Img: aditya-chinchure

ISO 27001 – A6 People Controls

SieuwertExplains

youtube.com/@sieuwertexplains

Agenda

How do people controls fit into the overall structure

ISO 27001 A6 People controls

People related controls from A5, A7

How to implement

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	

8 **people** controls

6.1
6.2
6.3
6.4
6.5
6.6
6.7
6.8

Focus of this video

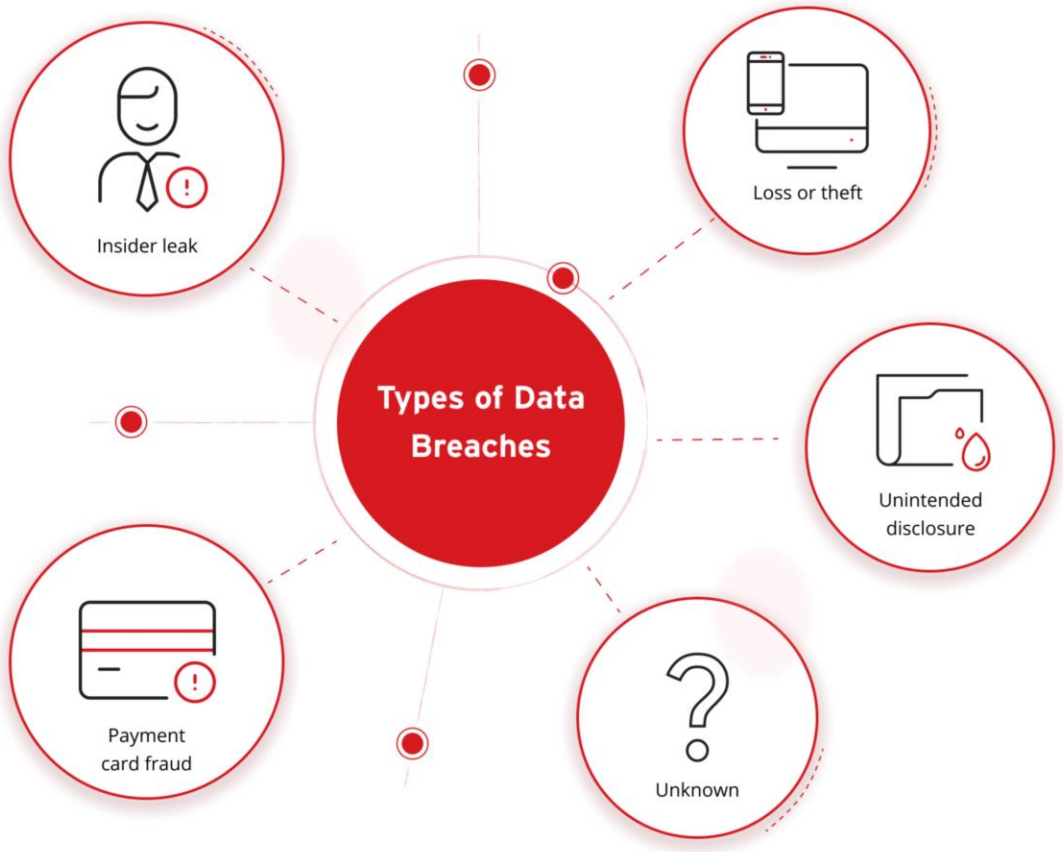
14 **physical** controls

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	

Sources of data breaches



What Is a Data Breach? Trend Micro staff - Last updated Oct 14, 2025
https://www.trendmicro.com/en_gb/what-is/data-breach.html

Many companies want to minimize the risk that they experience a data breach.

