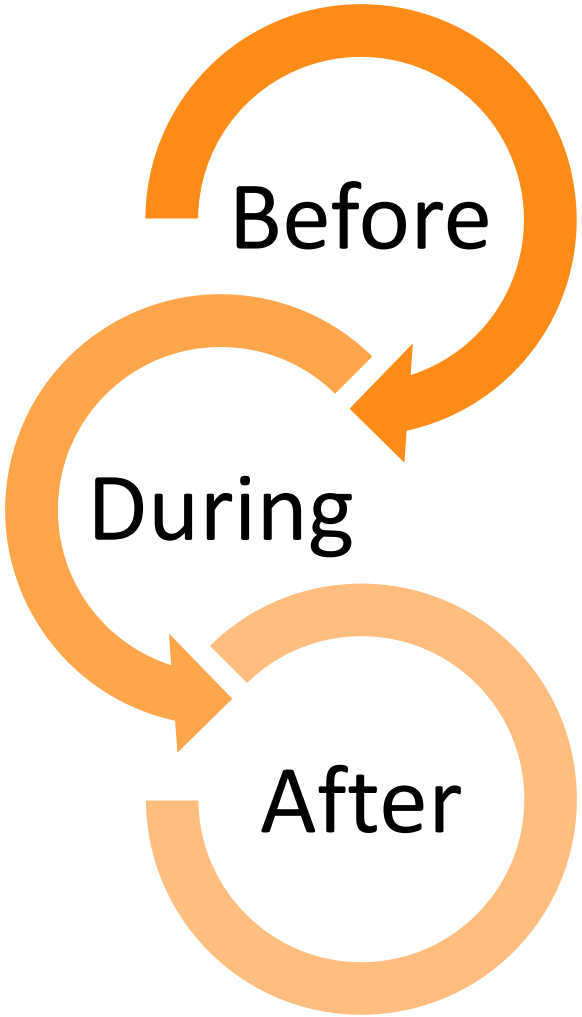
ISO 27001:2022. How to prepare for a certification audit

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001

www.patreon.com/AndreyProzorov

1.0, 23.11.2022

Agenda



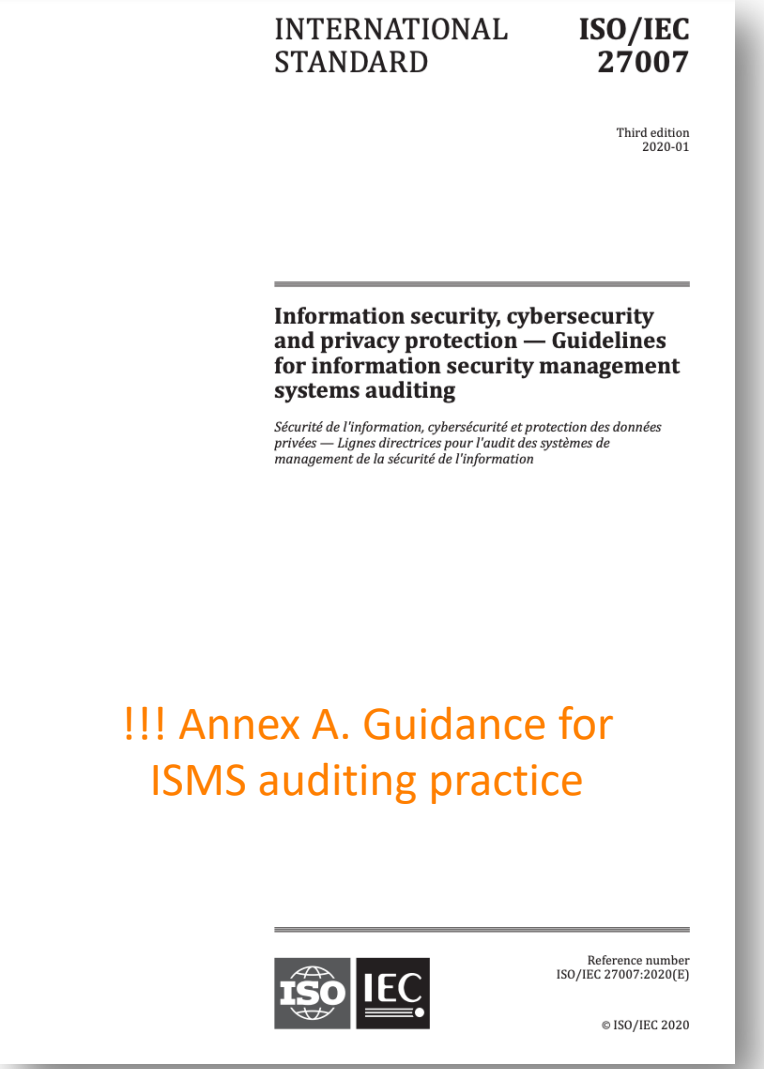
00. ISMS Implementation plan
0. Read the standards
1. Before the audit
2. During the audit
3. After the audit

ISMS Implementation plan

1. Conduct awareness trainings for the top management
2. Conduct a Gap analysis
3. Understand the Context
4. Plan the implementation
5. Conduct the first IS Committee meeting
6. Establish Information Security Policy and Information Security Objectives
7. Take an inventory of the assets
8. Define a method of risk assessment, identify and assess information security risks
9. Prepare Statement of Applicability (SoA) and Risk Treatment Plan (RTP)
10. Define requirements for documentation management
11. Develop ISMS Framework and define roles and responsibilities
12. Develop and implement a set of ISMS policies and procedures
13. Plan and implement additional information security measures
14. Plan, prepare and conduct awareness trainings
15. Operate the ISMS
16. Monitor the ISMS
17. Audit the ISMS
18. Conduct ISMS Management reviews
19. Practice continual improvement
20. **Prepare for the certification audit**

