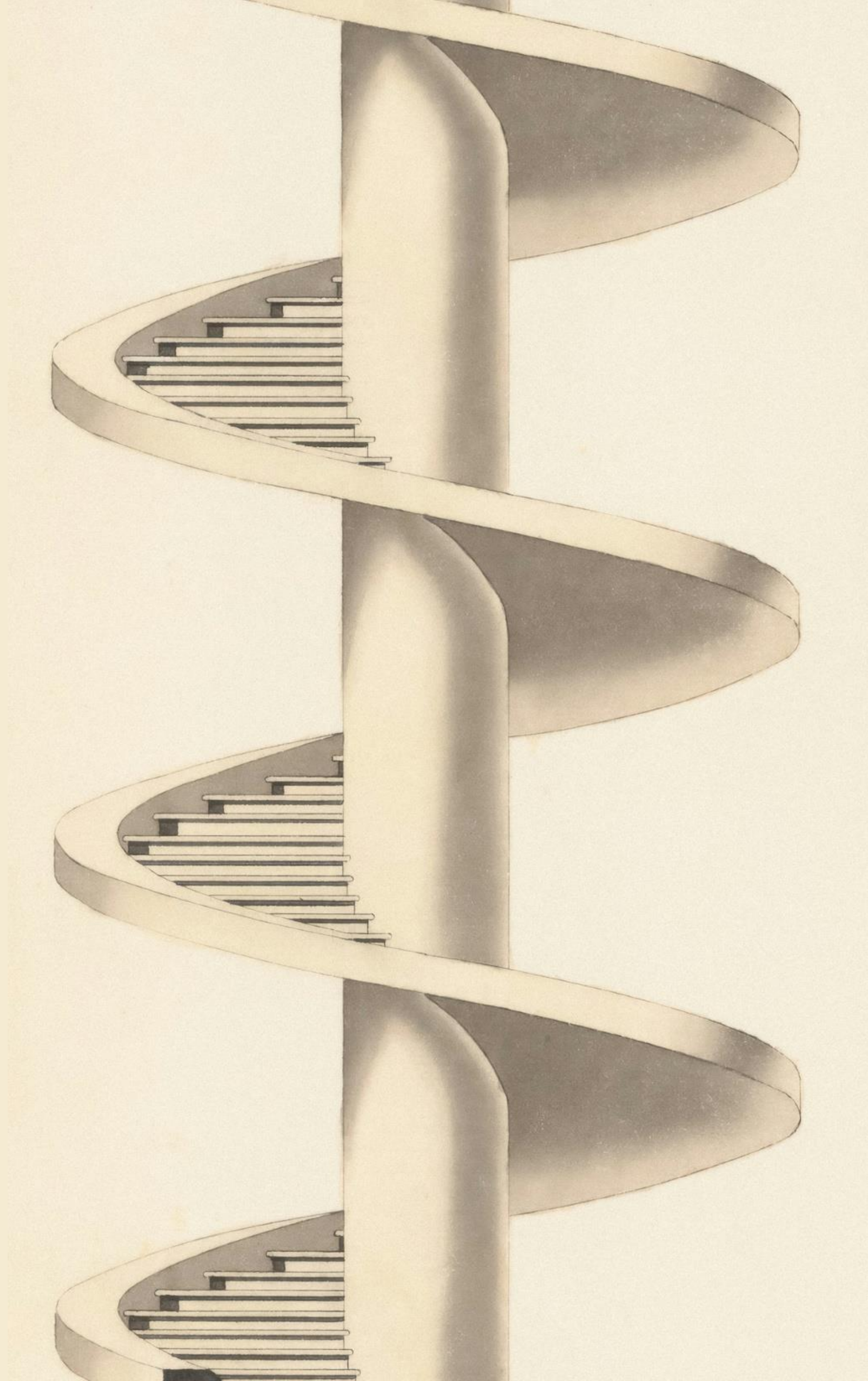


ISO 27001 – Harmonized structure

SieuwertExplains

youtube.com/@sieuwertexplains

Reminder: Why ISO 27001

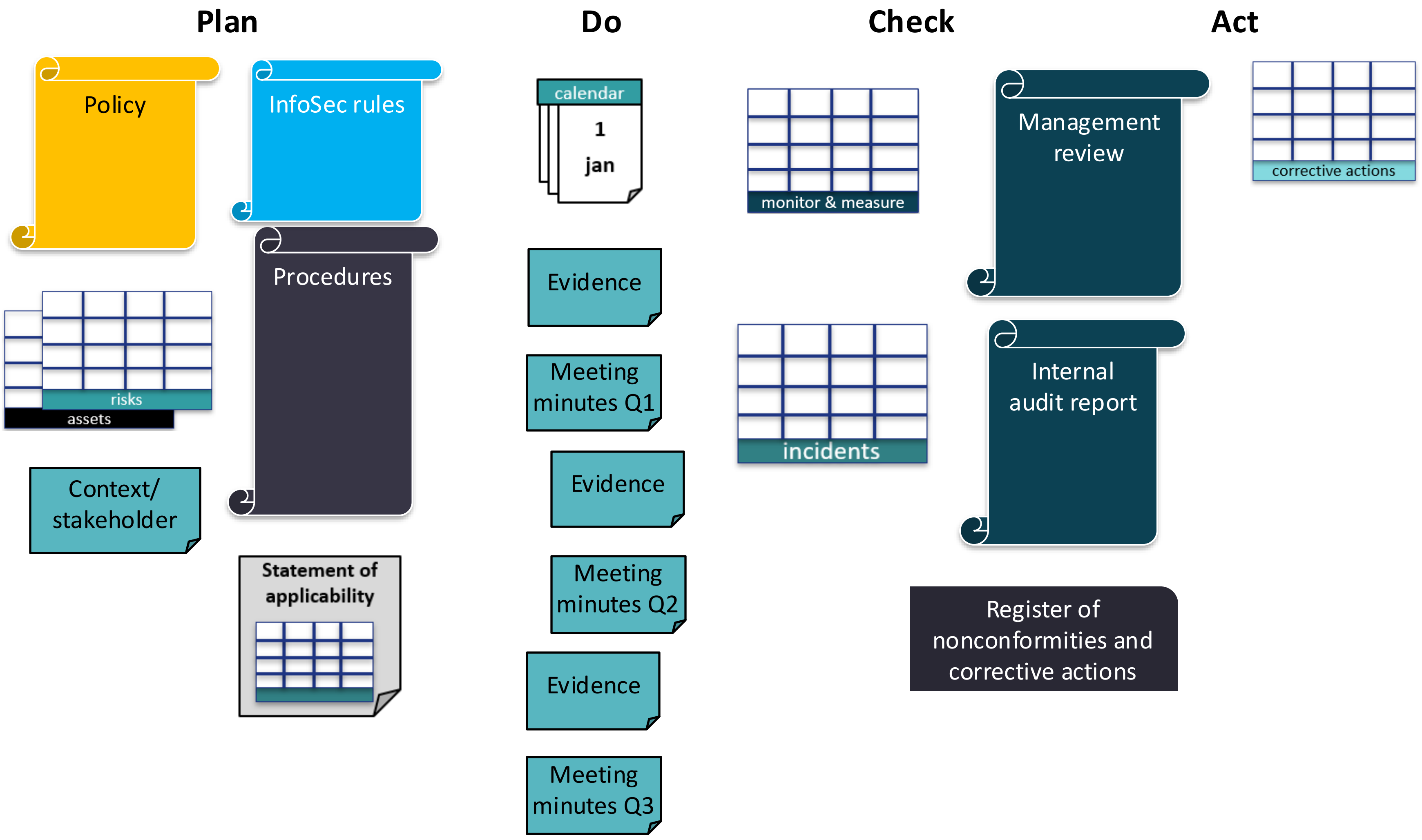
- ISO 27001 is a certifiable standard for information security of organisations. It is the entire organisation (not a product) that can become certified

- ISO 27001 is important for companies with government, public sector or business clients that need proof that their information is secure.