'Human factors' is an important source of data breaches. The human factors include:

- **Mistakes**: e.g. clicking phishing links, carelessness in sending
- **Ignorance / miscommunication**: People not using IT correctly
- **Bad people in the organisation** (**'malicious actors'**). Angry or blackmailed employees can steal things or do damage

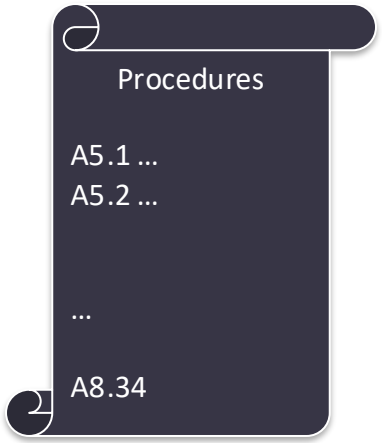
Resulting documentation

Many controls require you to put rules in place for all staff. For this you need **one clear document**:

- Shared with all employees
- Easy to read, no jargon
- Clear mandatory rules, no room for misinterpretations
- Also clear on what you can do and can use

Relation with policy and procedures

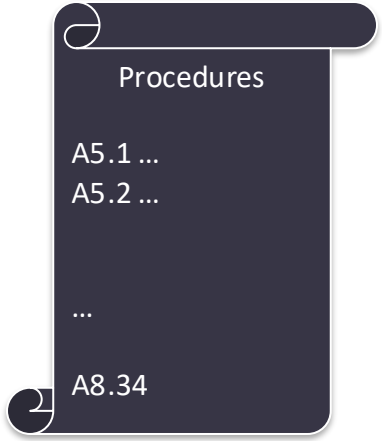
Main policy
- Tells what the company is aiming for
- Needs to be filled in



Information security procedures
- Details on what the security team / CISO does, e.g. where it registers incidents
- Should be known to CISO, IT staff

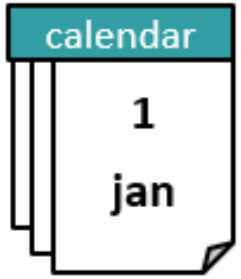
Infosec rules and training
- Make sure people report incidents so that they can be handled
- Tell people when to go to IT of CISO

Some controls are implemented as a procedure



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.

Agenda

How do people controls fit into the overall structure

ISO 27001 A6 People controls

People related controls from A5, A7

How to implement

6.1 Screening

Img src: adrian-dascal via unsplash

"Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks."

Procedures

- This control describes how the **HR department or hiring managers** make sure you hire reliable. People.
- The focus is on making sure you do not hire **criminals or fraudsters**, it is not about whether people are mediocre or excellent
- It does not have to be for every role. You can limit it to for instance: CISO, management, people with database access, people with access to client documents (e.g. translators, service agents)
- You need to consider how to treat interns and short term temporary staff