We are here

0. Read the standards and understand the process



INTERNATIONAL STANDARD

ISO/IEC 27007

Third edition
2020-01

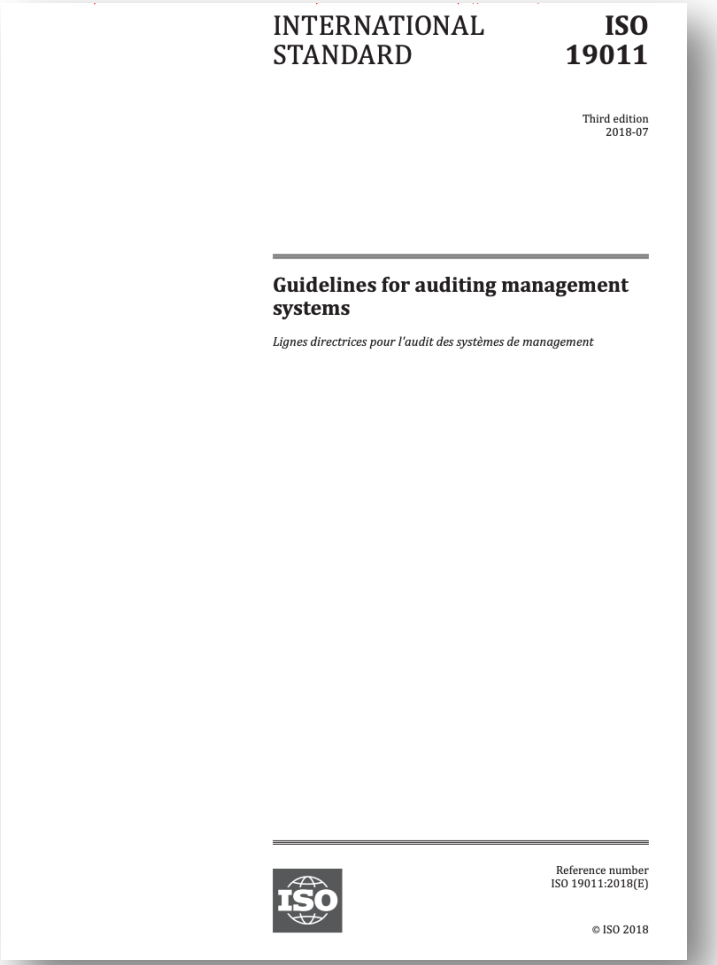
Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

!!! Annex A. Guidance for ISMS auditing practice

Reference number
ISO/IEC 27007:2020(E)

© ISO/IEC 2020



INTERNATIONAL STANDARD

ISO 19011

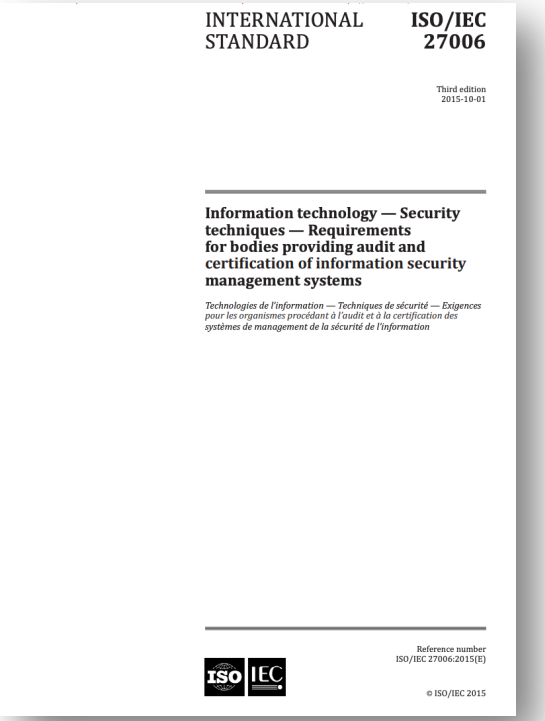
Third edition
2018-07

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

Reference number
ISO 19011:2018(E)

© ISO 2018



INTERNATIONAL STANDARD

ISO/IEC 27006

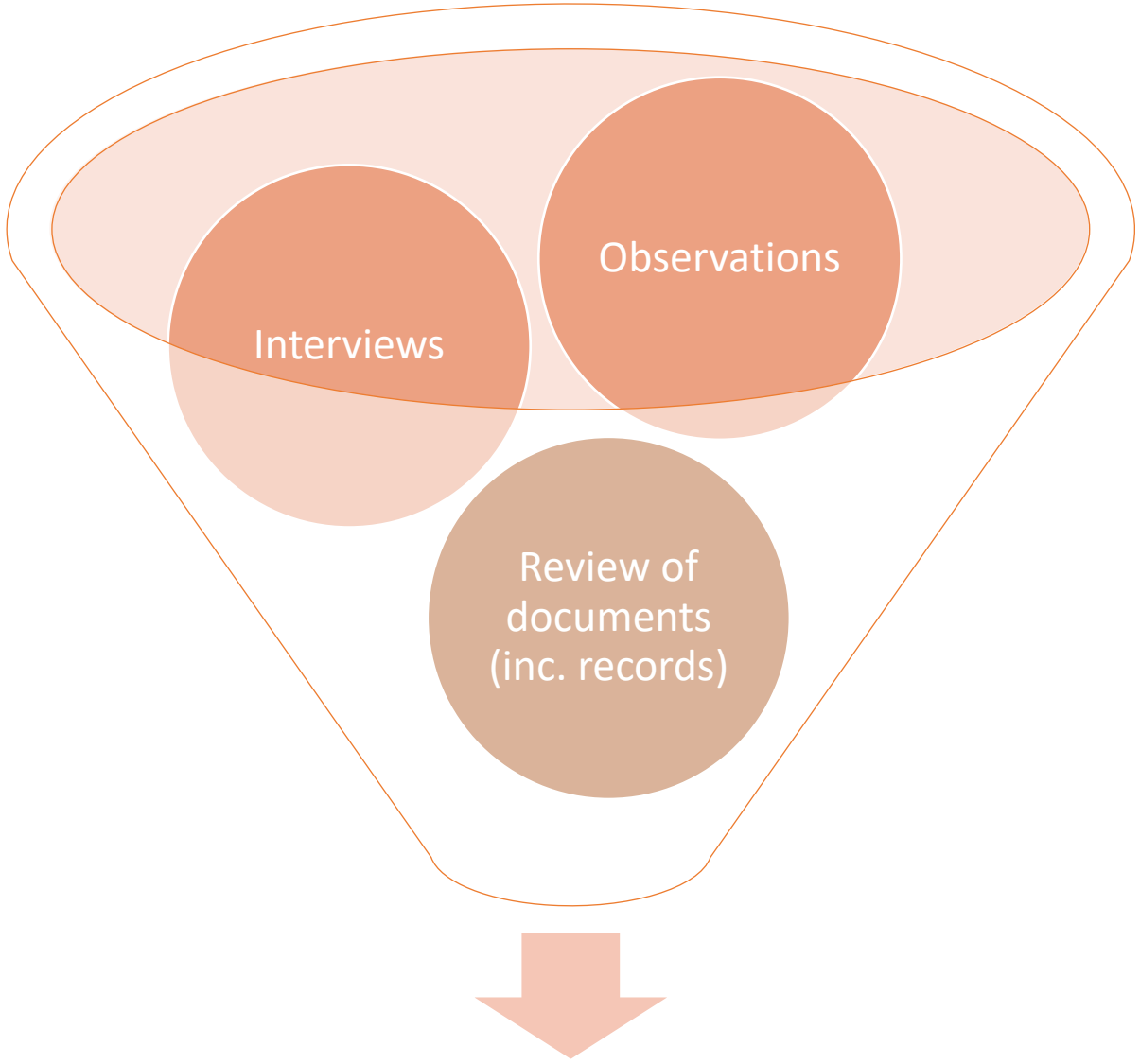
Third edition
2015-10-01

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27006:2015(E)

