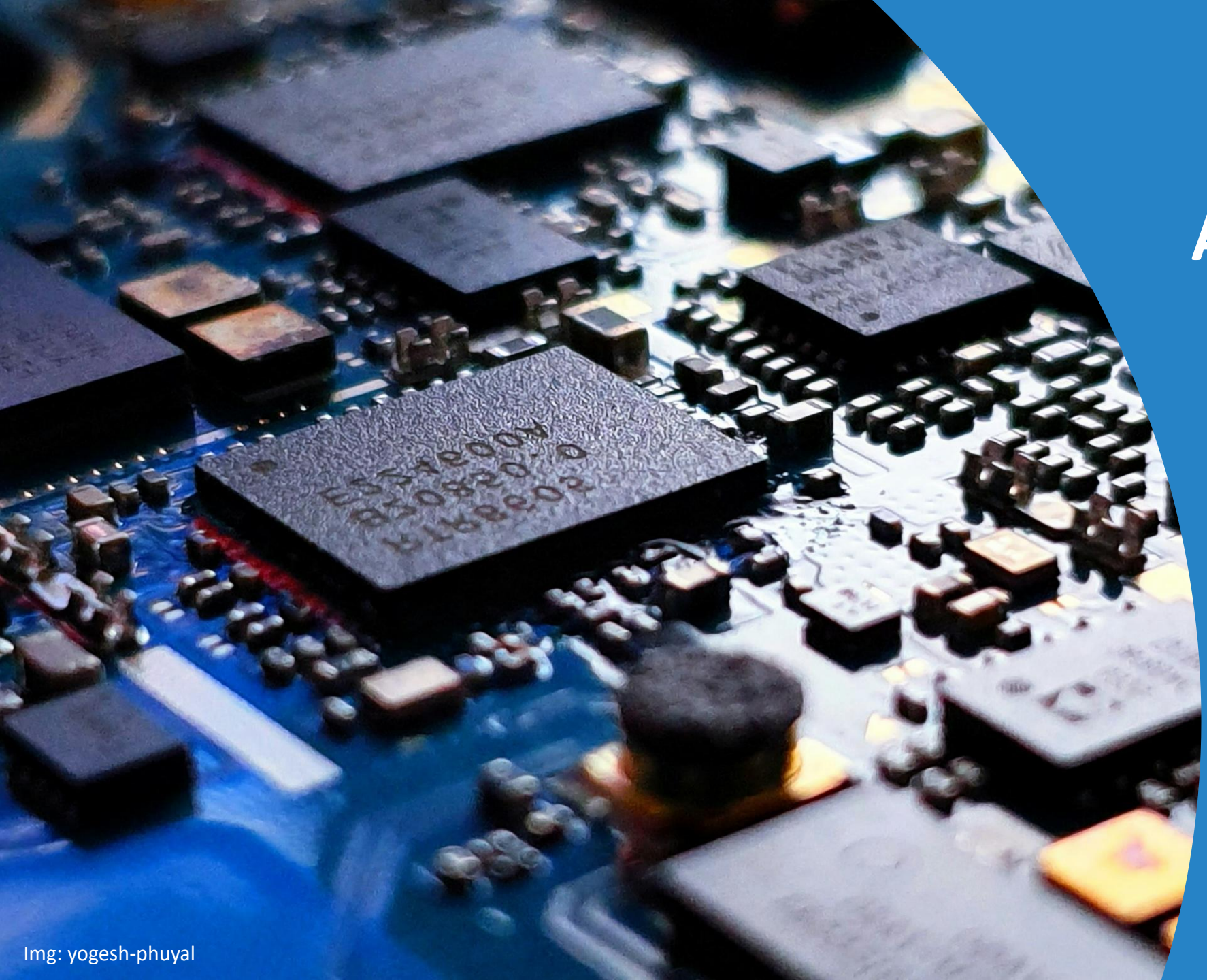


ISO 27001 – A8 Technological Controls

SieuwertExplains

youtube.com/@sieuwertexplains

Img: yogesh-phuyal

Agenda

What are technological controls

Explanation of each control

Tips and tricks for implementing these controls

Technological controls

- The ISO 27001 standard aims to be product- and technology independent. It avoids mentioning specific technological solutions, such as network equipment of firewalls
- As a result, chapter A8 is rather vague. You need to learn about typical solutions and apply these to each control
- It is smart to look for automated, tool based solutions and avoid time-consuming manual checks. These are allowed but not practical