6.1 Screening options

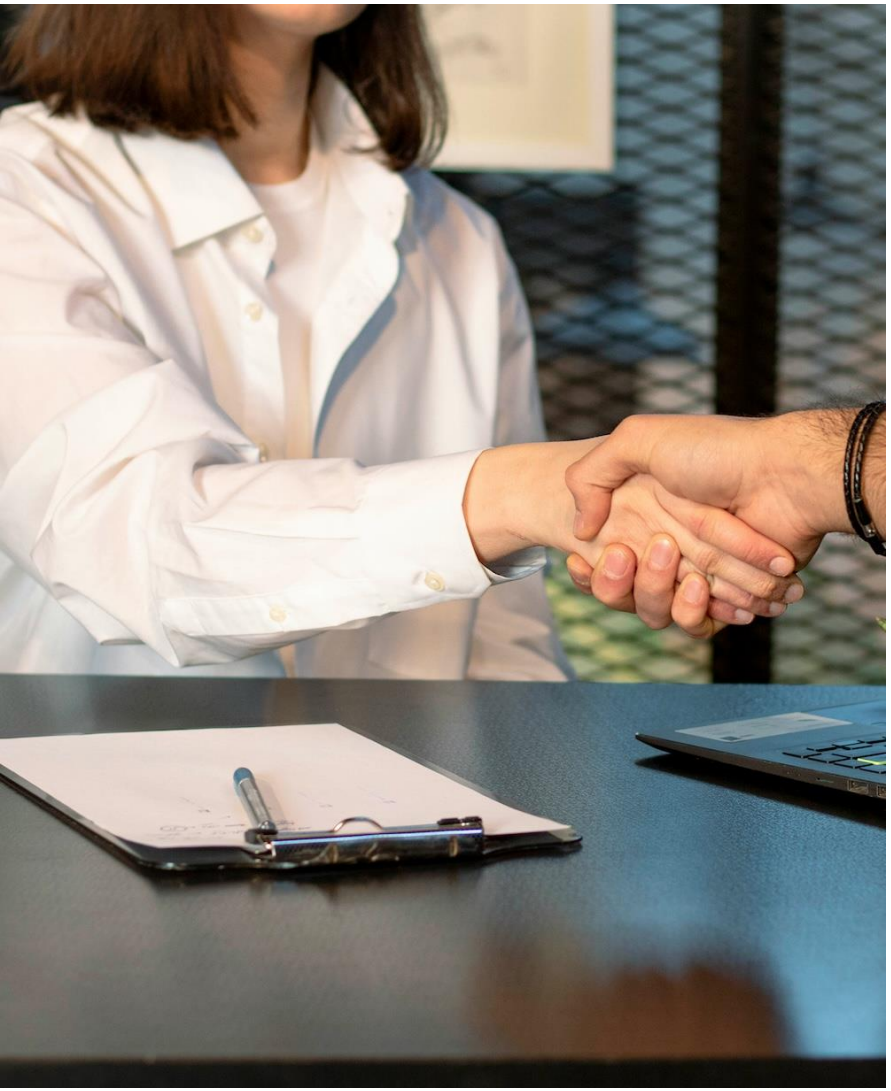
Netherlands

- It is forbidden in labor law and privacy law to do your own research, e.g. check social media account, ask for credit scores or collect other information considered irrelevant
- Your only option therefore is to use the government-approved "***Verklaring Omtrent Gedrag (VOG***)".
- You can extend this with other relevant fraud-reducing measures:
  - check university registration,
  - ask proof of address,
  - ask for EU bank account,
  - see diploma

Other countries

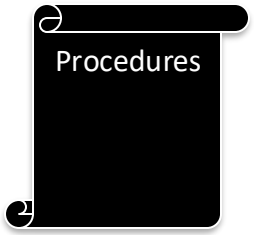
- You must check local regulation and use available, commonly used instruments for your region and sector
- Make sure any screening is fairly communicated to people, e.g. in the job opening description

6.2 Terms and conditions of employment



Img scr: Mina Rad via unsplash

"The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security."



Proposed implementation:

Create a template employment contract. Include in the contract:

- **With this contract, you have also received the "information security rules". You must read and follow these instructions.**
- **Deliberately or repeatedly not following the information security rules will lead to disciplinary measures such as formal warnings or further steps.**

Use the template.