© ISO/IEC 2015



Audit findings

Audit: *systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled*

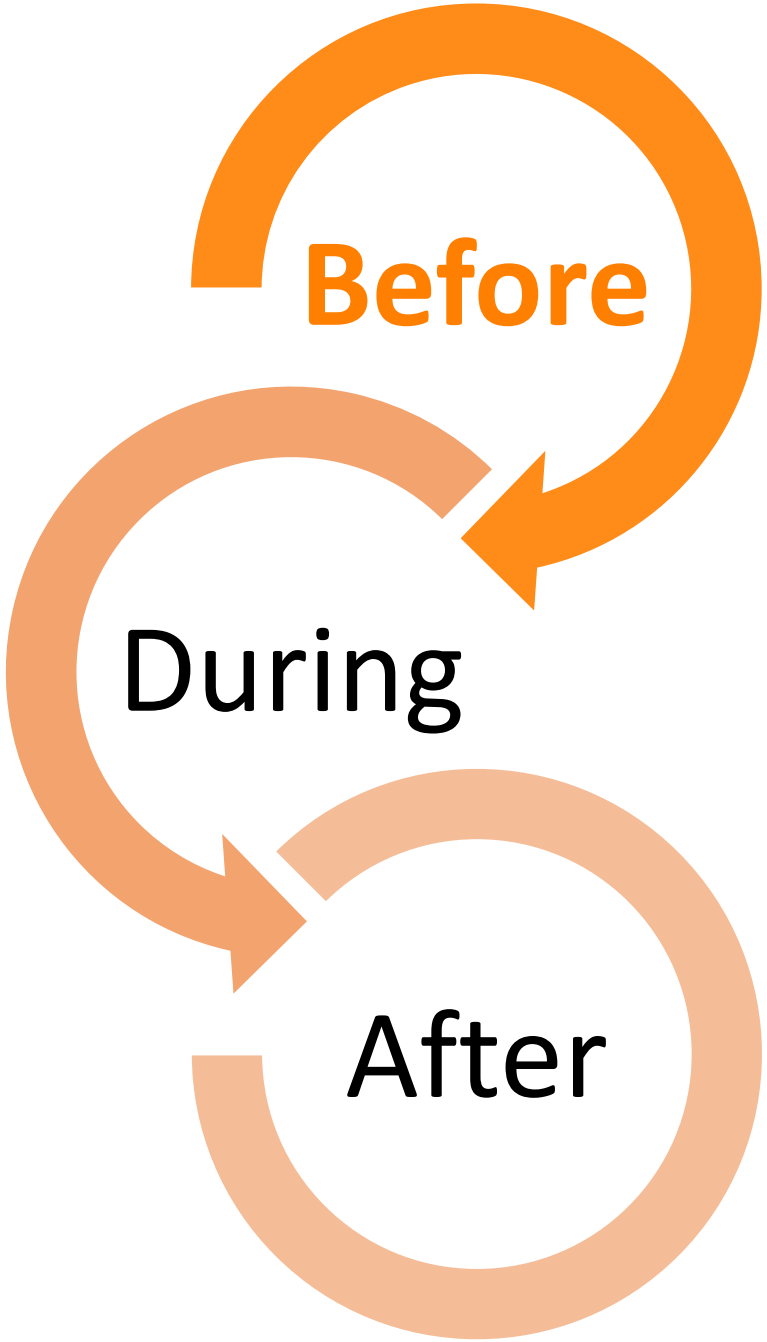
Audit criteria: *set of requirements used as a reference against which objective evidence is compared*

Audit findings: *results of the evaluation of the collected audit evidence against audit criteria*

Note 1 to entry: Audit findings indicate conformity or nonconformity.

Our main objective is to show the auditors that the ISMS is **implemented**, **managed** and **continuously improving**

Show the evidence (records)!



1. Choose a certification body
2. Request and check the audit plan in advance
3. Conduct a brief self-assessment
4. Check the mandatory documents
5. Prepare and send documents to the lead auditors
6. Take care of the auditors
7. Strengthen the motivation of employees
8. Hold an internal briefing meeting
9. Train your employees to avoid common mistakes
10. Prepare a detailed presentation about the company and the ISMS
11. Check again that the clear desk and clear screen policy is followed by employees

How to choose a certification body?

1. Select a UKAS-accredited certification body, www.ukas.com/find-an-organisation
2. Pay attention to experience in your industry and country
3. Don't choose unknown companies
4. Price should not be the main criterion

I have positive experience with the BSI and Bureau Veritas

Request and check the audit plan in advance

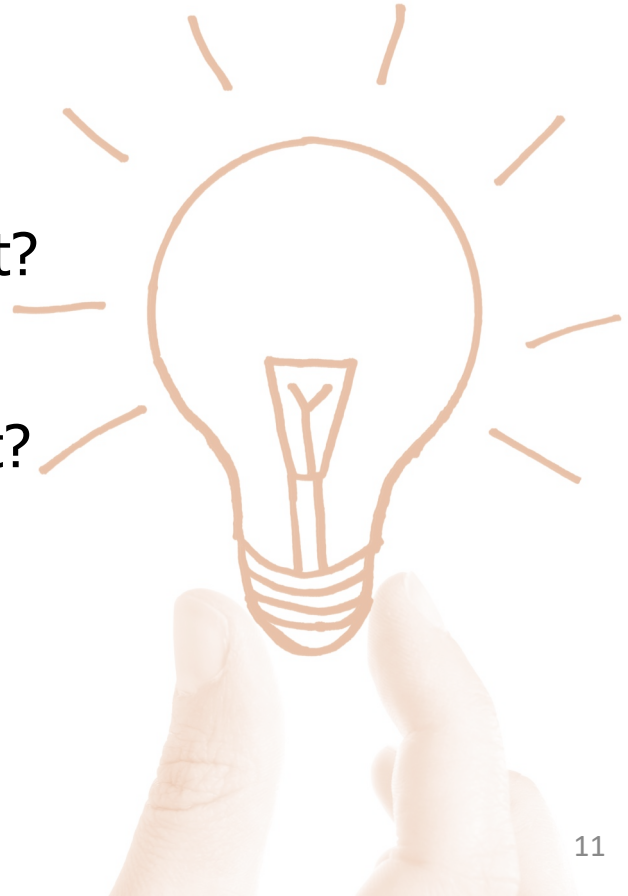
1. Scope
2. Audit format (on-site or remote)
3. Schedule:
   - Holidays and major events
   - Availability of key persons
   - Business travel plan
   - Time between the audit stages (1-6 months)
4. Auditors' security clearance procedure (if applicable)
5. Official language (Do we need an interpreter?)
6. Observers (e.g., from the parent company)
7. Other restrictions (e.g., equipment, access, audit methods)

Once you have received the audit plan, expand it by listing the names of responsible persons within your organisation. The list of persons should be agreed in advance with their direct supervisors.

Who will escort the auditors during the audit?

