TLP:AMBER Limited distribution — recipients may share within their organisation on a need-to-know basis. Do not share externally without authorisation. TLP definitions: https://www.first.org/tlp/ | DK: https://www.cfcs.dk/da/handelser/traffic-light-protocol/

Defencia.dk

Business Impact Analysis
BIA

Document Title	Business Impact Analysis (BIA)	**Classification**	**TLP:AMBER**
Revision	*X.X*	**Date**	*[DATE]*
Responsible	*[Management Name]*	**System Owner**	*[Name]*

TEMPLATE GUIDANCE *This is a template. All placeholder text in grey italics or [brackets] must be replaced with organisation-specific content. Red guidance boxes are for the author and should be deleted before finalising. Consider GDPR obligations and NIS2 requirements where applicable.*

Version History

Version	Date	Author	Change Description
1.0			Initial version

1 — Introduction

1.1 Purpose of the BIA

TEMPLATE GUIDANCE *Describe why this BIA is being conducted. Link to organisational risk management framework, business continuity policy, or regulatory requirement (e.g. NIS2 Article 21, ISO 22301, DORA).*

[Describe the purpose of this Business Impact Analysis — what drove the need, what it will be used for, and how it supports continuity planning]

1.2 Scope of the BIA

TEMPLATE GUIDANCE *Define the boundaries clearly: which business units, systems, processes, and geographic locations are in scope. Explicitly state what is OUT of scope.*

In scope	*[List business units, systems, processes, and locations included]*
Out of scope	*[List what is explicitly excluded and why]*
Regulatory drivers	*[e.g. NIS2, GDPR, DORA, ISO 22301, sector-specific requirements]*

2 — Business Unit Information

TEMPLATE GUIDANCE *Complete one copy of this section per business unit in scope. Duplicate section 2 as needed.*

Business Unit Name	*[Full name of the business unit]*
Business Unit Manager	*[Name and contact information]*
Primary Contact	*[Name, role, phone, email]*
Backup Contact	*[Name, role, phone, email — if primary is unavailable]*
Location(s)	*[Physical and/or cloud locations where this unit operates]*
Key Personnel	*[List names and roles of staff critical to continuity of this unit]*
Staff count	*[Number of employees in this unit]*
GDPR relevance	*[Does this unit process personal data? If yes — what categories? Data flows?]*
NIS2 relevance	*[Is this unit part of an essential or important entity under NIS2? Which sector?]*

3 — Critical Functions and Processes

TEMPLATE GUIDANCE *List all business functions and processes that, if disrupted, would significantly impact the organisation. For each: describe what it does, who depends on it, what systems support it, and what happens if it fails. Add rows as needed.*

#	Function / Process	Description	Supporting Systems	Impact if Unavailable
1				
2				
3				
4				
5				

4 — Dependencies

4.1 Internal Dependencies

TEMPLATE GUIDANCE *List systems, teams, or processes within the organisation that this unit depends on. Note what would break if the dependency failed.*

[List internal dependencies: e.g. IT infrastructure, HR systems, finance systems, shared services. Note the impact of each failing.]

4.2 External Dependencies and Partners

TEMPLATE GUIDANCE *List all external suppliers, cloud providers, outsourced services, and critical partners. For each, assess the impact of disruption. This is especially important for NIS2 supply chain risk management obligations.*

Partner / Supplier	Service / Product Provided	Contact Information	Criticality (H/M/L)	Impact if Disrupted

5 — Impact Assessment

TEMPLATE GUIDANCE *Rate each impact dimension on a 1–5 scale (1 = negligible, 5 = catastrophic). Provide a likelihood rating as well. The combination of impact and likelihood informs prioritisation. Consider NIS2 Article 23 reporting thresholds for significant incidents.*

Area	Rating (1-5)	Likelihood	Notes / Description
Financial Impact			Revenue loss, extra expenses, fines, penalties, insurance claims
Operational Impact			Production delays, service degradation, efficiency loss, staff overtime
Customer / Stakeholder Impact			Service interruption, SLA breaches, customer dissatisfaction, reputational damage
Regulatory / Compliance Impact			GDPR breach notification, NIS2 reporting, sector regulator notification, legal exposure
Reputational Impact			Media coverage, brand damage, loss of market trust, partner confidence
Safety Impact			Physical safety of staff, public, or critical infrastructure (if applicable)

5.1 NIS2 & GDPR Specific Considerations

TEMPLATE GUIDANCE *If the organisation is subject to NIS2 (as an essential or important entity), document the impact thresholds that trigger notification obligations. For GDPR, document data breach risk to individuals.*

