Img: Eduardo Garcia-Nieto

ISO 27001 – A7 Physical Controls

SieuwertExplains

youtube.com/@sieuwertexplains

Agenda

How do physical controls fit into the overall structure

ISO 27001 A7 physical controls

How to implement the controls

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

14 **physical** controls

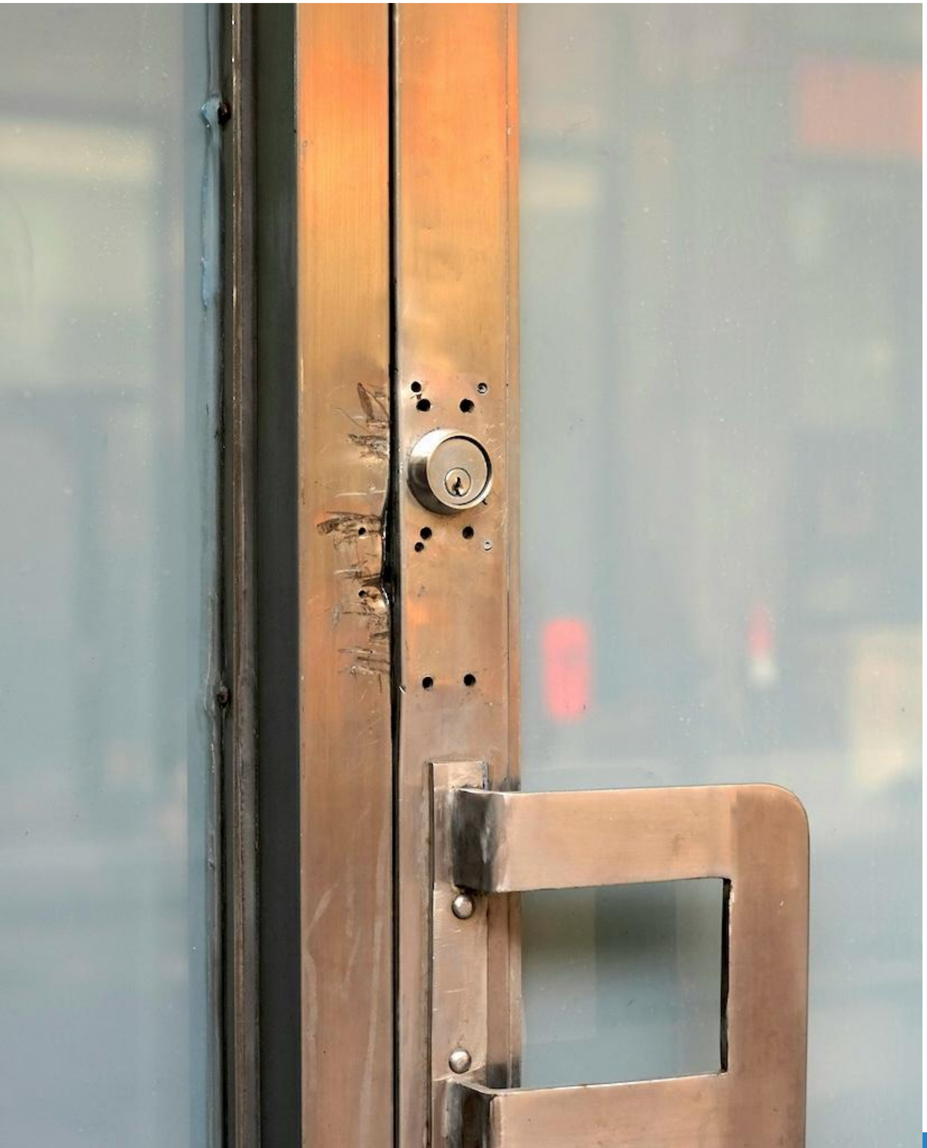
7.1
7.2
7.3
7.4
7.5
7.6
7.7
7.8
7.9
7.10
7.11
7.12
7.13
7.14