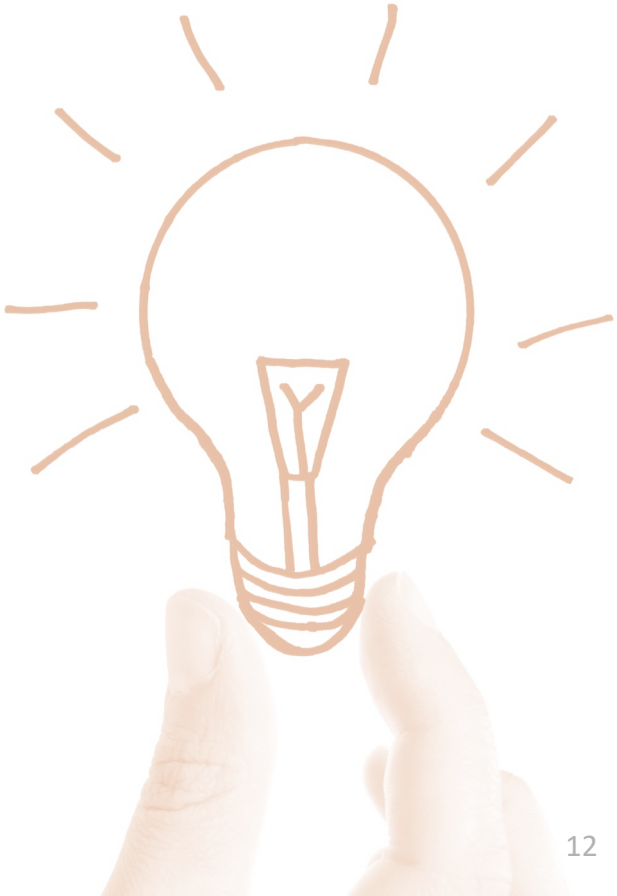
Conduct a brief self-assessment

1. What is our level of preparedness?
2. What are our strengths?
3. What are our weaknesses?
4. What nonconformities are still open?
5. What requirements have not been met?
6. What could be a problem?
7. What can we improve before the audit?



If something has not been implemented before the audit, document the Action Plan...

This may help to avoid nonconformities.



Check that the mandatory documents are available and up to date

#	Requirement for documented information concerning	ISO 27001:2022
1.	Scope of the ISMS	4.3
2.	Information security policy	5.2
3.	Information security risk assessment process	6.1.2
4.	Information security risk treatment process	6.1.3
5.	Statement of Applicability (SoA)	6.1.3 d)
6.	Information security objectives	6.2
7.	Evidence of competence	7.2 d)
8.	Documented information determined by the organization as being necessary for the effectiveness of the ISMS	7.5.1 b)
9.	Operational planning and control	8.1
10.	Results of the information security risk assessments	8.2
11.	Results of the information security risk treatment	8.3
12.	Evidence of the monitoring and measurement results	9.1
13.	Evidence of the audit programme(s) and the audit results	9.2 g)
14.	Evidence of the results of management reviews	9.3
15.	Evidence of the nature of the nonconformities and any subsequent actions taken	10.2 f)
16.	Evidence of the results of any corrective action	10.2 g)

Prepare and send documents to the lead auditor (if requested)

Lead auditor (LA) may request:

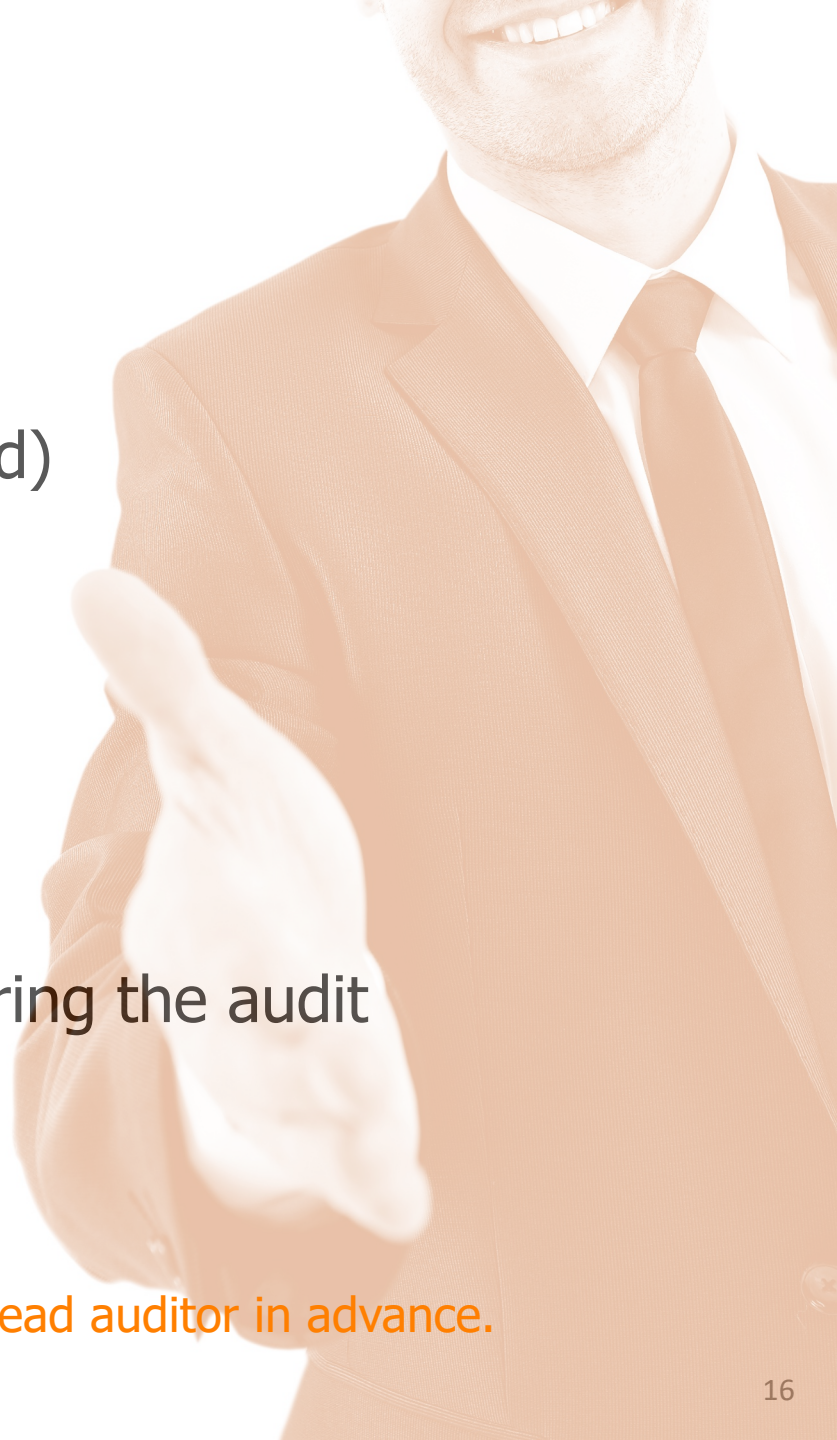
1. Organizational chart
2. ISMS Scope
3. List of requirements
4. List of ISMS documents
5. ISMS Management review report
6. Internal ISMS audit report
7. An official letter that states:
   - Company name
   - Address
   - ISMS Scope statement
   - Number of printed copies of certificate (usually only one is included)

In general, try to avoid sharing documents with the auditors.
It is better to show them on your site and on your equipment.

