials Relationships Breach of contract	ERP Supplier network Purchasers	1
Quality control	QA-responsible	H	12 hours	0 hours	Delivery of defective products Financial loss Customer trust Violation of legislation	QA-staff Measurement equipment	2
Sales	Sales Manager	M	48 hours	12 hours	Loss of revenue Customer dissatisfaction	CRM-system Salespersons	3

Notes: H = High, M = Medium and L = Low.
RTO = Recovery Time Objective (a measure of how quickly critical systems and processes must be up and running again after an incident).
RPO = Recovery Point Objective (the amount of data that a company can tolerate losing in the event of an unforeseen incident, without causing excessive harm to the company).