- Certification audits are expensive, but for some companies it makes sense to have one audit instead of questions and visits from each customer

- ISO 27001 does not guarantee that nothing happens, but it drastically reduces the risk of an information security breach

ISMS documents: how do they work



Plan

Policy

InfoSec rules

Procedures

risks

assets

Context/ stakeholder

Statement of applicability

Do

calendar

1 jan

Evidence

Meeting minutes Q1

Evidence

Meeting minutes Q2

Evidence

Meeting minutes Q3

Check

monitor & measure

Management review

incidents

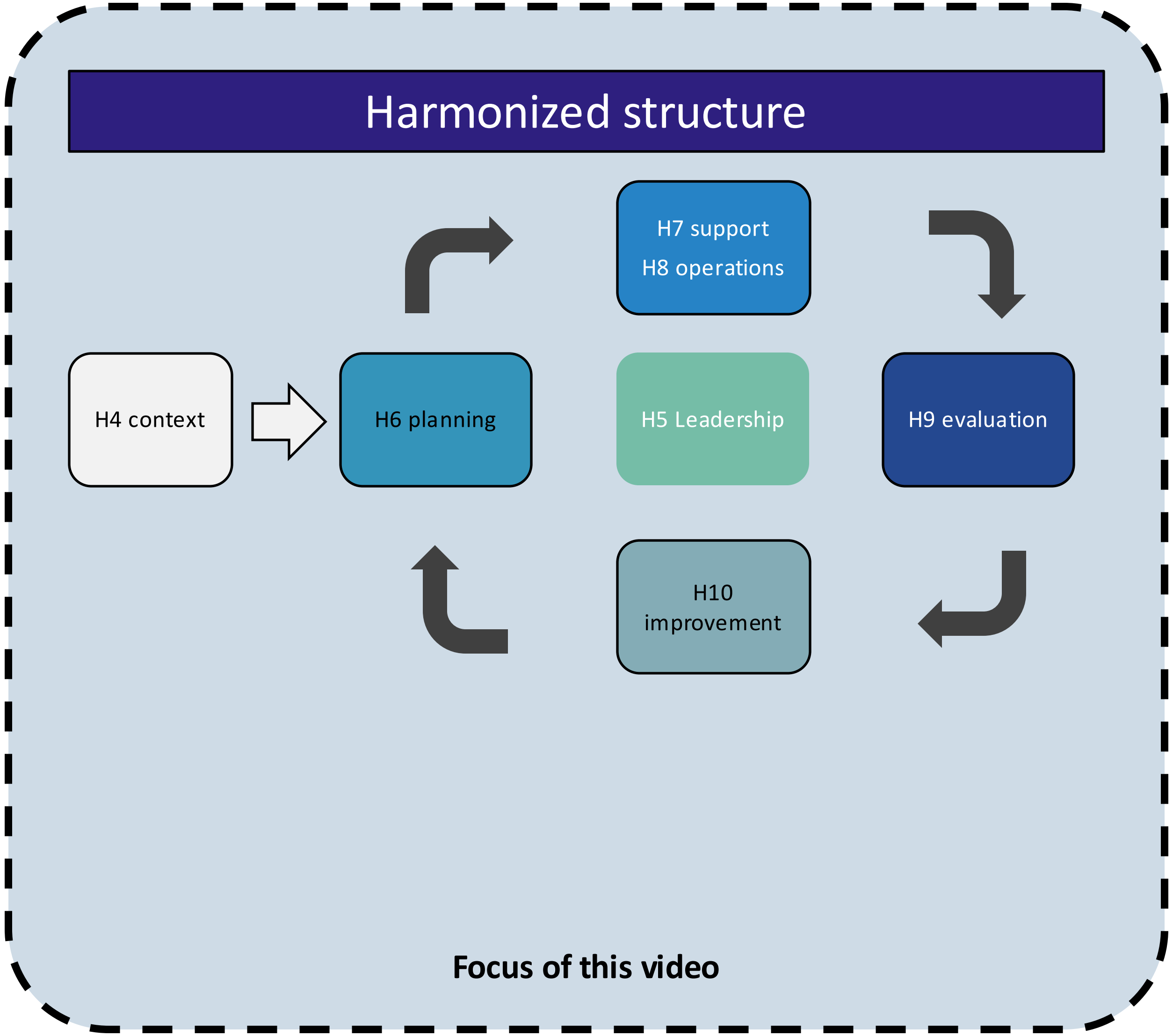
Internal audit report

Register of nonconformities and corrective actions

Act

corrective actions

ISO 27001 = Harmonized structure + control measures



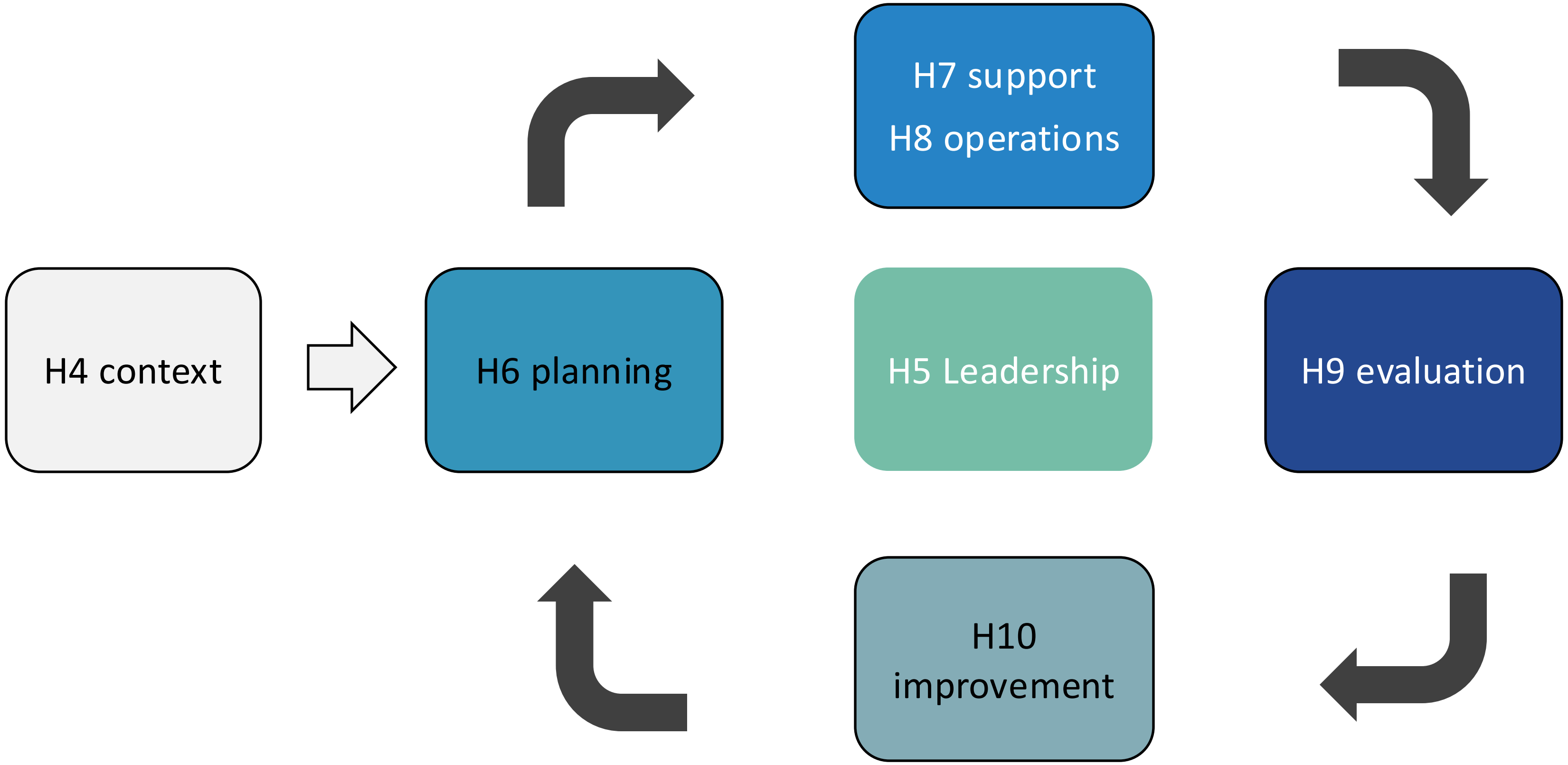
Focus of this video

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

ISO ‘harmonized structure’