Focus of this video

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	

Physical controls risk

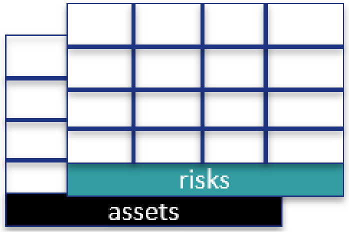


Many organisations have their data stolen or IT disrupted due to physical no-digital events:

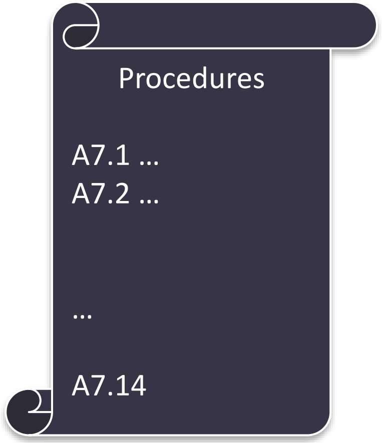
- Break-in and theft from their office at night
- People sneaking into their office and stealing equipment
- Cleaners accidentally working in the server room
- Fires

ISO 27001 has therefore included multiple controls aimed at physical security.

Where/how to implement physical controls



- Describe your assets (e.g. buildings / offices, archives)
- Identify physical security risks



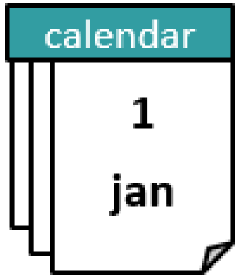
Procedures

A7.1 …
A7.2 …

…

A7.14

- Describe how you apply / implement each control



Plan recurring activities from your controls. E.g.

- Building inspections

Per action / control, some unique, original document, e.g.:

- Office design docs
- Inspection reports

Agenda

How do physical controls fit into the overall structure

ISO 27001 A7 physical controls

How to implement the controls and fit into the overall ISO 27001 structure

7.1 Physical security perimeters

“Security perimeters shall be defined and used to protect areas that contain information and other associated assets.”

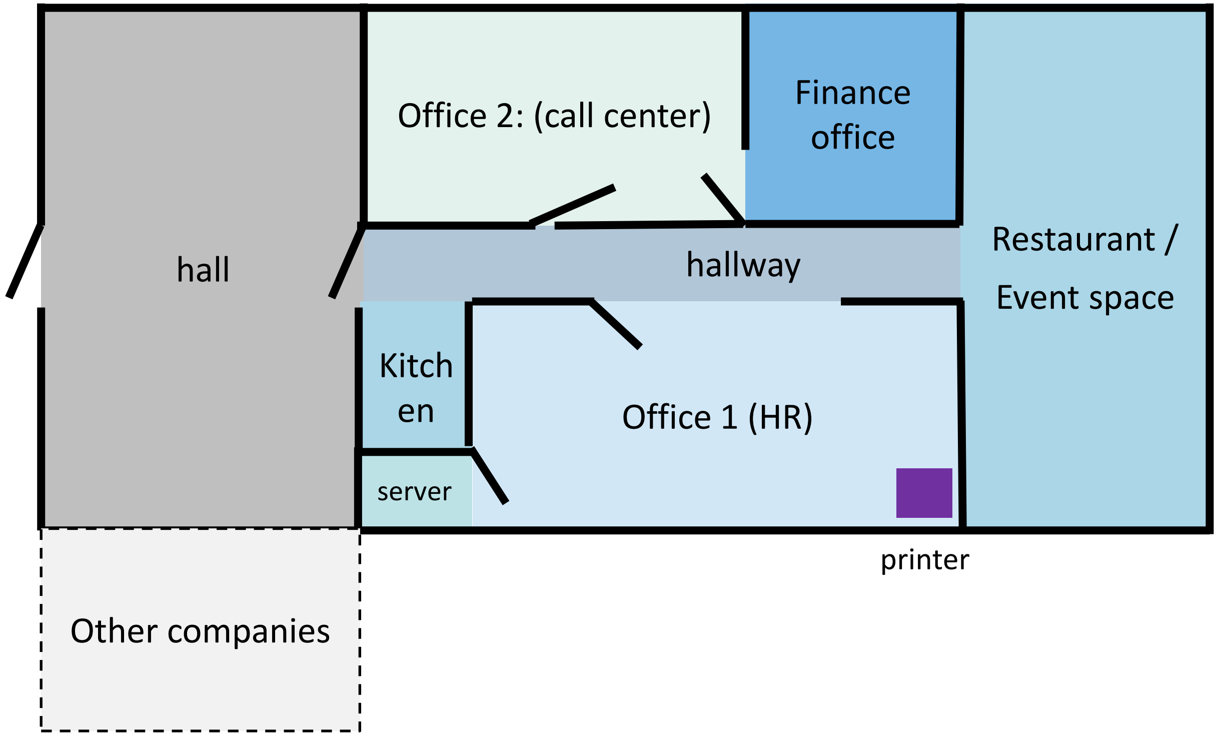
You must created a design document for your office, that defines how the physical security intends to work.

