What is ISO 27001?

and why do organisations need it?

SieuwertExplains

youtube.com/@sieuwertexplains

Contents

- Why companies need ISO 27001
- What is the essence of ISO 27001
- How you can use ISO 27001 in your career

Why ISO 27001

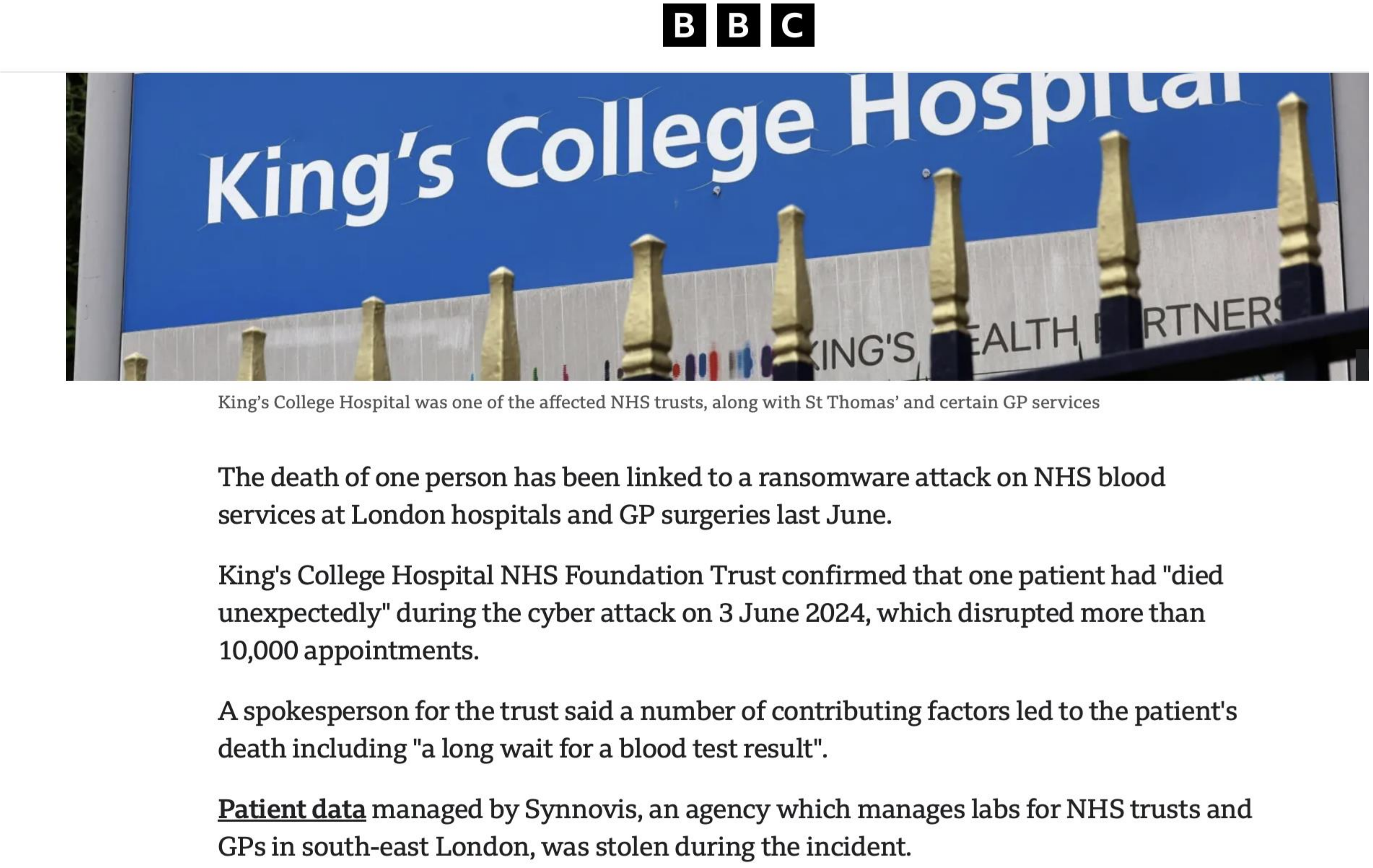
Our society faces many digital threats, including:

- Cybercrime
- Loss of data
- Mismanagement of information

Consequences:

- Significant direct damage, e.g. loss of material, loss of reputation
- Liability and claims for companies, since companies are required to take care of information
- Impact on people, e.g. loss of privacy

Example: ransomware



King's College Hospital was one of the affected NHS trusts, along with St Thomas' and certain GP services

The death of one person has been linked to a ransomware attack on NHS blood services at London hospitals and GP surgeries last June.

King's College Hospital NHS Foundation Trust confirmed that one patient had "died unexpectedly" during the cyber attack on 3 June 2024, which disrupted more than 10,000 appointments.

A spokesperson for the trust said a number of contributing factors led to the patient's death including "a long wait for a blood test result".

Patient data managed by Synnovis, an agency which manages labs for NHS trusts and GPs in south-east London, was stolen during the incident.

In a ransomware attack, cybercriminals take control of computers and data and lock them.