6.3 Information security awareness, education and training


Img: aditya-chinchure

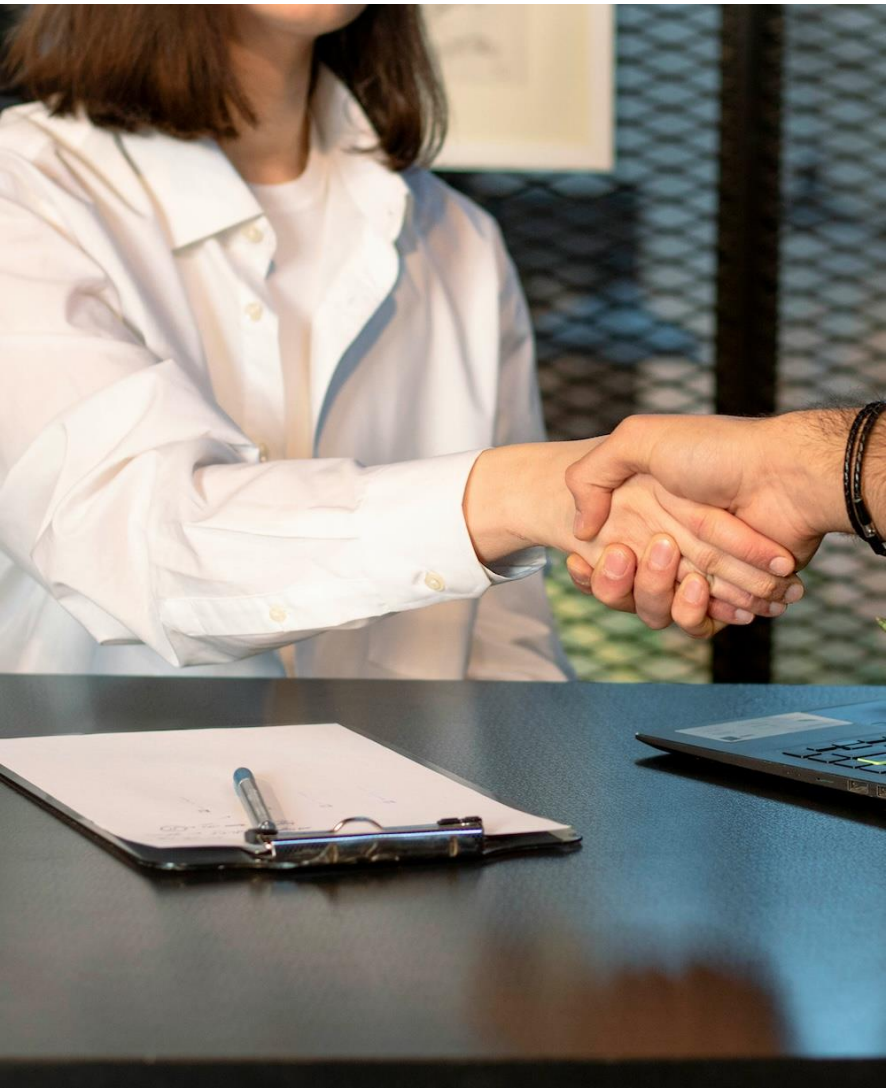
"Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function."

You will probably need:

- **Onboarding training** – during onboarding, make new employees aware of responsibilities
- **Recurring information security awareness training**– at least once a year, get everyone together and explain risks and rules.
- **Job-specific training** – some jobs, such as software development, require more in-depth sessions to learn how to perform them securely

Hint: Make an attendance list so you can prove attendance during audits

6.4 Disciplinary process



Img scr: Mina Rad via unsplash

“A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.”

Create a template employment contract. Include in the contract:

- With this contract, you have also received the ”information security rules”. You must read and follow these instructions.
- **Deliberately or repeatedly not following the information security rules will lead to disciplinary measures such as formal warnings or further steps.**

Organize warnings and sanctions in line with local labor laws

6.5 Responsibilities after termination or change of employment

Img src: Nikh Mter via unsplash

"Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties."

Step 1: In the employment contract, include a non-disclosure clause for confidential information, that states it also applies after exit!

Step 2: Provide people with an exit letter, where you repeat this clause

Step 3: Use an offboarding checklist to manage all other steps:

- Hand back assets
- Change or revoke access rights
- Reminder of the continuing Non-Disclosure Agreement clause

6.6 Confidentiality or non-disclosure agreements

"Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties."

Step 0: Create a template employment contract.

Step 1: In the employment contract, include a non-disclosure clause for confidential information, that states it also applies after exit.

Hint: consider to also make a standard 'freelancer' contract or a checklist for freelancer / external staff contracts

Example from the ICT Institute ISMS

6.7 Remote working

"Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises."

