ISO 27001 – Organizational Controls A5

SieuwertExplains

youtube.com/@sieuwertexplains

Agenda

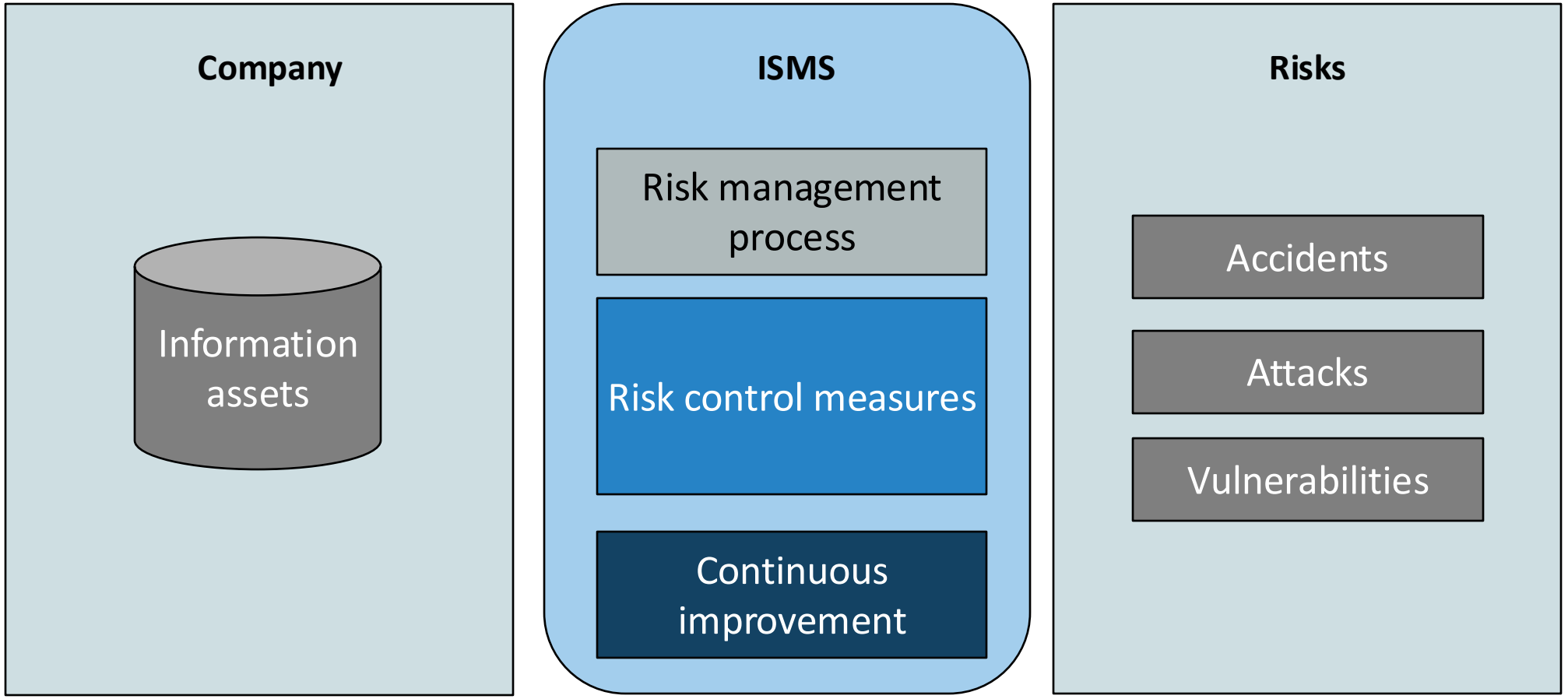
What are controls and how to implement

ISO 27001 Organisational controls

Practical implementation recommendations

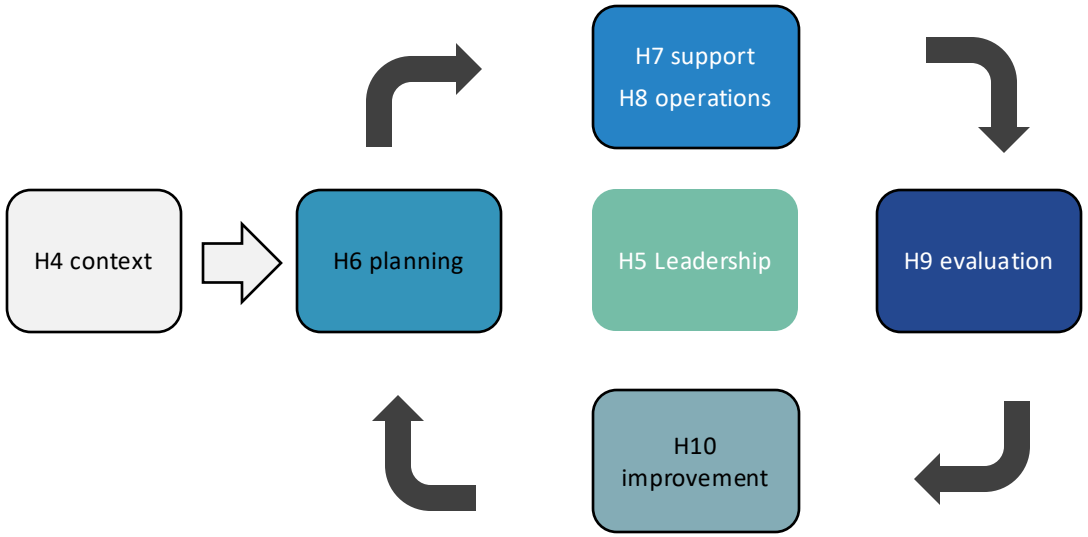
The purpose of an ISMS

An ISMS, or Information Security Management System, protects your organisation's information assets against accidents, attacks and vulnerabilities.