Take care of the auditors

Plan and organize:

1. Access permit (in advance)
2. Transfer or Parking (if needed)
3. Interpreter (if needed)
4. Meeting room
5. Guest WiFi
6. Dedicated printer
7. Water, tea/coffee, snacks during the audit
8. Lunch



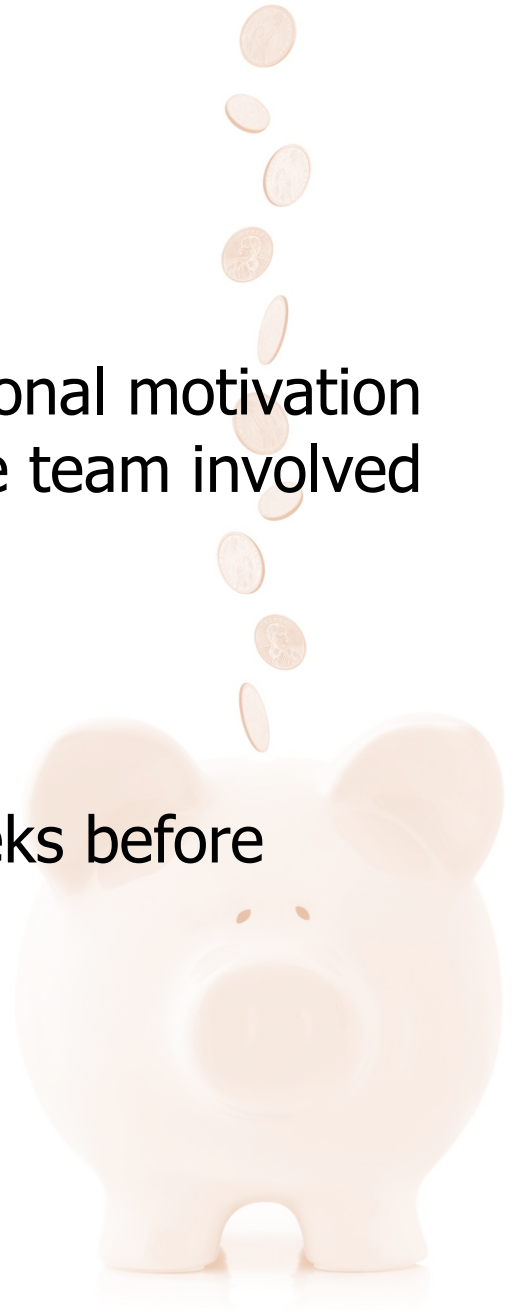
Exchange contacts with the lead auditor in advance.

Take a look at the auditors' LinkedIn profiles.

This will help predict potential areas of high interest

Strengthen the motivation of employees

- Negotiate with management the additional motivation (e.g., bonus and other benefits) for the team involved in the audit.
- Don't forget the related departments (e.g., IT, QM, HR, Legal).
- They will have to work hard in the weeks before and during the audit…



Hold an internal briefing meeting 1-2 days before the audit

Agenda:

1. Audit plan and schedule
2. Our strengths and weaknesses
3. Common questions
4. IS Policy and IS Objectives
5. Clear desk and clear screen policy
6. Rules for communication with auditors:
   - Say and show only what is asked
   - Access to systems and presenting of confidential information (including personal data) only in the presence of information security personnel and with their direct approval
   - Do not take removable media from the auditor
7. Additional motivation

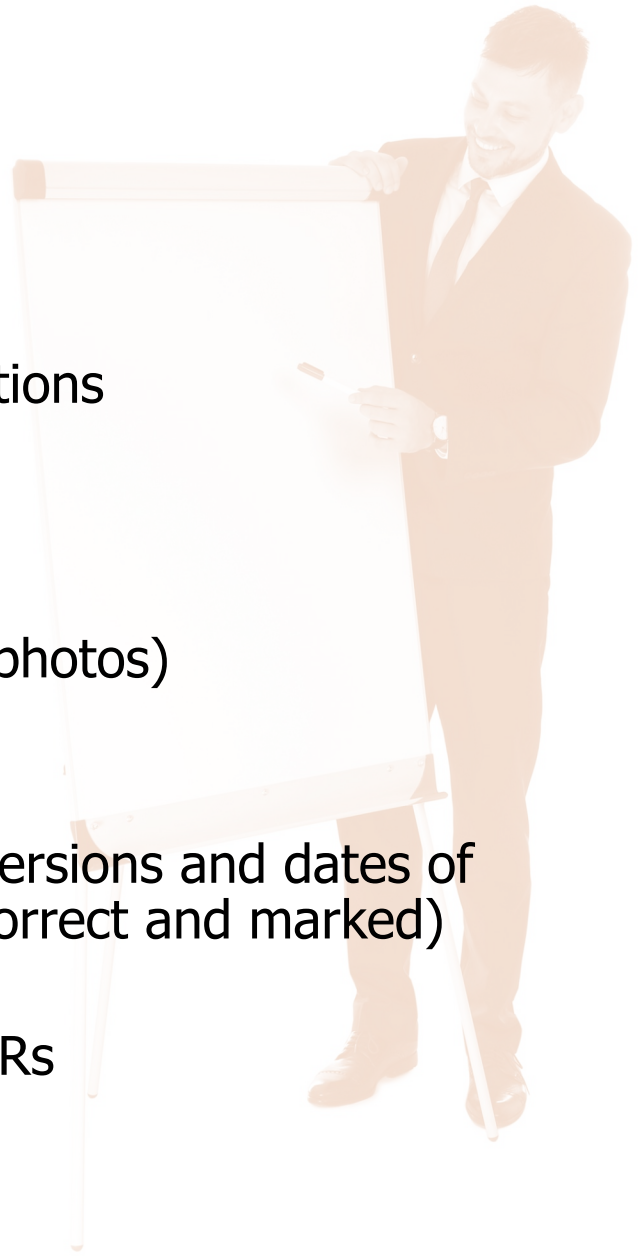
Send a short memo/presentation about the ISMS

Train your employees to avoid common mistakes highlighted by auditors

1. Lack of awareness:
   - The IS policy and where to find it
   - How to notify IS incidents
   - Information classification and labeling
   - What to do in case of an emergency (e.g., fire)
2. Using outdated versions of documents
3. Violating the clear desk and clear screen policy
4. Discussing confidential information in front of unauthorised people
5. Not wearing badges
6. Presenting the personal data of other employees and clients to the auditor
7. Taking external storage media from unauthorized persons (e.g., to print something out when asked by an auditor)
8. Allowing strangers access to protected areas (e.g., “Piggyback attack”)

Prepare a detailed presentation about the company and the ISMS

1. Company name (official)
2. Address
3. Website
4. Brief company description
5. Management structure
6. Main interested parties and their expectations
7. List of requirements
8. ISMS Scope
9. IS Policy and Objectives
10. ISMS Implementation team (ideally with photos)
11. ISMS RACI
12. Significant ISMS milestones and events
13. List of ISMS documents (check that the versions and dates of approval of documents and records are correct and marked)
14. Brief description of ISMS processes
15. Results of past audits and list of open NCRs
16. Important contacts