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

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	

Agenda

What are technological controls

Explanation of each control

Tips and tricks for implementing these controls

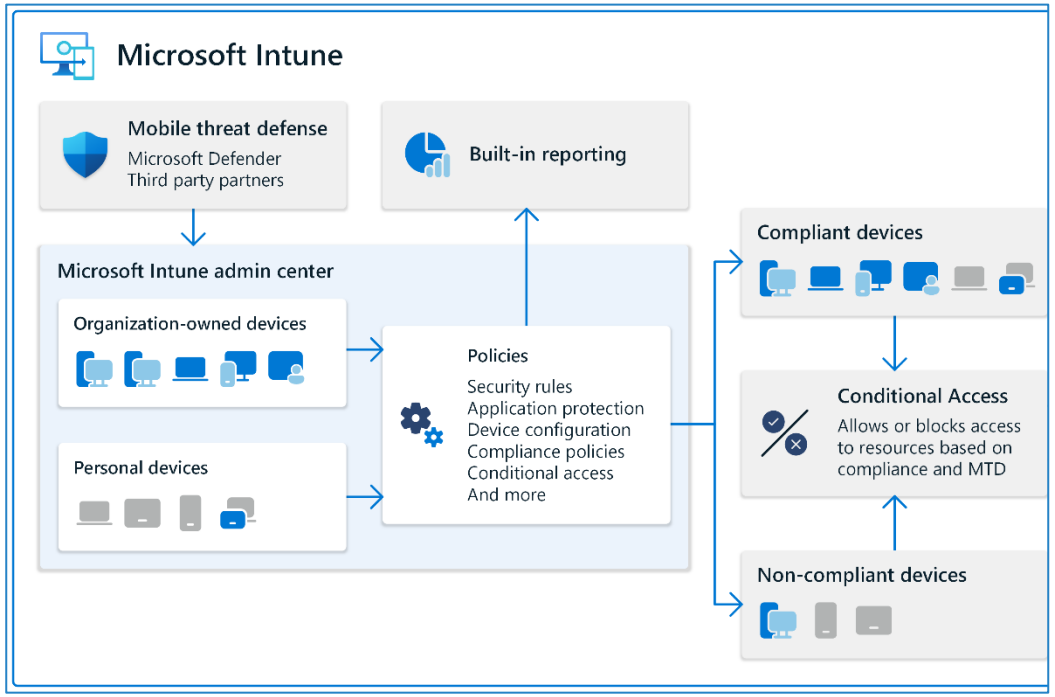
8.1 User endpoint devices

“Information stored on, processed by or accessible via user end point devices shall be protected.”

The goal of this control is to make sure laptops and/or phones have suitable protection:

- Firewall
- Anti-virus software
- Automatic updates
- Restrictions on installed software

The recommended method is to use a Mobile Device Management solution (MDM) so your system administrator can check all devices remotely. Common solutions are Microsoft Intune, Miradore, Kandji, ScaleFusion, …



Src: https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/manage-devices

8.2 Privileged access rights

“The allocation and use of privileged access rights shall be restricted and managed.”

For example: database admin; AWS root accounts; CRM admin rights

Privileged accounts:
- are not for daily/normal use
- should be a separate (unique) identity
- should be given to as few people as possible
- cannot be distributed by a select group of people
- may only be changed based on (service) ticket requests

Draft in the InfoSec procedures document:

Admin access and other unrestricted access (e.g. database passwords) is only given to a very limited set of active administrators who have received additional instructions. These are reserved for platform administrators or IT administrators. One can review in the platform database who is platform admin.

Other users are only provided with regular, non-admin accounts.

8.3 Information access restriction

“Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.”

Draft in the InfoSec procedures document:

…[ORGANIZATION] has an access rights policy that states access to certain systems, assets or information should be limited. These access rights are in practice restricted in exactly that way. Access is reviewed in the quarterly review.

- Mention here the role-based access that you have set up

8.4 Access to source code

“Read and write access to source code, development tools and software libraries shall be appropriately managed.”

Draft in the InfoSec procedures document:

All source code is stored in [STORAGE_SOFTWARE]. Source code of internal applications can by no means be accessible to unauthorized personnel, and personnel authorization is reviewed regularly.

- Choose GitHub, GitLab or another version management system. Split code into multiple repositories and give access to people as needed, based on their role.
- Plan a monthly check of access, to see that no-one that no longer works on that repository still has access to it

8.5 Secure authentication

“Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.”

Draft in the InfoSec procedures document:

The access rights policy states that access to systems is secured, and how users can log on.

- It is important that the role-based access control that you implemented for A5, is also supported by the technology. Describe here how you restrict / provide access (e.g. using Entra groups), who maintains this (e.g. IT manager) and how often you check if access rights are set correctly

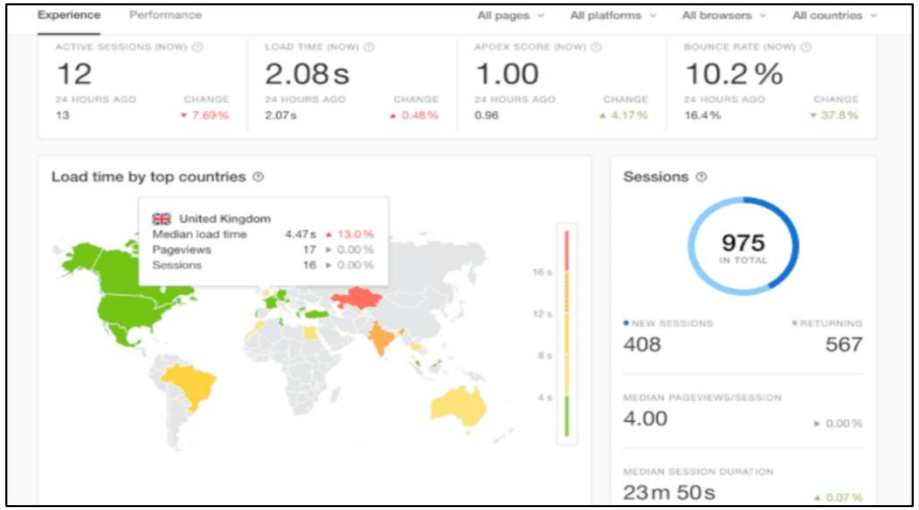
8.6 Capacity management

“The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.”