ISO 27001 = Harmonized structure + control measures

Harmonized structure



control measures

Annex 27001 A5-A8, containing a long list of recommended practices:

- Employee screening
- Supplier reviews
- Regular backups
- Developer training
- Encryption policy
- Offboarding procedure

Focus of this video

ISO 27001 has an ‘annex’ of recommended controls

BS 7799 - 1995

“primarily a description of some 127 information security controls in 10 sections or categories”

ISO 9001

A management system for (improving) quality, based on plan do check act. It can be applied to all products/processes

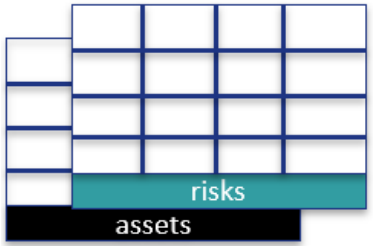
ISO 27001-Annex

ISO 27001-Harmonized Structure

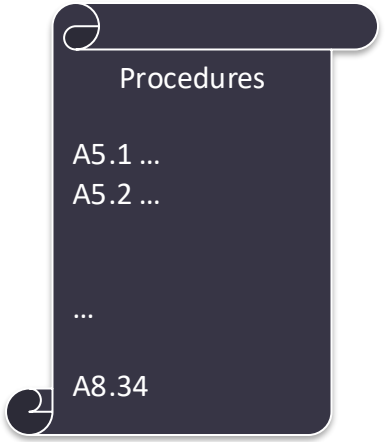
Versions: 2005, 2013, 2022

Resulting documentation

Main policy
- High level
- For outsiders



Risk register
- Using by IS team
- Links all controls to links
- Contains risk assessment and treatment



Information security procedures
- Used internally by entire company
- Provides overview, very useful during audits
- Each control is supported by a relevant register or evidence

Infoset training
- Basic training for all employees
- Used in internal training

Annex A – ISO 27001 Standard Controls

ISO 27001

Annex A
(normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

5	**Organizational controls**	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.
5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.
5.4	Management responsibilities	**Control** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.
5.5	Contact with authorities	**Control** The organization shall establish and maintain contact with relevant authorities.
5.6	Contact with special interest	Control

- Each control is only a very high level description of a relevant topic
- You can/must choose a suitable implementation for your company.
- If the implementation works for your company and is auditable, it is good enough for the auditor
- You need to decide each year if it is good enough for your risks and objectives

ISO 27002 Explanation for each control

ISO 27002

- ISO 27001 is an optional document that explains how each control is intended
- It is a good source of inspiration, but the ideas in this document are not mandatory
- The document is very useful to understand the idea behind each control

Agenda

What are controls and how to implement

ISO 27001 Organisational controls

Practical implementation recommendations

ISO 27001 Standard Controls

37 **organizational** controls

5.1	5.20
5.2	5.21
5.3	5.22
5.4	5.23
5.5	5.24
5.6	5.25
5.7	5.26
5.8	5.27
5.9	5.28
5.10	5.29
5.11	5.30
5.12	5.31
5.13	5.32
5.14	5.33
5.15	5.34
5.16	5.35
5.17	5.36
5.18	5.37
5.19	

Focus of this video

8 **people** controls

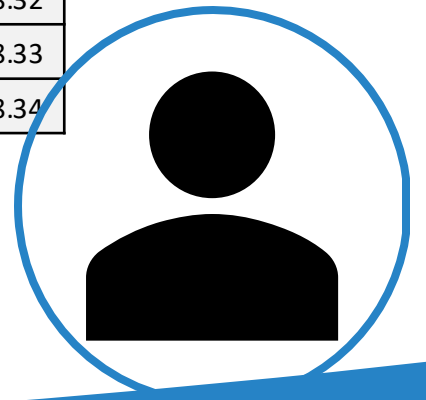
6.1
6.2
6.3
6.4
6.5
6.6
6.7
6.8

14 **physical** controls

7.1
7.2
7.3
7.4
7.5
7.6
7.7
7.8
7.9
7.10
7.11
7.12
7.13
7.14

34 **technological** controls

8.1	8.20
8.2	8.21
8.3	8.22
8.4	8.23
8.5	8.24
8.6	8.25
8.7	8.26
8.8	8.27
8.9	8.28
8.10	8.29
8.11	8.30
8.12	8.31
8.13	8.32
8.14	8.33
8.15	8.34
8.16	
8.17	
8.18	
8.19	



Informal subchapters

5.1 - 5.8 Official information

5.9 - 5.14 assets and labelling

5.15 - 5.18 Identity and access management

5.19-5.23 Supplier management

5.24-5.27 Incident management

5.28- 5.36 Compliance

5.1 Policies for information security

"Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur."

					2022						
Item	Norm-element	Activity	Responsible	More information	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23
1	Other	Information Security Team Meeting	IS-team	Handbook	x		x		x		x
2	H9	Management review	Directie	Handbook							
3	H6	Update risk analysis	IS-team and management	Handbook						x	
4	H9	Internal audit	Internal auditor	Auditplan		x			x		
5	5.1	Update infosec policies	IS-team and management	Handbook							
6	5.8	Check project plans	Security officer	Handbook							
7	6.3	awareness	Security officer	Handbook, SoA							
8			officer	Handbook							
9			officer	Handbook							
10			officer	Handbook							
11			officer	SoA							
12			officer	Handbook							
13	8.32	Check change management	IS-team and management	SoA							
14	8.15	Check logs and monitoring	CTO	SoA	x						
15	5.29	Work from home day / evacuation exercise	Security officer	Bus. Continuity plan	x						
16	8.25	Developerstraining and quiz/survey	CTO	SoA		x					
17	5.20	Supplier review	Management	Supplier overview		x					
18	5.26	Check incident analysis and response	Security officer	SoA		x					
19	5.35	PEN-test	CTO	Handbook				x			

You must have an operational planning. It must include a review of policies. We recommend to do this annually

Planned action, in annual planning

Publishing the **IS policy** on your website is the easiest way to make it 'published'.

