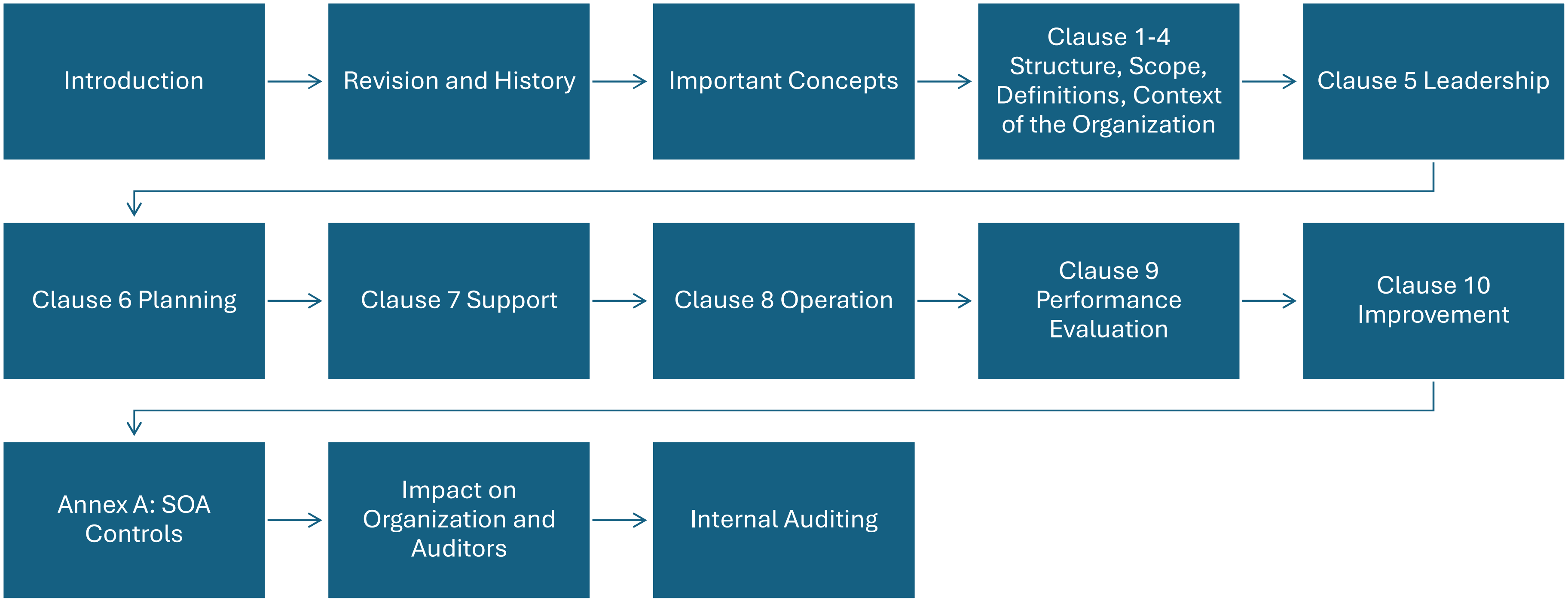
# Free ISO 27001:2022 Internal Auditor Training

From Quality Asia Certifications Private Limited

QUALITY ASIA

# Structure of the Course



Introduction

Revision and History

Important Concepts

Clause 1-4 Structure, Scope, Definitions, Context of the Organization

Clause 5 Leadership

Clause 6 Planning

Clause 7 Support

Clause 8 Operation

Clause 9 Performance Evaluation

Clause 10 Improvement

Annex A: SOA Controls

Impact on Organization and Auditors

Internal Auditing

# Objectives of the course

- Gain a clear understanding of the clauses and annex controls of ISO 27001:2022.
- Interpret the requirements and apply them to the organization's context.
- Understand how to assess the effectiveness of an ISMS in achieving organizational security objectives.
- Learn auditing principles, techniques, and practices as per ISO 19011:2018 guidelines.
- Support the organization in driving continual improvement in its ISMS.

# Trainer Introduction

QUALITY ASIA

- **Mr. Atul Suri**
- BE (Electrical), MBA
- Certified Lead Auditor:
  - ISO 9001, 14001, 45001, 50001, 22000, 27001, 13485, and 26000
- BEE Certified Energy Auditor (CEA)
- Professional Experience:
  - 30+ Years in the industry, with a strong foundation in engineering and management.
  - 20+ Years as a seasoned Management Systems Auditor and Trainer, delivering expertise across multiple sectors.
- Worked with Various Top Notch Certification Bodies as a Lead Auditor and Reviewer like Quality Asia, Intertek, Apave, Moody International, IRQS, etc

# About Quality Asia

**Mission:** To empower organizations with world-class quality standards and sustainable practices.

**Vision:** To be the leading provider of quality assurance and certification solutions in India.

**NABCB accredited:** Quality Asia is accredited by the National Accreditation Board for Certification Bodies (NABCB), which means that their certifications are recognized internationally.

**Ethical Certifications:** We are committed to providing 100% audit and compliance services, ensuring transparency and integrity in every certification we issue.

**Comprehensive Expertise:** We specialize in ISO 27001, ISO 9001, ISO 14001, and more, offering a full spectrum of certification services tailored to your organization's needs.

**Free ISO Internal Auditor Training:** We empower your team with free training, helping you build internal expertise and maintain compliance with international standards.

**Global Reach, Local Touch:** Serving clients across multiple Indian cities and international locations, we combine global expertise with personalized local service.

**Commitment to Excellence:** Our mission is to support businesses in achieving and maintaining their certification, unlocking new opportunities and improving operational efficiency.

# ABOUT FREE LIVE INTERNAL AUDITOR PROGRAM

QUALITY ASIA

**Monthly Training Programs**

We offer a focused training session on a different ISO standard each month, ensuring continuous learning and up-to-date knowledge for your team.

**Flexible Learning Options**

Missed a session? No problem! Our training programs are available for later viewing through the Quality Asia School on our website, allowing you to learn at your own pace. Log on to our Quality Asia website.

**Our Mission**

We are dedicated to increasing awareness about ISO standards and enhancing internal auditor competence. Our goal is to uplift industry operational standards by empowering professionals with the knowledge and skills they need to drive excellence in their organizations.

# Happy Republic Day

- Happy 76th Republic Day! On 26th January 1950, India adopted its Constitution, becoming a sovereign, democratic republic. Jai Hind!
- Republic Day celebrates the governance framework that safeguards our nation's sovereignty and values.
- Similarly, ISMS provides a structured approach to protect critical information, ensuring accountability and resilience against evolving threats.
- Let us pledge to uphold the Constitution's values while protecting our digital infrastructure for a secure future.

QUALITY ASIA
January 26
INDIA REPUBLIC DAY
Honoring the spirit of democracy & unity within our corporate fraternity this Republic Day.
www.qualityasia.in

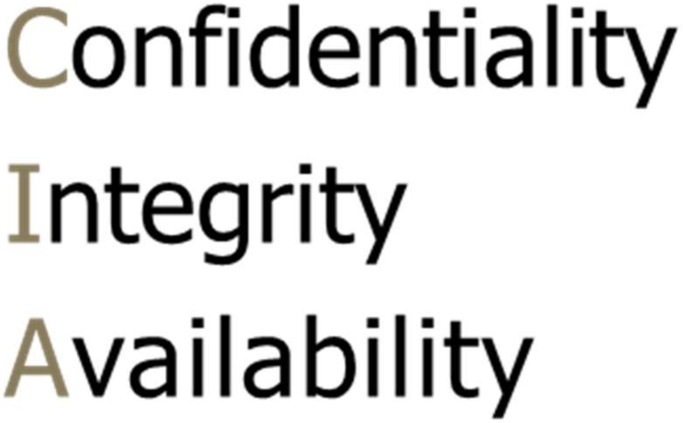
QUALITY ASIA

# ISO/IEC 27001:2022 Information Security Management System

What is Information Security?

## Information Security

- Information security is a concept, a concept that refers to the preservation of three properties of information which are confidentiality, integrity and availability.
- All those three properties are equally important for information security to be achieved.



Confidentiality

Integrity

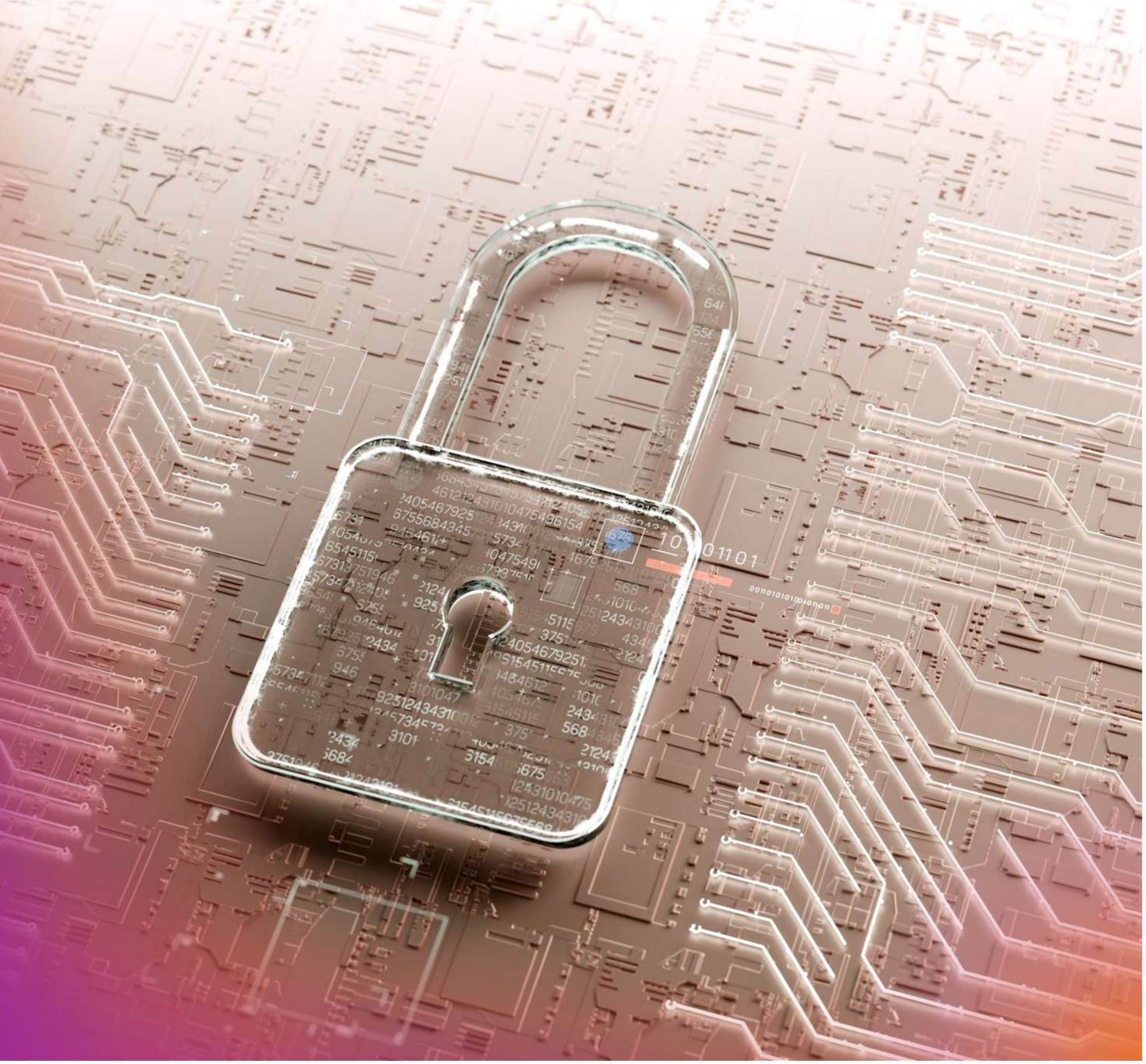
Availability

# Information Security

**Confidentiality** refers to information not being available or not being disclosed to unauthorized individuals or entities.

**Integrity** is about the accuracy and completeness of information, in other words, preventing information from being corrupted.

**Availability** refers to that property of information that makes it accessible and usable on demand by an authorized person or entity.



# Information security management

- Coordinated activities to achieve, maintain and improve information security, by identifying security risks and applying suitable controls to address them.

# Information security management system

- An ISMS consist of policies, procedures, guidelines, resources and activities that are managed by an organization with the aim of **protecting its information assets**.

# Principles for the successful implementation of an ISMS

**Awareness** of the need for information security.

Assignment of **responsibility** for information security.

Incorporating management **commitment** and the interests of stakeholders.

Enhancing **societal values**.

**Risk assessments** and determining appropriate controls.

Security incorporated as an essential element of **information networks and systems**.

Active prevention and detection of **security incidents**.

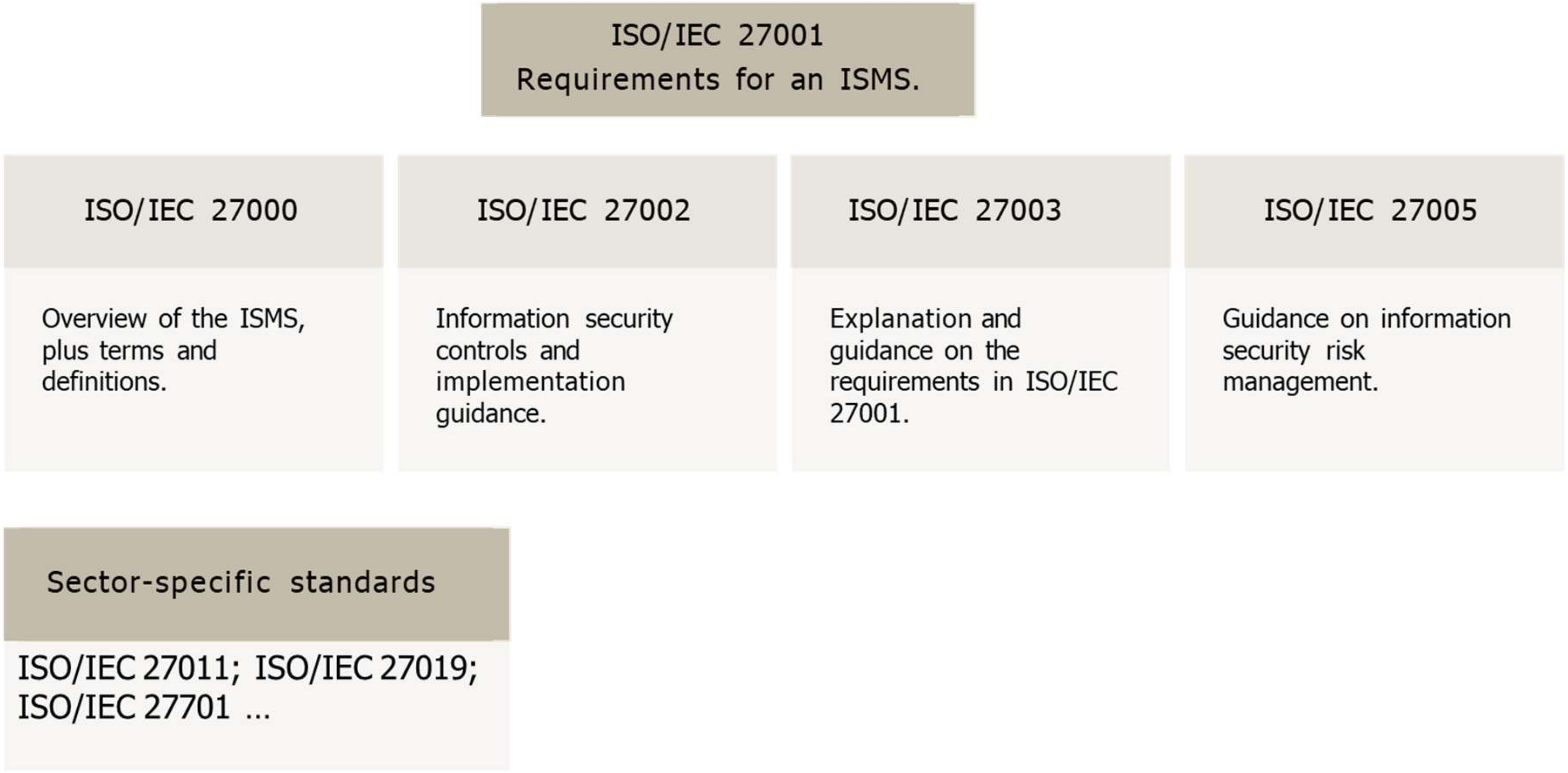
**Comprehensive approach** to information security management.

Continual **reassessment** of information security and making modifications, as appropriate.

# Benefits of Implementing ISO 27001 in the organization

- **Enhanced Information Security**: Protects sensitive data, minimizes risks of breaches, and ensures confidentiality, integrity, and availability of information.
- **Regulatory Compliance**: Helps organizations meet legal, contractual, and regulatory obligations related to data protection and cybersecurity.
- **Improved Risk Management**: Identifies, assesses, and mitigates security risks systematically, reducing vulnerabilities and potential disruptions.
- **Improved Business Continuity**: Enhances resilience to cyber threats, ensuring operations can continue smoothly during and after security incidents.
- **Competitive Advantages**: Establishes the organization as a trusted and secure partner, distinguishing it in the market and attracting new business opportunities.
- **Increased Stakeholder Confidence**: Demonstrates a commitment to information security, building trust with customers, partners, and other stakeholders.

# ISO/IEC 27000 Series of standard



ISO/IEC 27001
Requirements for an ISMS.