The company then has to pay money (a ransom) to get access to their data

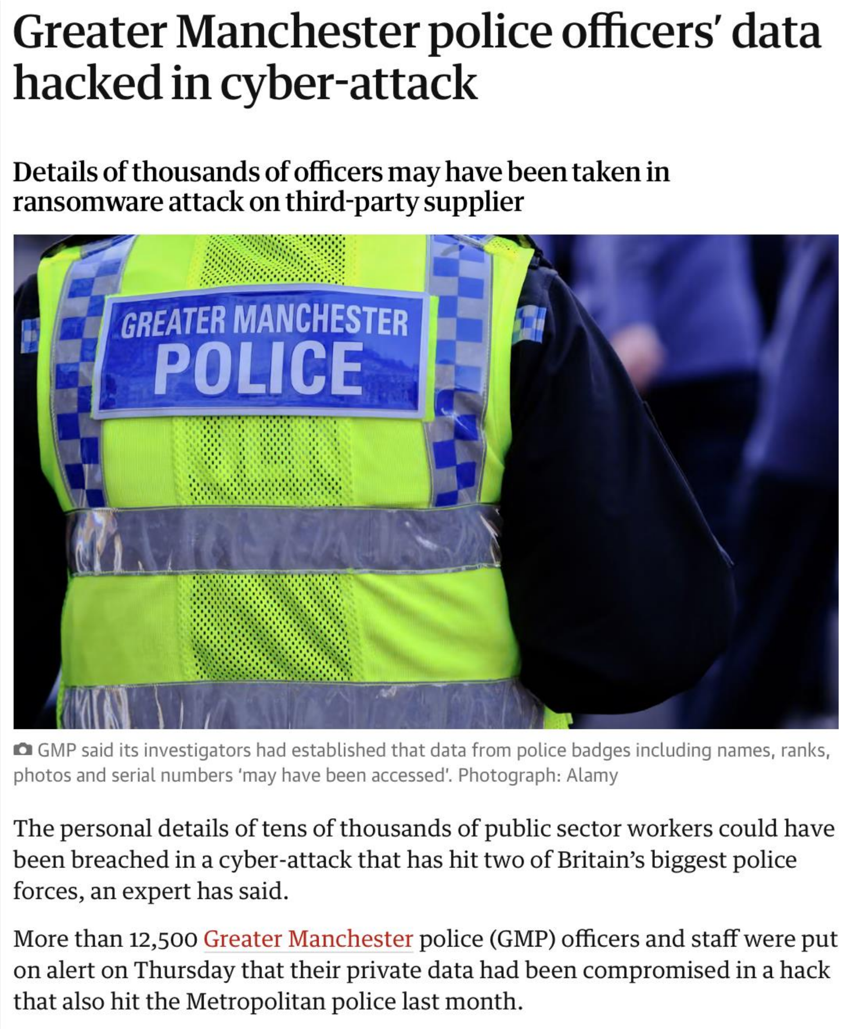
Ransomware attacks are very successful and there is an entire ransomware industry

https://www.bbc.com/news/articles/cp3ly4v2kp2o

Data breaches

In a data breach, personal data is leaked or stolen and this has an impact on the privacy of the people involved (police officers in this case).

Data breaches must be reported, so there is an immediate effect on company reputation



Greater Manchester police officers' data hacked in cyber-attack

Details of thousands of officers may have been taken in ransomware attack on third-party supplier