Published document

5.2 Information security roles and responsibilities

"Information security roles and responsibilities shall be defined and allocated according to the organization needs."

Role	Responsibility	Requirements for role
CEO / general manager	Ultimately responsible for Information Security. Establish goals and policies.	[X] years of experience in a management role.
CISO	Maintaining the ISMS in order to conform to goals and polies. Report ISMS status to CEO.	Completed [EDUCATION]. [CERTIFICATION REQS?] Experience with InfoSec audits.
Privacy Officer	Checks compliance with GDPR and other privacy laws. Data breach and data subject request follow-up.	CIPP/E-certified, or followed other relevant privacy training.
Head of HR	Responsible for employee screening and on/off-boarding.	Completed HR education.
Internal auditor	Performing the annual internal audit.	Experience with InfoSec audits. Certified ISO 27001 lead auditor.
Software developer	Apply secure development principles and privacy by design in development and maintenance. Include security aspects when doing testing.	Understanding of OWASP.
All staff	Knowing and following the InfoSec policies, rules, and procedures.	Complete onboarding training

We recommend defining at least these roles or similar roles to become certified.

A best practice would be to have an HR department and complete function profiles, that you update.

You use these when hiring.

5.3 Segregation of Duties

"Conflicting duties and conflicting areas of responsibility shall be segregated."

To prevent theft, embezzlement, and fraud by individual employees you should split up high-risk tasks. Examples are:

- Salary administration (split into creating pay slips and making payments)
- Supplier contract management (split into drafting contracts and signing contracts)
- Vendor selection (split into choosing candidates and choosing between candidates)
- System administration (split into performing admin tasks and auditing admin activity)
- Software development (split into deployment in test and deployment in production)

- If you have one good example, document it and you have implemented this control
- If this is impossible (e.g. small company), provide motivation why this control is not applicable

5.4 Management responsibilities

“Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.”

Make sure that policies are clearly announced, training is available and that the mandatory character is also clearly explained. Ideally, state in employment contract that people must read and follow policies.

5.5 Contact with authorities

“The organization shall establish and maintain contact with relevant authorities.”

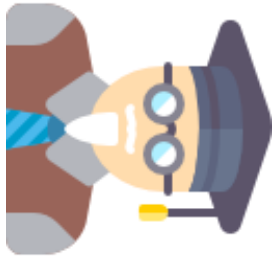
Authorities need to be notified in case of an incident, while others require a periodic status update. Examples of authorities are:

- Police in case of theft
- Tax authorities
- Privacy Supervisory Authority (Autoriteit Persoonsgegevens)
- Sector-specific Supervisory Authority (e.g. in banking)
- National CSIRT (NCSC in The Netherlands for vital sector)

Make sure you document the complete list of relevant authorities, and who should contact them when.

5.6 Contact with special interest groups

"The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations."



Draft in the InfoSec procedures document:

The security team will make sure they are up to date on security developments by following and interacting with. Any threats are discussed in the information security team

- The Information Security NL security group https://www.linkedin.com/groups/13533313/
- The International Association of Privacy Professionals (https://iapp.org)
- Platform voor Informatiebeveiliging (PvIB**)** (NL)
- The National Cyber Security Center (ncsc.nl)

- Use these sources or choose your own sources in your procedures
- Find and store one relevant news item in a folder evidence / 5.6-authorities
- Discuss the news item in your next information security team meeting

5.7 Threat intelligence

"Information relating to information security threats shall be collected and analysed to produce threat intelligence."

Choose at least two categories and one source each.

Name	Description	Source
Advisories	Advisories from national CERT	https://advisories.ncsc.nl https://cert.europa.eu https://www.cisa.gov/news-events/cybersecurity-advisories
Trends and news	Tools, techniques, and procedures used by hackers	https://www.security.nl https://thehackernews.com
Newsletters	News and analyses	https://krebsonsecurity.com https://www.schneier.com/ Substack(s)
Vendor and tech specific	Operation and technical info	https://www.cvedetails.com https://msrc.microsoft.com

Draft in the InfoSec procedures document:

Threats are possible future events with a negative impact on your organization's CIA of information

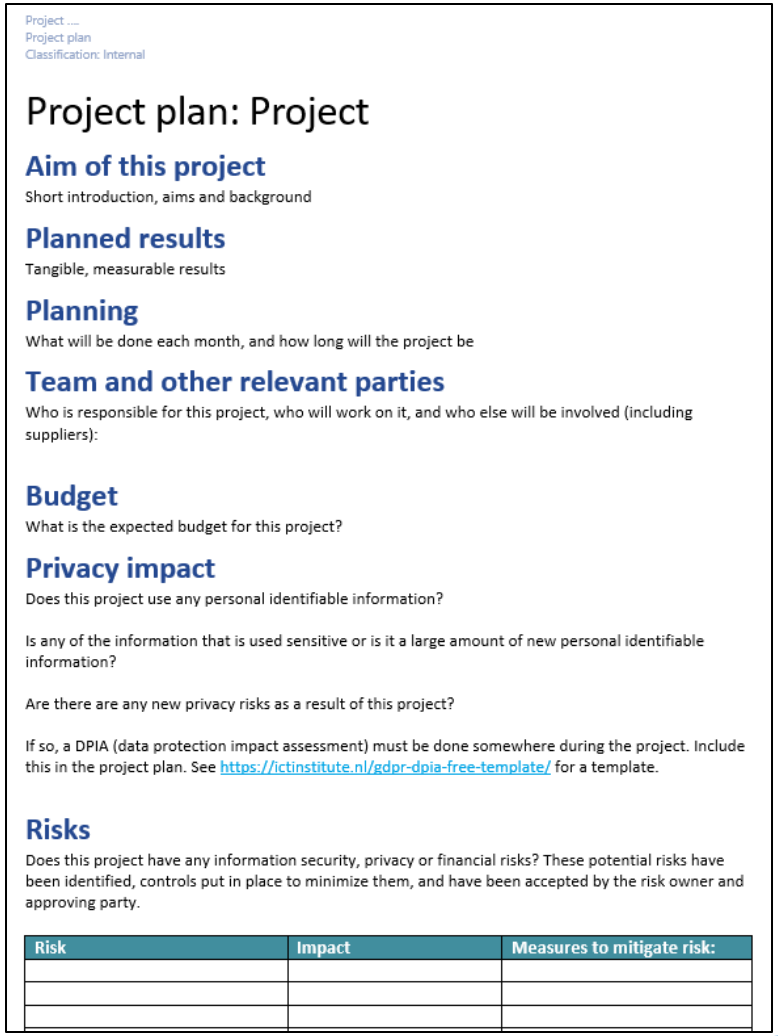
The IS team scans the sources quarterly/before IS meetings to share and discuss relevant threats, vulnerabilities and reports within the IS team.