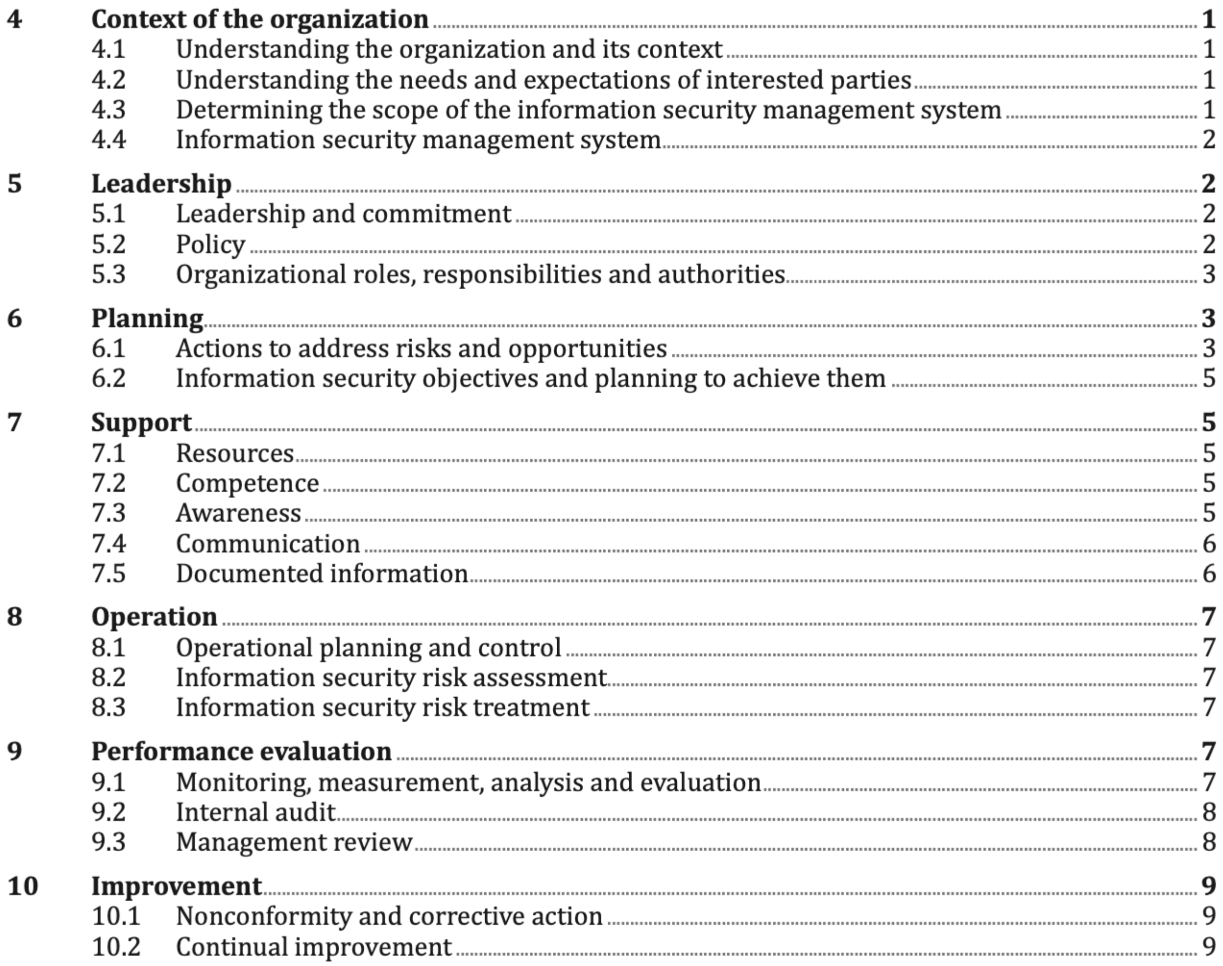


These are the main chapters of the standard.

It is important to not get lost into detailed controls, but understand that this is the main process.

It is an annual process: it repeats every year

ISO 27001 contents



You should buy the standard and then you will see this table of contents.

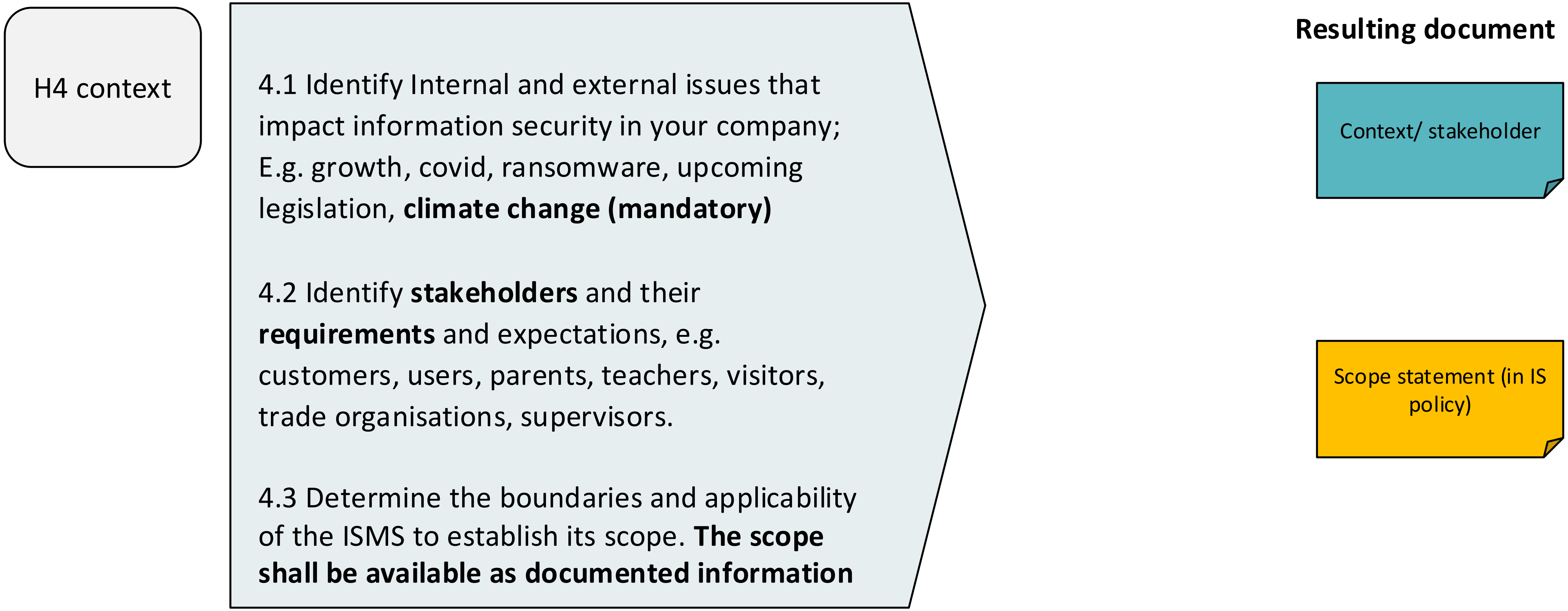
Many ISO standards have the same chapter structure (harmonized structure; previously: high level structure).