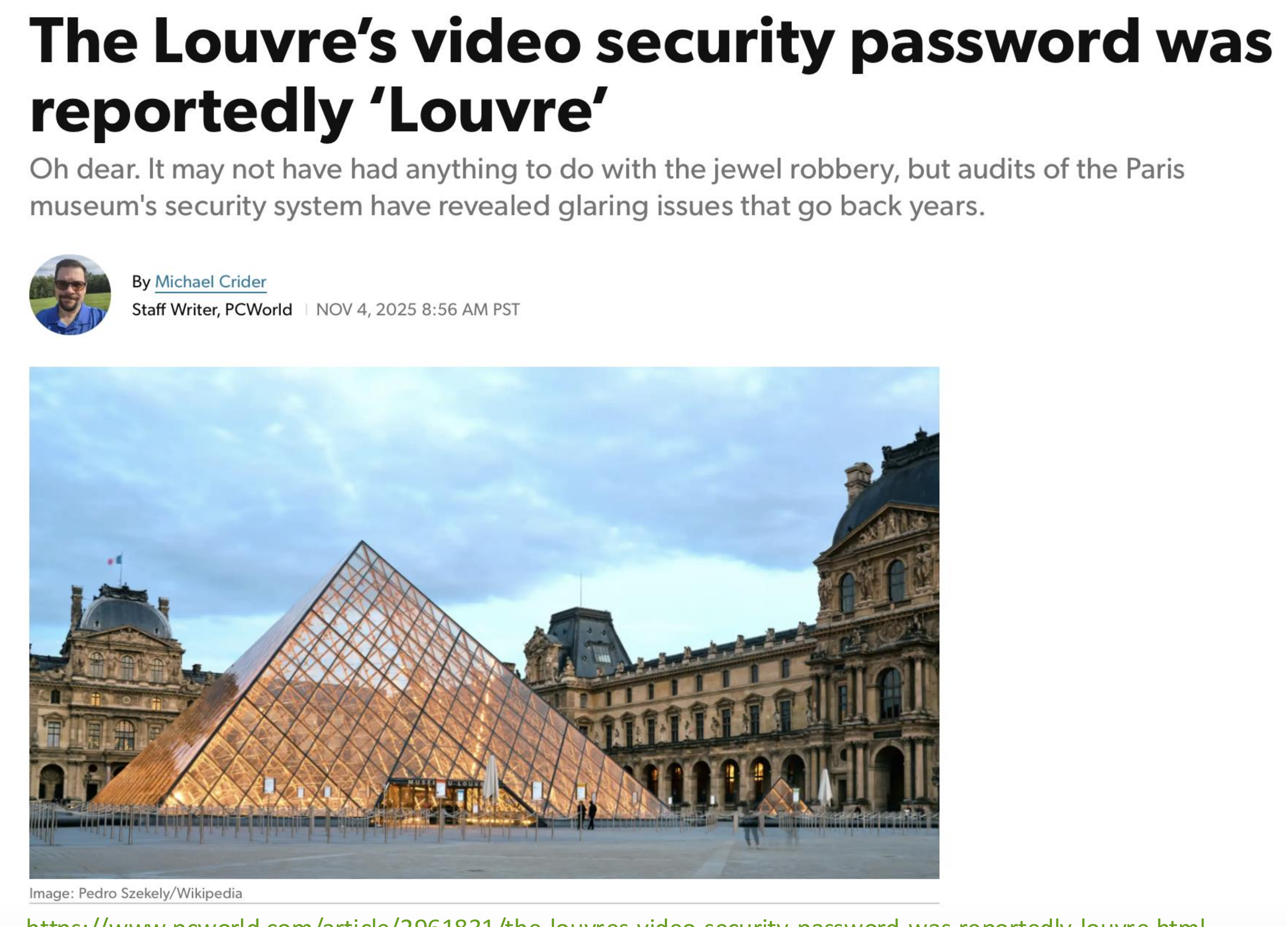
GMP said its investigators had established that data from police badges including names, ranks, photos and serial numbers 'may have been accessed'. Photograph: Alamy

The personal details of tens of thousands of public sector workers could have been breached in a cyber-attack that has hit two of Britain's biggest police forces, an expert has said.

More than 12,500 Greater Manchester police (GMP) officers and staff were put on alert on Thursday that their private data had been compromised in a hack that also hit the Metropolitan police last month.

https://www.theguardian.com/uk-news/2023/sep/14/greater-manchester-police-officers-data-hacked-in-cyber-attack

Information Security at Louvre



The Louvre’s video security password was reportedly ‘Louvre’

Oh dear. It may not have had anything to do with the jewel robbery, but audits of the Paris museum's security system have revealed glaring issues that go back years.

By Michael Crider
Staff Writer, PCWorld | NOV 4, 2025 8:56 AM PST

Image: Pedro Szekely/Wikipedia

https://www.pcworld.com/article/2961831/the-louvres-video-security-password-was-reportedly-louvre.html

Information security measures, such as a good password policy, can help prevent physical theft such as the recent theft of paintings from the Louvre.

Rules for strong passwords is one of the recommended controls in ISO 27001. ISO 27001 thus helps strengthen organisations against incidents

Using ISO 27001 does not fully prevent incidents. It reduces risks but does not eliminate them fully.

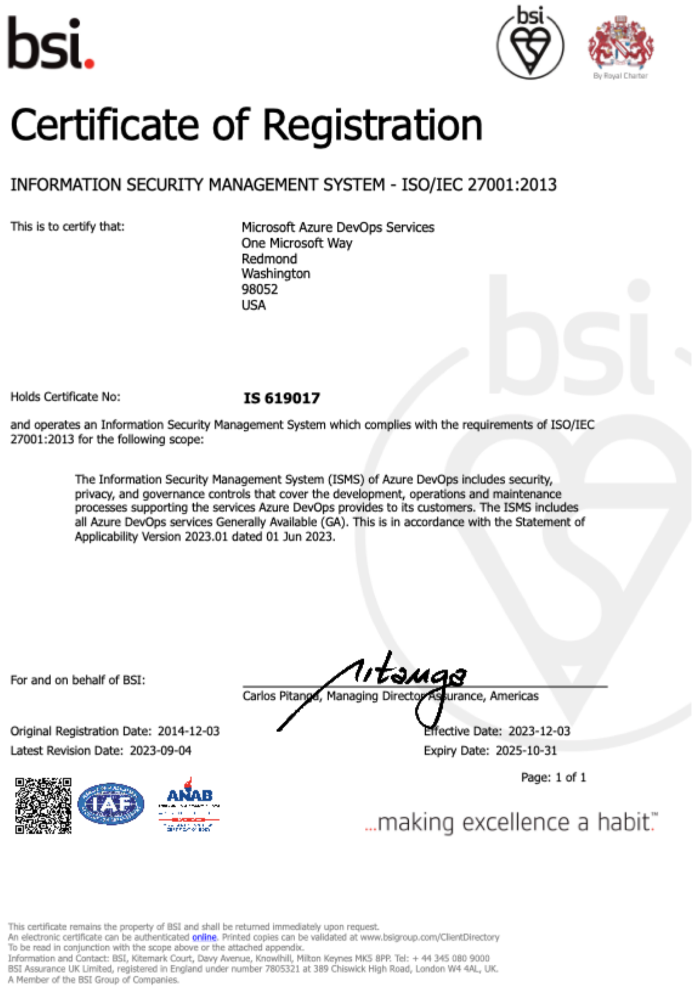
What does ISO 27001 offer to companies

- ISO 27001 is a structured approach to information security. It makes sure that all individual actions are coordinated and lead to genuine improvement.