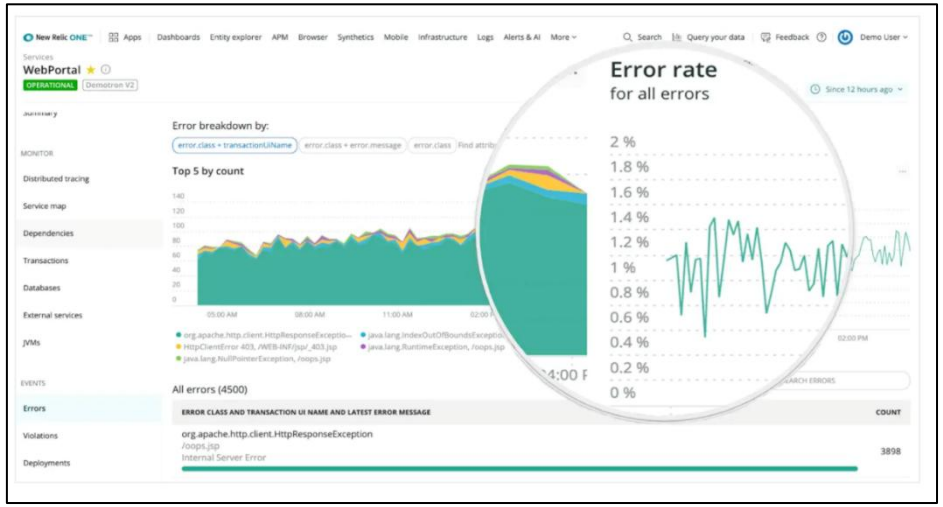
To manage capacity, you must know which systems there are, what the capacity of each system is, whether capacity will change in the future, and how you will monitor the capacity.

There are many different capacity monitoring tools in the market. Some examples include:

- **CloudWatch** for AWS, with metrics and alarms: https://aws.amazon.com/cloudwatch/
- **Pingdom** for testing website/web app availability and speed: https://www.pingdom.com/
- **New Relic** for testing application performance: https://newrelic.com/



Pingdom



New Relic

8.7 Protection against malware

“Protection against malware shall be implemented and supported by appropriate user awareness.”

Draft in the InfoSec procedures document:

All computers (servers, PCs and laptops) must be equipped with a regularly updated virus scanner and a firewall. If possible, users should be prevented from switching off scanners, firewalls or make other security changes. This is recorded using [BitLocker/manually checked by management.]

- You must select an anti-malware solutions, e.g. Bitdefender and roll it out. You might want to combine this with mobile device management
- You must warn people against phishing mails in your awareness training
- Additionally, you can restrict installation of software, use network monitoring, …

Home > Best Products > Security > Antivirus

The Best Antivirus Software for 2026

Antivirus apps protect your PC's personal information, data, bank accounts, and other sensitive information. We've tested more than two dozen utilities to help you choose the right antivirus for your needs.

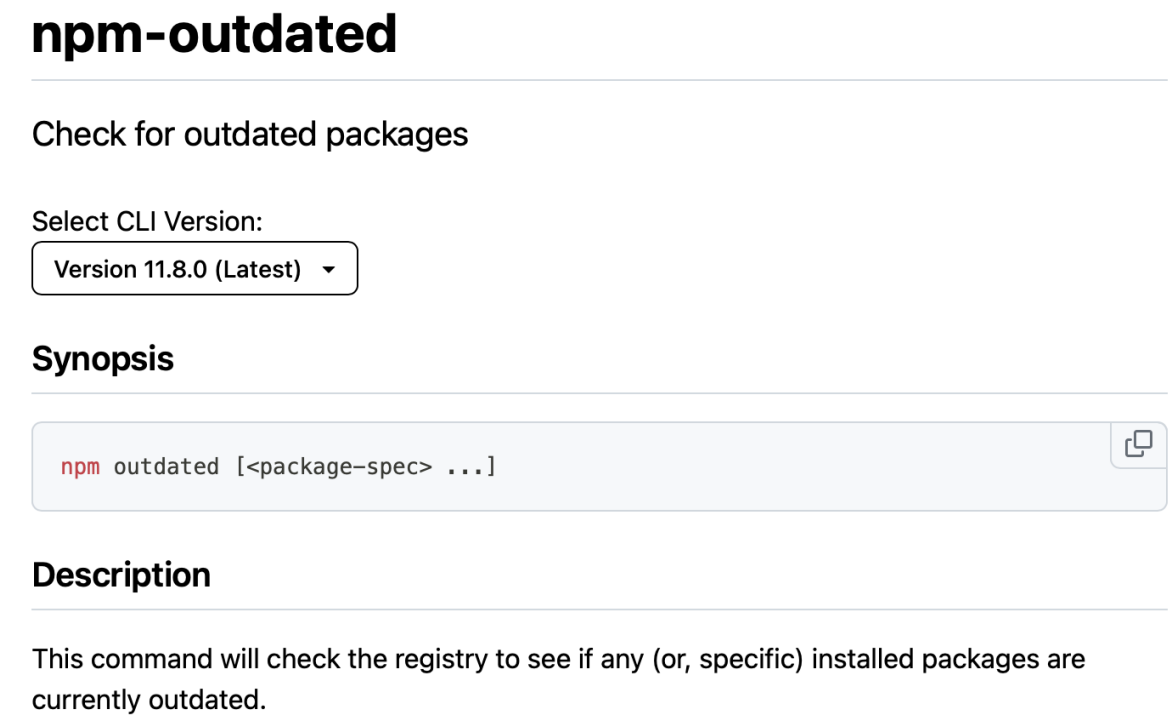
https://www.pcmag.com/picks/the-best-antivirus-protection

8.8 Management of technical vulnerabilities

"Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken."

Possible actions:

- Annual architecture review, identifying all versions of key software components
- Run a software scanning tool for detecting outdated software
- Treat vulnerabilities as incidents: record and take action



https://docs.npmjs.com/cli/v11/commands/npm-outdated

8.9 Configuration management

“Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.”