Relevant or interesting information is shared #channel or discussed directly with each other. In the event of an immediate risk, an event/incident is created and action is taken.
During the infosec meeting, interesting reports are discussed and noted in the agenda.

5.8 Information security in project management

“Information security shall be integrated into project management.”

The easiest way to implement this is, is to include mandatory chapters in project plans.



Project ....
Project plan
Classification: Internal

Project plan: Project

Aim of this project

Short introduction, aims and background

Planned results

Tangible, measurable results

Planning

What will be done each month, and how long will the project be

Team and other relevant parties

Who is responsible for this project, who will work on it, and who else will be involved (including suppliers):

Budget

What is the expected budget for this project?

Privacy impact

Does this project use any personal identifiable information?

Is any of the information that is used sensitive or is it a large amount of new personal identifiable information?

Are there are any new privacy risks as a result of this project?

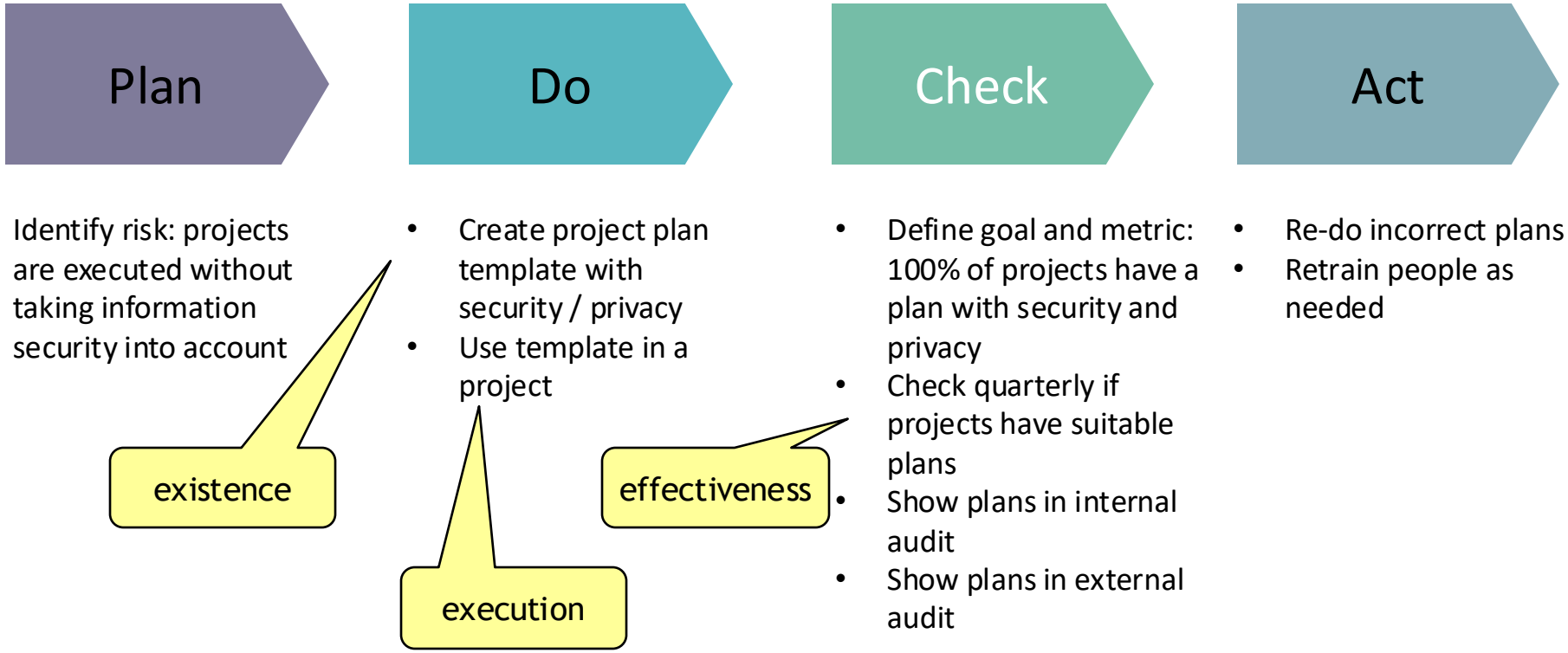
If so, a DPIA (data protection impact assessment) must be done somewhere during the project. Include this in the project plan. See https://ictinstitute.nl/gdpr-dpia-free-template/ for a template.

Risks

Does this project have any information security, privacy or financial risks? These potential risks have been identified, controls put in place to minimize them, and have been accepted by the risk owner and approving party.

Risk	Impact	Measures to mitigate risk:

Example of full implementation of 5.8



Informal subchapters

5.1 - 5.8 Official information

5.9 - 5.14 assets and labelling

5.15 - 5.18 Identity and access management

5.19-5.23 Supplier management

5.24-5.27 Incident management

5.28- 5.36 Compliance

5.9 Inventory of information and other associated assets

"An inventory of information and other associated assets, including owners, shall be developed and maintained."