- ISO 27001 is a standard that has a certification scheme. Companies with many customers can save a lot of time by getting one external audit and certificate and showing it to all customers, instead of having each customer ask about all security measures.

- ISO 27001 is not legally required, but the most convenient way to demonstrate compliance to broader goals such as “adequate security measures”

Example certified company



bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Microsoft Azure DevOps Services
One Microsoft Way
Redmond
Washington
98052
USA

Holds Certificate No: **IS 619017**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

> The Information Security Management System (ISMS) of Azure DevOps includes security, privacy, and governance controls that cover the development, operations and maintenance processes supporting the services Azure DevOps provides to its customers. The ISMS includes all Azure DevOps services Generally Available (GA). This is in accordance with the Statement of Applicability Version 2023.01 dated 01 Jun 2023.

For and on behalf of BSI:

Pitanga

Carlos Pitanga, Managing Director Assurance, Americas

Original Registration Date: 2014-12-03
Latest Revision Date: 2023-09-04

Effective Date: 2023-12-03
Expiry Date: 2025-10-31

Page: 1 of 1

...making excellence a habit.™

This certificate remains the property of BSI and shall be returned immediately upon request.
An electronic certificate can be authenticated online. Printed copies can be validated at www.bsigroup.com/ClientDirectory
To be read in conjunction with the scope above or the attached appendix.
Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Microsoft is a supplier to many hospitals, universities and government organisations that must ask their suppliers to demonstrate adequate information security.

Microsoft, being a practical company, has therefore asked an external company, BSI, to do a certification audit.

The external perspective is helpful to demonstrate compliance

https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

The legal basis for Information security requirements

The GDPR is one important law that requires companies to implement information security. Other laws (e.g. tax law, labor law) also require companies to protect their data.

In each case, the ISO 27001 standard is not required. Companies could use other standards.
ISO 27001 however is for many companies the most mature and practical standard

Art. 24 GDPR Responsibility of the controller
Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement ***appropriate technical and organisational measures*** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. [2]Those measures shall be reviewed and updated where necessary.

Art. 28 GDPR Processor
Where processing is to be carried out on behalf of a controller, the controller shall use ***only processors providing sufficient guarantees to implement appropriate technical and organisational measures*** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

https://gdpr-info.eu/art-24-gdpr/

Contents

- Why companies need ISO 27001
- What is the essence of ISO 27001
- How you can use ISO 27001 in your career

Definition of security: the CIA of information assets

Security = C + I + A

(NL: BIV)

Confidentiality

vertrouwelijkheid

- Only parties that are supposed to read the information can read the information
- (ISO 27000: information is not made available or disclosed to unauthorized individuals, entities, or processes)

Integrity

Integriteit

- The information is protected against accidental or malicious changes.
- (Alternative: maintaining and assuring the accuracy and completeness)