Draft in the InfoSec procedures document:

Since standard configuration of systems, devices, and software often do not conform to the “security by default” principle, [ORGANIZATION] performs a configuration check for all new systems, devices, networking equipment, and software.

Where possible, the following baseline is followed:

- Disabling unnecessary features/ports/accounts
- Restricting access to administrator features for non-admin users
- Changing default passwords
- …

For assets processing Confidential information, the CIS benchmarks are used.

Once an initial safe configuration is made, a back-up of this configuration is made. This back-up is tested annually.

8.10 Information deletion

“Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.”

When information has served its purpose, it must be deleted by the asset owner.

- The retention requirements for personal data are documented in the GDPR Register of processing activities.
- Different departments (E.g. HR, sales, operations) do an annual cleanup of data whose retention period is expired
- Log files are automatically deleted after the retention period (save a screenshot)

Note: for personal data, you can and should document the retention period in the “Register of processing activities”. For this control specifically, you should identify in which process you can actively delete data, schedule actions and collect evidence that data is actually deleted.

8.11 Data masking

“Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.”

Data, and not just personal data, should be exposed as little as possible. This decreases the risk of incidents. Several techniques to perform this so-called data masking are:

- **Anonymization**: removing identifiers that cause the data to be linked (to e.g. an individual) -> s*****t@ictinstitute.nl
- **Pseudonymization:** replacing identifiers with a reference, e.g. a user ID
- **Access control:** preventing unauthorized access to information

8.12 Data leakage prevention

“Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.”

Data leakage happens when any data is accessible to unauthorized individuals, internal and external. The chance of data leakage can be reduced using technical controls. If not available, you could also use organizational controls:

Technical controls

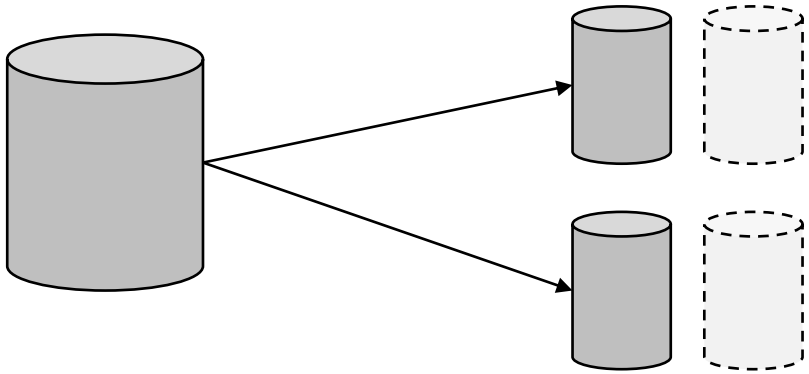
- Microsoft DLP
- ZIVVER
- Watermarking pdf files
- Firewall-level traffic inspection (volume, traffic, and content)
- USB-drive blockers
- Monitoring and alerting on admin activities
- …

Organizational controls

- NDA in place with employees
- NDA’s with contractors and suppliers
- Standard email footer
- Labelling on title page

8.13 Information backup

“Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.”



Three important values for back-ups:
Maximum Tolerable Downtime (MTD): How long can a system be down before serious business impact?
Recovery Time Objective (RTO): What is the time frame we should restore the back-up in?
Recovery Point Objective (RPO): How much data do we wish to restore? (what are we prepared to lose?)

- You must set goals (e.g. RPO of at most 24 hours). You can document this in you business continuity plan. You must then configure backups based on your goals.
- You must schedule a restore test, e.g. monthly or quarterly

8.14 Redundancy of information processing facilities

"Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements."

Draft in the InfoSec procedures document:

We rely om the availability of [STORAGE_SOFTWARE]. Security and availability of processing facilities are managed by [CLOUD] and their information security policies meet our requirements. They provide a flexible service allowing us to increase availability if necessary.

- Cloud providers can offer you redundancy even in different zones
- For large systems, you might want a load balancer and multiple application servers. Ask your architect!

8.15 Logging

"Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed."

Event logging must be enabled for all servers. Events to log include failed login attempts, access rights upgrades, account creation, access to log files, access to sensitive information, etc.

- Logs should be stored securely, protected from tampering, and should contain alerts/notifications for irregular activity
- Restrict administrator access to their own activity logs
- All servers must have a time synchronization service so that activity can be accurately tracked across multiple systems

Tools:

- AWS CloudWatch: https://docs.aws.amazon.com/AmazonCloudWatch/
- Logstash https://www.elastic.co/logstash/
- Papertrail https://www.papertrail.com/
- Datadog https://www.datadoghq.com/

https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

8.16 Monitoring activities

“Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.”

Draft in the InfoSec procedures document:

All logs from software, endpoints, networking hardware and our IAM-solution are sent to [SYSTEM]. Logs are analyzed for use cases and anomalies. The following use cases alert [ROLES]:

- Large data transfers
- Incorrect password more than three times in a row
- Log-in attempt from outside the EU
- …

- Cloud providers can offer you redundancy even in different zones
- For large systems, you might want a load balancer and multiple application servers. Ask your architect!

8.17 Clock synchronization

“The clocks of information processing systems used by the organization shall be synchronized to approved time sources.”

Draft in the InfoSec procedures document:

All servers must have a time synchronization service installed so that log files contain accurate timing information. This is handled by [SYSTEM], which is synchronized to [INTERNAL/EXTERNAL NTP SERVER]

- In case of a cyberattack, investigators will need logs times to be very accurate to help find the first point of entry.
- Please ask your hosting provider for the exact ntp server used and check that all systems / servers use the same reference

8.18 Use of privileged utility programs

“The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.”

Are there any programs that your system administrators use that end users are not allowed to use,? If so, name them in the procedure document and describe how you prevent them.