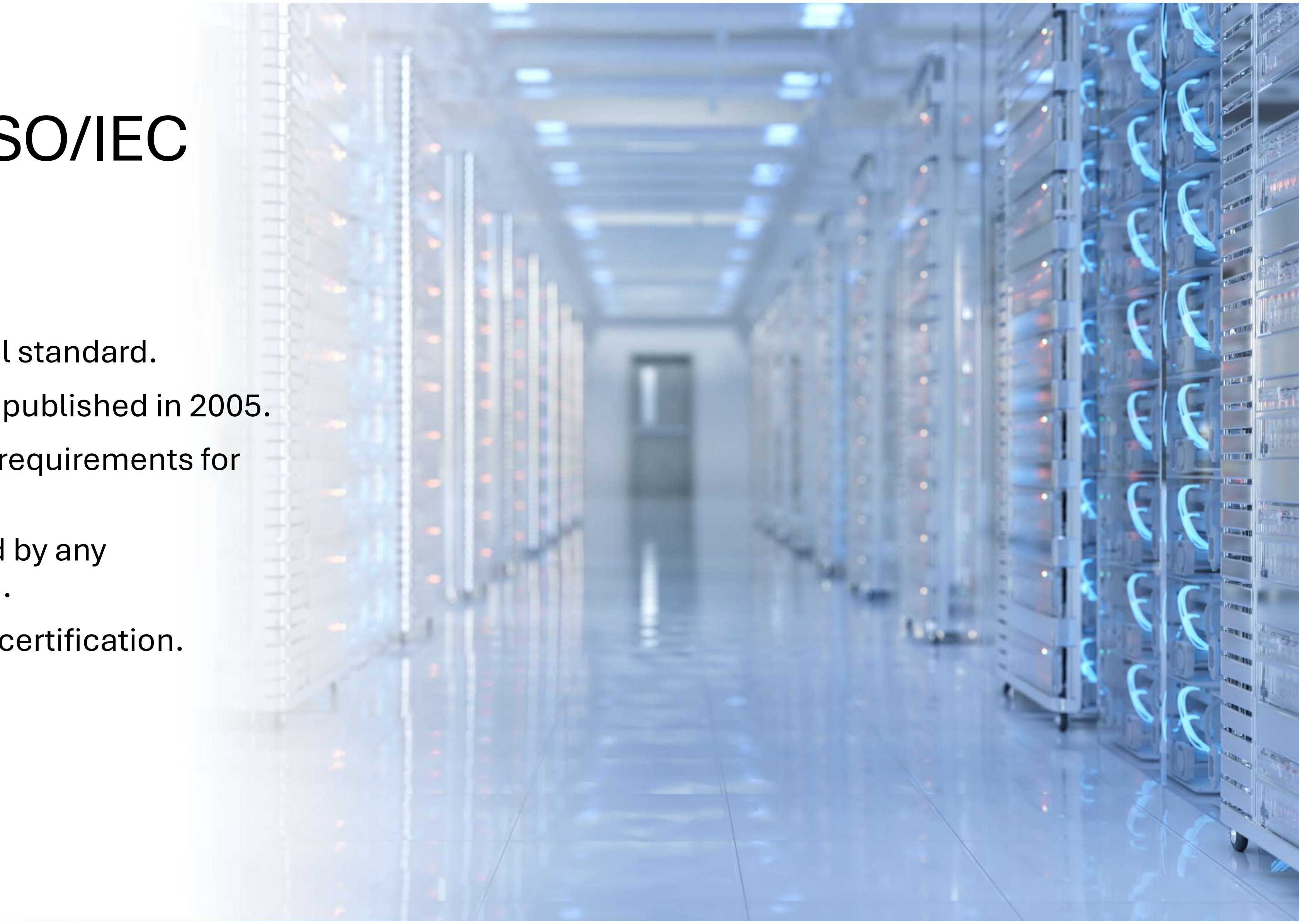
| ISO/IEC 27000 | ISO/IEC 27002 | ISO/IEC 27003 | ISO/IEC 27005 |
|---|---|---|---|
| Overview of the ISMS, plus terms and definitions. | Information security controls and implementation guidance. | Explanation and guidance on the requirements in ISO/IEC 27001. | Guidance on information security risk management. |

Sector-specific standards

ISO/IEC 27011; ISO/IEC 27019; ISO/IEC 27701 ...

# About ISO/IEC 27001

- International standard.
- First edition published in 2005.
- Defines the requirements for an ISMS.
- Can be used by any organization.
- Suitable for certification.

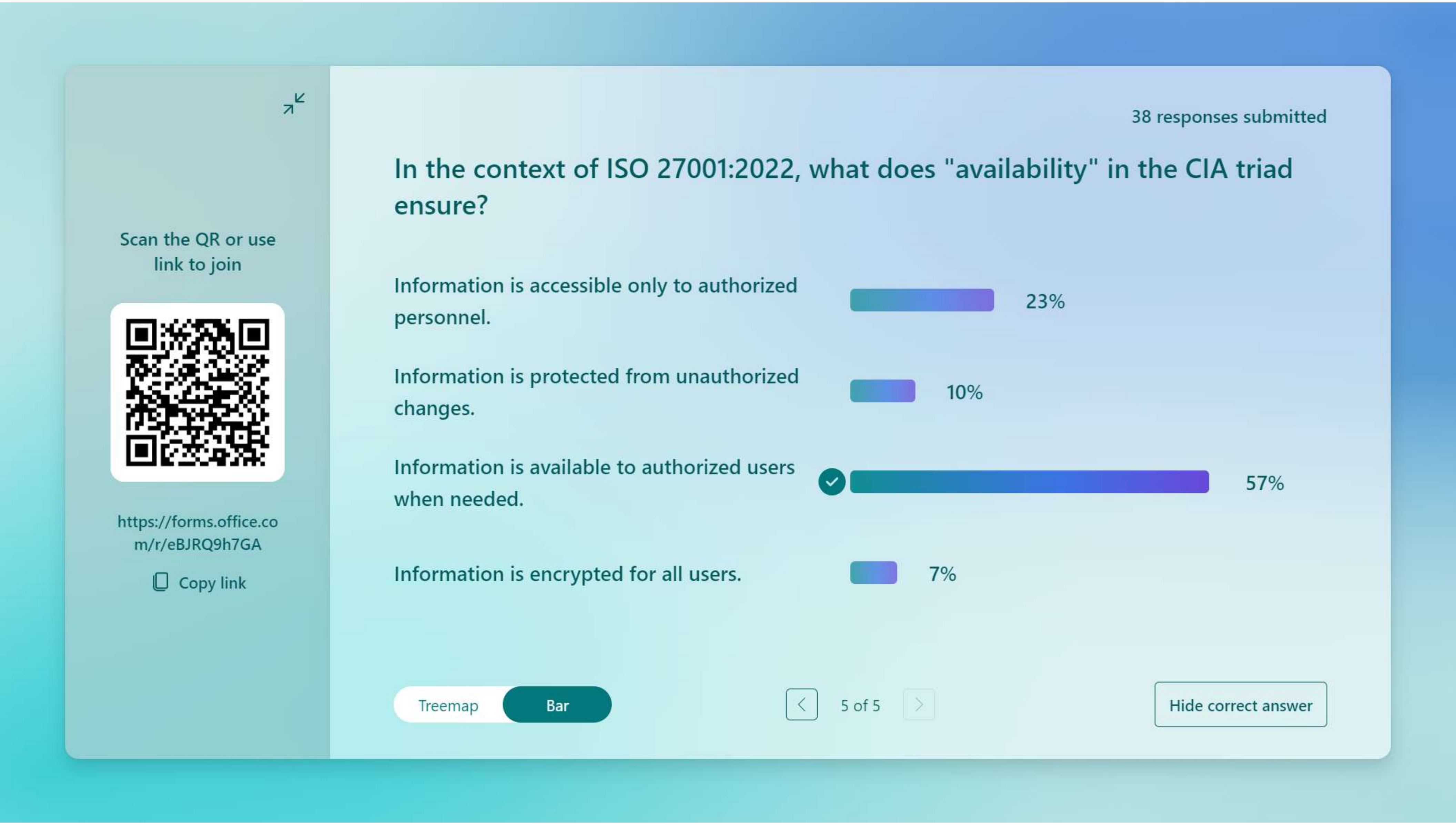


# Revision and History of ISO/IEC 27001:2022

- **First Edition (2005):** Published as ISO/IEC 27001:2005, it was based on the British Standard BS 7799-2.
  - Provided a systematic framework for managing information security risks through policies, controls, and processes.
- **First Major Revision (2013):** Released as ISO/IEC 27001:2013.
  - Adoption of Annex SL framework for management system standards, promoting easier integration with other standards like ISO 9001 and ISO 14001.
  - Introduction of risk-based thinking and removal of the Plan-Do-Check-Act (PDCA) model as a strict requirement.
  - Focused more on leadership involvement and context of the organization.
  - Updated control set in Annex A, aligned with ISO/IEC 27002:2013.

# Revision and History of ISO/IEC 27001:2022

- **Second Major Revision (2022):** Published as ISO/IEC 27001:2022, replacing the 2013 version.
  - Annex A control set aligned with ISO/IEC 27002:2022.
  - Controls reduced from 114 to 93, reorganized into 4 control themes.
  - Organizational: Focused on policies, roles, and management practices.
  - People: Addressed human resource and awareness issues.
  - Technological: Covered technical controls such as access management and encryption.
  - Physical: Included physical security measures like secure facilities.
  - Emphasis on addressing emerging threats like cloud security, data leakage prevention, and threat intelligence.
  - Inclusion of new controls for remote working, data masking, and monitoring.
- Transition Period for ISO/IEC 27001:2022: Organizations certified under ISO/IEC 27001:2013 have until October 31, 2025, to transition to the 2022 version.



Scan the QR or use link to join

https://forms.office.com/r/eBJRQ9h7GA

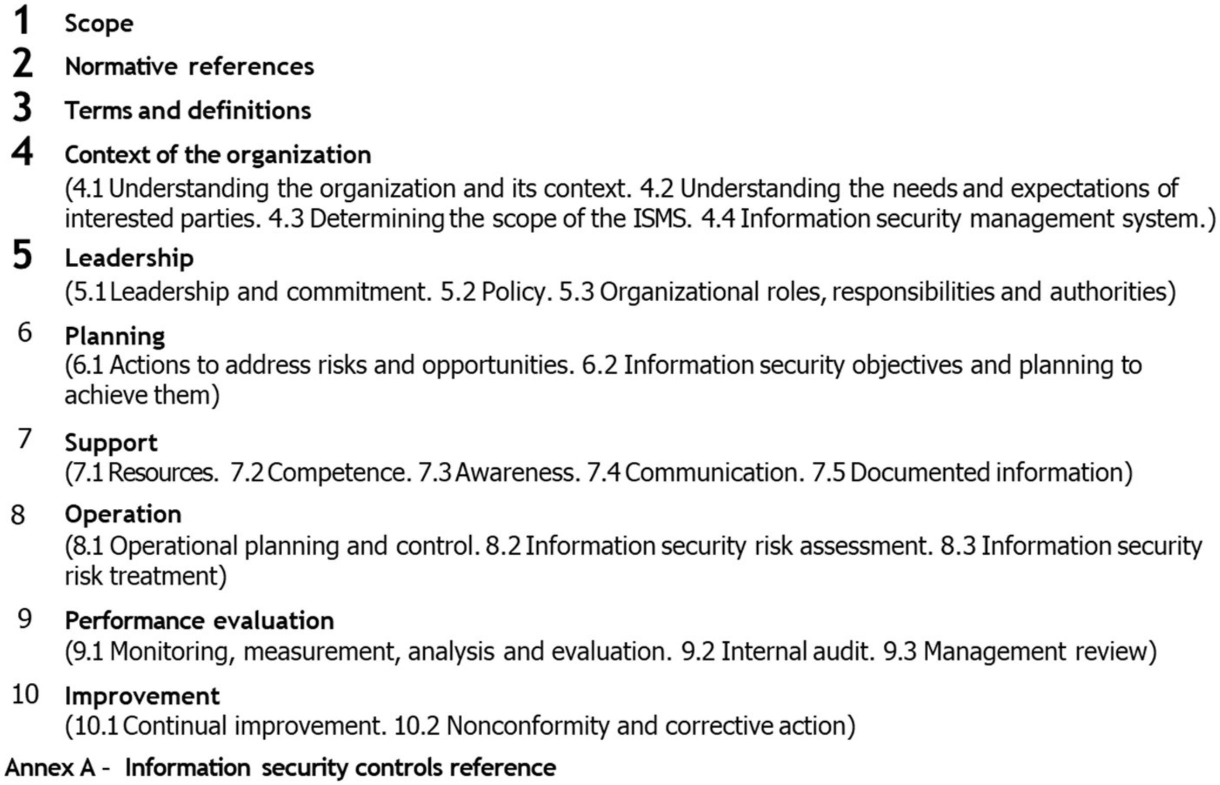
Copy link

38 responses submitted

In the context of ISO 27001:2022, what does "availability" in the CIA triad ensure?

| | |
|---|---|
| Information is accessible only to authorized personnel. | 23% |
| Information is protected from unauthorized changes. | 10% |
| ✓ Information is available to authorized users when needed. | 57% |
| Information is encrypted for all users. | 7% |

# Structure of ISO/IEC 27001:2022



**1 Scope**

**2 Normative references**

**3 Terms and definitions**

**4 Context of the organization**
(4.1 Understanding the organization and its context. 4.2 Understanding the needs and expectations of interested parties. 4.3 Determining the scope of the ISMS. 4.4 Information security management system.)

**5 Leadership**
(5.1 Leadership and commitment. 5.2 Policy. 5.3 Organizational roles, responsibilities and authorities)

6 **Planning**
(6.1 Actions to address risks and opportunities. 6.2 Information security objectives and planning to achieve them)

7 **Support**
(7.1 Resources. 7.2 Competence. 7.3 Awareness. 7.4 Communication. 7.5 Documented information)

8 **Operation**
(8.1 Operational planning and control. 8.2 Information security risk assessment. 8.3 Information security risk treatment)

9 **Performance evaluation**
(9.1 Monitoring, measurement, analysis and evaluation. 9.2 Internal audit. 9.3 Management review)

10 **Improvement**
(10.1 Continual improvement. 10.2 Nonconformity and corrective action)

Annex A - **Information security controls reference**

# Clause 4: Context of the organization

| S. No. | Clause No. | Clause name |
|---|---|---|
| 1. | 4.1 | Understanding the organization and its context |
| 2. | 4.2 | Understanding the needs and expectations of interested parties |
| 3. | 4.3 | Determining the scope of the ISMS |
| 4. | 4.4 | Information security management system |

# 4.1. Understanding the organization and its context

- Determine the **external and internal issues** that are relevant to the purpose of the organization and that affect its ability to achieve the intended outcome(s) of the ISMS.

# External and Internal Issues

- **External issues** - outside the organization’s control (e.g., political, legal, technological, social, cultural, competitive or natural factors, etc.).

- **Internal issues** – under the control of the organization (e.g., resources, knowledge, contractual relationships, objectives, etc.).

# 4.2. Needs and expectation of interested parties

- Determine the interested parties relevant for the ISMS.
- Determine the requirements of interested parties.
- Determine which requirements will be addressed through the ISMS.

# Interested parties

- Interested parties are individuals or organizations that can influence, be influenced by, or perceive themselves to be affected by the Information Security Management System (ISMS).
- Employees needs are secure access to systems and information.
- Regulatory Authorities needs are adherence to laws, standards, and regulations.
- Customers/Clients require assurance of confidentiality, integrity, and availability of their data.
- ....

# 4.3. Scope of the ISMS

- Determine the boundaries and applicability of the ISMS to establish its scope (what is covered by the ISMS).

The scope shall be documented.

# 4.4. Information security management system

- Establish, implement, maintain and continually improve an ISMS in accordance with the requirements of ISO/IEC 27001.
- Integrate the ISMS into the processes and the business activities of the organization.
- Don’t forget about the continual improvement of the ISMS.

# Climate action changes

- Amendment 1 to ISO 27001:2022 from February 2024

# CLIMATE ACTION CHANGES

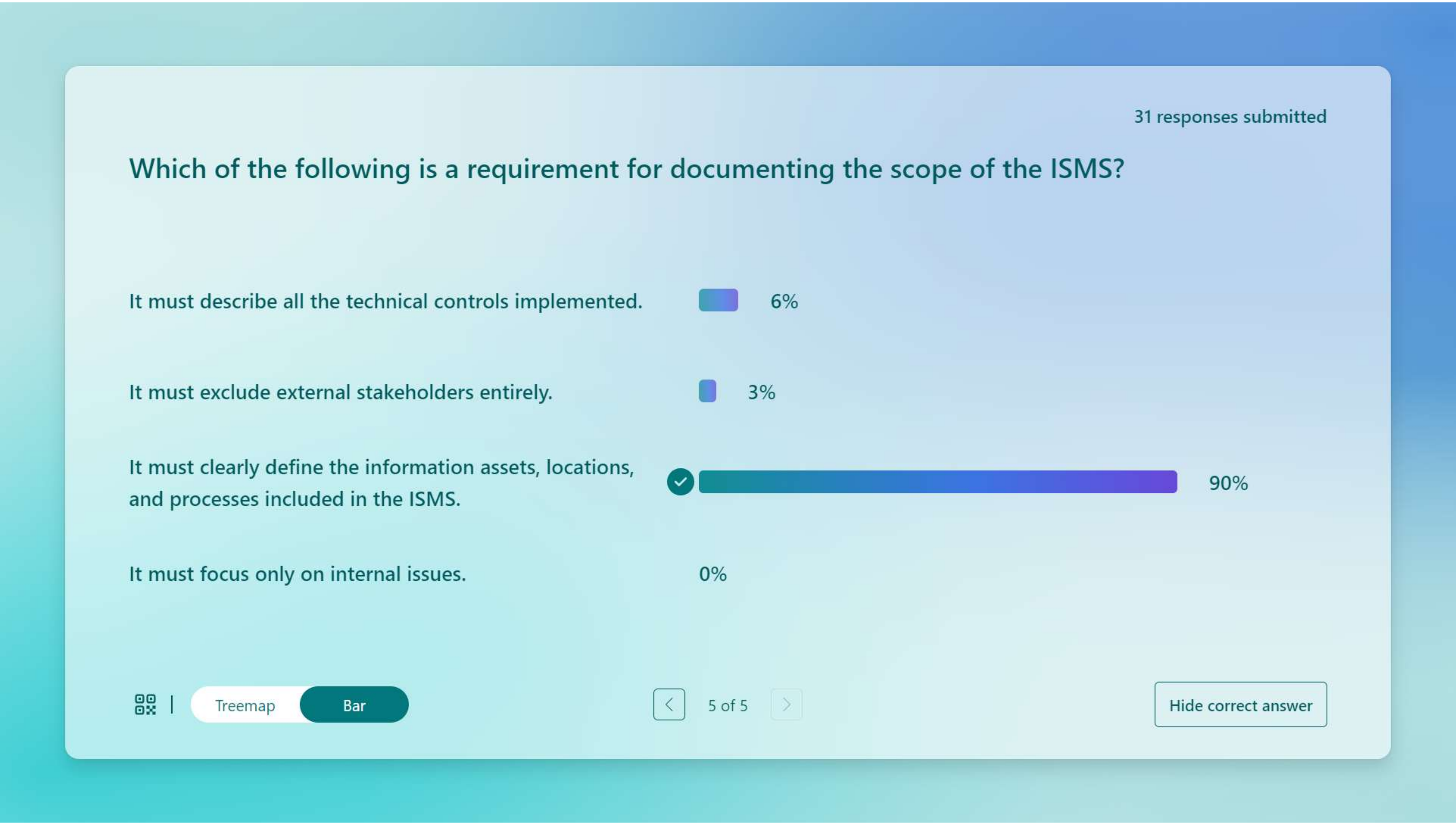
- The organization shall determine whether climate  change is a relevant issue (for its context)

# CLIMATE ACTION CHANGES

- Interested parties can have requirements related to climate change

# Recapitulation (Context of the organization)

- **Identify Factors Influencing the Information Security Management System (ISMS)**: Regulatory, market, technological, and organizational influences impacting ISMS.
- **Recognize Relevant Stakeholders**: Stakeholders (e.g., suppliers, customers, regulatory authorities, employees) and their information security needs and expectations.
- **Define the Scope and Applicability of the ISMS**: Determine internal and external issues and requirements of interested parties to set ISMS boundaries.
- **Commit to Continuous Improvement**: Develop, implement, maintain, and enhance the ISMS to achieve objectives and demonstrate continual improvement in information security.