It is useful to make a color scheme, with allowed use and access. An example color scheme could be:

- **Green:** accessible to staff and visitors. No sensitive information should be left in these areas
- **Yellow:** only accessible to our own staff.
  Red: Storage area/location for sensitive assets/information. These rooms/areas should be locked when not supervised.

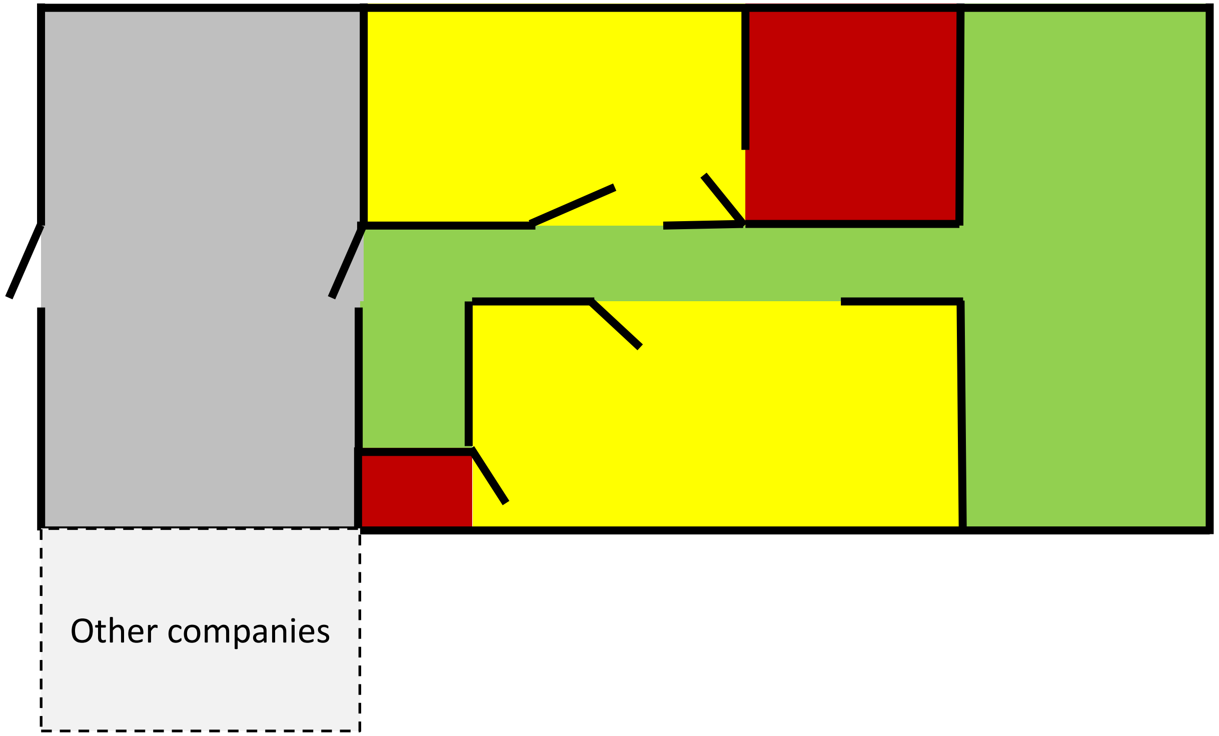
You can define more colors/zones as needed (e.g. chemical rooms, labs, therapy rooms)

Example office: how would you zone each room in this example?