Check again that the clear desk and clear screen policy is followed by employees

(Check all premises **1 hour** before the audit)

- ❑ No printed confidential documents at printers, shredders and waste bins
- ❑ Confidential documents are destroyed using shredders
- ❑ No printed confidential documents (or drafts) in meeting rooms, kitchens and lounge areas
- ❑ No confidential documents left unattended in workplaces
- ❑ Flipcharts and whiteboards are clean
- ❑ There are no written passwords on monitors, under keyboards and other visible places
- ❑ Server rooms and archives are locked
- ❑ Other rooms are locked and/or under control
- ❑ Switch cabinets are locked
- ❑ Safes and cabinets with confidential documents are locked
- ❑ Keys, access cards, external storage media and tokens are under control
- ❑ Monitors are placed so that visitors cannot see the information on them
- ❑ Computers are not left on unattended (e.g., during coffee and lunch breaks)

Company name (Auditor)		
Coordinator (Auditor)		☐ Contacts
Lead Auditor		☐ Contacts
Auditors and technical experts		
Observers		
Official language		
Criteria		
Date and Place		
Coordinator (Auditee)		
Reserved Meeting Room		

☐ The requested documents have been sent	☐ Access is requested and allowed	☐ NDA is checked
☐ Key employees are identified in accordance with the audit plan	☐ Meeting with the key employees has been held	☐ Employees are aware of the audit
☐ ISMS Records are collected	☐ ISMS Overview presentation is prepared	☐ Water / Coffee / Snacks ☐ Lunch
☐ Clear Desk and Clear Screen Policy is checked	▪ Employee desks, meeting rooms, server rooms, kitchen and corridors ▪ Printers and shredders, flip charts and boards, bins, safes and lockers	

List of key employees:	

Print:	☐ Checklist	☐ Audit Plan
	☐ IS Policy	☐ List of ISMS documents (with revisions)
	☐ ISMS Scope	☐ Order about the audit (if applicable)

ISMS: Audit Preparation Checklist
2.1, 30.11.2022

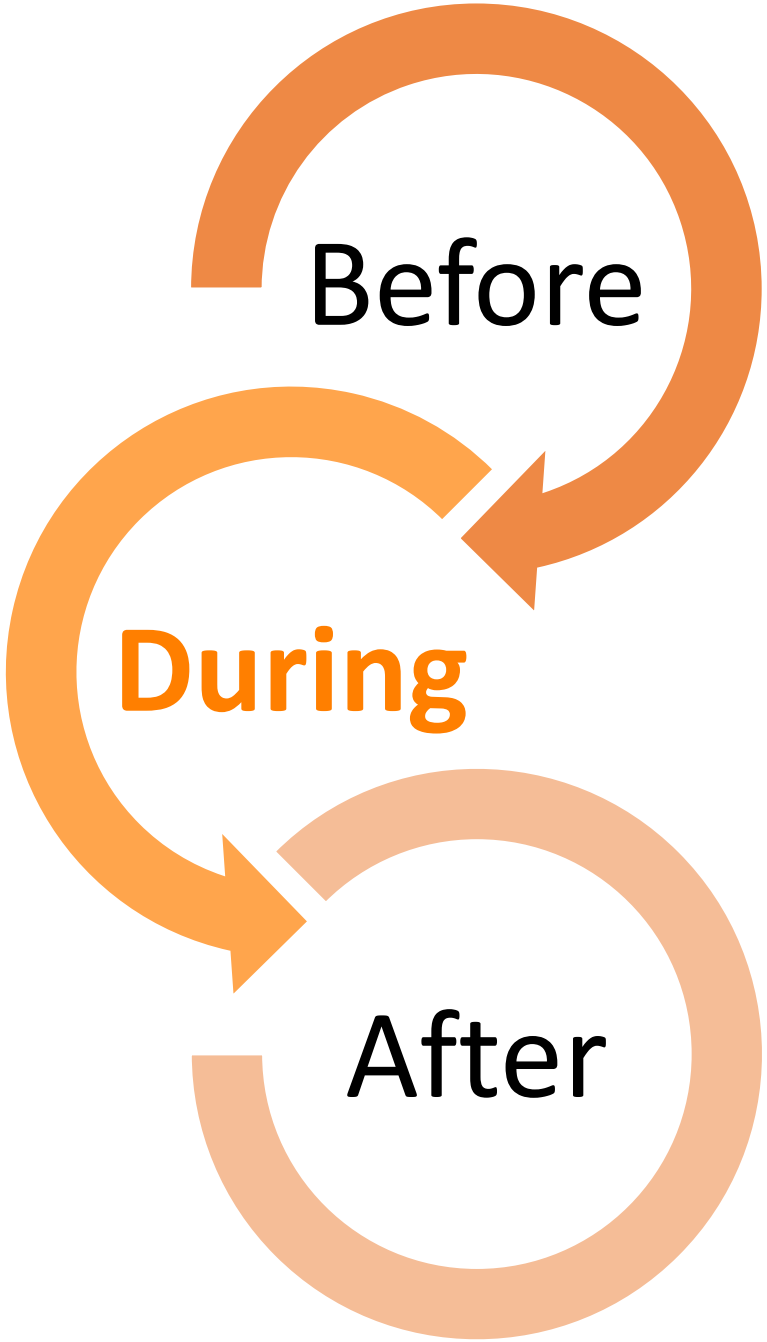
Other tasks

☐	
☐	
☐	
☐	
☐	
☐	
☐	
☐	
☐	
☐	

Notes

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov

www.patreon.com/posts/31763395



1. Invite top management to the meetings
2. Take notes during the audit
3. Hold a meeting with the ISMS team after each audit day

Invite top management representatives to the first and final meetings with the auditors.