31 responses submitted

Which of the following is a requirement for documenting the scope of the ISMS?

| | |
|---|---|
| It must describe all the technical controls implemented. | 6% |
| It must exclude external stakeholders entirely. | 3% |
| ✓ It must clearly define the information assets, locations, and processes included in the ISMS. | 90% |
| It must focus only on internal issues. | 0% |

# Clause 5: Leadership

| S. No. | Clause No. | Clause name |
|---|---|---|
| 1. | 5.1 | Leadership and commitment |
| 2. | 5.2 | Information security policy |
| 3. | 5.3 | Organizational roles, responsibilities and authorities |

# 5.1. Leadership and commitment

- Ensure that an information security **policy** and information security **objectives** are established.
- Ensure the ISMS is **integrated** into the processes of the organization.
- Ensure the necessary **resources** for the ISMS.
- **Communicate** about the need for information security.
- Ensure that the ISMS achieves its **intended outcomes**.
- Promote **continual improvement**.
- **Direct and support** persons to contribute to the ISMS.
- **Support managers** to demonstrate their leadership.

# 5.2. Information security policy

- The top management shall establish an information security policy.

# Information security policy

- **Appropriate** to the purpose of the organization.
- Includes the information security **objectives** or provides a framework for setting those objectives.
- **Includes commitments** to satisfy applicable requirements and for continual improvement.

- **Communicated** inside the organization.
- **Available** to interested parties, as appropriate.

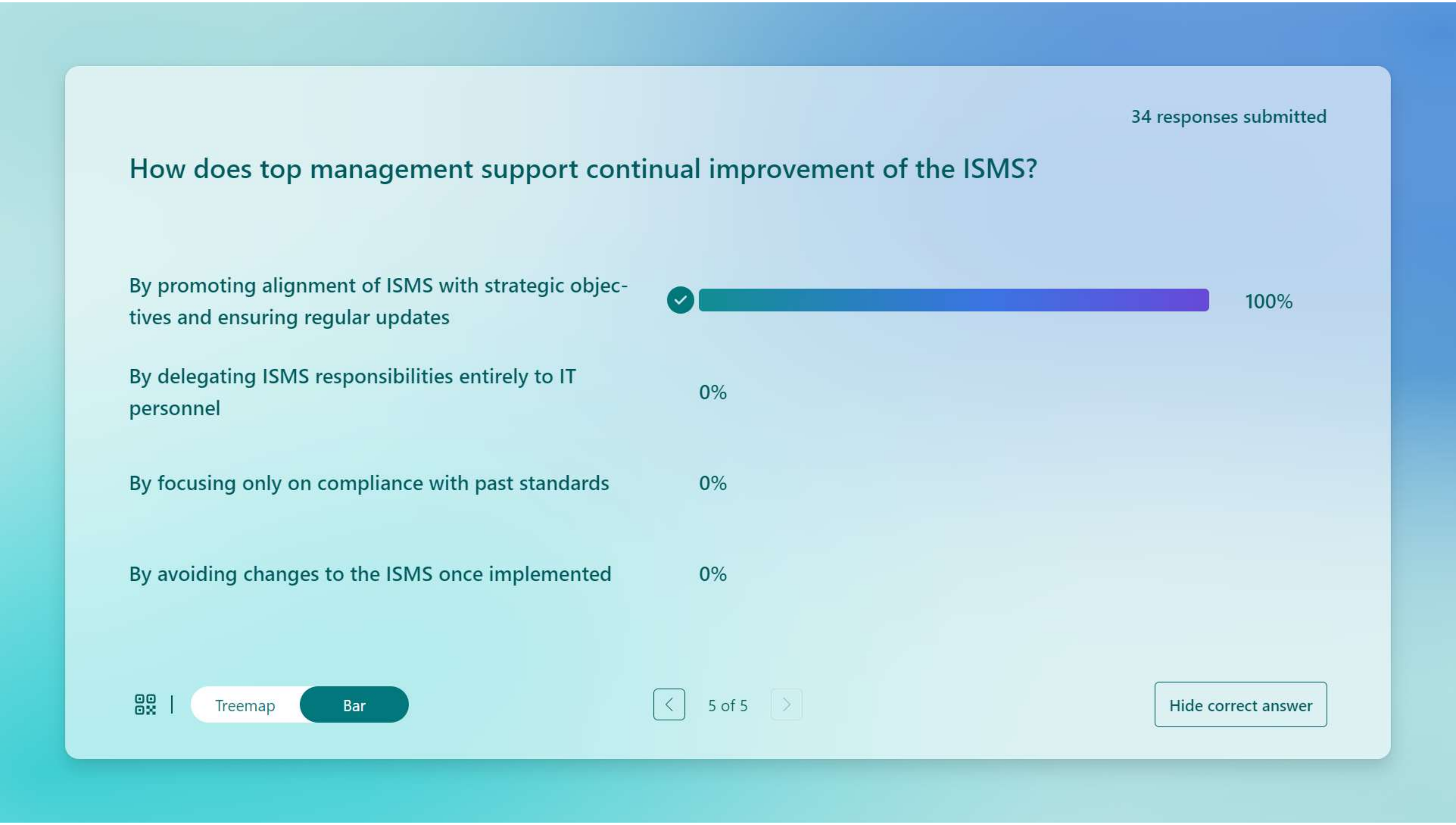
Documented.

# 5.3. Organizational roles, responsibilities and authorities

- The top management shall ensure that responsibilities and authorities for roles relevant to information security are assigned and communicated.
  - Ensure the ISMS conforms to requirements.
  - Report to the top management on the performance of the ISMS.

# Recapitulation (Leadership)

- **Integration of ISMS**: Top management ensures the ISMS is integrated into the organization's business processes.
- **Driving Strategic Alignment**: Promotes continual improvement of ISMS and ensures alignment with strategic objectives.
- **Information Security Policy**: Develop and maintain a policy that supports organizational goals, ensures compliance with regulatory requirements, and promotes secure practices.
- **Roles and Responsibilities**: Assign and communicate responsibilities across the organization to ensure effective implementation, maintenance, and improvement of the ISMS.
- **Leadership Commitment**: Actively support and demonstrate leadership in fostering an information security culture throughout the organization.



34 responses submitted

How does top management support continual improvement of the ISMS?

| | |
|---|---|
| By promoting alignment of ISMS with strategic objectives and ensuring regular updates | ✓ 100% |
| By delegating ISMS responsibilities entirely to IT personnel | 0% |
| By focusing only on compliance with past standards | 0% |
| By avoiding changes to the ISMS once implemented | 0% |

# Clause 6: Planning

| S. No. | Clause No. | Clause name |
|---|---|---|
| 1. | 6.1 | Action to address risks and opportunities |
| 2. | 6.1.1 | General |
| 3. | 6.1.2 | Information security risk assessment |
| 4. | 6.1.3 | Information security risk treatment |
| 5. | 6.2 | Information security objectives and planning to achieve them |
| 6. | 6.3 | Planning of changes |

# 6.1. Action to address risks and opportunities

- Determine risks and opportunities and plan actions to address them.

# 6.1.2. Information security risk assessment

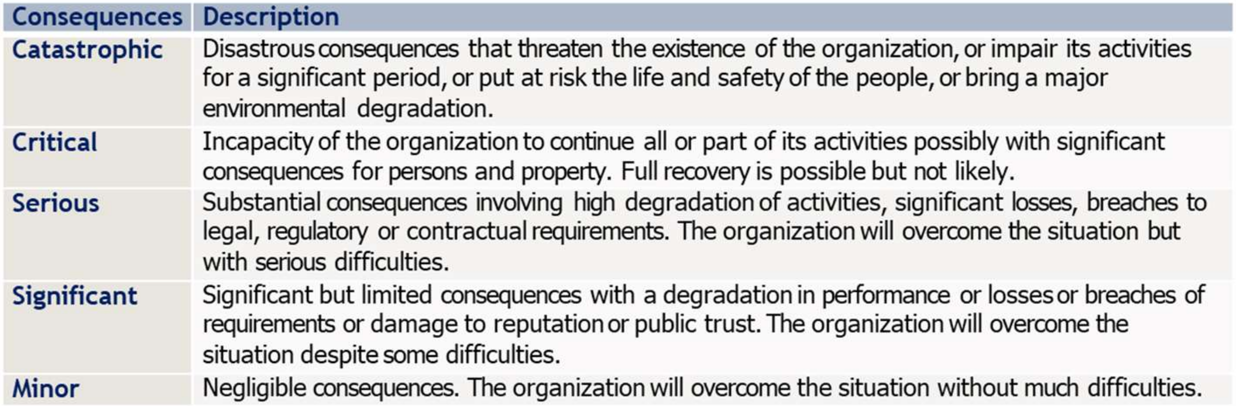
- **Risk** - the **effect of uncertainty** on objectives.
- **Information security risks** – associated with the potential that **threats will exploit the vulnerabilities** of an information asset and cause harm to an organization.

# Information security risk assessment

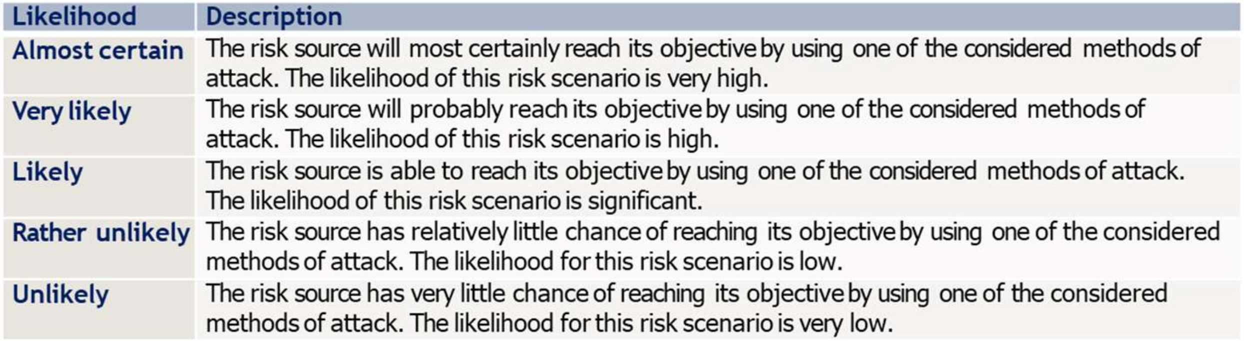
- Define and apply a process for the information security risk assessment.
- **RISK = Consequences x Likelihood**

- **Criteria** for risk acceptance and for performing risk assessments.

# Consequences and likelihood

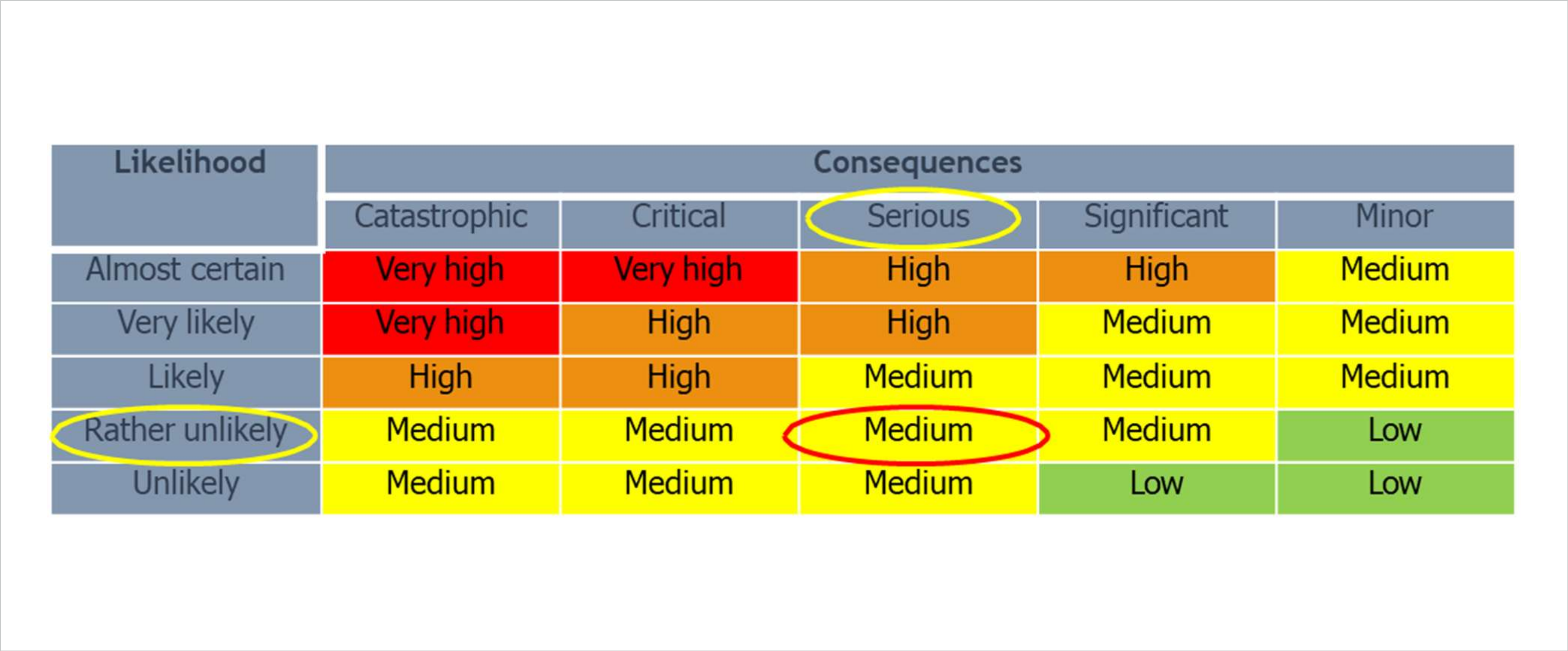


| Consequences | Description |
|---|---|
| Catastrophic | Disastrous consequences that threaten the existence of the organization, or impair its activities for a significant period, or put at risk the life and safety of the people, or bring a major environmental degradation. |
| Critical | Incapacity of the organization to continue all or part of its activities possibly with significant consequences for persons and property. Full recovery is possible but not likely. |
| Serious | Substantial consequences involving high degradation of activities, significant losses, breaches to legal, regulatory or contractual requirements. The organization will overcome the situation but with serious difficulties. |
| Significant | Significant but limited consequences with a degradation in performance or losses or breaches of requirements or damage to reputation or public trust. The organization will overcome the situation despite some difficulties. |
| Minor | Negligible consequences. The organization will overcome the situation without much difficulties. |



| Likelihood | Description |
|---|---|
| Almost certain | The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of this risk scenario is very high. |
| Very likely | The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of this risk scenario is high. |
| Likely | The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of this risk scenario is significant. |
| Rather unlikely | The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood for this risk scenario is low. |
| Unlikely | The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood for this risk scenario is very low. |

# Information security risk assessment

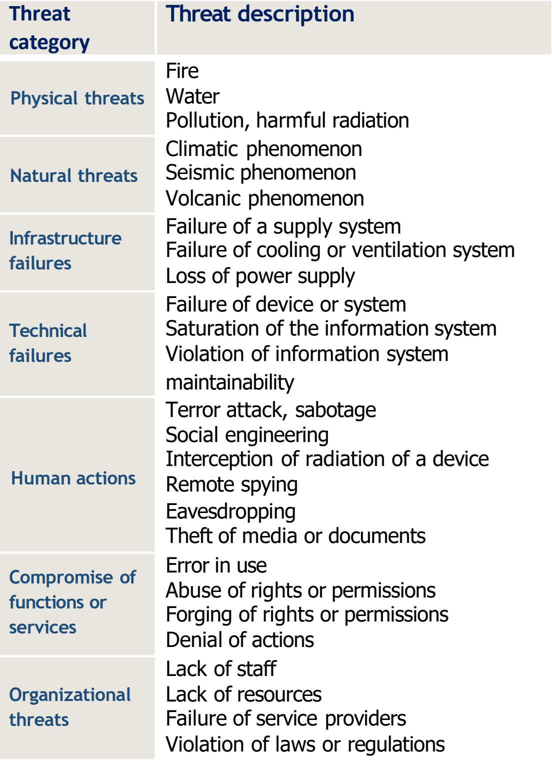


| Likelihood | Consequences | | | | |
|---|---|---|---|---|---|
| | Catastrophic | Critical | [✓ Serious] | Significant | Minor |
| Almost certain | Very high | Very high | High | High | Medium |
| Very likely | Very high | High | High | Medium | Medium |
| Likely | High | High | Medium | Medium | Medium |
| [✓ Rather unlikely] | Medium | Medium | [✓ Medium] | Medium | Low |
| Unlikely | Medium | Medium | Medium | Low | Low |

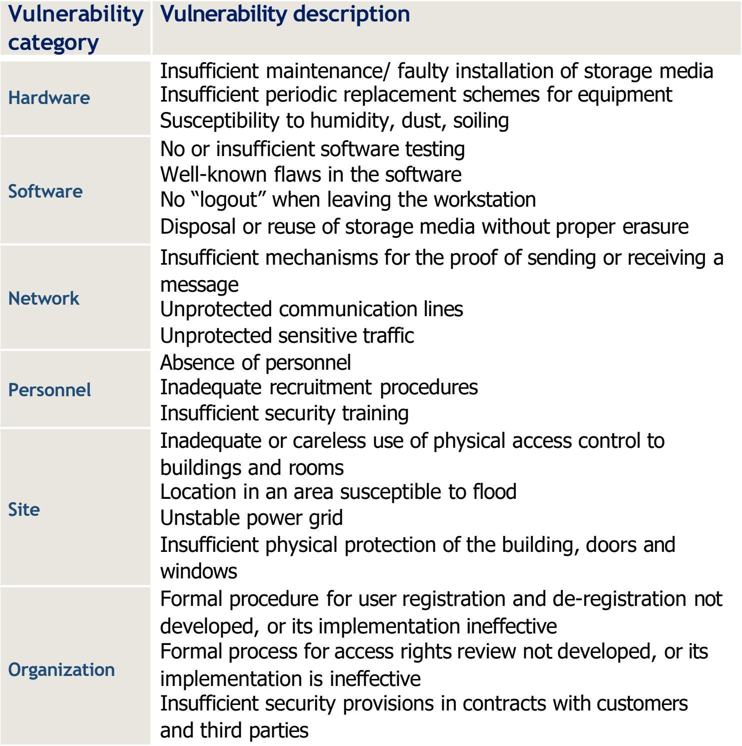
# Information security risk assessment

- Repeated information security risk assessments should produce **consistent, valid** and **comparable results.**
- **Risk identification** approaches: *event-based* and *asset-based*