- ⬜ Not in scope
- 🟩 Green: staff and visitors allowed
- 🟨 Yellow: Staff only
- 🟥 Red: restricted, locked when not used

7.1 Physical security perimeter - example



- ⬜ Not in scope
- 🟩 Green: staff and visitors allowed
- 🟨 Yellow: Staff only
- 🟥 Red: restricted

How physical security will be audited

The auditor will :

- check you have a clear and suitable design how each room should be used
- Check that you use each room as intended (e.g. no ultra secret assets in rooms not intended for such assets
- Check that you have security measures (doors, locks, alarms)

The auditor will use their experience to check practical aspects and risks. They may find practical issues, such as:

- Stacks of confidential documents
- Laptops / USB sticks not stored properly
- Packaging stored in server rooms

7.2 Physical entry

“Secure areas shall be protected by appropriate entry controls and access points.”

You need to document how you use doors, locks, keys, tags, access code panels. You need to describe which rooms/zones have doors, who gets a key.

- Depending on your organisation size, also document who hands out keys and whether you will keep a registry of keys.
- You can make additional procedures, e.g. annual key check, tags, alarm systems with code. Make sure you fully describe the actual situation so that it can be audited.

Draft in the InfoSec procedures document:

Secure areas are locked off from common areas, and the access to them are authorized and documented. Non-personnel such as visitors are accompanied, and their identity is authenticated.

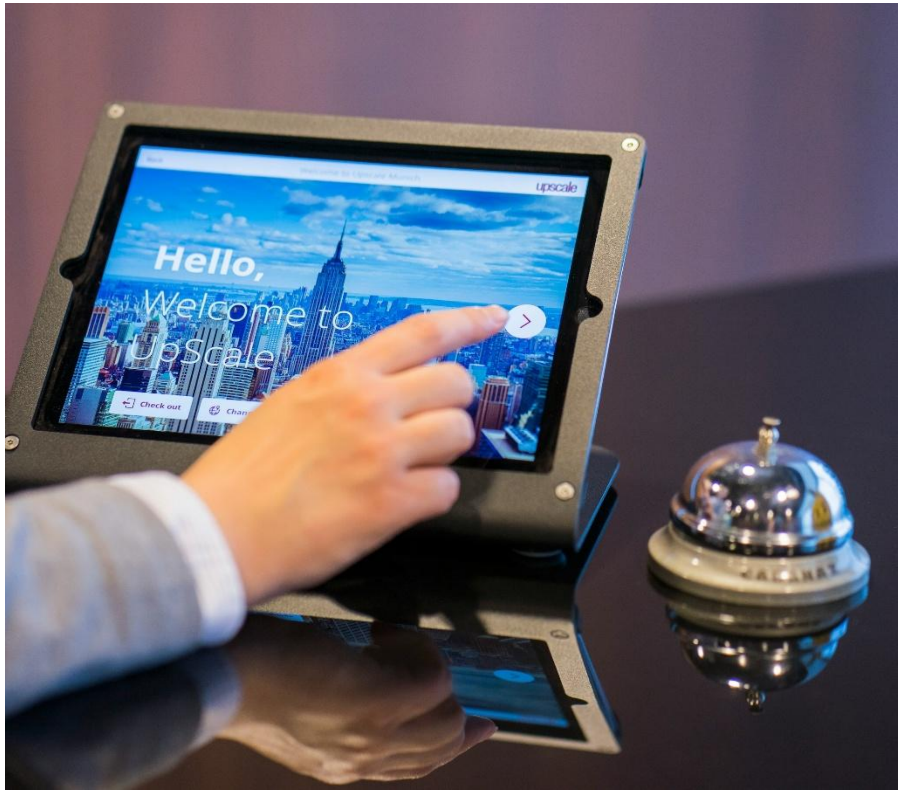
To avoid any (accidental) unauthorized access to other parts of the organization, the delivery takes place at the front desk or to employees’ home address.