Utility program examples:

- https://www.phpmyadmin.net
- Windows event manager,
- Remote administration tools

8.19 Installation of software on operational systems

“Procedures and measures shall be implemented to securely manage software installation on operational systems.”

Two considerations:

- Should users be allowed to install software?
- Are devices managed, e.g. using Intune, Miradore, or another mobile device management tool?

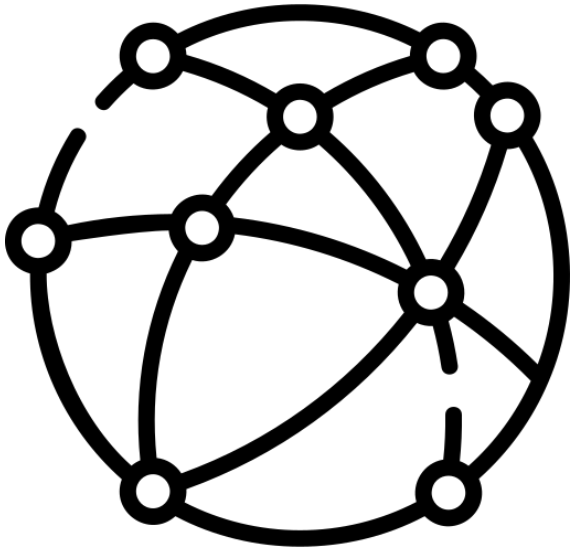
Installation on non-user devices (servers, networking devices, etc.)

- There should be a documented procedure for checking, installing, updating, verifying, and removing software
- Server software installation is automated as much as possible to minimize user errors

https://www.hellotech.com/blog/blue-screen-of-death

8.20 Networks security

“Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.”



Options:

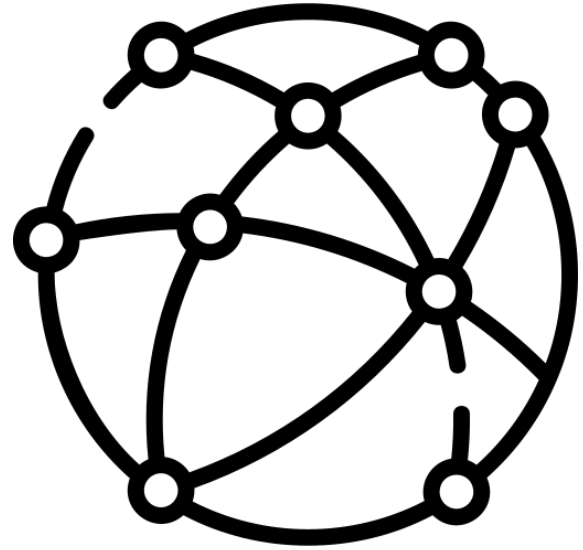
- Password protection on network equipment
- Network monitoring
- Physical security for network equipment
- Separate multiple networks using firewalls
- Mandatory TLS

Ask your network administrator to create a network design document

8.21 Security of network services

“Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.”

There are many ways to protect networks, of which most are technical. Some examples to consider:



Network architecture and segmentation (see control 8.22)

- Networks separation with VLANs
- Zero Trust design
- Demilitarized Zone (DMZ) for public-facing services
- Virtual Private Cloud (VPC) configurations

Technical Protections

- Custom firewall rules
- Network Access Control (NAC)
- MAC-filtering on switches
- Use of VPN’s
- Network-based Intrusion Detection/Prevention System (NIDS/NIPS)
- Network filtering (see control 8.23)

8.22 Segregation in networks [CLOUD CASE]

“Groups of information services, users and information systems shall be segregated in the organization’s networks ”

Draft in the InfoSec procedures document:

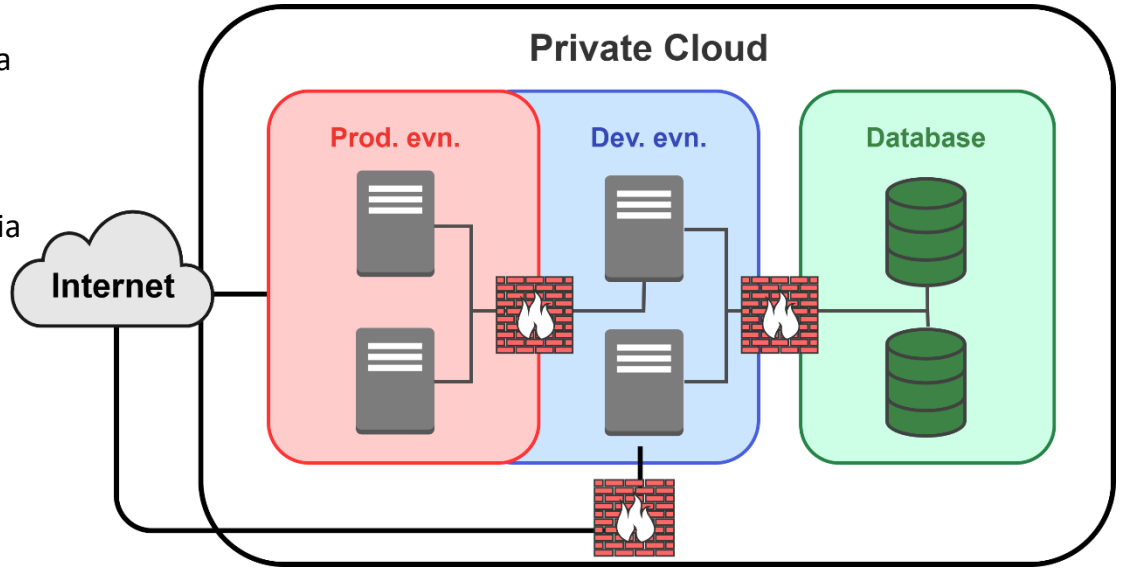
Cloud-specific security policies (e.g., Security Groups) control inbound/outbound traffic between public and internal VPCs, and between internal sub-networks in VPCs, such as development, staging and production environments. Private endpoints are used for service-to-service communication, such as storage and databases.