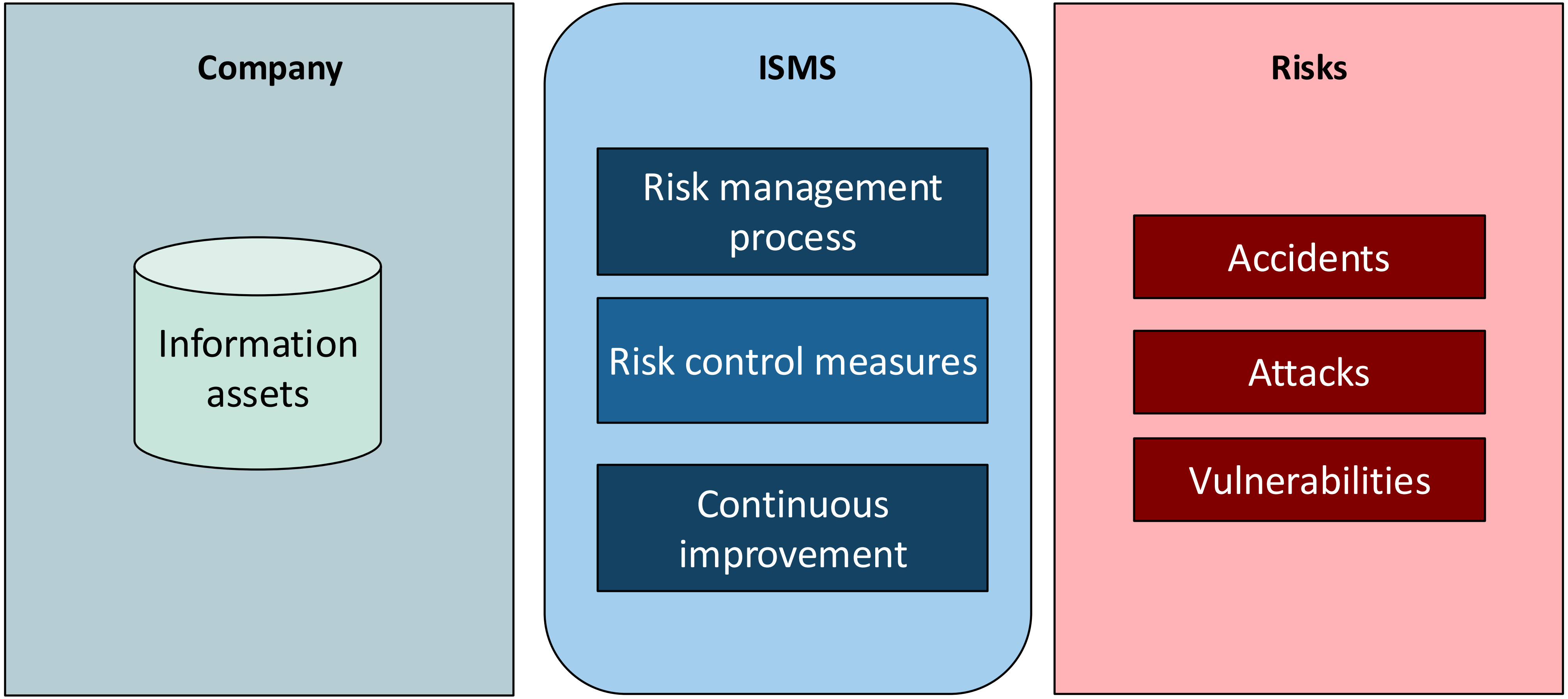
Availability

beschikbaarheid

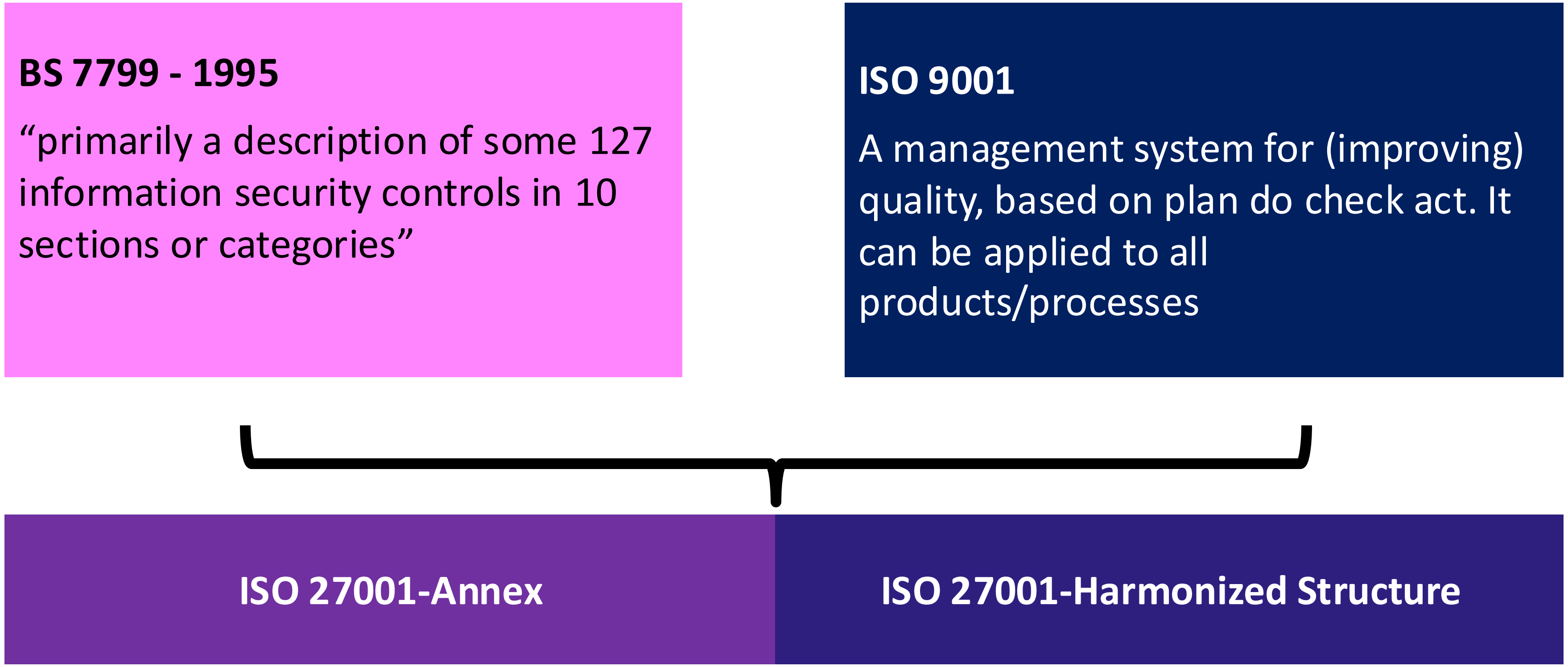
- The information can be used when needed