7.3 Securing offices, rooms and facilities

“Physical security for offices, rooms and facilities shall be designed and implemented.”

You can think of additional security measures here, such as:

- Bars for windows
- Frosted glass foil to make sure people cannot see sensitive docs from outside the rooms
- Manned reception desk and visitor log
- Rules for locking cabinets outside officer hours



Src: proxyclick-visitor-management-system

7.4 Physical security monitoring

“Premises shall be continuously monitored for unauthorized physical access.”

- You need to carefully consider how you will use monitoring equipment, such as camera’s and alarm systems.
- When applying these, you need to balance security with privacy laws and employee laws. E.g. you cannot continuously monitor employees or record visitors without warning.

If you use camera’s, document somewhere:

- When camera’s are on (24/7 or only at night and in weekends)
- Who watches the cameras
- If the camera footage is stored, where and for how long

Src: MF Mohomed

7.5 Protecting against physical and environmental threats

“Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.”

You should decide what you are doing against fire, flood and earthquakes. You could for instance have:

- Sprinklers and fire drills
- Use watertight compartments or raise equipment from the floor
- Use earth quake resistant building codes or furniture

Draft in the InfoSec procedures document:

[ORGANIZATION] considers the risk of external and environmental threats to be low. All of our data are stored in the cloud and can be access remotely should the physical office be unavailable. All employees have the necessary equipment for homeworking.

7.6 Working in secure areas

“Security measures for working in secure areas shall be designed and implemented.”

You can define certain zones (e.g. red zones) as secure areas. These can be server rooms / data centers , certain labs or your offices for your top-secret government projects

You should then apply additional security measures, e.g. extra keys / tags, rules for accompanying visitors, no electronics allowed, …

Draft in the InfoSec procedures document:

The secure area in [ORGANIZATION] is the server room. The network system and servers are in a secure room, accessed only by [MANAGER]. External staff cannot work in the room alone

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.”

InfoSec rules

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.

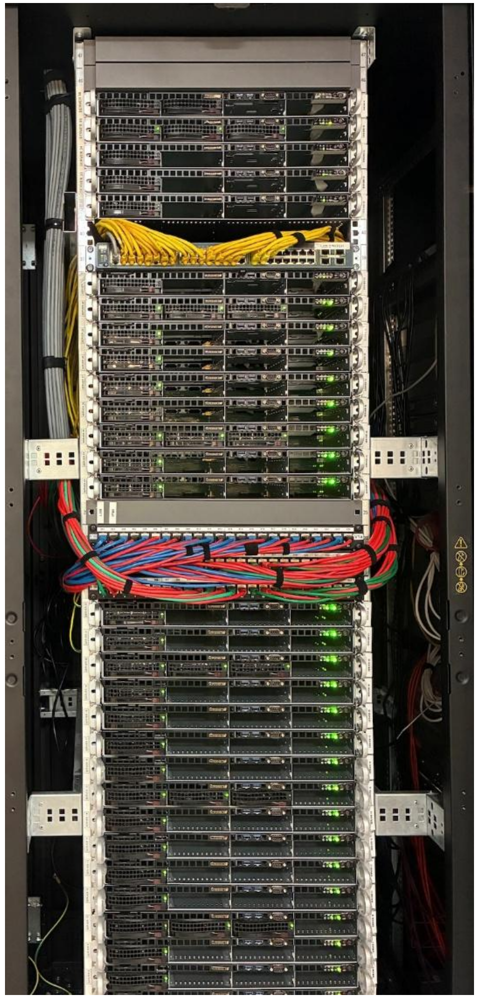
7.8 Equipment siting and protection

“Equipment shall be sited securely and protected.”

You need to document and apply some common-sense rules to prevent mistakes and fire for your server rooms

- All equipment fixed to rack or wall
- Cables are organized, color coded , joined with tie-wraps and / or labelled, no longer than necessary
- No paper storage on or within 1 meter of equipment
- Cooling / air conditioning installed in server room

Note: auditors will visit and inspect server rooms and check the organisation and safety in practice during an office walkthrough. Do your own walkthrough when preparing for audits



7.9 Security of assets off-premises

“Off-site assets shall be protected.”