NIS2 classification	*[Essential entity / Important entity / Not applicable]*
NIS2 reporting threshold	*[At what impact level triggers 24-hour early warning to national authority?]*
GDPR personal data affected?	*[Yes / No. If yes: categories of data, number of individuals, risk level]*
GDPR 72-hour breach notification	*[Would this disruption trigger Article 33 notification to supervisory authority?]*

6 — Recovery Objectives (RTO & RPO)

TEMPLATE GUIDANCE

RTO = Recovery Time Objective: maximum acceptable time a function can be unavailable. RPO = Recovery Point Objective: maximum acceptable data loss, measured in time. These values must be agreed with business owners — IT cannot set them alone. Priority 1 = most critical.

Business Function / Process	RTO (hours)	RPO (hours)	Priority (1-5)	Owner

6.1 Maximum Tolerable Downtime (MTD)

TEMPLATE GUIDANCE

MTD is the absolute maximum time a function can be disrupted before the impact becomes unrecoverable. RTO must always be less than MTD.

[List the Maximum Tolerable Downtime for the most critical functions. Note: RTO < MTD always.]

7 — Recovery Strategies

7.1 Recovery of Critical Functions

TEMPLATE GUIDANCE

For each critical function, describe the recovery strategy. This should reference existing DR/BC plans where available. Strategies include: hot standby, warm standby, cold standby, manual workaround, outsource, or accept downtime.

[Describe recovery strategies per critical function. Reference DR plans, runbooks, or playbooks where they exist.]

7.2 Alternative Operating Procedures

TEMPLATE GUIDANCE

What manual or degraded-mode procedures can the organisation fall back on if primary systems are unavailable? Document these explicitly — staff need to know about them before an incident.

[Describe manual workarounds, paper-based procedures, or degraded-mode operations for critical functions during outage.]

7.3 Contingency Plans for Partner / Supplier Disruptions

Alternate suppliers / partners	*[List pre-identified backup suppliers for critical services]*
Legal / contractual safeguards	*[Reference SLAs, uptime guarantees, liability clauses, termination rights]*
Communication plan	*[Who contacts the partner? What is the escalation path? What information is shared?]*
Supply chain risk (NIS2)	*[Has a supply chain risk assessment been performed per NIS2 Article 21(2)(d)?]*

8 — Resource Requirements

TEMPLATE GUIDANCE *Document the resources required to execute recovery. This feeds into continuity planning budgets and resource pre-positioning.*

Resource Category	Current Availability	Additional Requirements / Gaps
Personnel		
Technology (hardware, software, data)		
Facilities		
Telecommunications		
Third-party services		
Other resources		

9 — Plan Development and Maintenance

TEMPLATE GUIDANCE *A BIA that is not maintained becomes unreliable and potentially misleading. NIS2 Article 21 requires regular testing and review of business continuity measures.*

Review frequency	*[Minimum: annually. After significant organisational change. After any significant incident.]*
Owner of maintenance	*[Name and role of the person responsible for keeping this document current]*
Trigger for out-of-cycle review	*[Merger/acquisition, major system change, new regulation, significant incident, supplier change]*
Testing schedule	*[How and when will recovery strategies be tested? Tabletop exercises? Full DR tests?]*
Distribution list	*[Who receives this document? Who is notified when it is updated?]*

10 — Approval and Implementation

TEMPLATE GUIDANCE

This BIA must be approved by C-level or designated management before use. Approvers acknowledge they have reviewed the content and accept responsibility for the stated recovery objectives and strategies. This must be agreed BEFORE an incident occurs.

10.1 Approval Sign-off

Name	Role	Signature	Date

10.2 Implementation Plan

[Describe the steps to implement findings from this BIA: which gaps to address first, who is responsible, target completion dates, and how progress will be tracked.]

Instructions for Use

- Gather information: Collect data from all relevant business units, IT, legal, HR, and external partners. Do not rely on IT alone — business owners must define RTOs and RPOs.
- Analyse data: Understand how external partners influence critical operations and the impact of potential disruptions. Map dependencies thoroughly.
- Document and review: Ensure all content is reviewed by key stakeholders and the document is approved before filing. Remove all template guidance boxes before distributing.
- Update regularly: Review at least annually, after any significant incident, and whenever organisational structure, key systems, or supplier relationships change.
- NIS2 / GDPR: If in scope, validate that RTO/RPO values and impact ratings align with regulatory notification thresholds. Engage your DPO and legal counsel as needed.