- **Chapters 1-3** are reserved for definitions and other non-essential elements.
- **Chapters 4-10** contain the requirements you must implement and that you will be audited on.
- The **annex** with controls is mentioned briefly in chapters 6 and 8.

ISO Standards using the Harmonized structure

ISO 9001	Quality management systems (QMS)
ISO 27001	Information Security Management System (ISMS)
ISO 27701	Privacy Information Management System (PIMS)
ISO 42001	Artificial Intelligence Management System (AIMS)

4. Context of the organization



Requirements

H4 context

4.1 Identify Internal and external issues that impact information security in your company; E.g. growth, covid, ransomware, upcoming legislation, **climate change (mandatory)**

4.2 Identify **stakeholders** and their **requirements** and expectations, e.g. customers, users, parents, teachers, visitors, trade organisations, supervisors.

4.3 Determine the boundaries and applicability of the ISMS to establish its scope. **The scope shall be available as documented information**

Resulting document

Context/ stakeholder

Scope statement (in IS policy)

Example scope statement

- ***Information security related to** the development, delivery and support of a software platform for online education*

- ***Information security related to** the delivery of training and advice and supporting activities*

- ***Information security related to** delivering health care to elderly people in The Netherlands*

Policy

- The scope of an ISMS must start with the words “Information security related to”
- There must be a short scope statement that can be printed on the ISO 27001 certificate.
- It is common to have a short formal scope statement followed by a longer scope explanation mentioning locations, departments, legal entities and product names in scope

5. Leadership

H5 Leadership

Description

Top management must be directly involved in the ISMS (and will be interviewed in audit).

Top management expected roles:

- Make sure there is an approved, published information security policy.
- Communicate about the ISMS internally
- Make resources available (time, money)
- Make sure the ISMS reaches its goals
- Support the rest of management in the ISMS execution
- Promote continuous improvement

Policy

Meeting minutes Q1

Question

Your CEO states he want to support the ISMS in the next month.

How would you rate the following suggestions?

a) The CEO will participate in the training recommended for all staff
b) The CEO will remind people to be aware of phishing in the annual speech
c) The CEO will set and discuss the ISMS objectives in one-on-ones with direct reports
d) The CEO appoints people to information security roles
e) The CEO expects the CIO to take care of security

Answer: a-c are all good.
d) is technically correct but not very active.
e) does not sound like an action and would not be a good answer during an audit.

6. Planning

Requirements

H6 planning

Description

- Risk management process: Identify your information security risks in a structured way.
- Make treatment decisions for your risks, using standard controls and your own controls
- Add owners and deadlines to actions
- Make Statement of Applicability: a checklist which standard controls you have chosen

Resulting document

Risk	Probability	Treatment plan	Plan status

Risk register:

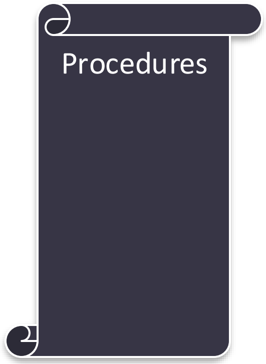
- Risk description
- Estimated impact & probability
- Accept / treat decision

6 Risk management process

The risk management process works as follows:

1. *Determine the definitions: what is high, what is low, and what do we find acceptable?*
2. *Create a list of relevant risks*
3. *Write down for every risk:*
   a) *Which measures we already take to reduce the risk*
   b) *What the current probability is, scored 0-3*
   c) *What the current impact is, scored 0-3*
   d) *What the current risk score is (probability x impact)*
4. *For all risks with a score above the risk acceptance threshold*, do the following:*
   a) *Determine additional controls needed to reduce the risk below the threshold; the treatment plan*
   b) *Estimate the probability with the additional controls*
   c) *Estimate the impact with the additional controls*
   d) *Add a risk owner and deadline to make sure the treatment plan is executed*

This process is repeated every year, with a risk workshop in [January]



** Risk threshold: all risks with score> 5 will be treated*

Risk register requirements

What should be in the register:

- Risk description
- Estimated impact & probability
- Accept / treat decision
- Detailed on treatment (who / what / deadline)
- Risk owner
- Date of approval of risk owner. This must be repeated every 12 months, since it must be risk management process

We recommend having enough risks to cover all controls (e.g. from an external source) of at least 30 risks, and each year have detailed treatment plans for 3-6 risks.

Risk register

Risk	Probability	Treatment plan	Plan status

Risk management – Example

Identification

Nr	Event	Conf., Integr., Avail. (CIA)	Source of risk	Already taken measures
1	Deletion of data by staff	IA	Issues / customer req / …	
2	Technical issues or bugs	IA	Issues / customer req / …	
3	Hosting issues	IA	Issues / customer req / …	
4	Loss of laptop	CA	Issues / customer req / …	

Assessment

Event	Probability (after taken measures)	Impact (after taken measures)	Risk score (after taken measures)	Proposed treatment in 2025 (Accept, Reduce)
Deletion of data by staff	High	High	9	Reduce
Technical issues or bugs	High	Medium	6	Reduce
Hosting issues	High	Low	3	Accept
Loss of laptop	Medium	High	6	Reduce

Treatment

Event	Risk Treatment Plan in 2024	Risk owner name	Risk owner approval date	Prob after trtmnt	Impact after trtmnt	Risk score after extra controls
Deletion of data by staff	Hourly backups	John Wick	01-Jan-23	Low	High	3
Technical issues or bugs	Automatic testing	John Wick	02-Jan-23	Medium	Medium	4
Hosting issues	n/a, accepted	n/a	n/a	High	Low	3
Loss of laptop	Encryption	John Cena	04-Jan-23	Medium	Low	2

Risk - controls examples 1

Consider the following risk:

- **Information compromised due to physical access to assets**

This includes assets such as laptops, phones, papers stolen from your office

What measures would you consider to minimize this risk?

Answer: Various physical security measures, locks, key management, floor plan with reception desks, covering windows, camera's, alarm system. Chapter 7 of the Annex.

Src: Steve Smith unsplash

Risk - controls examples 2

Consider the following risk:

- **Audits or inspections disturb operations**

What measure would you consider to minimize this risk?

a) The allocation and use of privileged access rights shall be restricted and managed (8.2)

b) The use of resources shall be monitored and adjusted in line with current and expected capacity requirements (8.6)

c) The clocks of information processing systems used by the organization shall be synchronized to approved time sources (8.17)

d) Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management (8.34)

Source: Nathan Dumlao Unsplash

It is useful to use a standard risk set

We recommend to use a list of standard risks with controls to ***start*** your risk register. That way you have a risk for each control (this is required).

- You must add or modify the risks to make sure your register describes all risks for your organisation
- You must also consider taking additional steps to make sure the risk is treated correctly for your organisation
- You must improve the risk register every year.

Event	Applicable SoA controls/measures
Breach of information protection law or legislation	5.5, 5.31, 5.34, 8.10, 8.11
Breach of contractual information protection obligation	5.31
Loss of assets by employees	5.9, 5.10, 8.1,
Improper handling of information assets by employees	5.36, 5.37, 6.7, 7.13, 7.14
CIA of information compromised by employee by accident	6.2, 6.3
CIA of information compromised by (ex) employee on purpose	6.1, 6.2, 6.4, 6.5, 6.6, 8.12

Chapter 7 : Support

Requirements

H7 support

7.1 Sufficient resources: define team and estimate time required

7.2 Competences: Have simple verifiable requirements for ISMS roles, e.g. completed training

7.3 Awareness: You must have evidence of awareness activities and attendance

7.4: Communication plan. You can add this to the stakeholder register. Publishing your policy is a important element

7.4 Document management

Policy

Context/ stakeholder

7. Support - roles

Description

- Define requirements per role that have large impact on information security
- Make people with the right qualifications available
- Train people, both on general awareness and for their role

Question: which roles do you think have a significant impact on information security?