Depending on your business model, you might have ‘assets’ (equipment or documents) outside your office. Consider:

- Laptops at home or when travelling
- Printers, routers, devices at your clients
- Smart sensors in the city

You should make some common sense rules on how these assets are protected. Consider rules for handling laptops, labelling your equipment clearly, plan retrieval of assets in project closure, …

Draft in the InfoSec procedures document:

Equipment and assets should be properly secured, looked after, and protected.

Devices must have appropriate covers and be transported in suitable bags. They should never be left unattended in public places or in vehicles. All devices must be transported in cabin baggage on airplanes.

7.10 Storage media

“Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements.”

You will need rules for memory cards, USB sticks and portable hard drives since these are often lost. The easiest rule is to forbid the use in your rules document. You should then also inform people via awareness training of this rule.

7.11 Supporting utilities

“Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.”

- You can install a UPS Install a UPS (uninterruptible power supply) for critical systems (it also with surge protection and controlled shutdown procedures).
- Inspections can include monitoring power, cooling, and network availability.
- This control connects to A5.30 where you define fallback options for utility outages (e.g. remote work).

Draft in the InfoSec procedures document:

Supporting utilities are provided and maintained by the building services, who are responsible for inspection and testing. In the event of failures, employees can work remotely.

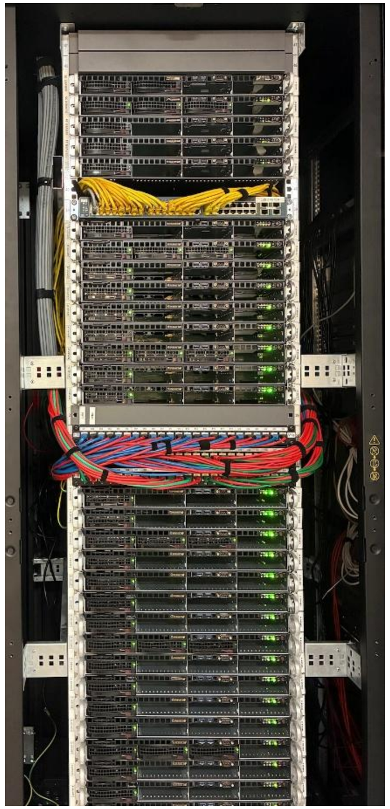
7.12 Cabling security

“Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.”

You can use the same common-sense rules from A7.8 to prevent mistakes. Put this in your procedures document

- Cables are organized, color coded , joined with tie-wraps and / or labelled, no longer than necessary

You can also consider other standards or ideas, e.g. use high quality cables, use VPNs/encryption, have dedicated, shielded cable paths.



7.13 Equipment maintenance

“Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.”

Make sure you have an overview of (types of equipment) you have. As asset register is useful here. Per equipment type you then need to decide if it needs maintenance:

- Routers / Firewalls: need regular information security updates
- UPS-es / equipment with batteries: need annual checks or battery replacements. Some batteries become fire hazards when not maintained!
- Large network-attached printers: might also need regular information security updates