Template: Assets and Risk register

Consider the following assets:

- Information
- Intellectual property
- Personnel
- Storage devices
- Software
- Contracts
- Source code
- PC's and laptops
- Phones and tablets
- Etc.

Information Asset Inventory

For explanation of categories, see below

nr.	Name	Description	Owner	relevant CIA aspects	Is this personal data?	Who should have access	Category
1	Dashboard1	Dashboard with weekly reports for the finance department	CFO	CIA	no	All developer roles	Data
2	CRM system	System from salesforce with data of all retail customers	Sales	CI	yes	Sales managers	Third parties
3	Dashboard1 source code	Report scripts for creating dashboard1	CFO	CIA	no	Developers	Software
4	Confluence	Documentation on Confluence	CTO	CI	yes	Own access management	Organisation
5	User data	User uploads		.			
6	Web Apps	Web applications		.			
7	Websites	Public websites		.			
8	Laptops	Laptops of employees		.			
9	Servers	Servers (in the cloud, mostly AWS)		.			
10	Phones	Mobile phones		.			
11	HR	HR files		.			
12	Finance	Finance and accounting		.			
13	Bank account	Bank account of company		.			
14	Documentation	Slack / wiki / confluence		.			
15	Logs	Log files (access log, error log)		.			
16	Headquarters	Main office room		.			
17	Cloud storage	Dropbox / Drive / Onedrive		.			
18				.			
19				.			

5.10 Acceptable use of information and other associated assets

"Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented."

	Public	Internal use	Confidential
How to store	…	…	…
Whom to share with	…	…	…
How to send	…	…	…
Physical storage	…	…	…

- **Public information:** Information that is already public may be freely shared with customers and others.
- **For internal use:** Information that has specific business or strategic value to us.
- **Confidential:** Information with a high business, strategic, or personal value, and can cause serious harm to our organization or a person if it ends up in the wrong hands.

5.11 Return of assets

“Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement.”

You need to document:

- Where you document which asset an employee has
- Which steps you do during offboarding

As evidence, make an offboarding checklist that is filled in when someone leaves a position or the company

5.12 Classification of information

“Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.”

Will be discussed further in a next video

5.13 Labelling of information

“An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.”

You should provide instructions for labelling in the infosec rules or procedures. Also discussed in a next video

5.14 Information transfer

"Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties."

Which tools and media may be used for what type of information transfer?

- **Microsoft Teams** may be used for communication with colleagues
- **WhatsApp** cannot be used for non-business-related communication with clients and colleagues
- Client portal must be used for final reports
- Secure mail solution is used for patient data
- Source code not sent via email, but using

Informal subchapters

5.1 - 5.8 Official information

5.9 - 5.14 assets and labelling

5.15 - 5.18 Identity and access management

5.19-5.23 Supplier management

5.24-5.27 Incident management

5.28- 5.36 Compliance

5.15 Access control

"Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements."

Role	Description	Examples	VOG categories	Office key	Tag	Telephone	Laptop	System 1 role	System 2 role	Website CRM role	Social media	May sign
Managing director	CEO, accountable for the entire organization	Sieuwert	Information, financial	x	x	x	x	User	User	User	n/a	Everything
CISO	Information Security Executive, accountable for InfoSeC	Joost	Information, financial	x	x	x	x	Security admin	Security admin	Security admin	n/a	Contracts <250k
IT-admin	Maintains internal systems and networks	Mitchell	Information		x	x	x	Global admin	Global admin	Global admin	n/a	n/a
Sales employee	Sales department, non-managers	John			x	x	x	User	User	n/a	User	n/a
Head of Sales	Sales Director	Frank	Information, financial		x	x	x	User	User	User	n/a	Contracts <1mln
...												

Template: Authorization Matrix

The following principles should be applied:

- **Role based access:** People have roles, which have associated rights
- **Need to know:** people have access to information needed for their job
- **Least privilege:** people are not granted higher access rights than needed for their job

5.16 Identity management

“The full life cycle of identities shall be managed.”

This is often implemented by having official work addresses (@ictinstitute.nl)a nd rules regarding:

- When created and for whom (e.g. only official employees)
- How people get the initial info / password securely
- When accounts are disabled, archived, deleted

Draft in the InfoSec procedures document:

The HR responsible is updated by the rest of the management team about changes in HR, and creates user accounts when a new employee onboards. After an employee leaves occupation, the HR responsible deactivates the user account and deletes it when all valuable information has been transferred and secured.

5.17 Authentication information

“Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.”

For each service, a fresh password not used before or for any other service

Employees are not allowed to leave passwords visible in the workplace.

Passwords should not be easy to guess: no names, birthdays, common words, nor less than 8 characters.

Personal passwords and accounts cannot be shared with anyone else.

Employees need to store their passwords in a secure way, e.g. using a password manager.

5.18 Access rights

“Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.”