Role	Responsibility	Requirements
CISO	Set up and run ISMS Report on ISMS to management	**Completed ISO 27001 training, e.g. from ICT Institute, or CISA, CISSP, Security+**
CEO/Management	Provide resources Lead by example	
Lead developer	Apply security and privacy by design Test on security	
Internal audit	Conduct internal audit	• CISO or ISO27001 lead auditor • 1+ year audit experience
All employees	*Follow instructions* *Report incidents and nonconformities*	*Complete introduction program, sign rules*

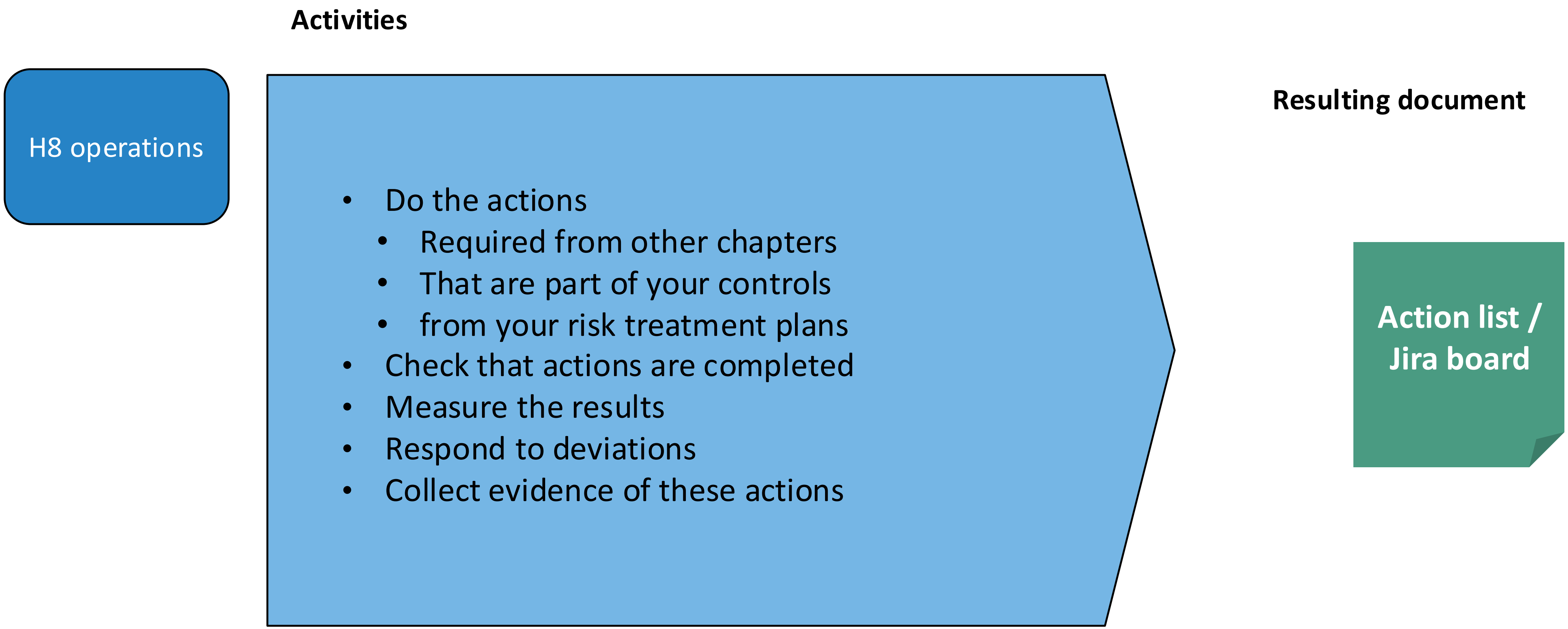
7. Internal communication: Agenda info-sec team meeting

- You should define an infosec meeting with an agenda so that internal communication is defined and planned.
- You can do this monthly or quarterly, depending on the size of your organisation

The InfoSec team has regular meetings for this (see annual planning). The following is discussed during these meetings:

- ***Incidents**: Have there been any recent incidents and are appropriate actions planned?*
- ***Changes**: Are there any new projects, changes or contracts that the InfoSec team should be looking at?*
- ***Annual planning**: What activities are planned for the past month in the annual planning? Have these been planned and executed?*
- ***Monitoring and measuring**: Are there any objectives or KPIs that need to be evaluated from last month or in the next month? What are the results?*
- ***Nonconformities**: Are there any new nonconformities? Are corrective actions properly implemented on audit findings or other non-conformities?*