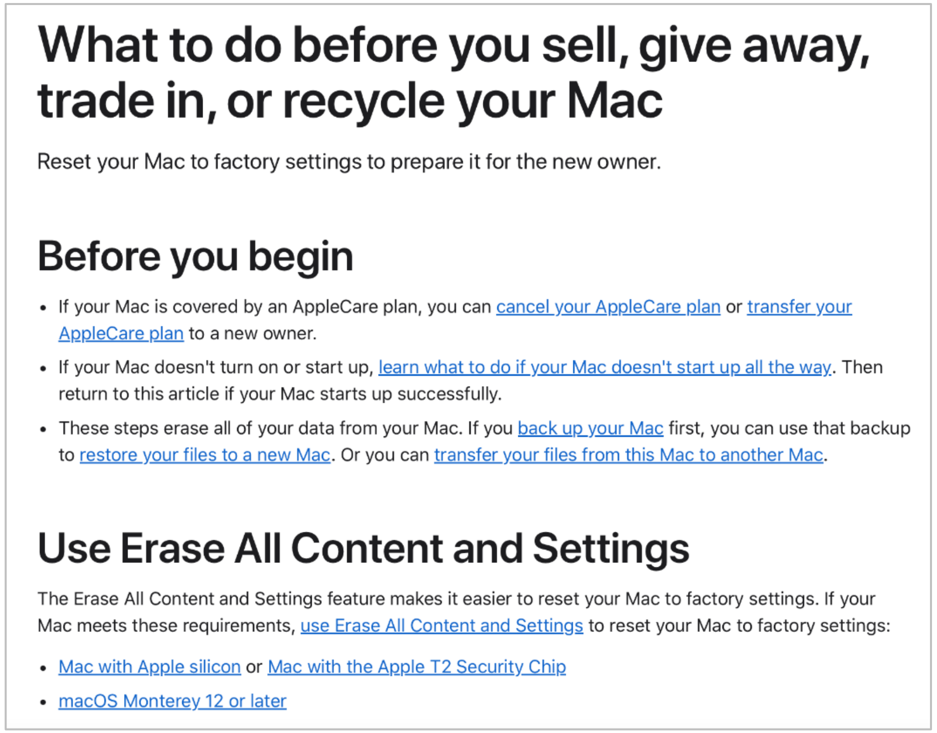
Hire a company to do maintenance, or add maintenance tasks to your annual planning. Make sure you document completed maintenance as evidence of execution

7.14 Secure disposal or re-use of equipment

"Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."

You also need a procedure for securely disposing of old laptops. You cannot give these away to staff or sell secondhand!

- You need to store them securely (in a defined zone) until deletion
- You must make a procedure to use special software or a dedicated company for wiping all data from devices
- You can use instructions from trusted suppliers, e.g. apple. Make sure you store evidence of completed wipes



What to do before you sell, give away, trade in, or recycle your Mac

Reset your Mac to factory settings to prepare it for the new owner.

Before you begin

- If your Mac is covered by an AppleCare plan, you can cancel your AppleCare plan or transfer your AppleCare plan to a new owner.
- If your Mac doesn't turn on or start up, learn what to do if your Mac doesn't start up all the way. Then return to this article if your Mac starts up successfully.
- These steps erase all of your data from your Mac. If you back up your Mac first, you can use that backup to restore your files to a new Mac. Or you can transfer your files from this Mac to another Mac.

Use Erase All Content and Settings

The Erase All Content and Settings feature makes it easier to reset your Mac to factory settings. If your Mac meets these requirements, use Erase All Content and Settings to reset your Mac to factory settings:

- Mac with Apple silicon or Mac with the Apple T2 Security Chip
- macOS Monterey 12 or later