# Threats and Vulnerabilities



| Threat category | Threat description |
|---|---|
| Physical threats | Fire<br>Water<br>Pollution, harmful radiation |
| Natural threats | Climatic phenomenon<br>Seismic phenomenon<br>Volcanic phenomenon |
| Infrastructure failures | Failure of a supply system<br>Failure of cooling or ventilation system<br>Loss of power supply |
| Technical failures | Failure of device or system<br>Saturation of the information system<br>Violation of information system maintainability |
| Human actions | Terror attack, sabotage<br>Social engineering<br>Interception of radiation of a device<br>Remote spying<br>Eavesdropping<br>Theft of media or documents |
| Compromise of functions or services | Error in use<br>Abuse of rights or permissions<br>Forging of rights or permissions<br>Denial of actions |
| Organizational threats | Lack of staff<br>Lack of resources<br>Failure of service providers<br>Violation of laws or regulations |



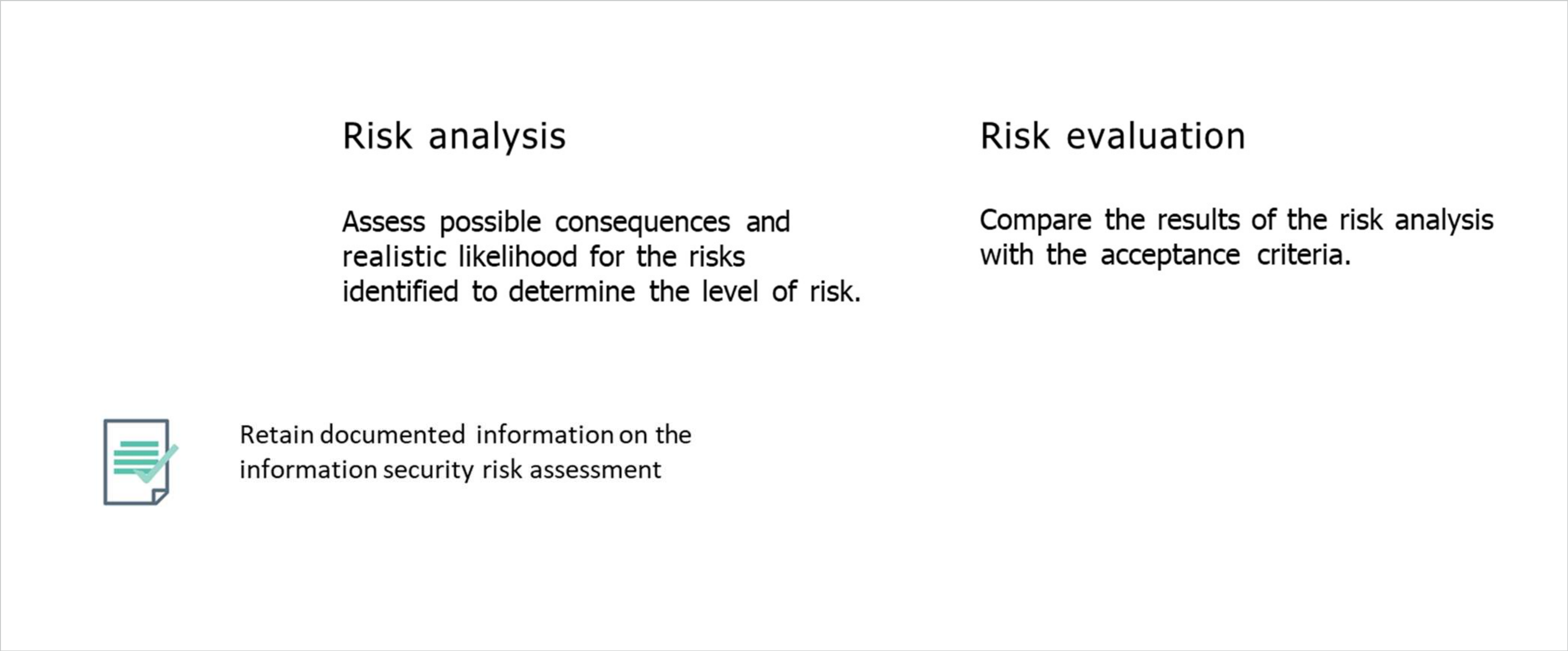
| Vulnerability category | Vulnerability description |
|---|---|
| Hardware | Insufficient maintenance/ faulty installation of storage media<br>Insufficient periodic replacement schemes for equipment<br>Susceptibility to humidity, dust, soiling |
| Software | No or insufficient software testing<br>Well-known flaws in the software<br>No "logout" when leaving the workstation<br>Disposal or reuse of storage media without proper erasure |
| Network | Insufficient mechanisms for the proof of sending or receiving a message<br>Unprotected communication lines<br>Unprotected sensitive traffic |
| Personnel | Absence of personnel<br>Inadequate recruitment procedures<br>Insufficient security training |
| Site | Inadequate or careless use of physical access control to buildings and rooms<br>Location in an area susceptible to flood<br>Unstable power grid<br>Insufficient physical protection of the building, doors and windows |
| Organization | Formal procedure for user registration and de-registration not developed, or its implementation ineffective<br>Formal process for access rights review not developed, or its implementation is ineffective<br>Insufficient security provisions in contracts with customers and third parties |

Source: ISO/IEC 27005:2022

# Risk owners

- **Identify risk owners** (persons or entities with the accountability and authority to manage risks).

# Risk analysis and evaluation



## Risk analysis

Assess possible consequences and realistic likelihood for the risks identified to determine the level of risk.

## Risk evaluation

Compare the results of the risk analysis with the acceptance criteria.

Retain documented information on the information security risk assessment

# Information security risk treatment

**Risk treatment process:**

- select appropriate treatment options;
- determine the appropriate controls;
- formulate a risk treatment plan;
- obtain the approval of risk owners for the plan, and acceptance for residual risks.

**Risk treatment options:**

Avoidance

Modification

Sharing

Retention

# Information security controls

- Preventive
- Detective
- Corrective

# Statement of applicability (SoA)

- The statement of applicability contains:

-necessary controls (including justification for inclusion and implementation status);

-justification for the controls excluded.

| Information security control | Included or not | Justification for inclusion | Implementation status | Justification for exclusion |
|---|---|---|---|---|
| **5.1 Policies for information security** | Included | The control is needed to treat the information security risks identified | Implemented | // |
| **5.2 Information security roles, responsibilities and authorities** | Included | The control is needed to treat the information security risks identified | Implemented | // |
| **5.3 Segregation of duties** | Included | The control is needed to treat the information security risks identified | Partially implemented | // |
| … | | | | |
| **8.30 Outsourced development** | Not included | // | // | All development is done in house. No outsourcing of system development. |

# Risk treatment plan

- For each information security risk:
- treatment option(s);
- actions to treat the risk;
- status of implementation;
- responsibilities, resources, timeframes

# Information security risk treatment

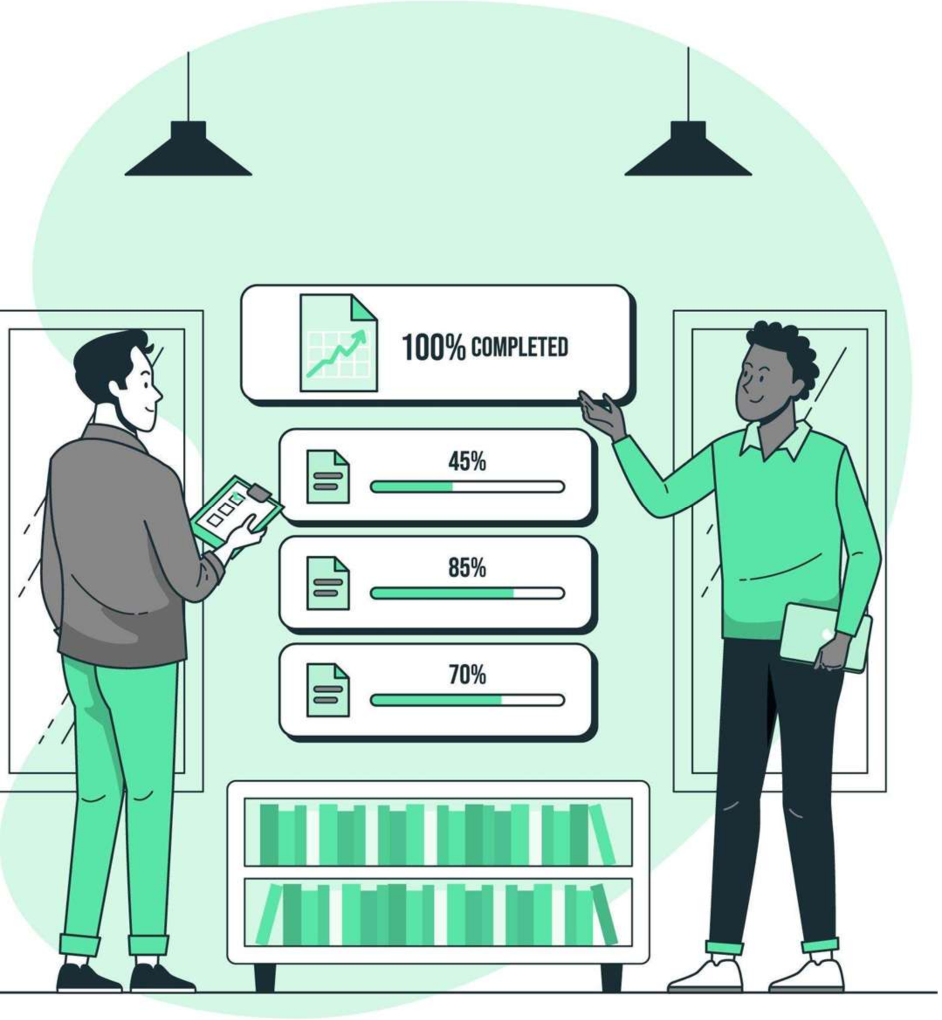
- Residual risk - the **risk that remains** after treatment (accepted by the risk owner).

Retain documented information about the risk treatment process.

# 6.2. Information security objectives

- Establish information security objectives at relevant functions and levels.

- Consistent with the policy.
- Measurable (if practicable).
- Take into consideration applicable requirements.
- Monitored, communicated and updated (as appropriate).



# Information security objectives

- Plan for the achievement of information security objectives.
- What will be done?
- What resources are necessary?
- Who will be responsible?
- When each objective will be completed? How the results will be evaluated?

Retain documented information on the information security objectives.

# 6.3. Planning of changes

- Changes to the ISMS shall be carried out in a **planned manner**, to avoid unwanted consequences.

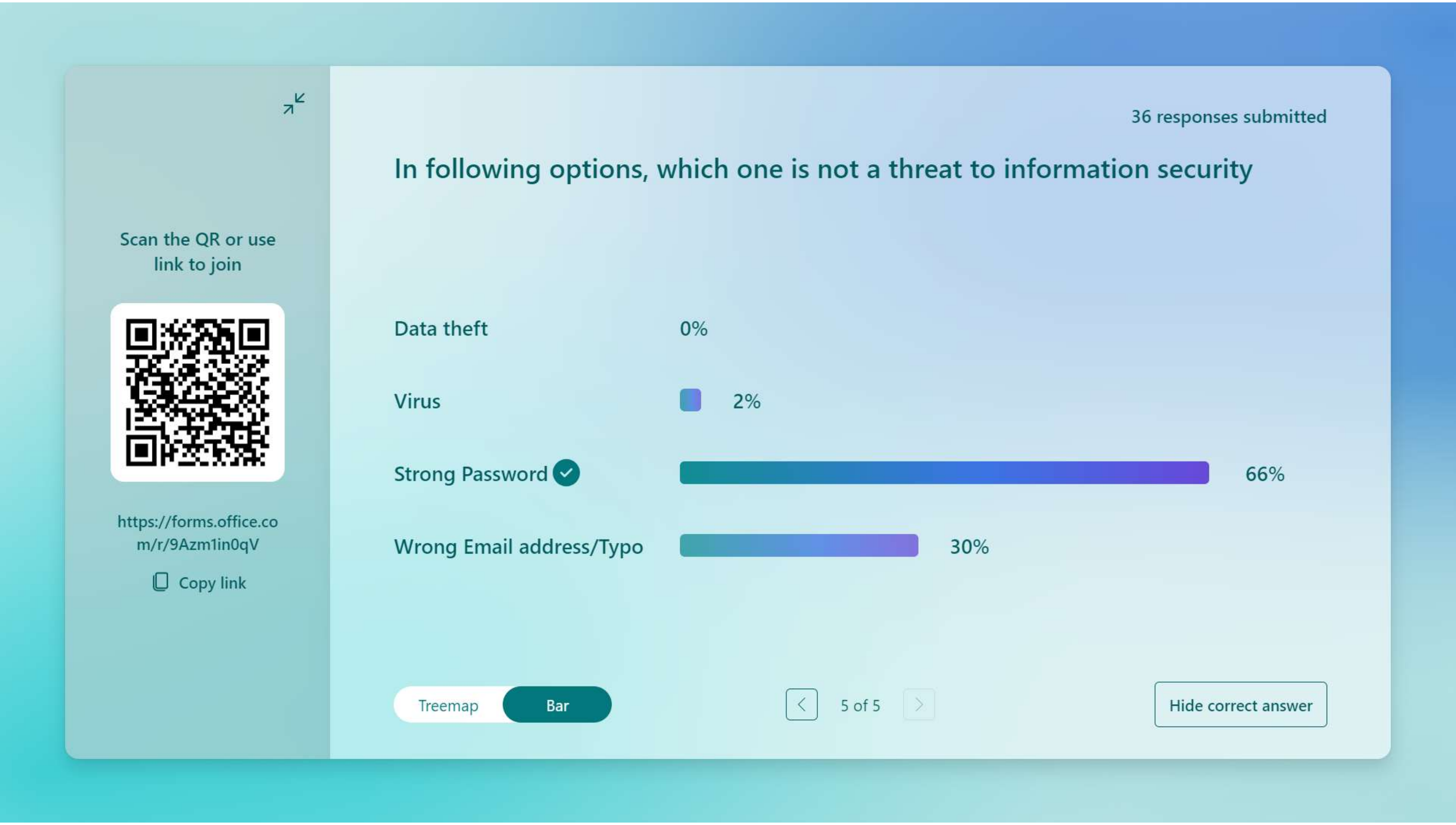
# Recapitulation (Planning)

Planning involves identifying and assessing risks to information security by evaluating potential threats and vulnerabilities.

Risks are addressed through treatment options like avoidance, modification, sharing, or retention, supported by a risk treatment plan.

The Statement of Applicability (SoA) justifies control inclusion/exclusion and tracks implementation. Measurable and consistent security objectives are set, monitored, and updated.

To ensure that planned changes are systematic and aligned with ISMS goals.


Scan the QR or use link to join
https://forms.office.com/r/9Azm1in0qV
Copy link
Treemap
Bar
5 of 5
Hide correct answer

36 responses submitted

In following options, which one is not a threat to information security

| | |
|---|---|
| Data theft | 0% |
| Virus | 2% |
| Strong Password ✓ | 66% |
| Wrong Email address/Typo | 30% |

# Guest Speaker – Mr. Shridhar Dangety (Stallion Professional Services LLC)

- Hello, My name is Shridhar Dangety, Founder of Stallion Professional Services LLC. With over 25 years of industry experience, I've had the privilege of successfully leading teams and working independently across multinational corporations and three startups. My expertise lies in setting up operational processes from the ground up, as well as reviewing and refining compliance documentation to ensure seamless functionality.
- Stallion Professional Services LLC is a Dallas, Texas based IT staff Augmentation company catering to the needs of IT start up companies in the US. We provide tailored staffing solutions for IT startups, connecting you with top-tier tech talent to drive innovation and growth. From developers to project managers, our experts match your unique needs with the right skills. Our flexible approach ensures quick scaling and seamless team integration. Let us help you build the future, one hire at a time.

# Benefits of Implementing ISO 27001 in Organization

### Enhanced Information Security

- Protects sensitive client data, proprietary business information, and intellectual property.
- Reduces the risk of breaches, data loss, and cyberattacks through robust security measures.

### Compliance with Regulatory Requirements

- Demonstrates adherence to global regulatory standards, improving compliance with data protection laws like GDPR, HIPAA, and others.
- Facilitates compliance in industries served by organization, such as finance, healthcare, and telecommunications.

### Employee Awareness and Responsibility

- Promotes a culture of security awareness among employees through training and documented procedures.
- Clarifies roles and responsibilities in safeguarding information assets.

### Business Continuity

- Supports the development of a robust business continuity plan (BCP) by identifying critical assets and ensuring their protection.
- Minimizes downtime and ensures resilience during incidents or disasters.

### Improved Risk Management

- Provides a structured framework to identify, assess, and mitigate risks related to information security.
- Ensures continuity of operations by proactively addressing vulnerabilities and preparing for potential threats.

### Increased Client Trust

- Builds confidence among clients by ensuring that their data is managed securely.
- Acts as a competitive differentiator when bidding for projects or contracts, especially in highly regulated industries.

# Career benefits of ISO 27001 Internal Auditor credentials for Professionals

**Enhanced Career Prospects:** Boost employability with a globally recognized certification, unlocking roles like Information Security Manager, IT Auditor, and Compliance Specialist.

**Advanced Skill Development:** Master ISO 27001:2022 standards and ISMS auditing practices, enhancing your ability to assess and improve security frameworks.

**Networking Opportunities:** Build connections with cybersecurity experts, industry professionals, and ISO practitioners through events, forums, and workshops.

**Improved Job Performance:** Apply effective auditing techniques to identify vulnerabilities, strengthen information security practices, and ensure organizational compliance.

**Increased Value to Employers:** Support your organization in achieving ISO 27001 certification, bolstering security measures and regulatory adherence.

**Personal Achievement:** Attain a significant professional milestone, gaining confidence in conducting impactful ISMS audits.

**Commitment to Learning:** Stay updated with emerging trends, cybersecurity threats, and industry best practices for ongoing relevance in the field.

**Organizational Impact:** Drive improvements in risk management, data protection, and compliance, contributing to the organization’s strategic goals.

# Clause 7: Support

| S. NO. | CLAUSE NO. | CLAUSE NAME |
|---|---|---|
| 1. | 7.1 | Resources |
| 2. | 7.2 | Competence |
| 3. | 7.3 | Awareness |
| 4. | 7.4 | Communication |
| 5. | 7.5 | Documented Information |

# 7.1. Resources

- Determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS.