Public zone:
API gateway, load balancer, production environment via allow-list port (HTTP/S)

Private application zone:
App servers, microservices, containers (admin access via AD, web admin, SSH)

Private dev/testing zone:
Dev. environment (access via SSH, web admin)
Testing/Staging environment

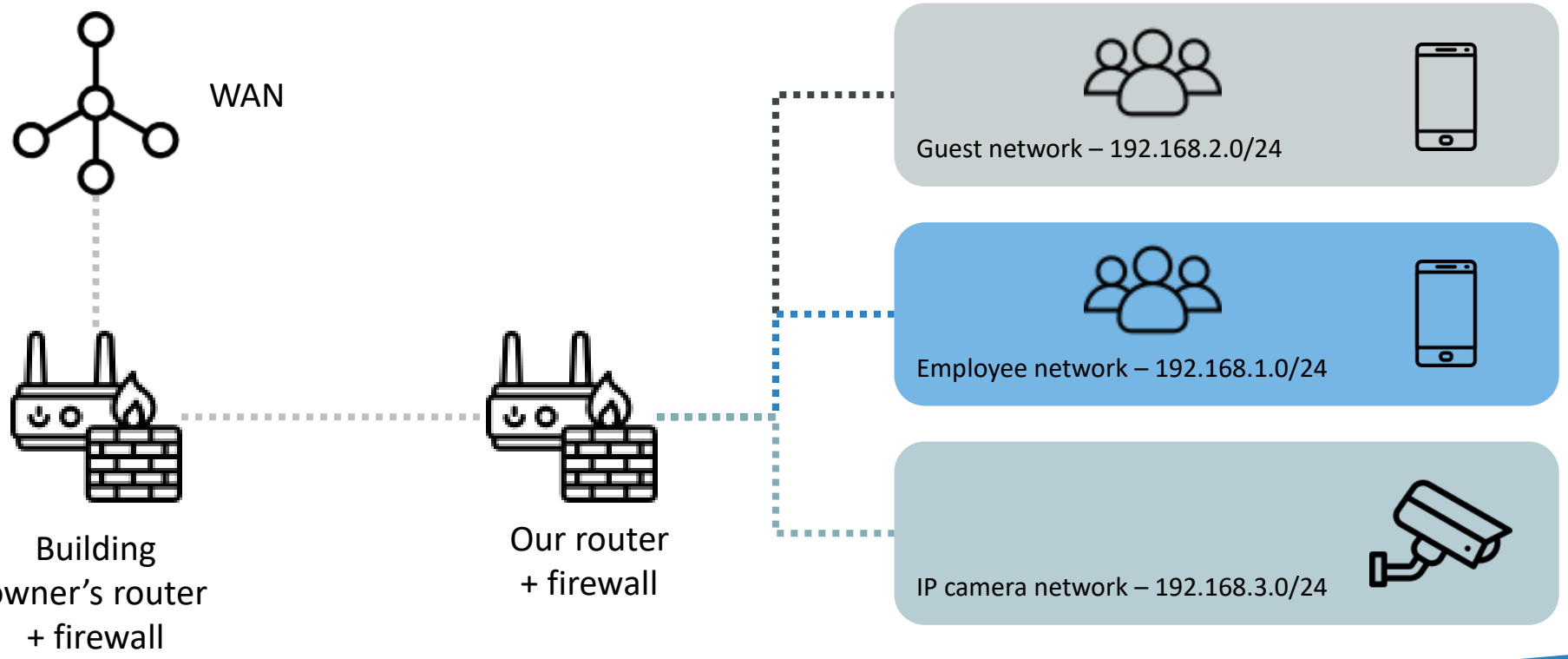
Private data zone:
Databases, storage accessible only within the VPC.



8.22 Segregation in networks [ON-PREM CASE]

"Groups of information services, users and information systems shall be segregated in the organization's networks."

Every device on the network is a possible point of compromise, intended or not. You should, therefore, create separate (virtual) networks. The bare minimum is to create a separate network for guests, but many organizations have several networks that are logically or even physically separated.



8.23 Web filtering

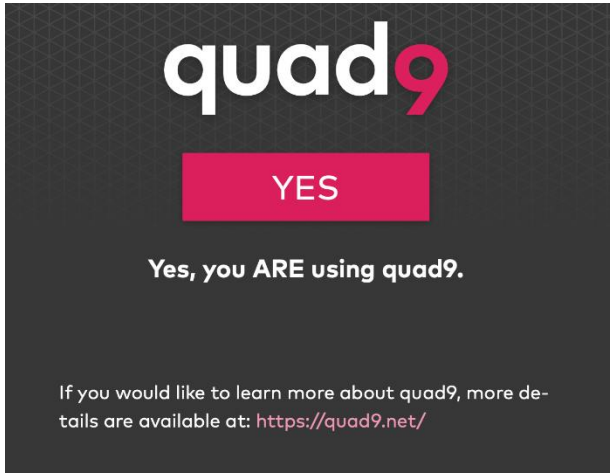
“Access to external websites shall be managed to reduce exposure to malicious content.”