Make sure you have rules on at least the following topics in the InfoSec rules:

- Whether working from home is allowed, whether people can bring / print documents when doing so, and if there are rules for desk / separate room
- Whether working in public spaces (train, Starbucks) is allowed
- To which types of networks employees may connect to (StarBucks free WiFi?)

Note: Shoulder surfing happens. Make people aware of this risk in your training

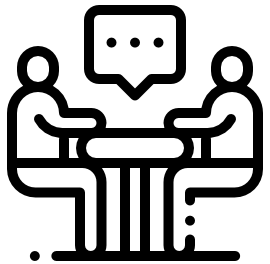
6.8 Information security event reporting

“The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.”

Include this in the information security rules and training:

Please report any information security event, incident or data breach directly. Examples include service disruptions, malfunctions, damages to equipment, unusual activities in IT systems, unusual digital traffic. You must report it to the CISO via ciso@myorganisation.nl, our ticketing system / slack channel, …

A6. People controls - summary



The people controls describe

On-boarding
- A formal statement of conduct (VOG) when sensitive information will be handled
- Contract with NDA clause, making rules mandatory and sanctions
- Register which devices have been handed out to the new employee

Off-boarding
- Exit letter
- Hand in company devices and remove company information from BYODs
- Disable user account in systems and mark account for deletion

Rules
- Teleworking
- Event reporting

Agenda

How do people controls fit into the overall structure

ISO 27001 A6 People controls

People related controls from A5, A7

How to implement

5.12 Classification of information

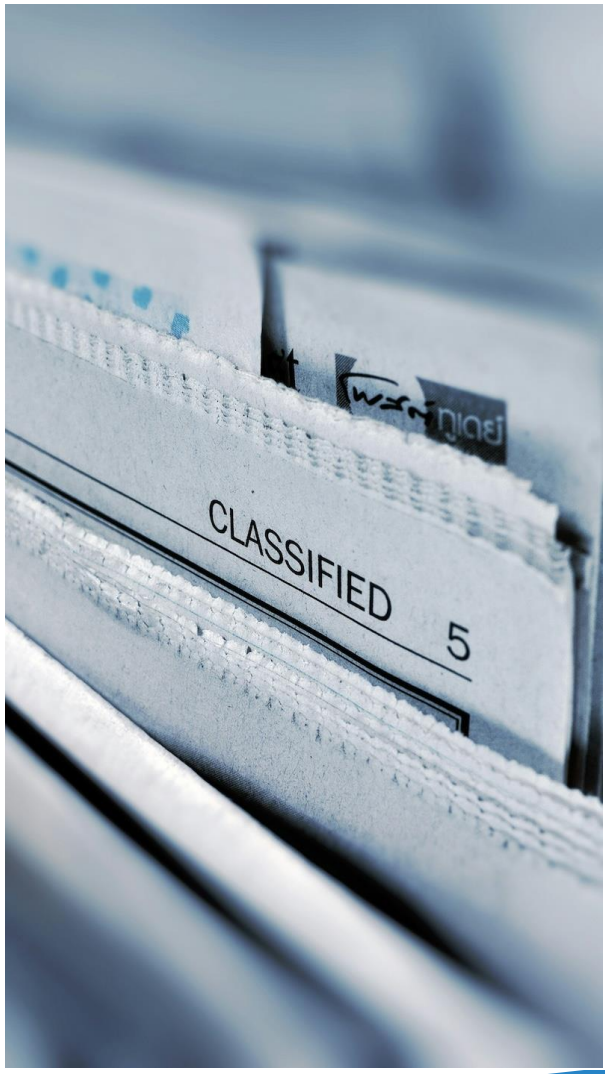
"Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements."

InfoSec rules

Define explicitly what labels you will use and what do they mean. We recommend the following labels:

- **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.

Do not use other labels that you have not defined (top secret, highly sensitive, restricted, need to know) since this makes your instructions unclear



Img src: absolutvision

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.”

