

Document nr: [DOC NR]	Title: Business Continuity and Disaster recovery	[LOGO]
Classification: Confidential	Date: 01-12-2022	
Owner: CEO	Version: 0.7	

Business Continuity and Disaster Recovery

This template was created by the people of ICT Institute. You can find the latest version and other templates here: <https://ictinstitute.nl/free-templates/>

*You can use this template freely under the Create Commons Attribution license
<https://creativecommons.org/licenses/by/4.0/>*

You can do the following with the templates:

Share. You can share the templates and any documents made with these templates freely, with any one that you want to share it with.

Adapt. You can make new documents based on the templates, make changes, add elements or delete elements as much as you want. You can even do this in commercial organisations of for commercial purposes.

*If you are a customer, you do not have to mention ICT Institute anywhere. If you are not a customer, you must keep the text "create by the people of ICT Institute" somewhere
Note that the use of these templates is of course at your own risk. Note also that the ISO standards are copyrighted. You must buy the standard from NEN or ISO before using it*

Background

About this document

This document contains the procedures for Business Continuity (BC) and Disaster Recovery (DR). It covers ISO 27001:2022 controls 5.29 and 5.30. With this document, we aim to keep an adequate level of information security in case of events that disrupt our day to day operations and a solid plan get back on track. Personnel safety is always the most important.

This document must be stored in three locations:

- A digital copy in [GOOGLE DRIVE/SHAREPOINT/DROPBOX/ ETC.]
- A physical copy in a closed cabinet in the office
- A physical copy stored in a closed cabinet at the CEO's home

Definitions

Maximum Tolerable Downtime (MTD): How long a process or system can be down before irreparable damage is done. *Example: three days down before we lose clients.*

Recovery Time Objective (RTO): The maximum amount of time it may take for a process or system to be operational again, always < MTD. *Example: no more than 24 hours.*

Recovery Point Objective (RPO): The stage/point/version a process or system needs to be restored to be considered operational again. *Example: the latest daily database back-up.*

Roles and responsibilities

The BC-team consists of the following:

Role and name	Responsibilities	Contact information
CEO, [NAME]	Contact with authorities, approval of asset purchasing, decision on personnel re-location	[NAME@COMPANY.COM] [PHONE NUMBER]

Document nr: [DOC NR]	Title: Business Continuity and Disaster recovery	[LOGO]
Classification: Confidential	Date: 01-12-2022	
Owner: CEO	Version: 0.7	

CISO [NAME]	DR and BC coordinator, lessons learned	[NAME@COMPANY.COM] [PHONE NUMBER]
CTO, [NAME]	Internal system recovery, software platform recovery	[NAME@COMPANY.COM] [PHONE NUMBER]
COO, [NAME]	Personnel evacuation	[NAME@COMPANY.COM] [PHONE NUMBER]
Head of Legal, [NAME]	Contact with insurance, communication with stakeholders	[NAME@COMPANY.COM] [PHONE NUMBER]

Resource prioritization (BIA)

Business Continuity Objectives

[COMPANY] has the following five Business Continuity Objectives:

- Keeping personnel safe (main priority)
- Maintain the standard level of information security
- Remain operational in the capacity to prevent bankruptcy
- Return to normal operation within the described RTO's
- Restore systems to the described RPO's

Legal and contractual requirements

We have the following legal and contractual obligations regarding Business Continuity:

Source	RTO and/or RPO requirements
Clients using our software platform	SLA of 99% on weekly basis. RTO < 1h40.
...	[REQUIREMENTS]
...	[REQUIREMENTS]

Besides the requirements in the table above, [COMPANY] might need to notify the Autoriteit Persoonsgegevens within 72 hours after a personal data breach has occurred. [COMPANY] has a data breach process in place for this. [LINK PROCESS DOCUMENT]

In the table below [COMPANY] identified what the importance of each process is and what systems are necessary to make sure the process is operational.