You need to plan access right checks, where the system owner reviews all accounts.
These should be in your annual planning

Informal subchapters

5.1 - 5.8 Official information

5.9 - 5.14 assets and labelling

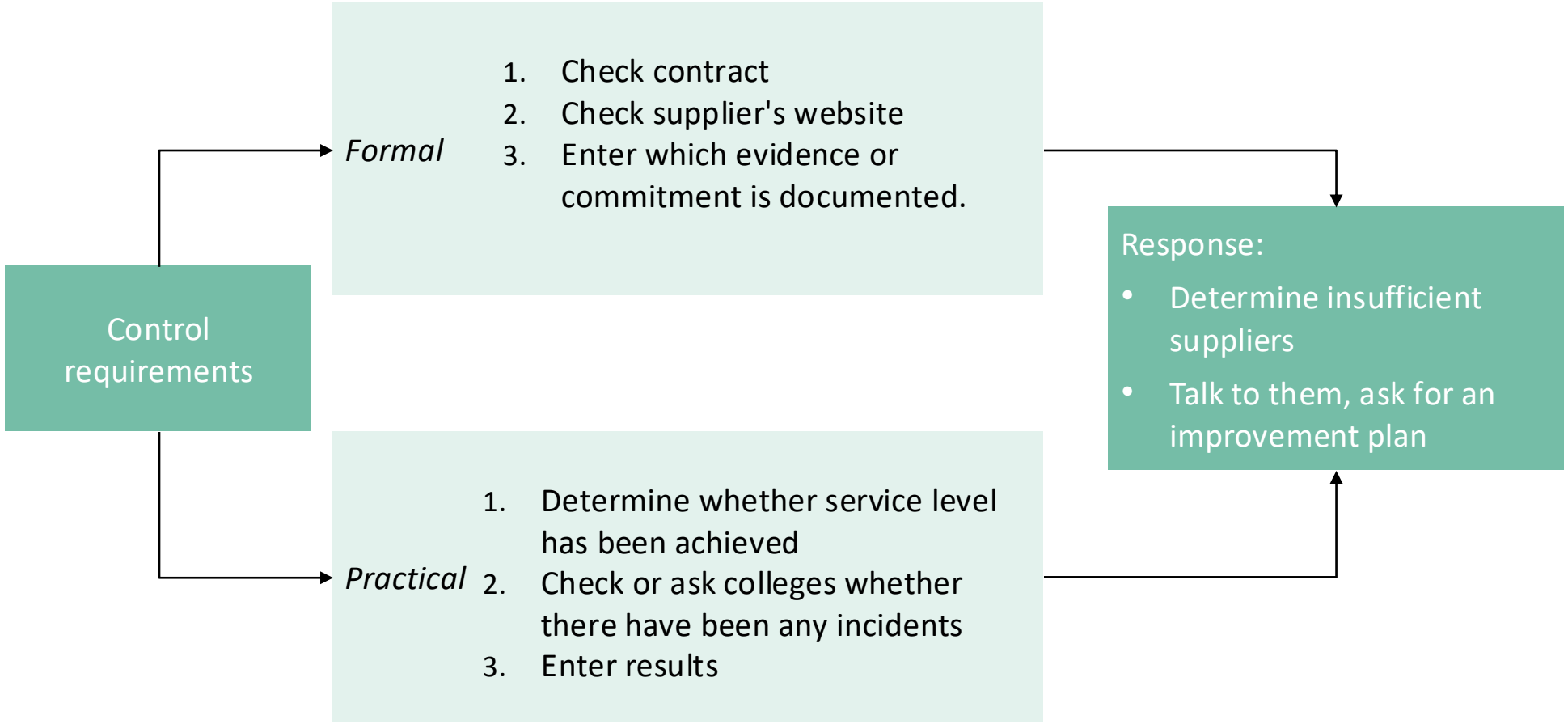
5.15 - 5.18 Identity and access management

5.19-5.23 Supplier management

5.24-5.27 Incident management

5.28- 5.36 Compliance

Supplier management: high level process



Suggested requirements

Typical formal requirements:

- For large suppliers or standard services where suppliers with ISO27001 certification are available, an ISM**S based on ISO 27001 or comparable standard** is required.

- If personal data is shared (this is often the case with SaaS), a **data processing agreement** is required.

- Suppliers are **preferably located in the EU.** Otherwise, there must be a check whether the supplier can and wants to comply with GDPR (Corporate clauses?). We check whether there is an appropriate privacy policy.

Typical practical requirements:

- No disruptions or incidents caused by supplier
- Meets SLA

5.19 Information security in supplier relationships

“Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.”

Supplier data			Requirement	
Name	Product/service	Contact details	Documentation requirement	Practical requirements
ICT Institute	IS consultancy	Sieuwert van Otterloo sieuwert @ …	ISO 27001 certification	No incidents
Microsoft	Azure	Not applicable	Compliance with ISO27001	No loss of data 99.99% uptime

Register of suppliers

5.20 Addressing information security within supplier agreements

“Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.”

Draft in the InfoSec procedures document:

We maintain a register of suppliers, which includes our information security requirements, relevant documentation and contact details. All new suppliers are added to the register, and the register is reviewed once per year.

5.21 Managing information security in the information and communication technology (ICT) supply chain

"Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain."

Draft in the InfoSec procedures document:

We determine the relevant information security requirements for our suppliers. For business critical suppliers, we required evidence of ISO27001 compliance, which ensures the supply chain is secure.

5.22 Monitoring, review and change management of supplier services

“The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.”

Supplier		Requirements		Evidence of review in Jan 2025	
Name	Product/service	Documentation requirement	Practical requirements	Score/assessment documentation	Score / assessment practical requirement
ICT Institute	IS consultancy	ISO 27001	No incidents / data breaches	https://ictinstitute.nl/iso-27001-certified/	No incidents in 2025

- Action in annual planning
- Extra columns per year for annual review of all suppliers
- Some detailed notes for key suppliers

5.23 Information security for use of cloud services

"Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements."

We use several cloud services.
The most important ones are as follows:
*Software as a Service (**SaaS**): [LIST]*
*Platform as a Service (**PaaS**): [LIST]*
*Infrastructure as a Service (**IaaS**): [LIST]*

Acquisition rules:
- *EU based*
- *Support MFA*
- *Exists for at least X years*

Use and management:
- *Will assign two admins*
- *Admins review logs / get release notes*

Exit:
- *For supplier X, external backups*
- *Return of data clause in contract*

Informal subchapters

5.1 - 5.8 Official information

5.9 - 5.14 assets and labelling

5.15 - 5.18 Identity and access management

5.19-5.23 Supplier management

5.24-5.27 Incident management

5.28- 5.36 Compliance

5.24-5.27 Assessment and decision on information security events

5.24 "The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities."
5.25 "The organization shall assess information security events and decide if they are to be categorized as information security incidents."
5.26 : "Information security incidents shall be responded to in accordance with the documented procedures."
5.27 "Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls."