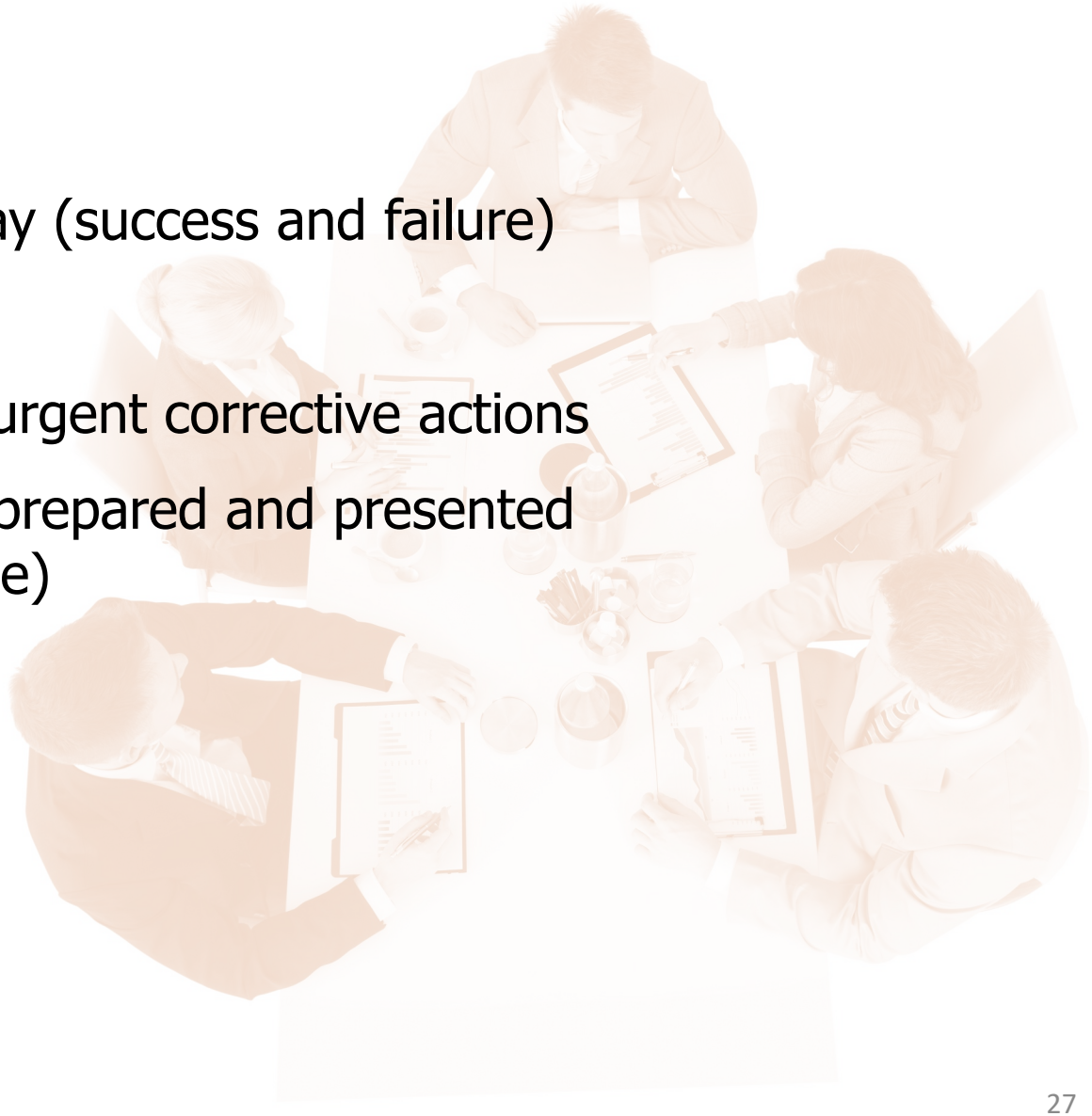
Auditors expect this.

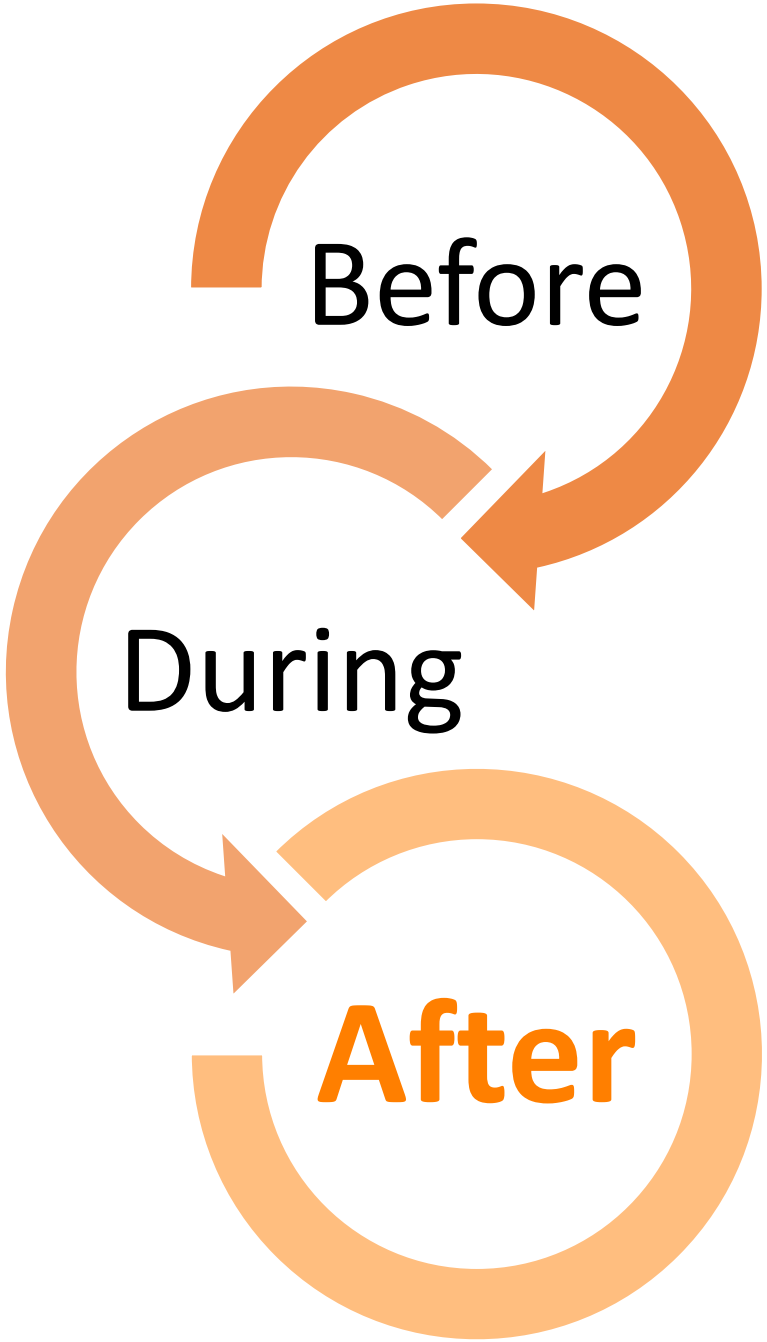
Take notes during the audit.

You can get a lot of useful ideas and advice from auditors

Hold a meeting with the ISMS team after each audit day

1. Summary of the day (success and failure)
2. Lessons learned
3. Potential NCs and urgent corrective actions
4. What needs to be prepared and presented (additional evidence)
5. Plan for tomorrow





1. Check the audit report
2. Plan for improvements and corrective actions
3. Discuss the results and thank the team

Check the audit report

1. Company name and address
2. Audit dates
3. ISMS scope
4. Observation and comments
5. **Nonconformities**
6. Recommendations for improvement
7. Names and versions of ISMS documents
8. Names of the people interviewed

Plan for improvements and corrective actions

- In general, you can try to dispute the identified nonconformities...
- Minor non-conformities can be covered by the plan and will be re-checked during the next surveillance audit.
- Major non-conformities have to be corrected in 90 days. Discuss the plan with the lead auditor.