The purpose of an ISMS

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



How ISO 27001 was created



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

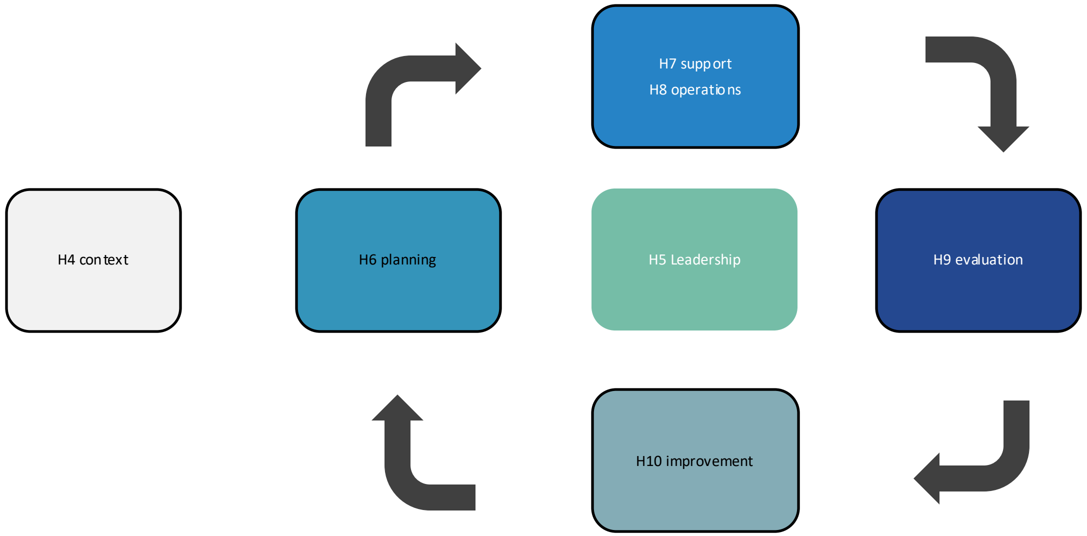
ISO 27001-Annex

ISO 27001-Harmonized Structure

Versions: 2005, 2013, 2022

The engine and the payload

Risk management process



H4 context

H6 planning

H7 support
H8 operations

H5 Leadership

H9 evaluation

H10 improvement

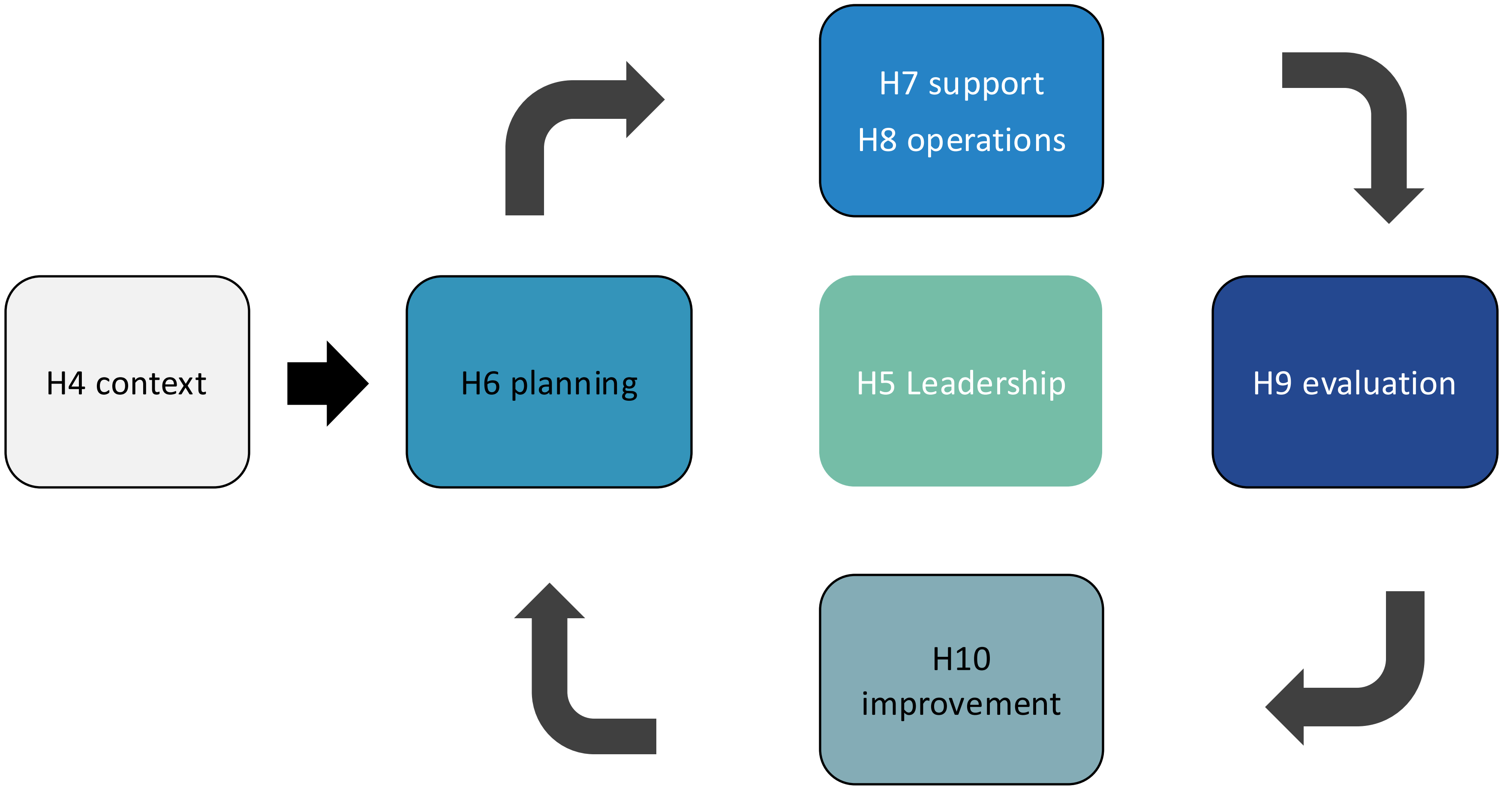
Using and improving the ISMS should be your focus in the long term