Register of incidents

Incident Register

Overview of all past and current incidents. Must be maintained by the InfoSec team and reviewed monthly

Organization:

ID	Short description	Cause of the incident	Start incident	End incident	Is it an incident*	Current status	Personal data involved?	Personal data breach?	Measure taken to control situation	For big incidents, provide a link to more information:	Root cause analysis: why did this happen?	Measures taken to prevent repetition
example	laptop stolen	A laptop was stolen after office hours. Someone broke in and stole a laptop a staff member forgot to take home.	Evening of 02/04/2019	Evening of 02/04/2019	incident	Closed	Yes	No, the laptop was encrypted and is remotely wiped	Remote wipe the laptop, mgmt filed police report. New laptop ordered.	document stolen-laptop-2019.docx		Extra awareness training to remind of danger leaving devices
1												
2												
3												
4												
5												

The register can any tool, containing at least the following:

- A short description of the event
- Whether it is an incident
- What caused the incident
- When the incident started
- When the incident ended
- What the current status is
- Whether personal data was involved
- What measure has been taken to handle the situation
- For larger incidents, a link to a document containing more information (incident report)

- Make / pick a register. You can use our template
- Add at least one event / incident

https://ictinstitute.nl/information-security-incident-management

5.28 Collection of evidence

"The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events."

- Make a folder for additional evidence
- Store some evidence (e.g. screenshots, report email) for one incident

5.29 Information security during disruption
5.30 Information security readiness

5.29 "The organization shall plan how to maintain information security at an appropriate level during disruption."

5.30: "ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements."

These two controls are best covered in a separate business continuity plan. It must contain:

- Business impact assessment: what are important processes and systems
- Objectives, such as return time objective (RTO)
- Scenario's
- Some annual or more frequent test

Informal subchapters

5.1 - 5.8 Official information

5.9 - 5.14 assets and labelling

5.15 - 5.18 Identity and access management

5.19-5.23 Supplier management

5.24-5.27 Incident management

5.28- 5.36 Compliance

5.31 Legal, statutory, regulatory and contractual requirements

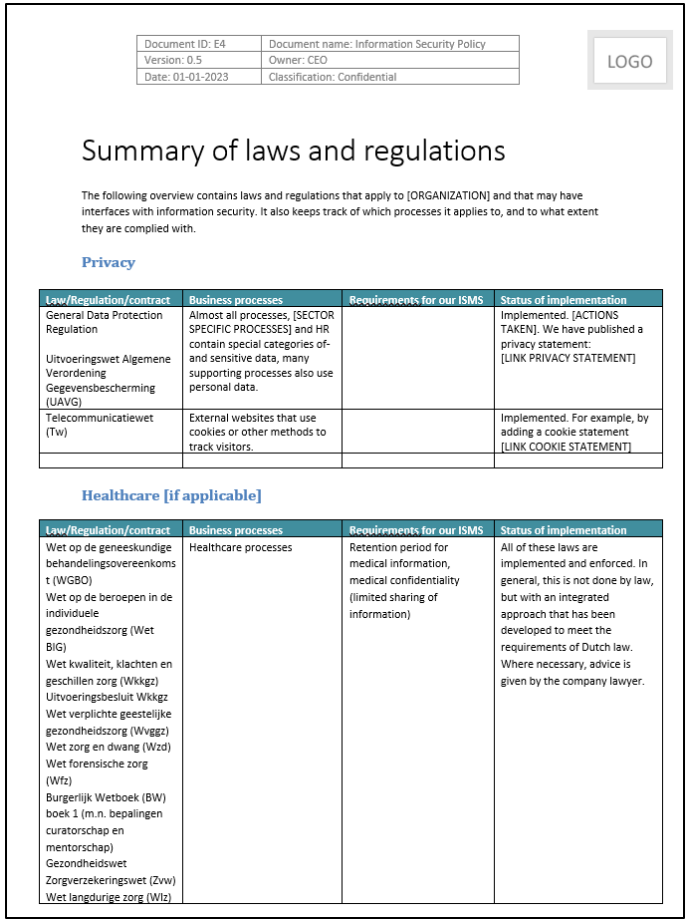
"Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date."

There should be documentation that shows we took a serious look at relevant laws, legislation, and other requirements.

Template: Summary of laws and regulations

Suggestions for content:

- GDPR for personal data
- HR / labor law
- Finance / tax law



Document ID: E4	Document name: Information Security Policy
Version: 0.5	Owner: CEO
Date: 01-01-2023	Classification: Confidential

LOGO

Summary of laws and regulations

The following overview contains laws and regulations that apply to [ORGANIZATION] and that may have interfaces with information security. It also keeps track of which processes it applies to, and to what extent they are complied with.

Privacy

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
General Data Protection Regulation Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)	Almost all processes, [SECTOR SPECIFIC PROCESSES] and HR contain special categories of- and sensitive data, many supporting processes also use personal data.		Implemented. [ACTIONS TAKEN]. We have published a privacy statement: [LINK PRIVACY STATEMENT]
Telecommunicatiewet (Tw)	External websites that use cookies or other methods to track visitors.		Implemented. For example, by adding a cookie statement [LINK COOKIE STATEMENT]

Healthcare [if applicable]

Law/Regulation/contract	Business processes	Requirements for our ISMS	Status of implementation
Wet op de geneeskundige behandelingsovereenkomst (WGBO) Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) Wet kwaliteit, klachten en geschillen zorg (Wkkgz) Uitvoeringsbesluit Wkkgz Wet verplichte geestelijke gezondheidszorg (Wvggz) Wet zorg en dwang (Wzd) Wet forensische zorg (Wfz) Burgerlijk Wetboek (BW) boek 1 (m.n. bepalingen curatorschap en mentorschap) Gezondheidswet Zorgverzekeringswet (Zvw) Wet langdurige zorg (Wlz)	Healthcare processes	Retention period for medical information, medical confidentiality (limited sharing of information)	All of these laws are implemented and enforced. In general, this is not done by law, but with an integrated approach that has been developed to meet the requirements of Dutch law. Where necessary, advice is given by the company lawyer.