Process	Required assets	MTD	RTO	RPO
A. Sales	[CRM SYSTEM, OFFICE SOFTWARE, EMAIL, MOBILE PHONE]	1wk	24h	24h
B. Finance	[PAYMENT PROCESSING (MOLLIE), INVOICING (MONEYBIRD)]
C. Online platform	[PRODUCTION ENVIRONMENT, PRODUCTION DATABASE]
D. Service desk	[OFFICE SOFTWARE, OFFICE NETWORK / HOME NETWORK, SUPPORT TOOL (ZENDESK)]
E. Software development	[ACCEPTANCE ENVIRONMENT, DEVELOPMENT ENVIRONMENT, OFFICE NETWORK / HOME NETWORK]
F. Marketing	[REGULAR WEBSITE, MARKETING TOOL]

Document nr: [DOC NR]	Title: Business Continuity and Disaster recovery	[LOGO]
Classification: Confidential	Date: 01-12-2022	
Owner: CEO	Version: 0.7	

G. Operations	[OFFICE SOFTWARE, OFFICE NETWORK]
---------------	-----------------------------------	-----	-----	-----

Disaster scenarios

We have identified several business discontinuity scenarios:

1. Amsterdam office becomes unusable (fire, flooding at office)
2. Major disruption at cloud provider – affecting production environment
3. Production database crash
4. Ransomware attack on PC's and laptops
5. Ransomware attack on product
6. Loss of key personnel (CEO, CTO)
7. ...

Affected processes

The effect of the disaster scenarios on [COMPANY]'s processes is as follows:

	A	B	C	D	E	F	G	.
1	Y	N
2	N	Y
3
4
5
6
7

Disaster response

Response to one of the [AMOUNT] disaster scenarios always has two processes: Disaster Recovery and Business Continuity. Disaster Recovery is focused on “getting back online”. Business Continuity is focused on “staying in business”. [COMPANY] will act as follows in the identified disasters:

Scenario 1: Amsterdam Office becomes unusable

Disaster Recovery

If personnel is present during the event, they are evacuated immediately. This is lead by the management team, who calls 112 (firemen/police/ambulance) during the evacuation. All employees converge at [LOCATION OUTSIDE] if possible.

Business Continuity

Questions to answer:

- Do we move to an alternate site OR do we work remote
- Do we look for a new office space OR wait for the old one to be declared safe
- Who contacts the IT supplier for lost hardware?

Scenario 2: Major disruption at cloud provider – production environment down

Disaster Recovery

...

Document nr: [DOC NR]	Title: Business Continuity and Disaster recovery	[LOGO]
Classification: Confidential	Date: 01-12-2022	
Owner: CEO	Version: 0.7	

Business Continuity

...

Scenario 3: Production database crash

Disaster Recovery

...

Business Continuity

...

Scenario 4: Ransomware attack on PC's and laptops

Disaster Recovery

...

Business Continuity

...

Scenario 5: Ransomware attack on product

Disaster Recovery

...

Business Continuity

...

Scenario 6: Loss of key personnel

Disaster Recovery

...

Business Continuity

...

Verification, review and evaluation

The measures listed above are tested every year, through the following measures:

	Scenario	How to test	When to test
1	Amsterdam office becomes unusable (fire, flooding at office)	Everyone works from home for two days. [FIRE DRILL?]	Annually, first week of March
2	Major disruption at cloud provider – production environment down	Clone production, shut down to see if failover works.	Annually, third week of March
3	Production database crash	Back-up restore test.	n/a, see nr. 4
4	Ransomware attack on PC's and laptops	Wipe and fully restore one laptop remotely.	Annually, first week of March
5	Ransomware attack on product
6	Loss of key personnel (CEO, CTO)

Document nr: [DOC NR]	Title: Business Continuity and Disaster recovery	[LOGO]
Classification: Confidential	Date: 01-12-2022	
Owner: CEO	Version: 0.7	

This document is reviewed annually to make sure all relevant scenarios are included.