Risk control measures

- Annex 27001 A5-A8
- ISO 27002: implementation guidelines

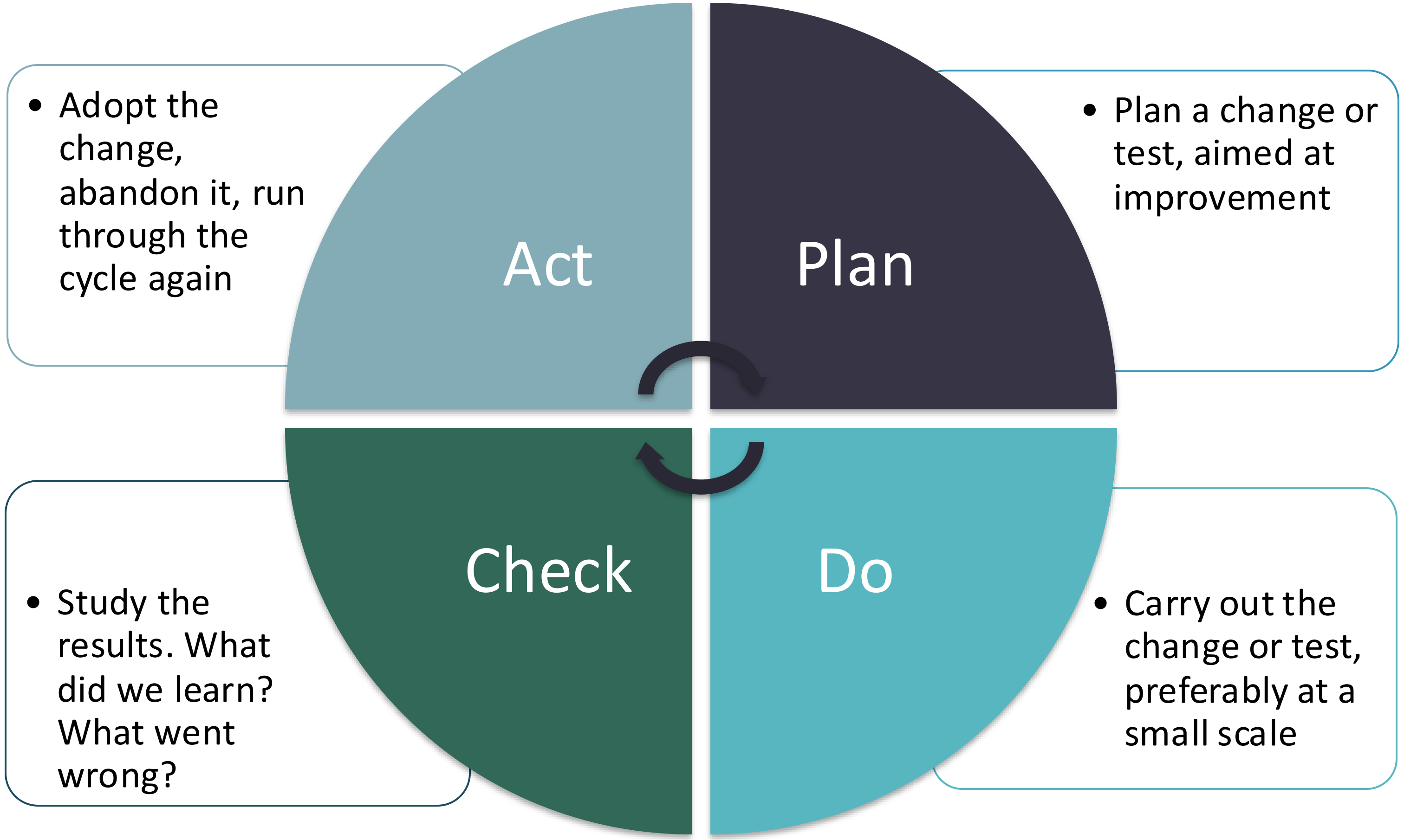
The annex measures are technically not required, you just consider them.
In practice, you should do 95%+ if you want to become certified.
The correct, clear, demonstratable implementation is the most work in the short term