QUALITY ASIA

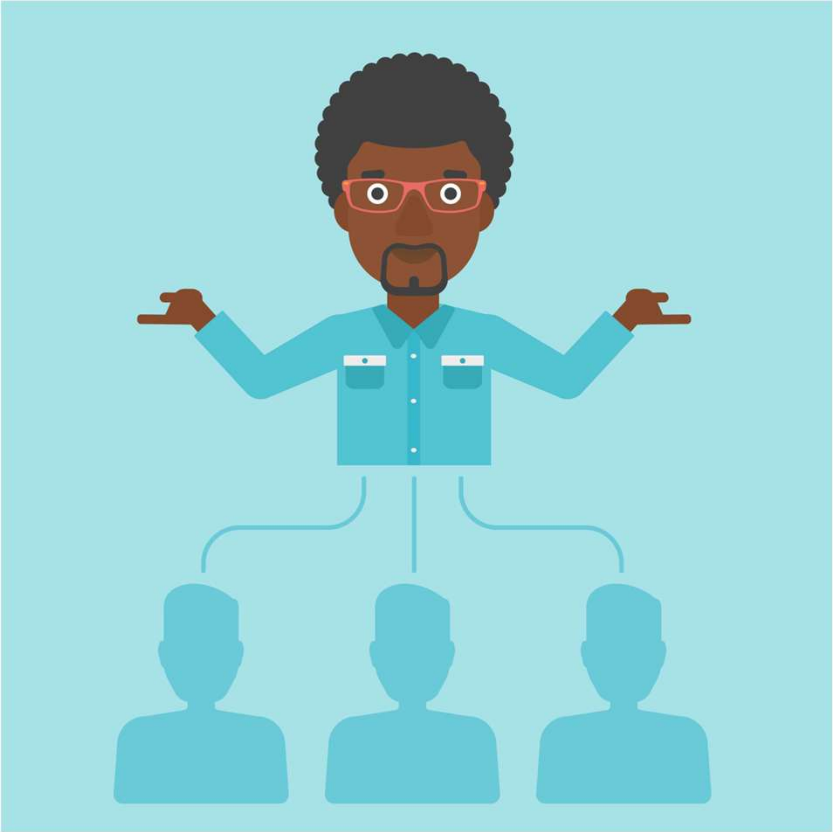
# 7.2. Competence

- Define **requirements.**
- Ensure **competency** (education, training, experience).
- **Act** to improve or maintain competence. Evaluate the **effectiveness** of actions.

Retain documented information (evidence of competence)

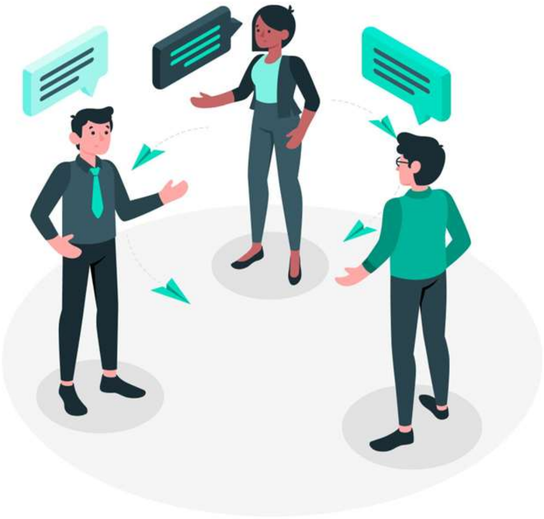
# 7.3. Awareness

- Personnel shall be **aware** of:
  - the information security policy;
  - their contribution to the ISMS and the benefits of improved security performance;
  - the implications of not conforming to requirements.



# 7.4. Communication

- Determine the need for internal and external communications relevant for the ISMS.



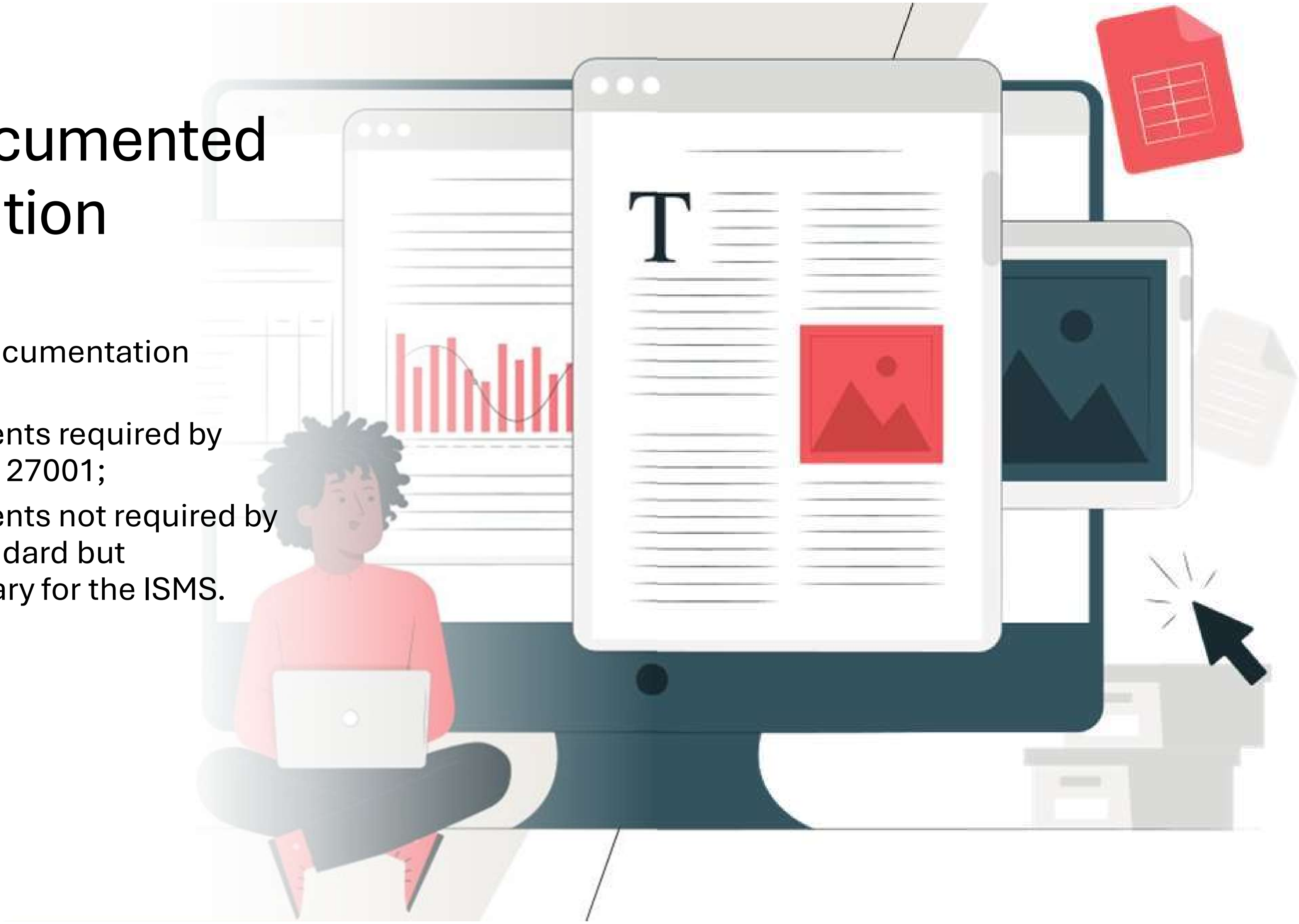
On what?

When?

With whom?

How?

# 7.5. Documented Information



- The ISMS documentation includes:
  - documents required by ISO/IEC 27001;
  - documents not required by the standard but necessary for the ISMS.

# Creating and updating isms documents

- **Identification and description**
- **Format**
- **Review and approval**

# Control of documented information

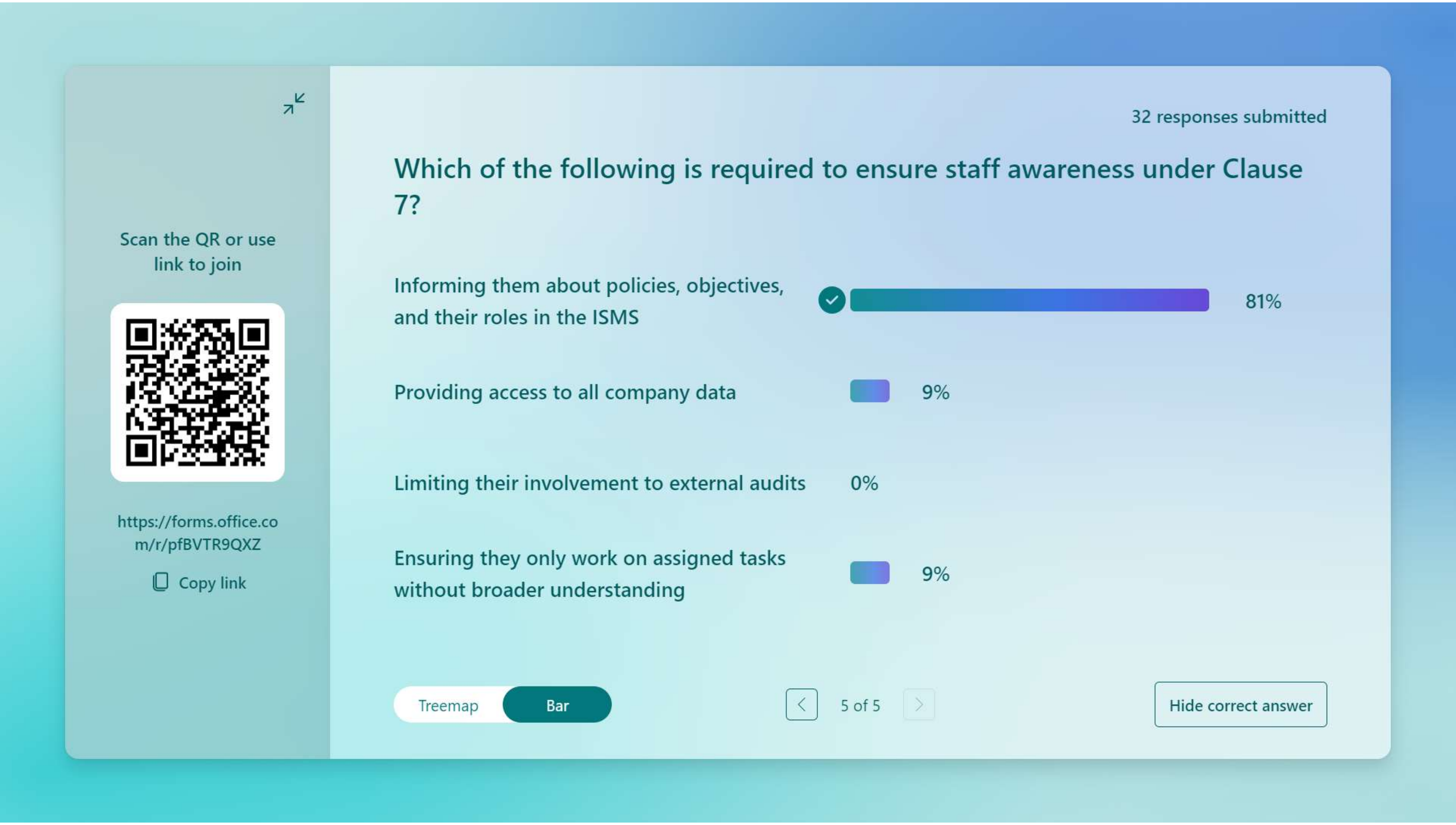
- **Documents shall be controlled** to protect them from improper use, from loss of confidentiality or integrity, and to ensure that they are available and suitable for use where and when needed.

# Control of documented information

- Distribution
- Access
- Retrieval
- Use
- Storage and preservation
- Version control
- Retention
- Secure disposition

# Recapitulation (Support)

| | |
|---|---|
| Provide | Provide adequate resources and ensure personnel are competent through education, training, or experience. |
| Maintain | Maintain necessary infrastructure and a suitable work environment to support ISMS processes. |
| Ensure | Ensure staff are aware of policies, objectives, and their roles. |
| Establish | Establish effective internal and external communication channels. |
| Create, maintain, and control | Create, maintain, and control documented information to ensure effective ISMS operations and compliance. |



Scan the QR or use link to join

https://forms.office.com/r/pfBVTR9QXZ

32 responses submitted

Which of the following is required to ensure staff awareness under Clause 7?

✓ Informing them about policies, objectives, and their roles in the ISMS 81%

Providing access to all company data 9%

Limiting their involvement to external audits 0%

Ensuring they only work on assigned tasks without broader understanding 9%

# Clause 8: Operation

| S. NO. | CLAUSE NO. | CLAUSE NAME |
|---|---|---|
| 1. | 8.1 | Operational planning and control |
| 2. | 8.2 | Information security risk assessment |
| 3. | 8.3 | Information security risk treatment |

# 8.1. Operational planning and control

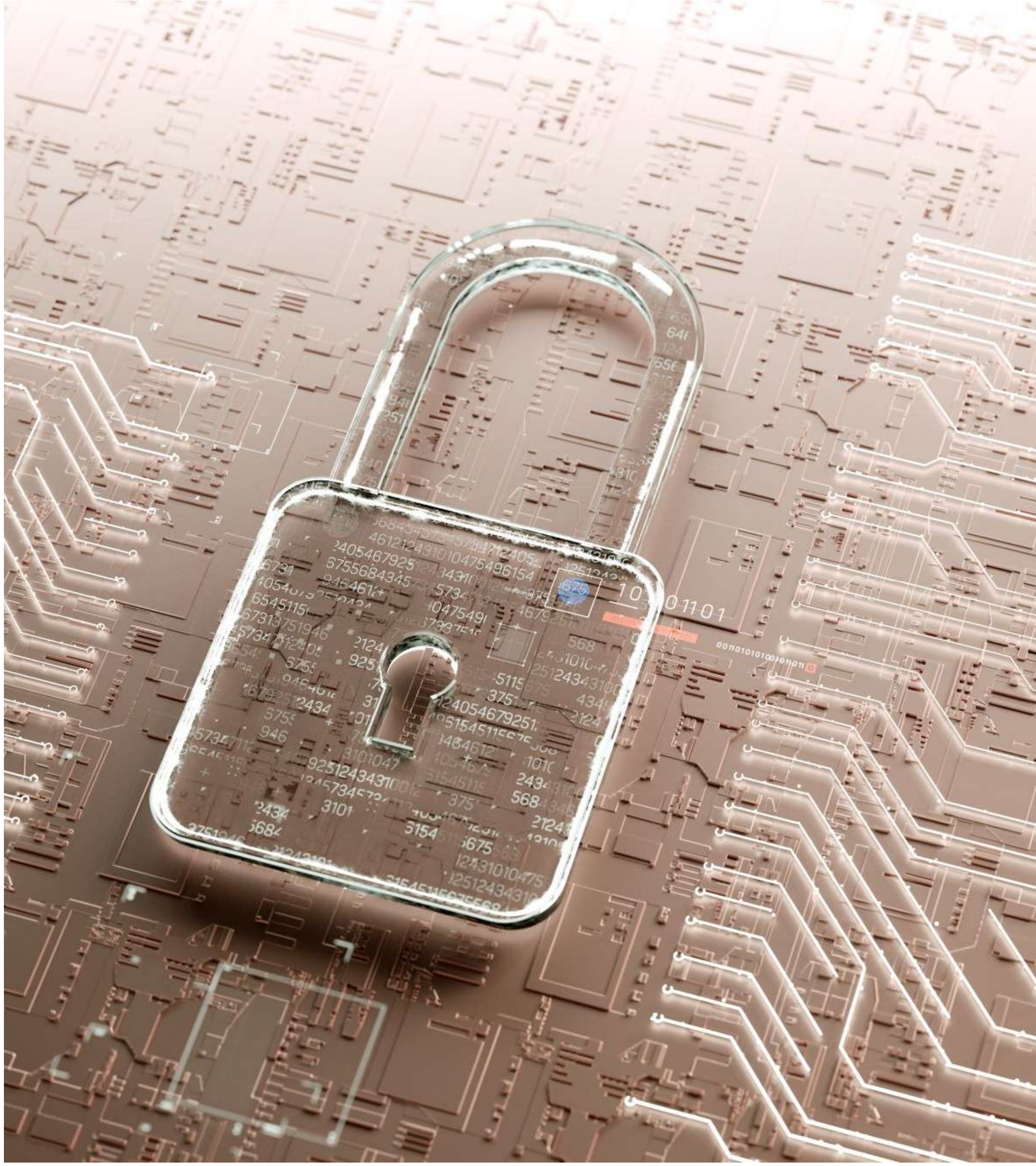
- The organization shall plan, implement and control the processes needed to meet requirements.

- Control **changes**.
- Control **externally provided processes, products or services**.

# 8.2. Information security risk assessment

- **Conduct information security risk assessments** at planned intervals (possibly once per year), and in case of significant changes.