On your company network and device, you can block access to certain websites to maintain a professional and secure environment. The following is often blocked:

- Websites
  - containing violence
  - adult content
  - Gambling
  - Torrenting, pirate and illegal content
- Known malicious websites, phishing URLs
- Command and Control servers, Malvertising

Implemented via DNS filtering on company gateway or user device (Quad9, Cloudflare Gateway, AdBlock lists)

Note: Some jobs might require access to blocked content, so make sure someone is authorized to create exceptions and maintains an overview.



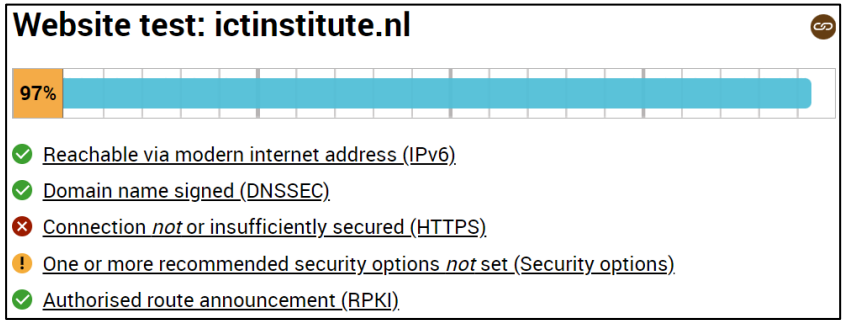
8.24 Use of cryptography

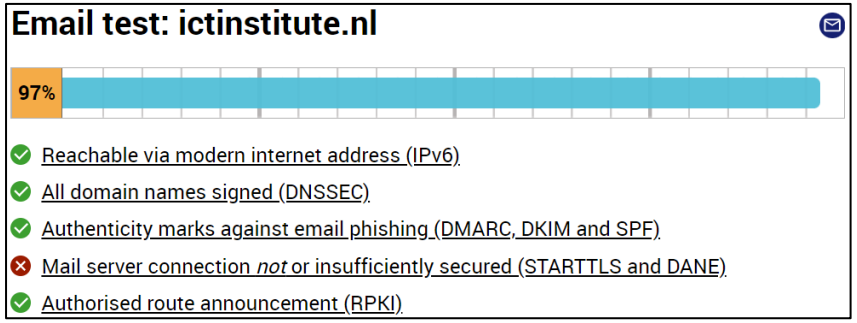
"Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented."

What are the domains/websites you use? Is there an app.xyz.com subdomain? Are the domains and websites adequately secured?

Good practices for cryptography:

- Use of https for all web traffic (TLS version 1.2 or above)
- Minimum server score of "A" in SSL Labs (ssllabs.com)
- **A minimum email score of 70% on internet.nl**
- Algorithm + key combinations create sufficiently strong work functions
- Passwords are stored in hashed format and salted.
- Only currently secure and collision-resistant algorithms are used. (e.g. no MD5)
- Keys are be stored securely in a (password) vault





8.25 Secure development lifecycle

“Rules for the secure development of software and systems shall be established and applied.”

Having a Secure Development Life cycle means that software is not just coded, but there is a structured process including requirements, design, implementation (coding), verification (testing) and release. In each step, information security should get attention:

- **Requirements**: The requirements for each change are documented in tickets / stories, and must contain acceptance criteria. Where applicable, the acceptance criteria include security requirements, such as role based access restrictions, how incorrect input is handled or checks to ensure data integrity.
- **Design**: When needed, the lead developer / CTO creates a design and has this peer reviewed by another developer / architect to make sure it preserves security. This includes checking for sufficient availability/redundancy, proper data storage and ability to reach required performance and not introducing hard to maintain new technologies.
- **Implementation/coding**. Developers must know and apply our coding guidelines
- **Verification/testing**: Code is checked by developer against the acceptance criteria and peer reviewed when checked in. Where possible the development pipeline is automated with automated unit tests and other quality gates are defined.
- **Release**: Software is tested in a staging / acceptance environment first and must be approved by the CTO or product owner before being deployed into production.

https://ictinstitute.nl/iso-27001-controls-software-development/

8.26 Application security requirements

“Information security requirements shall be identified, specified and approved when developing or acquiring applications.”

Example requirements:

- All applications that communicate using the Internet or public networks must use encrypted secure connections for data transport, using TLS.
- The web applications must use encryption that scores at least 60% on internet.nl
- The supplier of each SaaS solution (Software as a Service application) must have a GDPR compliant privacy policy on their website.
- Larger vendors must have ISO 27001 or similar certification
- Applications that are use for confidential data must offer secure authentication, preferably based on single sign on or multi factor authentication
- Applications that are use for confidential data must have role-based access, so that we can give different access rights to different roles in our organisation

https://owasp.org/www-project-application-security-verification-standard/

8.27 Secure system architecture and engineering principles

"Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities."

Example principles that you might want to document for software systems are:

- Use of standard web frameworks when developing web systems. E.g. use of Laravel for PHP or Django/Flask for Python
- Use of cloud infrastructure to ensure secure hosting and scalability
- Implementation of logging of significant events through a standard logging library or service
- Use of REST APIs to protect against data loss or replay attacks
- Securing APIs using session management
- The use of 'least privilege': each component gets only access rights needed
- The use of 'zero trust'. Authorisation should be checked before sharing information
- Ensuring that any traffic is encrypted

Note: if your company makes hardware/devices, this control also covers the hardware design process. Example principles that you might want to document for hardware devices are:

- The application of hardening: configure devices so that the least number of services are exposed
- The use of security-oriented design reviews when making significant changes
- Documentation of security features

8.28 Secure coding

“Secure coding principles shall be applied to software development.”