8. Operations



Activities

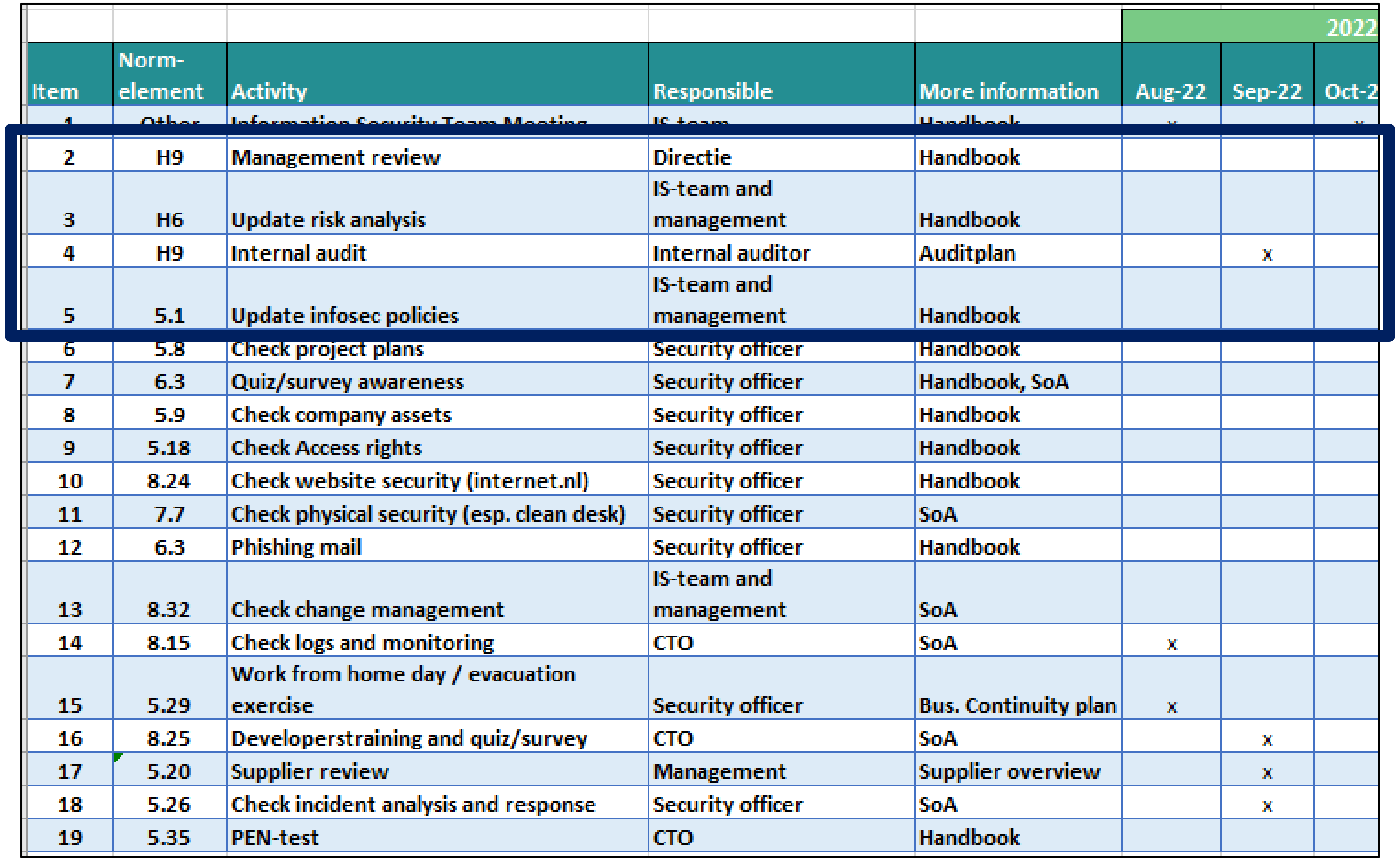
H8 operations

- Do the actions
  - Required from other chapters
  - That are part of your controls
  - from your risk treatment plans
- Check that actions are completed
- Measure the results
- Respond to deviations
- Collect evidence of these actions

Resulting document

Action list / Jira board

Annual ISMS planning – HLS cycle

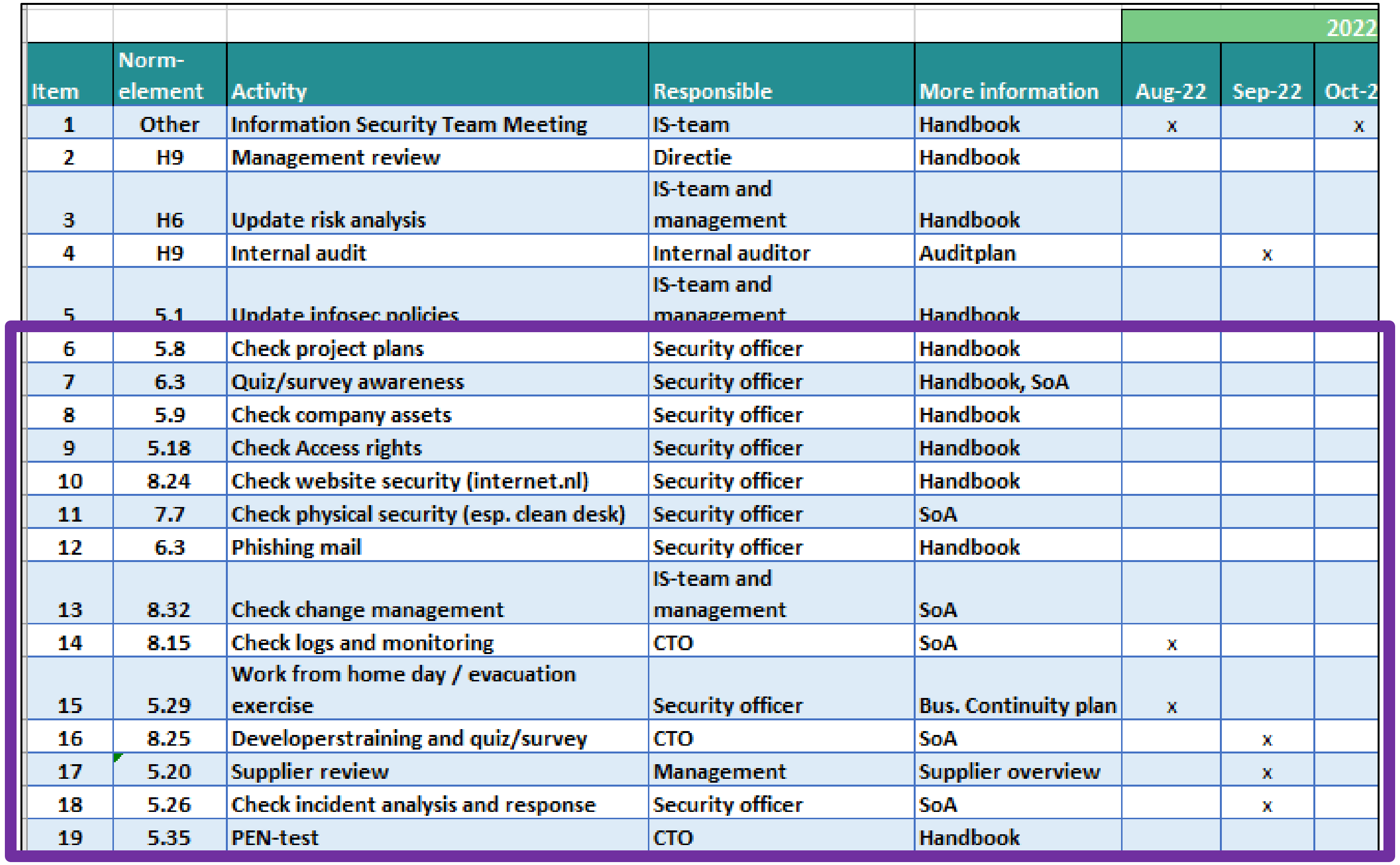


					2022		
Item	Norm-element	Activity	Responsible	More information	Aug-22	Sep-22	Oct-2
1	Other	Information Security Team Meeting	IS-team	Handbook	x		x
2	H9	Management review	Directie	Handbook			
3	H6	Update risk analysis	IS-team and management	Handbook			
4	H9	Internal audit	Internal auditor	Auditplan		x	
5	5.1	Update infosec policies	IS-team and management	Handbook			
6	5.8	Check project plans	Security officer	Handbook			
7	6.3	Quiz/survey awareness	Security officer	Handbook, SoA			
8	5.9	Check company assets	Security officer	Handbook			
9	5.18	Check Access rights	Security officer	Handbook			
10	8.24	Check website security (internet.nl)	Security officer	Handbook			
11	7.7	Check physical security (esp. clean desk)	Security officer	SoA			
12	6.3	Phishing mail	Security 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			

The HLS has several steps that have an annual cycle:

- Update/review context and risks
- Set objectives, and define KPIs
- Review / re-approve policies
- Annual management review
- Annual audits

Annual ISMS planning – execution of controls



					2022		
Item	Norm-element	Activity	Responsible	More information	Aug-22	Sep-22	Oct-2
1	Other	Information Security Team Meeting	IS-team	Handbook	x		x
2	H9	Management review	Directie	Handbook			
3	H6	Update risk analysis	IS-team and management	Handbook			
4	H9	Internal audit	Internal auditor	Auditplan		x	
5	5.1	Update infosec policies	IS-team and management	Handbook			
6	5.8	Check project plans	Security officer	Handbook			
7	6.3	Quiz/survey awareness	Security officer	Handbook, SoA			
8	5.9	Check company assets	Security officer	Handbook			
9	5.18	Check Access rights	Security officer	Handbook			
10	8.24	Check website security (internet.nl)	Security officer	Handbook			
11	7.7	Check physical security (esp. clean desk)	Security officer	SoA			
12	6.3	Phishing mail	Security 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			

Several controls, especially in A5 and A8, require a recurring practical check.

Ideally the check delivers some measured result (e.g. number of findings) and is then input for “monitoring and measurement”. The “monitoring and measurement” in input for the recurring IS team meeting.

Quiz question (Chapter 8)

You have chosen to implement this control:
6.3 Information security awareness, education and training

What are concrete steps that you can take to implement this control?

- In person all-hand training
- Poster campaign
- Quizzes during the year
- Phishing campaign

What kind of evidence can you collect from these activities?