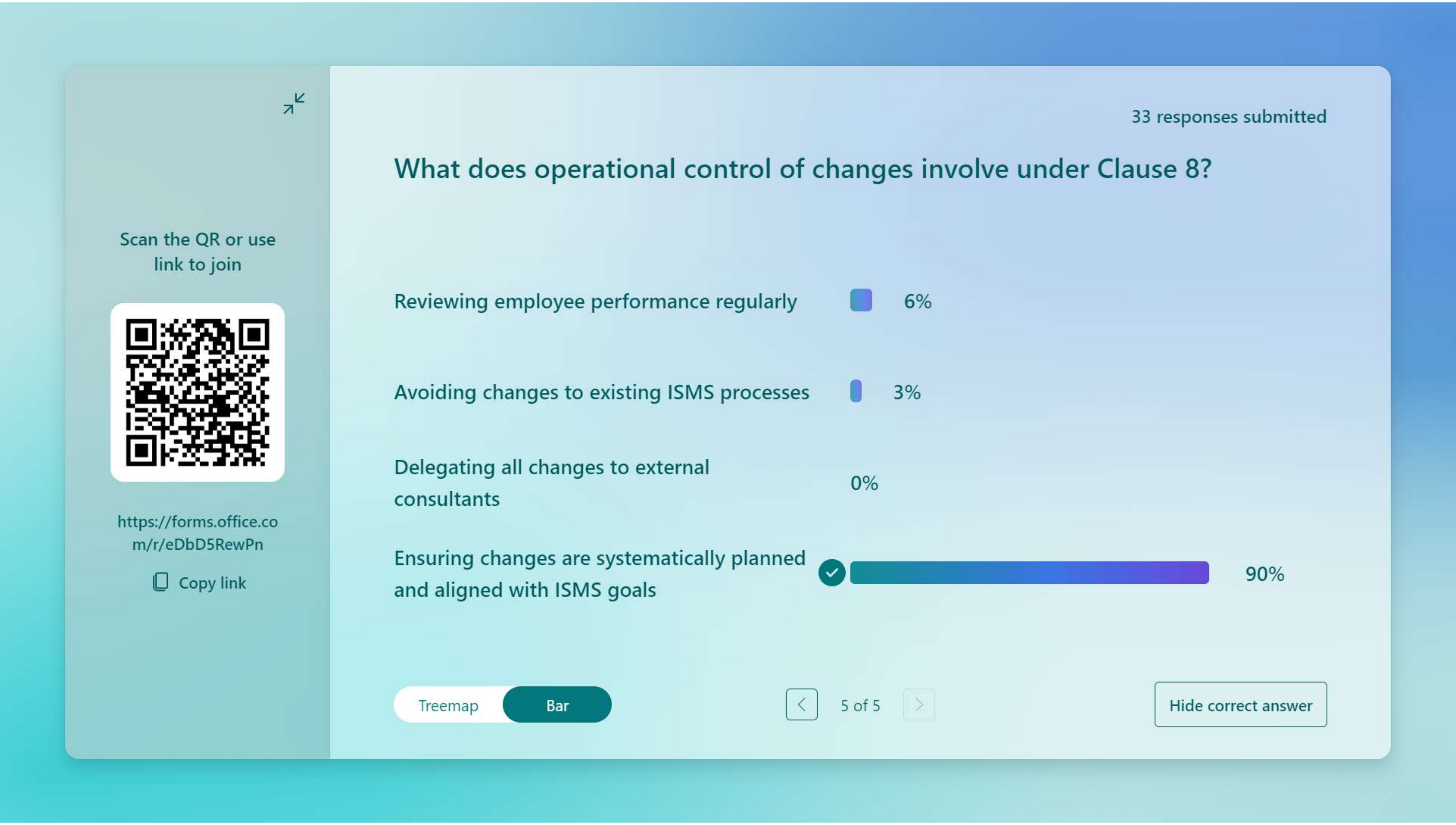
# 8.3. Information security risk treatment



- **Implement** the information security risk treatment plan.

# Recapitulation (Operation)

- Plan, implement, and control processes to meet ISMS requirements.
- Ensure proper control of changes and externally provided processes, products, or services.
- Conduct regular risk assessments at planned intervals or when significant changes occur to ensure the security of information assets.
- Implement the risk treatment plan effectively to address identified risks and maintain ISMS compliance.



Scan the QR or use link to join

https://forms.office.com/r/eDbD5RewPn

33 responses submitted

## What does operational control of changes involve under Clause 8?

| | |
|---|---|
| Reviewing employee performance regularly | 6% |
| Avoiding changes to existing ISMS processes | 3% |
| Delegating all changes to external consultants | 0% |
| Ensuring changes are systematically planned and aligned with ISMS goals ✓ | 90% |

# Clause 9: Performance Evaluation

| S. No. | Clause No. | Clause name |
|---|---|---|
| 1. | 9.1 | Monitoring, measurement, analysis and evaluation |
| 2. | 9.2 | Internal audit |
| 3. | 9.3 | Management review |

# 9.1. Monitoring, measurement, analysis and evaluation

- **Determine:**

- what needs to be monitored and measured;
- methods;
- when to monitor and measure;
- responsibilities;
- when the results are analyzed and evaluated.

Documented information as evidence of the results.

# 9.2. Internal audit

- Conduct internal audits of the ISMS **at planned intervals.**

- Plan, establish, implement and maintain an **internal audit programme.**

- Consider the **importance of processes** and the **results** of previous audits.

# The internal audit of ISMS

- Select **objective** auditors.
- Elaborate an **audit plan** for each audit.
- **Report** the results to the relevant management

Documented information as evidence of internal audits.

ISO 19011 – Guidelines for auditing management systems

# 9.3. Management review

- Conduct management reviews at planned intervals, to ensure that the ISMS continues to be **suitable**, **adequate** and **effective**.

# Management review – Inputs and results

**INPUTS**

Status of actions from previous reviews.

Changes to the context of the organization.

Feedback on the information security performance.

Feedback from interested parties.

Results of the risk assessment and risk treatment plan.

Opportunities for improvement.

**RESULTS**

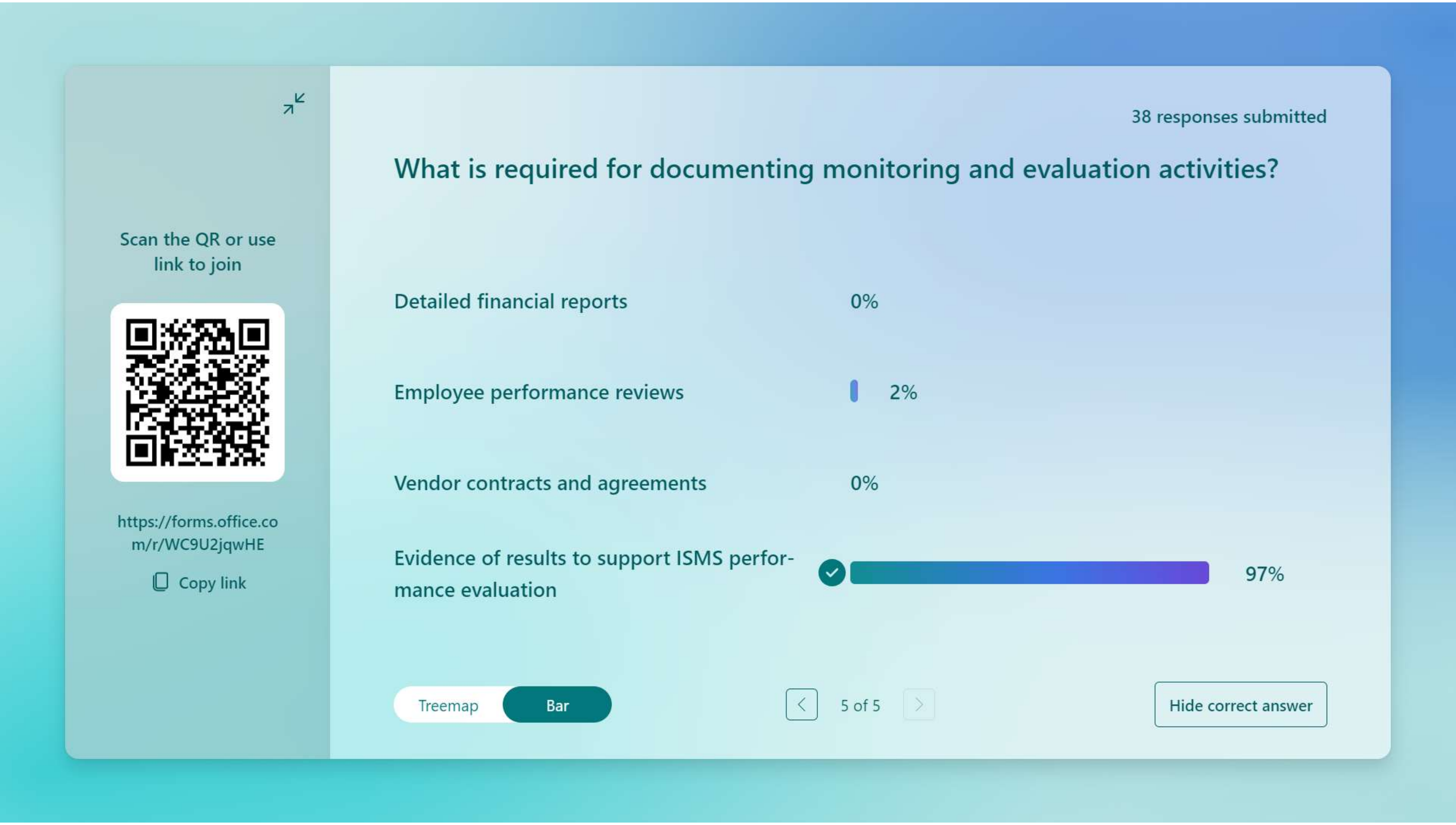
Decisions related to continual improvement.

Changes to the ISMS.

Documented information on the results of management reviews.

# Recapitulation (Performance Evaluation)

- Determine what needs to be monitored, methods, timing, responsibilities, and analysis of results.
- Maintain documented evidence of monitoring and evaluation activities.
- Conduct internal audits at planned intervals to assess ISMS performance.
- Conduct management reviews at planned intervals to ensure the ISMS remains suitable, adequate, and effective.



Scan the QR or use link to join

https://forms.office.com/r/WC9U2jqwHE

Copy link

38 responses submitted

## What is required for documenting monitoring and evaluation activities?

Detailed financial reports 0%

Employee performance reviews 2%

Vendor contracts and agreements 0%

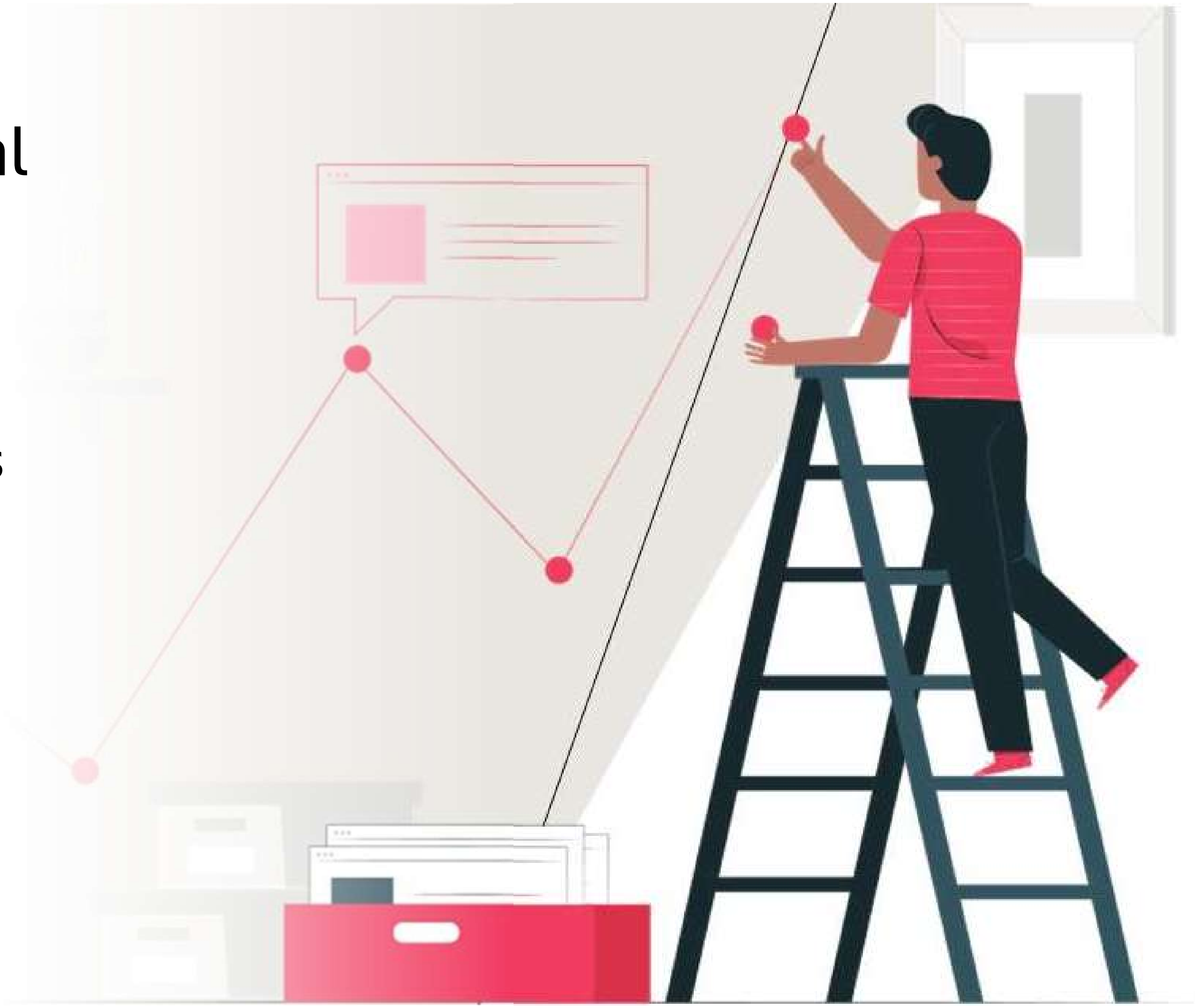
✓ Evidence of results to support ISMS performance evaluation 97%

# Clause 10: Improvement

| S. No. | Clause No. | Clause name |
|---|---|---|
| 1. | 10.1 | Continual Improvement |
| 2. | 10.2 | Nonconformity and corrective actions |

# 10.1. Continual improvement

- **Improve continually** the suitability, adequacy and effectiveness of the ISMS



# Nonconformity and corrective action

- **Nonconformity –** non-fulfilment of a requirement.

QUALITY ASIA

# Managing nonconformities

**React** Correct and control the situation, deal with the consequences.

**Investigate** Evaluate the need for corrective action(s).

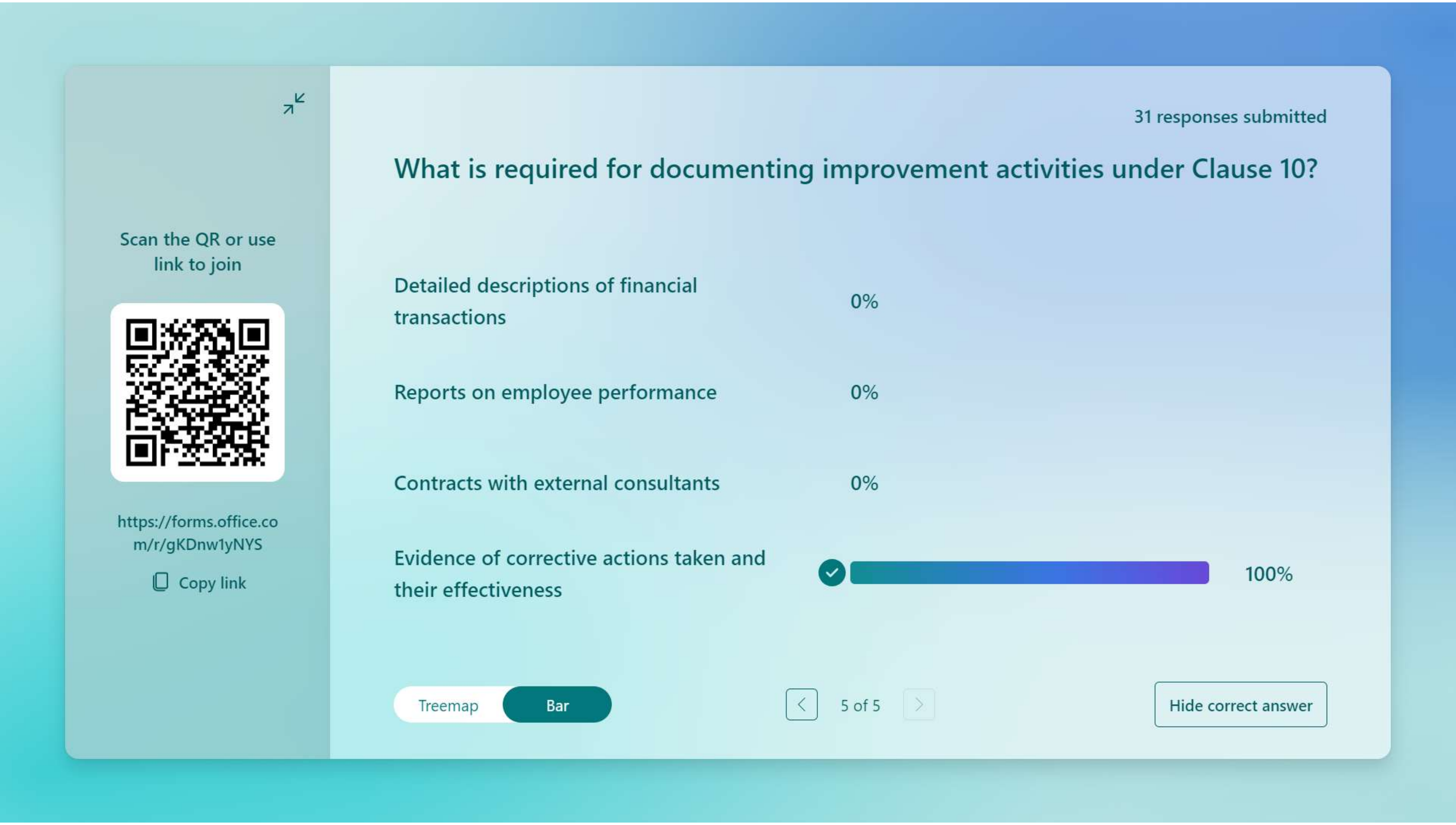
**Identify cause** Propose corrective action(s).

**Evaluate** Evaluate the effectiveness of corrective action(s).

Documented information on
nonconformities and corrective actions

# Recapitulation (Improvement)

- Continuously improve the suitability, adequacy, and effectiveness of the ISMS to ensure it aligns with organizational goals and addresses emerging risks.
- Identify, correct, and prevent recurrence of nonconformities.