Discuss the results and thank the team

Thanks and good luck!

www.linkedin.com/in/andreyprozorov

www.patreon.com/AndreyProzorov

My ISMS Implemantation Plan + templates

ISO 27001: ISMS Implementation Plan
4.2, 15.11.2022

ISMS Implementation Toolkit - www.patreon.com/posts/47806655

Stage	ISMS Implementation Toolkit	Output
0. Read ISO 27001 and additional materials. Take a training course.	• *ISO Survey 2021: ISO 27001 certificates* • *ISO 27001, 27002, 27003, 27005, 27014 mindmaps* • *The ISO 27000 Family of Standards* • *ISO 27001. New information security controls, 2022* • *IS Controls Mapping (2013 and 2022)* • *ISMS Required activities* • *ISO 27001 implementation steps (Approaches)* • *My presentation "ISO 27001:2022. What has changed?"* • *Recommendations**	• Basic knowledge • Purchased standards (ISO 27001, 27002, 27003, 27005)
1. Conduct awareness training for the top management	• *ISO 27001 Intro Presentation**	• Presentation and MoM
2. Conduct a Gap analysis	• *Request documents for GAP analysis (ISMS and PIMS)* • *ISMS GAP Analysis Report (template)* • *ISMS Required activities* • *Requirements for documented information in ISO 27001 and ISO 27701* • *Cyber Security Principles by ACSC* • *List of documents (template)*	• ISMS Gap Analysis report • List of ISMS documents (draft)
3. Understand the Context	• *Privacy Pain Points and Trigger Events* • *Information Security and Data Protection context (mindmap)* • *List of interested parties (example)* • *List of Requirements (template)* • *ISMS Scope (template)*	• List of Requirements (draft) • ISMS Scope (draft) • List of interested parties (draft) • Slides for the first IS Committee meeting • Organization Chart
4. Plan the implementation	• *ISMS Implementation Plan* • *ISMS Implementation Schedule* • *ISMS Required activities* • *ISMS Communication plan (example and template)* • *ISMS issues and feedback register (template)*	• ISMS Project Charter • ISMS Implementation Plan (preliminary) • ISMS Communication plan (draft) • ISMS issues and feedback register

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov

ISO 27001: ISMS Implementation Plan
4.2, 15.11.2022

5. Conduct the first IS Committee meeting	• *ISMS presentation for the first IS Committee meeting (template)** • *MoM (template)**	• Presentation and MoM • ISMS Communication plan
6. Establish Information Security Policy and Information Security Objectives	• *Checklist for Information Security Policy and GDPR Policy* • *Information Security Policy (example)* • *Information Security Principles*	• Information Security Policy • Presentation, MoM and Orders
7. Take an inventory of the assets	• *List of information assets (template)* • *Information Asset Categories by SoGP 2022* • *Supporting assets mindmap by EBIOS RM*	• List of information assets
8. Define a method of risk assessment, identify and assess information security risks	• *ISO 27005:2022 Overview* • *ISO 27005:2022. Risk Assessment and Treatment processes, mindmaps* • *ISO 27005:2022. Information security risk assessment and treatment processes* • *Examples of typical threats, ISO 27005:2022* • *Lists of common information security threats* • *My list of information security threat events* • *Risk Register Template by ISACA* • *Risk Register Template by NIST* • *IS Risk Register (template)**	• Information security risk management procedure • Information security risk assessment methodology • Information security risk assessment report / register
9. Prepare Statement of Applicability (SoA) and Risk Treatment Plan (RTP)	• *ISMS Maturity Levels and Statement of Applicability (SoA) template, 2013 and 2022* • *Risk Treatment Plan (template)**	• Statement of Applicability, SoA (draft) • Risk Treatment Plan, RTP
10. Define requirements for documentation management	• *ISMS Documented Information Policy (template)*	• ISMS Documented Information Policy • Templates

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov

ISO 27001: ISMS Implementation Plan
4.2, 15.11.2022

11. Develop ISMS Framework and define roles and responsibilities	• *ISMS RACI Chart (example)* • *ISMS Framework (mindmap)* • *ISMS core process by Knut Haufe* • *Information Security Principles*	• ISMS Framework Annexes: – RACI Chart – ISMS Scope – List of interested parties – List of Requirements • Orders • Changes in the Job Descriptions
12. Develop and implement a set of ISMS policies and procedures	• *ISO 27002:2022 5.1 Policies for information security* • *ISMS Documented Information* • *Information Security Policies. Templates and resources for inspiration* • *Simple Policy Template* • *Set of example policies** • *Process description (checklist and template)* • *Sanity checklist for ISMS/PIMS documentation*	• Set of ISMS policies and procedure • SoA (updated)
13. Plan and implement additional information security measures	• *N/A* • *Information Security Controls. People Controls by ISO 27002:2022* • *Security Levels of Shredders*	• Implemented controls (records) • SoA (updated)
14. Plan, prepare and conduct awareness trainings	• *Competence for ISMS Professionals* • *Cybersecurity Profiles by ENISA* • *How to develop an IS awareness program, mindmap* • *Information Security and Data Protection awareness* • *Information Security and Data Protection Awareness Topics* • *Information Security and Data Protection culture* • *Interview questions for CISOs and DPOs* • *Chief Information Security Officer (CISO) by ACSC*	• Information security awareness programme and plans • Awareness materials and other records • Evidence of competence

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov

ISO 27001: ISMS Implementation Plan
4.2, 15.11.2022

15. Operate the ISMS	• *N/A*	• Records (all procedures) • ISMS Communication plan (updated) • ISMS issues and feedback register (updated) • IS Committee meetings (Presentations and MoMs)
16. Monitor the ISMS	• *Objective and Key Results (OKRs)* • *BCP and DRP. Failure and Recovery Metrics*	• List of objectives, KPIs and metrics • ISMS monitoring, measurement, analysis and evaluation reports
17. Audit the ISMS	• *Guidelines for ISMS auditing (mindmap)* • *Internal Audit Plan (template)* • *Internal Audit Report (template)* • *Nonconformity Report (template)* • *List of NCs** • *Audit Meetings Checklist* • *ISO 19011:2018 Guidelines for auditing management systems, Mindmap*	• Internal information security audit programme and plans • Internal information security audit reports • List of Nonconformities (NCs)
18. Conduct ISMS Management reviews	• *ISMS Management Review Report (template)*	• ISMS management review reports (MRR) • IS Committee meetings (Presentations and MoMs)
19. Practice continual improvement	• *N/A*	• Corrective Action Plan(s) • Continual Improvement Plan(s) • ISMS Framework (reviewed and updated) • Set of ISMS documents (reviewed and updated) • SoA (reviewed and updated) • RTP (reviewed and updated)
20. Prepare for the certification audit	• *ISMS Audit Preparation Checklist (short template)* • *Recommendations**	• Request for proposal (RFP) • ISMS Overview (presentation) • List of ISMS documents (updated) • Organization Chart

*Soon

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov

www.patreon.com/posts/isms-plan-iso-74660190