Activity	Example plan	Evidence
In person all-hand training	Invite people via outlook (CEO, Jan) Create PowerPoint (CISO, Feb) Give training (CISO and CFO, march)	Calendar invitation PowerPoint presentation Signed attendee list Filled in quiz forms
Poster campaign	Design poster (Jan, designer) Print posters (CISO, mid Feb) Hang poster (office mngr, end of Feb)	Digital poster design Printing invoice Photos from poster

9. Performance evaluation

H9 evaluation

Description

- Have monitoring in place, using 5-10 concrete, relevant measurements
- Have an internal audit program to covers ISO 27001 completely
- Conduct a regular management review meeting

9.1 Example dashboard

Example performance dashboard

What is monitored	Who monitors	Target value	Q1 2025	Q2 2025	Q3 2025
Internet.nl score	CISO	90%	70%	75%	91%
Intune errors	IT manager	<100	123	75	120
Participation in awareness training	HR	80%	90%	Not planned	88%
…					
…					

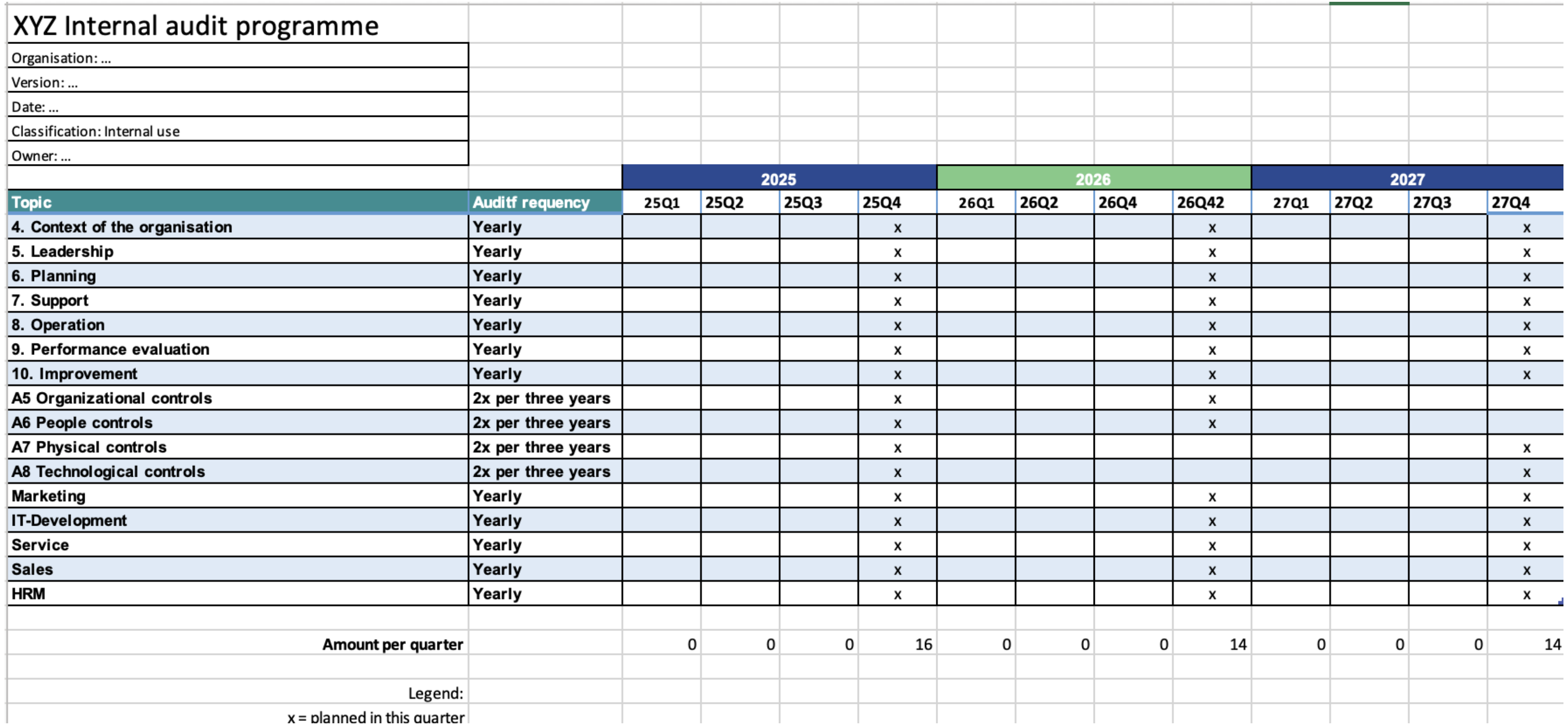
Recommendations:

- Choose metrics to cover different chapters. E.g., 2 for A5, 2 for A6, 1 for A7, 2-3 for A8.
- Make sure it is very clear to you what exactly is measured and how. Do an example measurement
- Match the frequency with your IS team meetings. Monthly, Quarterly or every six months often works

9.2 Internal audit

- The ISO 27001 standard requires you to have an internal audit programme.
- Make sure the entire ISMS (harmonized structure and all controls) are audited in the first year before the external audit.
- You can do shorter risk-based audits in year 2 and 3

Note: The auditor must be independent and experienced and is therefore often an external professional (like ICT Institute)



XYZ Internal audit programme

Organisation: ...

Version: ...

Date: ...

Classification: Internal use

Owner: ...

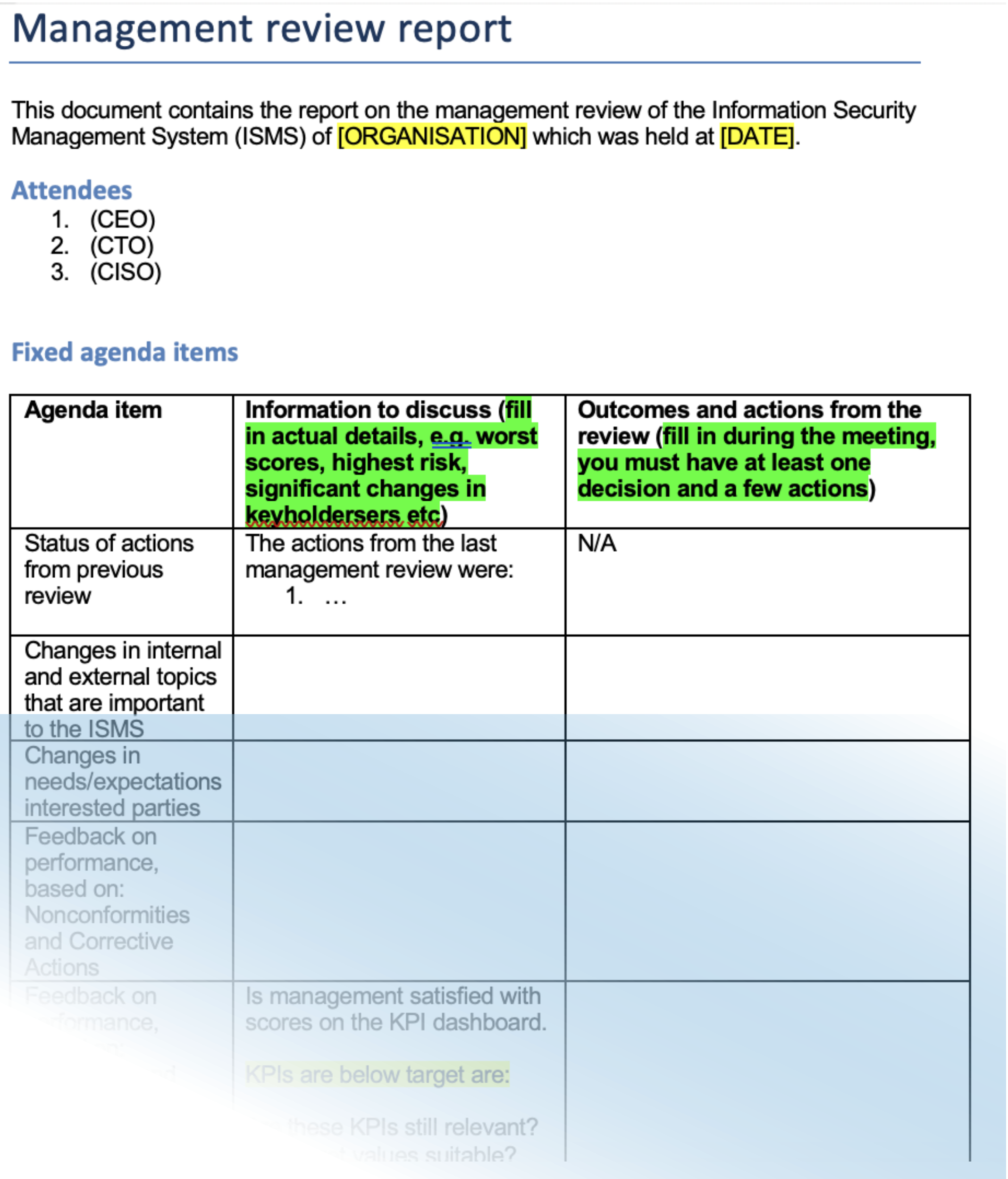
		2025				2026				2027			
Topic	Auditf requency	25Q1	25Q2	25Q3	25Q4	26Q1	26Q2	26Q4	26Q42	27Q1	27Q2	27Q3	27Q4
4. Context of the organisation	Yearly				x				x				x
5. Leadership	Yearly				x				x				x
6. Planning	Yearly				x				x				x
7. Support	Yearly				x				x				x
8. Operation	Yearly				x				x				x
9. 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
Amount per quarter		0	0	0	16	0	0	0	14	0	0	0	14