Draft in the InfoSec procedures document:

All software created by [ORGANIZATION] must conform to the Secure Coding Standard. This standard is as follows:

- No hardcoded passwords/secrets
- No hand-made cryptography
- Input validation
- Cross-Site Scripting prevention
- Cross-Site Domain Forgery protection
- Timing attack prevention
- Parameterization
- Signing new builds
- Fail secure (no revealing information in errors)
- …

All staff are trained at least annually in secure software development. The basis for the training is the OWASP top 10 or OWASP ASVS

8.29 Security testing in development and acceptance

“Security testing processes shall be defined and implemented in the development life cycle.”

Internal procedures
- Checklist new systems should adhere to
- Criteria for when to test.
- Automated functionality tests

Tools
- Invicti: web application security scanner www.invicti.com
- SonarQube: open-source static code analysis www.sonarqube.org

Acceptance testing:
- Telerik: UI testing www.telerik.com
- Burp Suite: web vulnerability scanner www.portswigger.net/burp
- Nessus: vulnerability scanner www.tenable.com/products/nessus

8.30 Outsourced development

“The organization shall direct, monitor and review the activities related to outsourced system development.”

Not all development can be done in-house, so you should establish procedures and keep a close eye on external development. The purpose is to supervise and manage the external party. Examples are:

- A thorough agreement must be drawn up prior to the collaboration
- The requirements must be crystal clear
- The organization must be able to check the development process
- Deliverables should be tested before formal acceptance

Don’t forget: website development is also development!

8.31 Separation of development, test and production environments

“Development, testing and production environments shall be separated and secured.”

Draft in the InfoSec procedures document:

For all major IT systems, tests must be carried out in separate test environments before and after changes or tests can be run in production.

Developers do not have unregulated access to the production environment.

We have a secure development policy, based on the OWASP top 10 web application risks. Only developers have access to the development environment. The development environment is fully segregated from production and acceptance environments.

[IN CASE APPLIES]

No specific controls are in place, since our risk analysis has indicated this is not a significant risk. The same security measures are in place for production and acceptance.

8.32 Change management

“Changes to information processing facilities and information systems shall be subject to change management procedures.”

Draft in the InfoSec procedures document:

Any changes to and inside the organization that may affect the information security are controlled and approved by management. Such changes can, for example, be the use of a new system or change in an important business process.

The ticketing system [TICKETING_SOFTWARE] is used to document all changes. Changes are reviewed by [ROLE] before implementation and must meet the quality standards set out in our development policy.

After a change, operational systems are reviewed on their performance and security. The change might have negatively influenced the system or overall information security and/or performance.

Software packages require updates every once in a while, which can be minor or major. A procedure for updating software is in place: The major version is pinned and minor version are accepted when they become available.

8.33 Test information

“Test information shall be appropriately selected, protected and managed.”

You have two options here:

1. Create a completely made-up dataset that will be used in testing. This is the best option when there are many external and/or temporary testers that have not gone through background verification. Screenshots based on this dataset can be safely used in bug reports or user documentation without risk of data breaches.
2. Use an anonymised copy of production data. You can anonymise a dataset by replacing full names and numbers with shortened versions (Anthony becomes A****y), and perhaps shorten some fields and swap other fields. The benefit of this option is that you have a better opportunity to catch errors that only happen with certain input. The downside is a high risk of data breaches. In some fields, e.g. medical fields, specific regulations exist that forbid the use of customer data in acceptance environment.

Draft in the InfoSec procedures document:

Anonymized copy of production data is used in acceptance. In test environments no production data is used.

[IN CASE APPLIES]

Dummy dataset is used in testing. Screenshots based on this dataset can be safely used in bug reports or user documentation without risk of data breaches.

Development and testing tips

Rules for secure software development:

- *Validate all user input in the backend. Test for unreasonable length and unexpected characters.*
- *Make sure that database queries are well structured by using special functions to compose queries.*
- *When displaying user input, be careful that there is no JavaScript in the text. Make sure the code is not running.*
- *Always use authentication and authorization.*
- *Test on unhappy flows: wrong input, users with too few rights, functions that do not work.*
- *Always make sure to log problems and unexpected things.*
- *Do not provide information in error messages.*
- *Remove or move default pages, such as wp-admin to a unique location.*
- *Use unique usernames, not default names like admin, system, default.*
- *Always use strong passwords, for example for database access.*
- *Document how risks from the OWASP Top-10 are mitigated.*

8.34 Protection of information systems during audit testing

“Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.”

Audits may require in-depth access to a lot of information, which should not interfere with the day-to-day activities of staff nor the functioning of operational systems.

To ensure a smooth audit, required access and scope must be approved in advance by management and auditors must be given read-only access.

For this, you should create a procedure for internal security audits, requested by management, carried out outside the information security team.

Agenda

What are technological controls

Explanation of each control

Tips and tricks for implementing these controls

Roles to be involved

Role	ISMS responsibility	Requirements
CIO / IT manager	Decide in technological control implementations Monitor correct execution of controls and procedures	M SC in IT or related field
Software architect	Define and help implement secure engineering principles	5+ years of sw development experience
Software developers	Apply secure coding guidelines and do security testing	Completed secure sw development training
IT operation staff	Implement selected technological controls and store measurements and results	B Sc in IT or related field

How to document controls

Scan

- Check for existing policies / documentation, and reuse text or refer to existing documents
- Ask current dev-ops staff for the current way of working

Fix

- Fix obvious risks and fill in “risk treatment plan” in the risk inventory
- Make sure all knowledge resides with multiple people
- If required, set explicit goals or define policy

Document

- Document your decisions on controls in a practical document (e.g. procedures document)
- Fill in “Statement of Applicability”

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/