Make rules that state when and how labels should be applied. Options are:

- On title pages of documents
- In document headers and footers
- In file names or folder names

Also make a rule that unlabelled documents should be treated as confidential, or something similar to cover all cases.

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.”

InfoSec rules

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

You must provide rules for each label type on how information should be handled.

- Make sure the rules are specific for your company, processes and systems.
- Make sure they cover paper and digital documents

5.11 Return of assets

Img src: Nikh Mter via unsplash

“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, e.g. block account, change passwords, ask keys and car back

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

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."

InfoSec rules

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

- **Microsoft Teams** may be used for communication with colleagues
- **WhatsApp/Signal** cannot be used for non-business-related communication with clients and colleagues
- Client portal must be used for final reports
- Source code not sent via email, but only stored and shared via gitlab / github

5.32 Intellectual property rights

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

InfoSec rules

Suggested / example rules

ABC-Co respects intellectual property. Staff must check if an image or software 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.

7.7 Clear desk and clear screen

"Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced."

Suggested / example rules

- When leaving the office, all documents must be removed from desks and stored in a non-visible way. Confidential documents must be stored in locked drawers or filing cabinets.
- Computers and phones must have a screensaver with a password or similar security measure (e.g. fingerprint reader). Employees must always lock devices when leaving them unattended.
- Screens need to be clear of company information (also no notifications popping up) when shown to people outside of the company, e.g. hooked up to an external projector. Virtual desktops need to be clean of documents.
- Confidential data should never be viewed in a public place or open office space.

Agenda

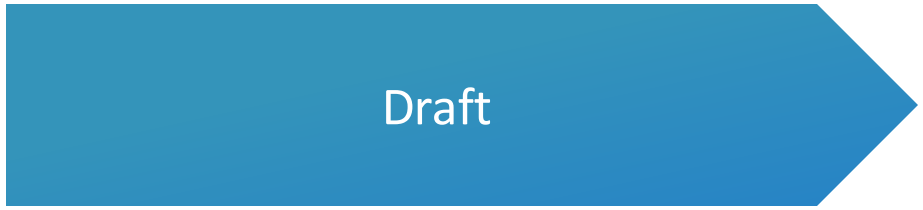
How do people controls fit into the overall structure

ISO 27001 A6 People controls

People related controls from A5, A7

How to implement

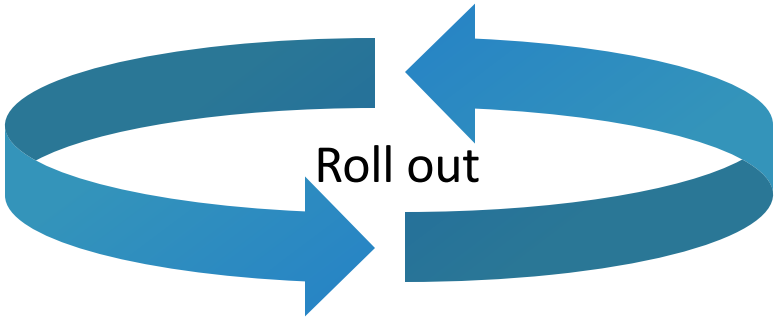
Creating Information Security rules in a new organisation:



Create Information Security rules

- Organise a first meeting with the entire staff (small companies) or staff representatives (large companies). In an interactive workshop, explain information security and the risks and selected controls.
- Adapt this template in and after the workshop, until it fits your organisation.
- Let management approve a final version.

Rolling out new rules



Roll out Information Security rules

- Make the final version available inside the company.
- Include the rules in **security awareness training** for all current staff. Make sure the training matches the rules!
- Include the rules in **HR templates** (new contracts, internship agreements). Every employee should receive a copy of this document as appendix to the employment contract and sign this version as part of the contract.
- Ask people to sign a new contract when they get their next raise

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/