Legend:

x = planned in this quarter

9. 3 Management review

- ISO 27001 requires the CISO to present all the main documents of the ISMS to management, after internal audit before the external audit.
- The management review was added to make sure management understands all the risks, incidents, weaknesses and agrees with decisions taken.
- The results must be documented and will be reviewed by the external auditor.
- The CISO makes a presentation beforehand: risk management results, incidents, audit results, objectives and status, …
- The results must be captured in a report



Management review report

This document contains the report on the management review of the Information Security Management System (ISMS) of [ORGANISATION] which was held at [DATE].

Attendees

1. (CEO)
2. (CTO)
3. (CISO)

Fixed agenda items

Agenda item	Information to discuss (fill in actual details, e.g. worst scores, highest risk, significant changes in keyholdersers etc)	Outcomes and actions from the review (fill in during the meeting, you must have at least one decision and a few actions)
Status of actions from previous review	The actions from the last management review were: 1. …	N/A
Changes in internal and external topics that are important to the ISMS		
Changes in needs/expectations interested parties		
Feedback on performance, based on: Nonconformities and Corrective Actions		
Feedback on performance,	Is management satisfied with scores on the KPI dashboard. KPIs are below target are: these KPIs still relevant? values suitable?	

10. Continual improvement

Activities

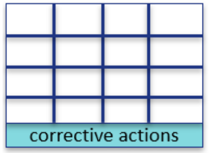
Formal requirements:

- Register nonconformities
- Take immediate action
- Do root cause analysis
- Take preventive action to prevent similar errors

Informal requirement:

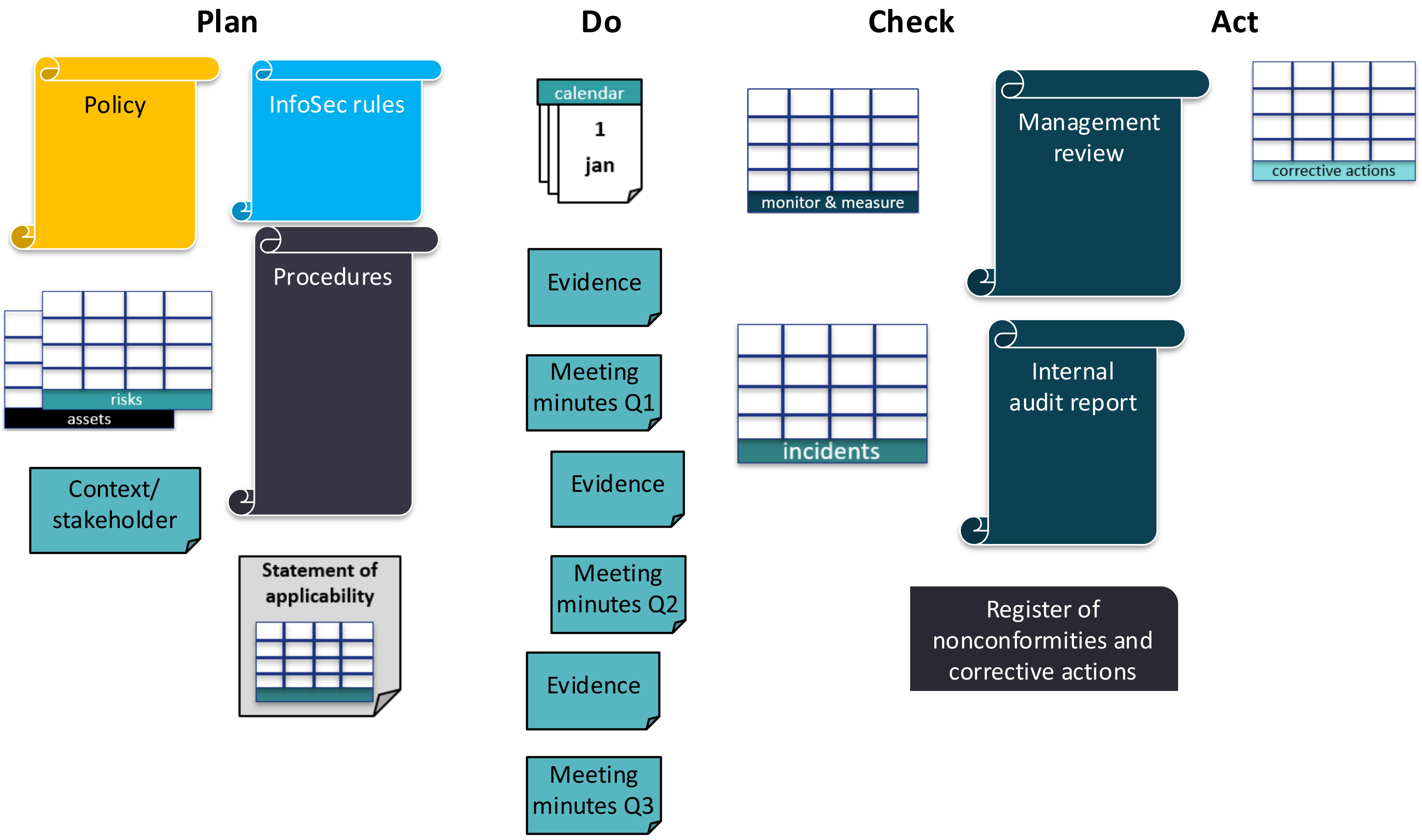
- The entire organisation must demonstrate that they aim for continual improvement
- Management itself promotes continual improvement

Resulting document



Register of nonconformities and corrective actions

Recap : A good ISMS has many auditable documents



Plan

Policy

InfoSec rules

Procedures

risks

assets

Context/ stakeholder

Statement of applicability

Do

calendar

1

jan

Evidence

Meeting minutes Q1

Evidence

Meeting minutes Q2

Evidence

Meeting minutes Q3

Check

monitor & measure

Management review

incidents

Internal audit report

Register of nonconformities and corrective actions

Act

corrective 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/