ISO 9001 / 27001 ‘harmonized’ structure



These chapters describe an annual process for a company to reach goals. These can be quality goals, risk-reduction goals, compliance goals, …

An ISMS is based on continuous improvement



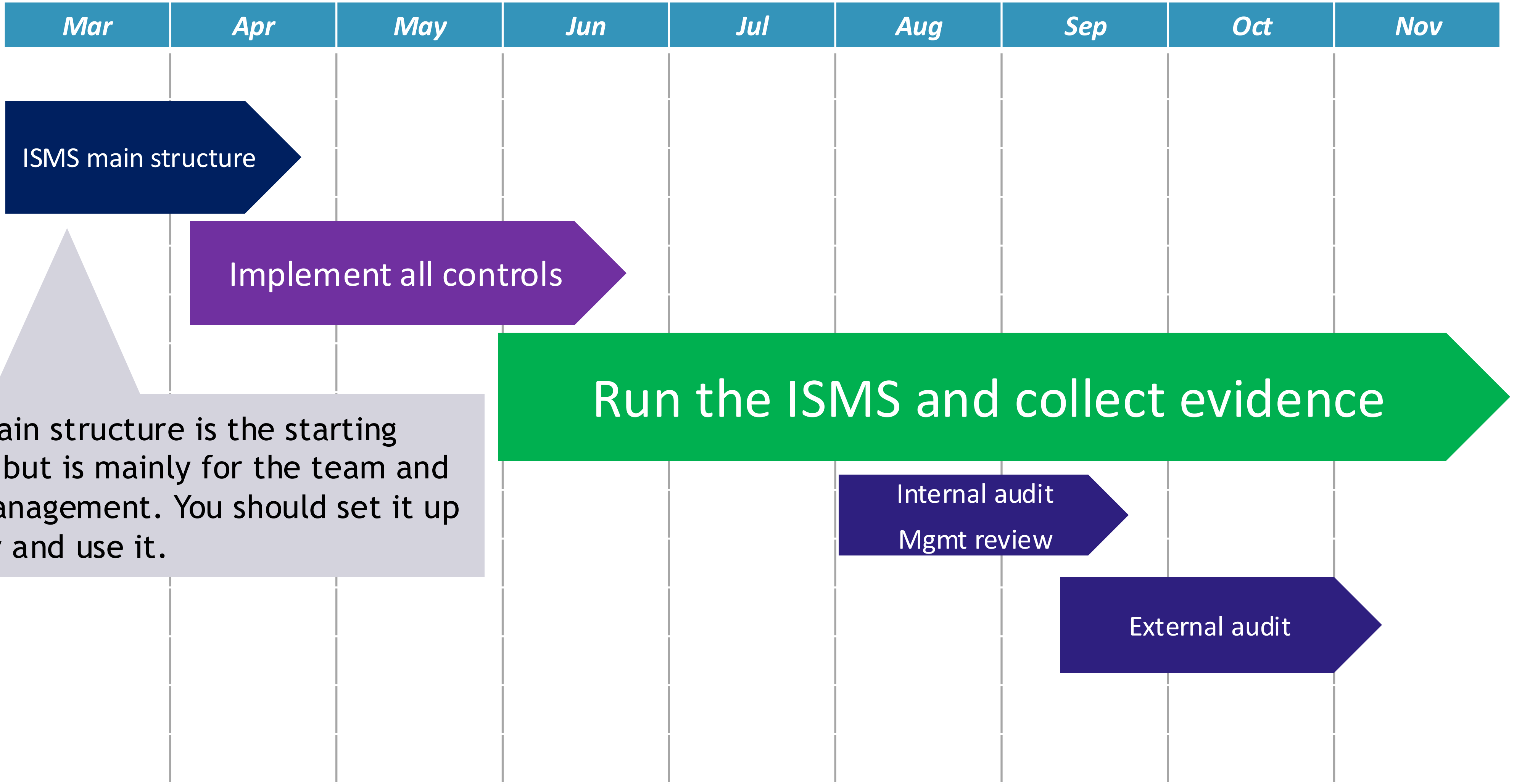
- Adopt the change, abandon it, run through the cycle again

- Plan a change or test, aimed at improvement

- Study the results. What did we learn? What went wrong?

- Carry out the change or test, preferably at a small scale

The ISMS setup should be short



The main structure is the starting point, but is mainly for the team and top management. You should set it up swiftly and use it.

Contents

- Why companies need ISO 27001
- What is the essence of ISO 27001
- How you can use ISO 27001 in your career

How ISO 27001 can help you in your career

Compliance careers:

- Security officer: Learn ISO 27001 and implementation experience
- Privacy officer: Learn GDPR and contractual experience
- ISMS auditor: learn interview / audit skills

We can help you learn the standards. You also need a BSc/MSc degree, and relevant work experience. Building a career is a long but rewarding journey

Engineering/business careers:

- Software developer: learn to implement ISO 27001 technological controls
- DevOps engineer: learn about infrastructure security
- Project / team manager: Manage security and compliance in projects

Many companies are looking for people good at a core task, but that also bring extra knowledge. Security and privacy are important areas of expertise than every team needs

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/