5.32 Intellectual property rights

“The organization shall implement appropriate procedures to protect intellectual property rights.”

Draft in the InfoSec procedures document:

[ORGANIZATION] respects intellectual property. Staff must validate if an asset can be used before using it. No use may be made of illegal software or software without a valid license.

Texts and images are subject to copyright, and we are not allowed to use all texts and images just like that. The following is allowed:

- You may quote 1-2 sentences at a time with source reference (name of document or URL). No permission is required for this. A screenshot of a website you are discussing is also allowed.
- You may use images from creative commons sources such as Noun Project, Unsplash, or Wikimedia Commons. State the maker's name on the same page or at the back of the document. Other images from the Internet are not allowed.
- For photos with recognizable people, you need permission from the person. The easiest is not to use photos where people are recognizable.

5.33 Protection of records

“Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.”

Examples of records are business transactions, HR files, accounting, signed contracts, etc. System logs are also records, but there is a dedicated control for this. (8.15)

You can implement this control by creating (digital) archives, separate systems or creating procedures for retaining information

5.34 Privacy and protection of personal identifiable information (PII)

"The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements."

If you handle personal data, you must comply with the General Data Protection Regulation (AVG, EN: GDPR).

Most Dutch organizations need:

- Register of processing activities
- Processing agreements with certain suppliers
- A privacy statement on the website
- Procedure for Data Protection Impact Assessments (DPIA)
- Decide whether a Data Protection Officer (DPO) role is needed
- Procedure and register of data breaches

5.35 Independent review of information security

"The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur."

XYZ Internal audit programme													
Organisation: ...													
Version: ...													
Date: ...													
Classification: Internal use													
Owner: ...													
		2025				2026				2027			
Topic	Auditf requency	25Q1	25Q2	25Q3	25Q4	26Q1	26Q2	26Q4	26Q42	27Q1	27Q2	27Q3	27Q4
4. Context of the organisation	Yearly				x				x				x
5. Leadership	Yearly				x				x				x
6. Planning	Yearly				x				x				x
7. Support	Yearly				x				x				x
8. Operation	Yearly				x				x				x
9. Performance evaluation	Yearly				x				x				x
10. Improvement	Yearly				x				x				x
A5 Organizational controls	2x per three years				x				x				
A6 People controls	2x per three years				x				x				
A7 Physical controls	2x per three years				x								x
A8 Technological controls	2x per three years				x								x
Marketing	Yearly				x				x				x
IT-Development	Yearly				x				x				x
Service	Yearly				x				x				x
Sales	Yearly				x				x				x
HRM	Yearly				x				x				x

5.36 Compliance with policies, rules and standards for information security

“Compliance with the organization’s information security policy, topic-specific policies, rules and standards shall be regularly reviewed.”

Draft in the InfoSec procedures document:

With all these security policies, standards and procedures, it is important for managers to regularly review whether the activities and/or processes they are responsible for are fully compliant. For this to be done correctly, they should be aware exactly which rules and requirement they need to comply with and check this.

Information systems are regularly reviewed on compliance as well. Vulnerability tests such as penetration tests are done yearly.

5.37 Documented operating procedures

“Operating procedures for information processing facilities shall be documented and made available to personnel who need them.”

Where are work instructions stored? e.g. Confluence, SharePoint?

Example procedures:

- Installation and configuration of systems;
- Backup, system restart and recovery procedures;
- Scheduling requirements;
- Error handling;
- Support contacts;
- Monitoring, logging and audit trails.

Agenda

What are controls and how to implement

ISO 27001 Organisational controls

Practical implementation recommendations

Expected process

Scan

- Check for existing policies / documentation
- Ask current staff to document current way of working

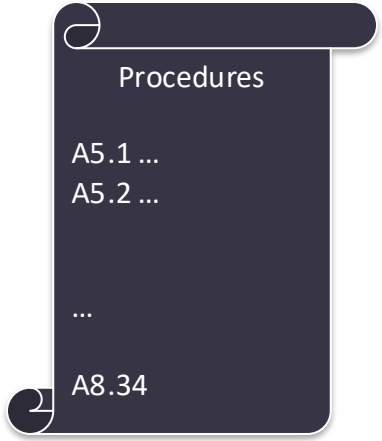
Fix

- Make sure all knowledge resides with multiple people
- Fix obvious, very big risks
- In other cases, just plan improvements, e.g. in a “risk treatment plan” in the risk inventory

Document

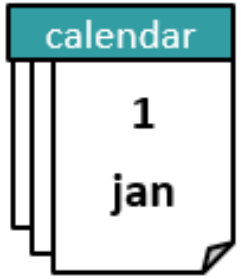
- Document the how, when, where in a ‘procedures’ document
- Make ‘procedures’ document available

Expected results



Information security procedures

- Used internally by entire company
- Provides overview, very useful during audits
- Each control is supported by a relevant register or evidence



Annual planning

- Overview of recurring actions

Per action / control, some unique, original document that shows you performed your own actions.

Thanks for watching *SieuwertExplains*

Subscribe at youtube.com/@sieuwertexplains

SieuwertExplains is a free learning resource, where you can learn about information security, privacy and standards such as ISO 27001. The channel is created by ICT Institute, an IT advisory firm. Call us for audits, compliance support or IT reviews!
https://ictinstitute.nl/sieuwertexplains/