https://support.apple.com/en-us/102773

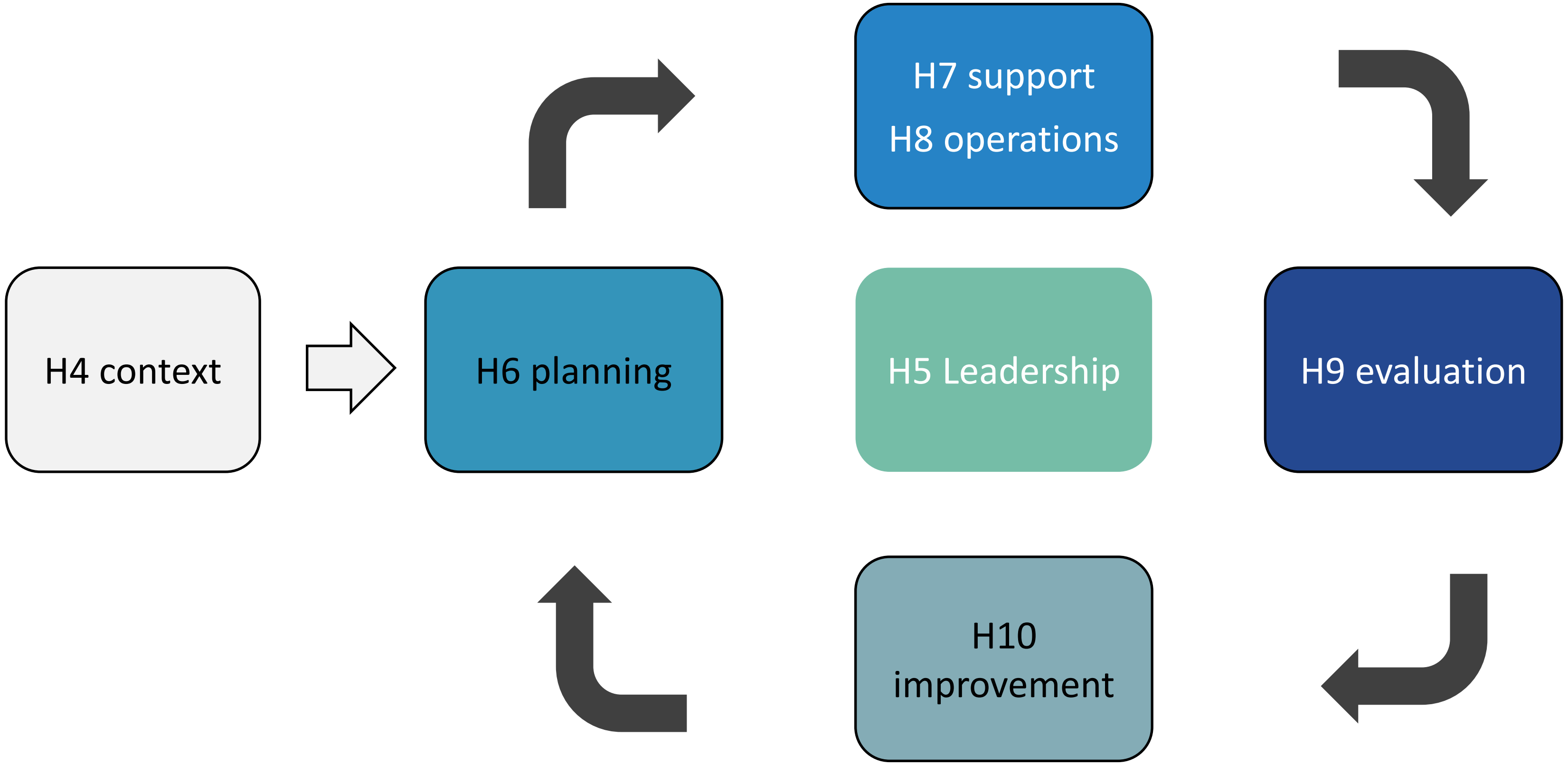
Agenda

How do physical controls fit into the overall structure

ISO 27001 A7 physical controls

How to implement the controls and fit into the overall ISO 27001 structure

ISO ‘harmonized structure’



Each year you use this to update and improve your ISMS:

- Are there new circumstances of new risks (H4, H6)
- Can the implementation be improved (e.g. better locks, better office use, more training) (H7, H8)
- Evaluate: are there any problems, incidents, nonconformities that are physical (H9)? If so, improve (H10)

How to do do physical security well

Short term:

- Take extra steps: Hire additional staff, e.g. reception, gatekeeping, or night managers.
- Organise technical security better. Make sure cameras are monitored, badges are checked and keys are registered
- Make more detailed zoning plans. Give people only access to rooms for their team / department

Long team:

- Use insights from ISO 27001, audits and incidents in your strategic office decisions. When moving buildings, choose more secure buildings
- Select IT suppliers that are interested and can contribute to your standards and practices

How to collect evidence for physical controls

Possible evidence:

- Contracts with specialised parties, e.g. building management, security
- Design drawings or project plans for building renovations
- Reports from completed activities, e.g. maintenance
- Work orders / invoices for improvements to server rooms
- Tickets from reported incidents involving physical security
- Schedule ‘desk checks’ as security officer. During the check make photos of unusual situations

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/