31 responses submitted

What is required for documenting improvement activities under Clause 10?

| | |
|---|---|
| Detailed descriptions of financial transactions | 0% |
| Reports on employee performance | 0% |
| Contracts with external consultants | 0% |
| ✓ Evidence of corrective actions taken and their effectiveness | 100% |

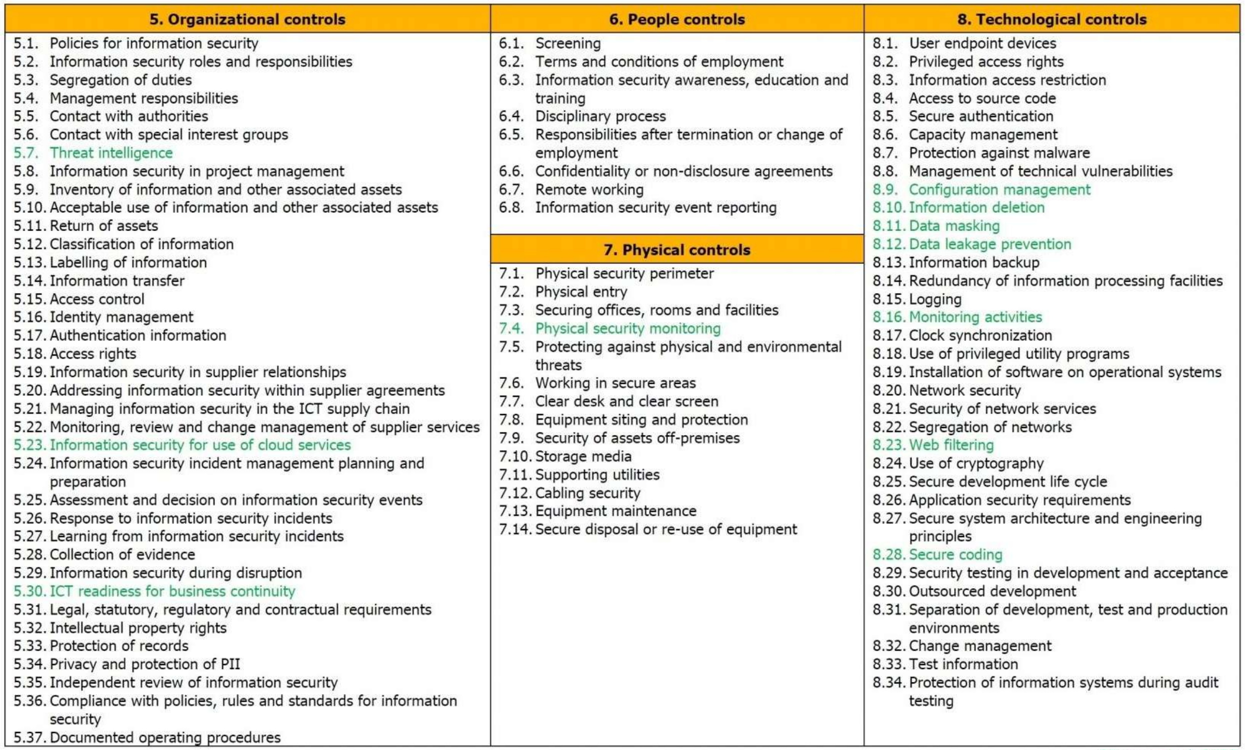
Scan the QR or use link to join
https://forms.office.com/r/gKDnw1yNYS
Copy link
Treemap
Bar
5 of 5
Hide correct answer

# Information security controls

- Annex A of ISO/IEC 27001:2022
- 93 information security controls in 4 themes (or categories):

- Organizational controls
- People controls
- Physical controls
- Technological controls

# IS controls – Annex A



| 5. Organizational controls | 6. People controls | 8. Technological controls |
|---|---|---|
| 5.1. Policies for information security | 6.1. Screening | 8.1. User endpoint devices |
| 5.2. Information security roles and responsibilities | 6.2. Terms and conditions of employment | 8.2. Privileged access rights |
| 5.3. Segregation of duties | 6.3. Information security awareness, education and training | 8.3. Information access restriction |
| 5.4. Management responsibilities | 6.4. Disciplinary process | 8.4. Access to source code |
| 5.5. Contact with authorities | 6.5. Responsibilities after termination or change of employment | 8.5. Secure authentication |
| 5.6. Contact with special interest groups | 6.6. Confidentiality or non-disclosure agreements | 8.6. Capacity management |
| 5.7. Threat intelligence | 6.7. Remote working | 8.7. Protection against malware |
| 5.8. Information security in project management | 6.8. Information security event reporting | 8.8. Management of technical vulnerabilities |
| 5.9. Inventory of information and other associated assets | | 8.9. Configuration management |
| 5.10. Acceptable use of information and other associated assets | **7. Physical controls** | 8.10. Information deletion |
| 5.11. Return of assets | 7.1. Physical security perimeter | 8.11. Data masking |
| 5.12. Classification of information | 7.2. Physical entry | 8.12. Data leakage prevention |
| 5.13. Labelling of information | 7.3. Securing offices, rooms and facilities | 8.13. Information backup |
| 5.14. Information transfer | 7.4. Physical security monitoring | 8.14. Redundancy of information processing facilities |
| 5.15. Access control | 7.5. Protecting against physical and environmental threats | 8.15. Logging |
| 5.16. Identity management | 7.6. Working in secure areas | 8.16. Monitoring activities |
| 5.17. Authentication information | 7.7. Clear desk and clear screen | 8.17. Clock synchronization |
| 5.18. Access rights | 7.8. Equipment siting and protection | 8.18. Use of privileged utility programs |
| 5.19. Information security in supplier relationships | 7.9. Security of assets off-premises | 8.19. Installation of software on operational systems |
| 5.20. Addressing information security within supplier agreements | 7.10. Storage media | 8.20. Network security |
| 5.21. Managing information security in the ICT supply chain | 7.11. Supporting utilities | 8.21. Security of network services |
| 5.22. Monitoring, review and change management of supplier services | 7.12. Cabling security | 8.22. Segregation of networks |
| 5.23. Information security for use of cloud services | 7.13. Equipment maintenance | 8.23. Web filtering |
| 5.24. Information security incident management planning and preparation | 7.14. Secure disposal or re-use of equipment | 8.24. Use of cryptography |
| 5.25. Assessment and decision on information security events | | 8.25. Secure development life cycle |
| 5.26. Response to information security incidents | | 8.26. Application security requirements |
| 5.27. Learning from information security incidents | | 8.27. Secure system architecture and engineering principles |
| 5.28. Collection of evidence | | 8.28. Secure coding |
| 5.29. Information security during disruption | | 8.29. Security testing in development and acceptance |
| 5.30. ICT readiness for business continuity | | 8.30. Outsourced development |
| 5.31. Legal, statutory, regulatory and contractual requirements | | 8.31. Separation of development, test and production environments |
| 5.32. Intellectual property rights | | 8.32. Change management |
| 5.33. Protection of records | | 8.33. Test information |
| 5.34. Privacy and protection of PII | | 8.34. Protection of information systems during audit testing |
| 5.35. Independent review of information security | | |
| 5.36. Compliance with policies, rules and standards for information security | | |
| 5.37. Documented operating procedures | | |

*New control, 2022

# Policies for information security

| Organizational control | 5.1 | Policies for information security |
|---|---|---|
| Define, approve by management, publish, communicate and acknowledge by relevant personnel and interested parties an information security policy and topic-specific policies. The policies must be reviewed at planned intervals and in case of significant changes. | | |

- A high-level information security policy supported by topic- specific policies on different subjects (e.g., incident management, access control, backup, asset management, etc.)

# Information security roles and responsibilities

| Organizational control | 5.2 | Information security roles and responsibilities |
|---|---|---|
| Define and allocate roles and responsibilities for information security, according to the needs of the organization. | | |

- Communicate roles and responsibilities for information security and ensure they are understood

# Segregation of duties

| Organizational control | 5.3 | Segregation of duties |
|---|---|---|
| Segregate conflicting duties and areas of responsibility. | | |

- Avoid the situation where a single person has full control.
- Consider key transactions, relationships or activities.

# Management responsibilities

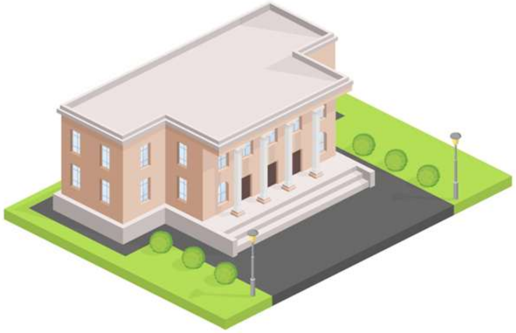
| Organizational control | 5.4 | Management responsibilities |
|---|---|---|
| All personnel shall be required by management to apply information security according to the policies and procedures of the organization. | | |

- Top management plays a key role for information security.

# Contact with authorities

| Organizational control | 5.5 | Contact with authorities |
|---|---|---|
| Establish and maintain contact with relevant authorities. | | |

- To prepare for upcoming legal changes, to improve legal and regulatory compliance and to be of use in case of security incidents.



# Contact with special interest groups

| Organizational control | 5.6 | Contact with special interest groups |
|---|---|---|
| Establish and maintain contacts with special interest groups, security forums or professional associations. | | |

- To stay informed about threats or security best practices and to get support when dealing with a security incident.

# Threat intelligence (New Control)

| Organizational control | 5.7 | Threat intelligence |
|---|---|---|
| Collect and analyze information relating to information security threats to produce threat intelligence. | | |

- Produce threat intelligence or rely on external parties (consultants, governmental agencies, etc.). Share threat intelligence with others.

# Information security in project management

| Organizational control | 5.8 | Information security in project management |
|---|---|---|
| Integrate information security into project management. | | |

- Treat information security as an integral part of any kind of project undertaken by the organization.

# Inventory of information and other associated assets

| Organizational control | 5.9 | Inventory of information and other associated assets |
|---|---|---|
| Develop and maintain an inventory of information and other associated assets, including owners. | | |

- Assets shall be included in one or several inventories and owned.

# Acceptable use of information and other associated assets

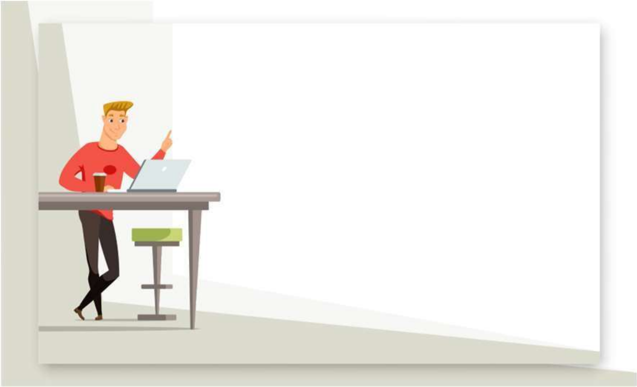
| Organizational control | 5.10 | Acceptable use of information and other associated assets |
|---|---|---|
| Identify, document and implement rules for the acceptable use and procedures for handling information and other associated assets. | | |

- Consider a topic-specific policy on the acceptable use of information and other associated assets.

# Return of assets

| Organizational control | 5.11 | Return of assets |
|---|---|---|
| Ensure personnel and other interested parties return the assets in their possession and belonging to the organization, when their employment, contract or agreement is terminated or changed. | | |

- Prevent confidential information being left on devices and restrict access to data for those ending or changing their relationship with the organization.



# Classification of information

| Organizational control | 5.12 | Classification of information |
|---|---|---|
| Classify information in accordance with the information security needs of the organization, based on confidentiality, integrity, availability and the relevant requirements of interested parties. | | |

- Consider a topic-specific policy on information classification.
- Adopt a classification scheme (e.g., Confidential, Restricted, Internal use, Public)

# Labelling of information

| Organizational control | 5.13 | Labelling of information |
|---|---|---|
| Develop and implement an appropriate set of procedures for information labelling, in accordance with the classification scheme adopted. | | |

- Labelling ensures that persons in the organization are aware of the classification of the information they use.
- For information on any support.

# Information transfer

| Organizational control | 5.14 | Information transfer |
|---|---|---|
| Ensure that rules, procedures or agreements are in place for the transfer of information within the organization and between the organization and other parties, for all types of transfer facilities. | | |

- Apply controls in line with the classification of the information transferred.
- Consider the transfer of information on electronic and paper support, as well as the verbal transfer of information.

designed by freepik

# Access control

| Organizational control | 5.15 | Access control |
|---|---|---|
| Rules to control the physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. | | |

- Consider a topic-specific policy on access control to define principles, generic provisions, rules or responsibilities.

- MAC – Mandatory Access Control. DAC – Discretionary Access Control
- RBAC – Role-Based Access Control. ABAC – Attribute-Based Access Control

# Identity management

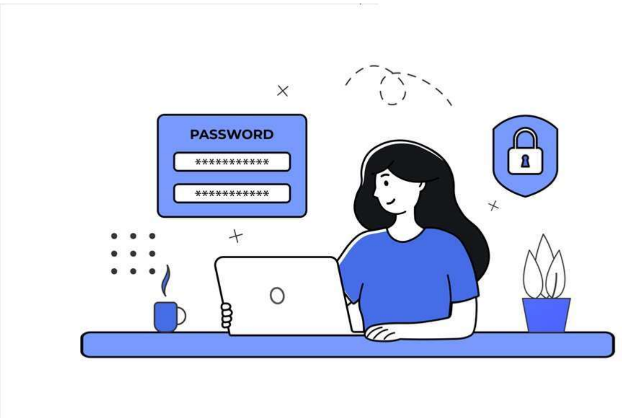
| Organizational control | 5.16 | Identity management |
|---|---|---|
| The full life cycle of identities shall be managed. | | |

- Identity management should allow for the unique identification of persons and systems accessing information assets, and it should enable the appropriate assignment of access rights.

# Authentication information

| Organizational control | 5.17 | Authentication information |
|---|---|---|
| Control the allocation and management of authentication information with a management process, including advising personnel on appropriate handling of authentication information. | | |

- Consider the allocation of authentication information, the responsibilities of users and a password management system.



# Access rights

| Organizational control | 5.18 | Access rights |
|---|---|---|
| Provide, review, modify and remove access rights to information and other associated assets in accordance with the topic-specific policy and rules on access control. | | |

- Ensure that only authorized users have access to information and associated assets.
- Separate the approval of access rights from their implementation.
- Review access rights periodically and make the necessary adjustments.

# Information security in supplier relationships

| Organizational control | 5.19 | Information security in supplier relationships |
|---|---|---|
| Define and implement processes and procedures to manage the information security risks that are associated with the use of products and services obtained from suppliers. | | |

- Consider a topic-specific policy to describe principles, requirements and basic security controls that suppliers are expected to apply.

# Addressing information security in supplier agreements

| Organizational control | 5.20 | Addressing information security within supplier agreements |
|---|---|---|
| Establish and agree with each supplier relevant information security requirements based on the type of supplier relationship. | | |

- Include information security requirements in the contracts or agreements.

# Managing information security in the information and communication technology (ICT) supply chain

| Organizational control | 5.21 | Managing information security in the information and communication technology (ICT) supply chain |
|---|---|---|
| Define and implement processes and procedures to manage the information security risks associated with the ICT products and services supply chain. | | |

- Require suppliers to propagate appropriate security practices throughout the supply chain.
- Work with suppliers to solve issues and share information about products and services.

# Monitoring, review and change management of supplier services

| Organizational control | 5.22 | Monitoring, review and change management of supplier services |
|---|---|---|
| Regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. | | |

- Ensure that services maintain an agreed level and changes to services do not come with a negative impact on information security.

# Information security for use of cloud services (New Control)

| Organizational control | 5.23 | Information security for use of cloud services |
|---|---|---|
| Establish processes for the acquisition, use, management and exit from cloud services in accordance with the information security requirements of the organization. | | |

- Consider a **topic-specific policy** for principles and generic requirements on the use of cloud services.
- As necessary, do a **risk assessment** and implement controls to address the security risks in relation to the use of cloud services.

# Information security incident management planning and preparation

| Organizational control | 5.24 | Information security incident management planning and preparation |
|---|---|---|
| Plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. | | |

- Event ≠ Incident
- Method for **reporting** information security events.
- Process for **managing** information security incidents.

# Assessment and decision on information security events

| Organizational control | 5.25 | Assessment and decision on information security events |
|---|---|---|
| Assess information security events and decide if they will be categorized as incidents. | | |

- **Triage** of events to determine which events represent information security incidents.

# Response to information security incidents

| Organizational control | 5.26 | Response to information security incidents |
|---|---|---|
| Respond to information security incidents in accordance with documented procedures. | | |

- Limit the impact.
- Coordinate with other parties.
- Escalate, if necessary.
- Collect evidence.
- Document the incident.
- Identify weaknesses and vulnerabilities.

# Learning form information security incidents

| Organizational control | 5.27 | Learning from information security incidents |
|---|---|---|
| Use the knowledge gained from information security incidents to strengthen and improve the information security controls. | | |

- The lessons learned while dealing with security incidents can prove useful for **preventing** future incidents and for **improving the response** of the organization.

# Collection of evidence

| Organizational control | 5.28 | Collection of evidence |
|---|---|---|
| Establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. | | |

- Collected evidence may help the organization in case of a contractual dispute or investigation.
- Consider the competence of those involved in the collection and protection of evidence.

# Information security during disruption

| Organizational control | 5.29 | Information security during disruption |
|---|---|---|
| Plan how to maintain information security at an appropriate level during disruption. | | |

- Prepare to maintain an adequate level of information security in case of a major incident.

# ICT readiness for business continuity (New Control)

| Organizational control | 5.30 | ICT readiness for business continuity |
|---|---|---|
| Plan, implement, maintain and test ICT readiness based on the business continuity objectives and ICT continuity requirements. | | |

- Key activities rely on ICT (Information and Communication Technology).
- Understand ICT readiness requirements and address the risks of prioritized activities being disrupted.

# Legal, statutory, regulatory and contractual requirements

| Organizational control | 5.31 | Legal, statutory, regulatory and contractual requirements |
|---|---|---|
| Identify, document and keep up to date the legal, statutory, regulatory and contractual requirements relevant for information security along with the organization’s approach to meet them. | | |

- **Assign responsibilities** for identifying and keeping up to date legal, statutory, regulatory and contractual requirements that refer to information security.

# Intellectual property rights

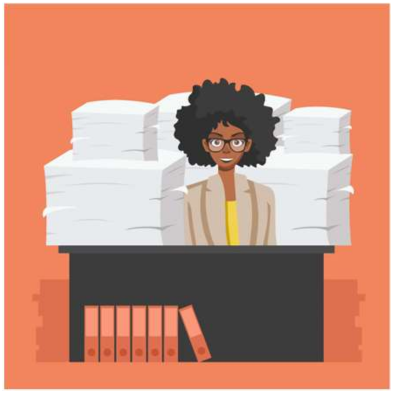
| Organizational control | 5.32 | Intellectual property rights |
|---|---|---|
| Implement appropriate procedures to protect intellectual property rights. | | |

- Consider a **topic-specific policy** to outline the commitment for the protection of intellectual property rights.

# Protection of records

| Organizational control | 5.33 | Protection of records |
|---|---|---|
| Protect records from loss, destruction, falsification, unauthorized access and unauthorized release. | | |

- Establish a **retention schedule** for the records generated.
- Implement rules for the **storage, handling or disposal** of records.



# Privacy and protection of personal identifiable information (PII)

| Organizational control | 5.34 | Privacy and protection of personally identifiable information (PII) |
|---|---|---|
| Identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws, regulations and contractual requirements. | | |

- **Identify** the applicable legislation, regulations and contractual requirements and **ensure compliance.**

# Independent review of information security

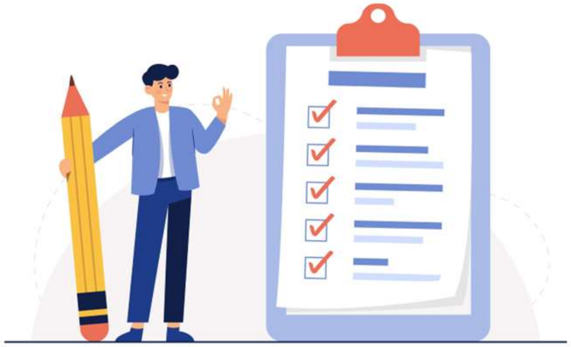
| Organizational control | 5.35 | Independent review of information security |
|---|---|---|
| Review independently at planned intervals and whenever significant changes occur, the approach to managing information security and its implementation, including people, processes and technology. | | |

- The reviews should be conducted by **competent** persons who are **independent** from the activities reviewed.

# Compliance with policies, rules and standards of information security

| Organizational control | 5.36 | Compliance with policies, rules and standards for information security |
|---|---|---|
| Review regularly compliance with the organization's information security policy, topic-specific policies, rules and standards. | | |

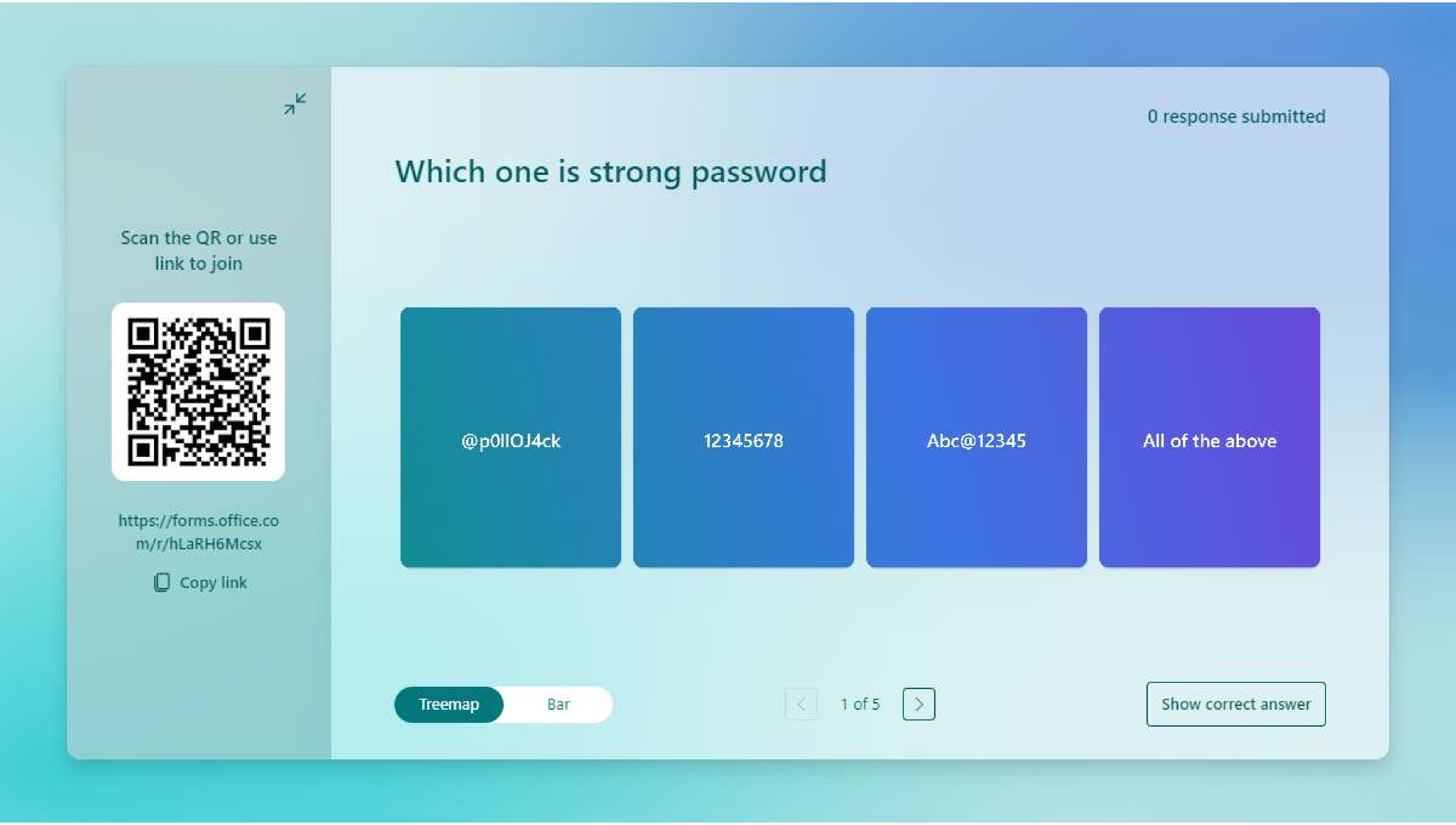
- The reviews should be conducted by managers, product, service or information owners. Consider inspections, observation or the use of automated tools.



# Documented operating procedures

| Organizational control | 5.37 | Documented operating procedures |
|---|---|---|
| Document and make available to the personnel who need them operating procedures for information processing facilities. | | |

- Consider documenting procedures for activities to be performed by many employees in the same way, for activities performed rarely, when activities are transferred to new personnel or for new activities.



Scan the QR or use link to join

https://forms.office.com/r/hLaRH6Mcsx

Copy link

0 response submitted

Which one is strong password

@p0llOJ4ck

12345678

Abc@12345

All of the above

# Screening

| People control | 6.1 | Screening |
|---|---|---|
| Carry out background checks on all candidates to become personnel before joining the organization and on an ongoing basis, considering the applicable laws, regulations and ethics. The checks must be proportional to the business requirements, the perceived risks and the classification of information to be accessed. | | |

- To prevent hiring the wrong person and to ensure personnel remain suitable for the job.
- The screening applies to all who work for the company (employees, consultants, free-lancers, temporary staff, etc.).

# Terms and conditions of employment

| People control | 6.2 | Terms and conditions of employment |
|---|---|---|
| Include in the employment contractual agreements the personnel’s and the organization’s responsibilities for information security. | | |

- Consider for inclusion in contracts the rules for access control, return of assets, protection of information in accordance with its classification level, the transfer of information, the relationship with suppliers, non-disclosure requirements or a mention of the disciplinary process.

# Information security awareness, education and training

| People control | 6.3 | Information security awareness, training and education |
|---|---|---|
| Ensure that personnel and relevant interested parties receive appropriate information security awareness, education and training, and regular updates of the organization’s information security policy, topic-specific policies and procedures, as relevant for their job functions. | | |

- Awareness refers to all who work for the organization, and it should focus also on “**why**” and not only on “**what**”.
- The education and training refer mainly to the technical personnel who need specific knowledge and skills.

# Disciplinary process

| People control | 6.4 | Disciplinary process |
|---|---|---|
| Establish and communicate a disciplinary process to take actions against personnel and other interested parties who have committed an information security policy violation. | | |

- **Everyone** in the organization should be **aware** of the disciplinary process.
- It may also include **rewards** for those who demonstrate excellent information security behavior.

# Responsibilities after termination or change of employment

| People control | 6.5 | Responsibilities after termination or change of employment |
|---|---|---|
| Define, enforce and communicate to relevant personnel and interested parties the information security responsibilities and duties that remain valid after termination or change of employment. | | |

- Determine if there are confidentiality requirements that extend beyond the period of employment.
- Apply a similar process for the **change of employment.**

# Confidentiality or non-disclosure agreements

| People control | 6.6 | Confidentiality or non-disclosure agreements |
|---|---|---|
| Personnel and other interested parties shall sign confidentiality or non-disclosure agreements that reflect the organization’s needs for protecting information. | | |

- Consider that there may be different confidentiality requirements for the different positions in the organization.

# Remote working

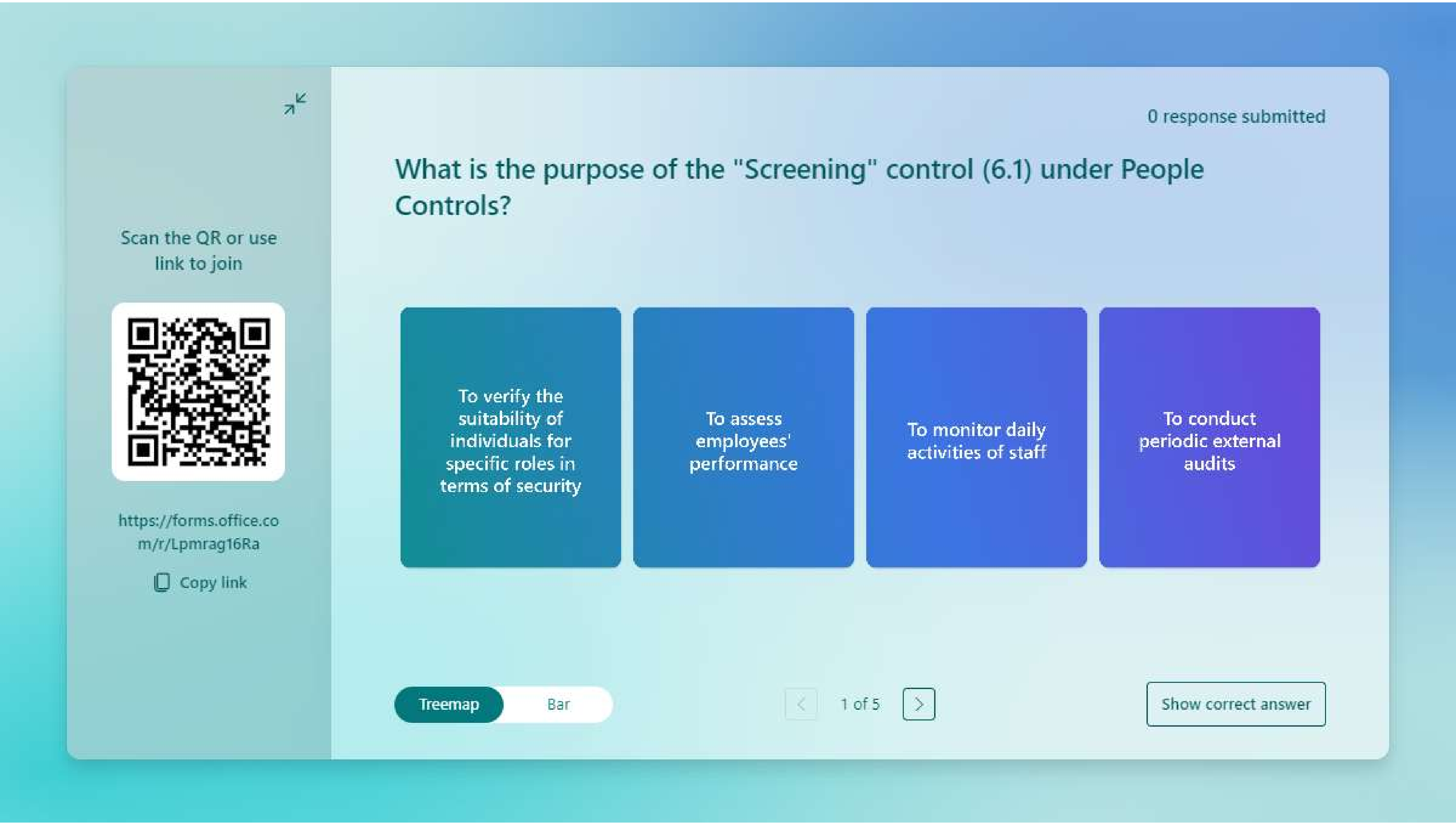
| People control | 6.7 | Remote working |
|---|---|---|
| Implement security measures when personnel are working remotely to protect the information accessed, processed or stored outside the organization's premises. | | |

- Consider a **topic-specific policy** for remote working, supported by procedure(s) to detail how the security risks associated with working remotely are to be managed.

# Information security event reporting

| People control | 6.8 | Information security event reporting |
|---|---|---|
| Provide a mechanism for personnel to report observed or suspected information security events in a timely manner, through appropriate channels. | | |

- Establish an **accessible and easy to understand system** for personnel to report information security events.


Scan the QR or use link to join
https://forms.office.com/r/Lpmrag16Ra
Copy link
0 response submitted
Treemap
Bar
1 of 5
Show correct answer

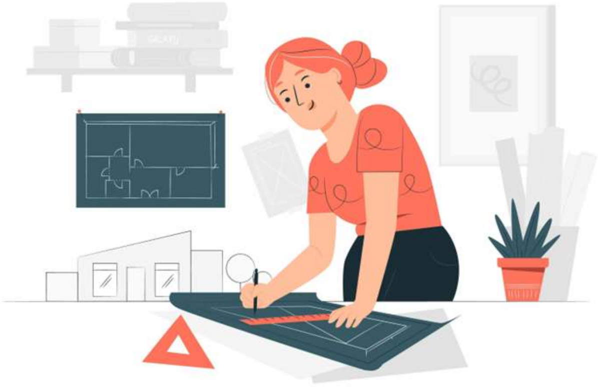
What is the purpose of the "Screening" control (6.1) under People Controls?

- To verify the suitability of individuals for specific roles in terms of security
- To assess employees' performance
- To monitor daily activities of staff
- To conduct periodic external audits

# Physical security perimeters

| Physical control | 7.1 | Physical security perimeters |
|---|---|---|
| Define and use security perimeters to protect areas that contain information and other associated assets. | | |

- Not all areas of the organization have the same importance in terms of information security.



# Physical entry

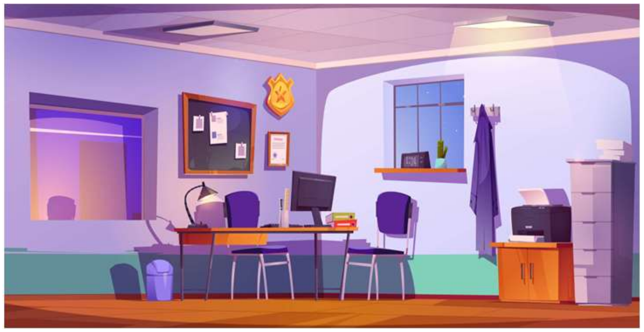
| Physical control | 7.2 | Physical entry |
|---|---|---|
| Protect secure areas by appropriate entry controls and access points. | | |

- Control physical access to the organization’s premises.

# Securing offices, rooms and facilities

| Physical control | 7.3 | Securing offices, rooms and facilities |
|---|---|---|
| Design and implement physical security for offices, rooms and facilities. | | |

- The controls intended to protect information and associated assets from unauthorized access should be **appropriate to the specifics of the organization**.



# Physical security monitoring (New Control)

| Physical control | 7.4 | Physical security monitoring |
|---|---|---|
| Monitor premises continuously for unauthorized physical access. | | |

- Choose the appropriate monitoring solutions (e.g., guards, intruder alarms, video monitoring, etc.).

# Protection against Physical and environmental threats

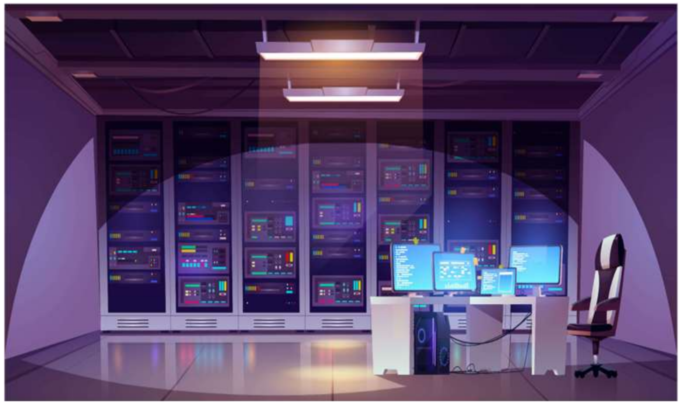
| Physical control | 7.5 | Protecting against physical and environmental threats |
|---|---|---|
| Design and implement protection against physical and environmental threats like natural disasters and other intentional or unintentional physical threats to infrastructure. | | |

- Consider a risk assessment focused on physical and environmental threats before starting critical operations in a new location.

# Working in secure areas

| Physical control | 7.6 | Working in secure areas |
|---|---|---|
| Design and implement security measures for working in secure areas. | | |

- Secure areas require **special protection measures** because of sensitive, critical or confidential activities undertaken.



# Clear desk and clear screen

| Physical control | 7.7 | Clear desk and clear screen |
|---|---|---|
| Define and enforce clear desk rules for papers and removable storage media, and clear screen rules for information processing facilities. | | |

- Consider a **topic-specific policy** for clear desk and clear screen.

# Equipment siting and protection

| Physical control | 7.8 | Equipment siting and protection |
|---|---|---|
| Equipment must be sited securely and protected. | | |

- **Protect equipment** from unauthorized access, from physical and environmental threats.

# Security of assets off-premises

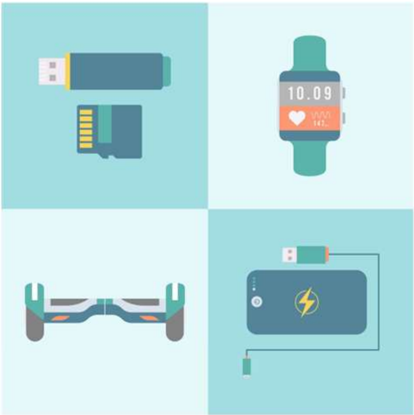
| Physical control | 7.9 | Security of assets off-premises |
|---|---|---|
| Protect assets off-site. | | |

- Apply **protection measures** for equipment that is intended to work outside (e.g., antennas, ATMs, etc.).
- Implement **rules** for taking assets outside the organization.

# Storage media

| Physical control | 7.10 | Storage media |
|---|---|---|
| Manage storage media through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements. | | |

- Consider a **topic-specific policy** on the use and handling of removable media.
- Address the **risks** associated with the use of removable storage media (theft, loss, damage, confidential information being disclosed, malware infestation, etc.).



# Supporting utilities

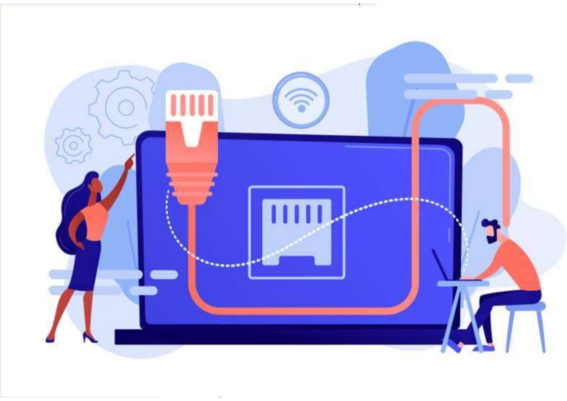
| Physical control | 7.11 | Supporting utilities |
|---|---|---|
| Protect information processing facilities from power failures and other disruptions caused by failures in supporting utilities. | | |

- **Configure and maintain** utility systems in accordance with the legislation and regulations.
- **Inspect** utility systems periodically. Implement redundancy, whenever possible.

# Cabling security

| Physical control | 7.12 | Cabling security |
|---|---|---|
| Protect cables carrying power, data or supporting information services from interception, interference or damage. | | |

- Prevent interruptions to operations, the theft or loss of important information, by protecting cables.



# Equipment maintenance

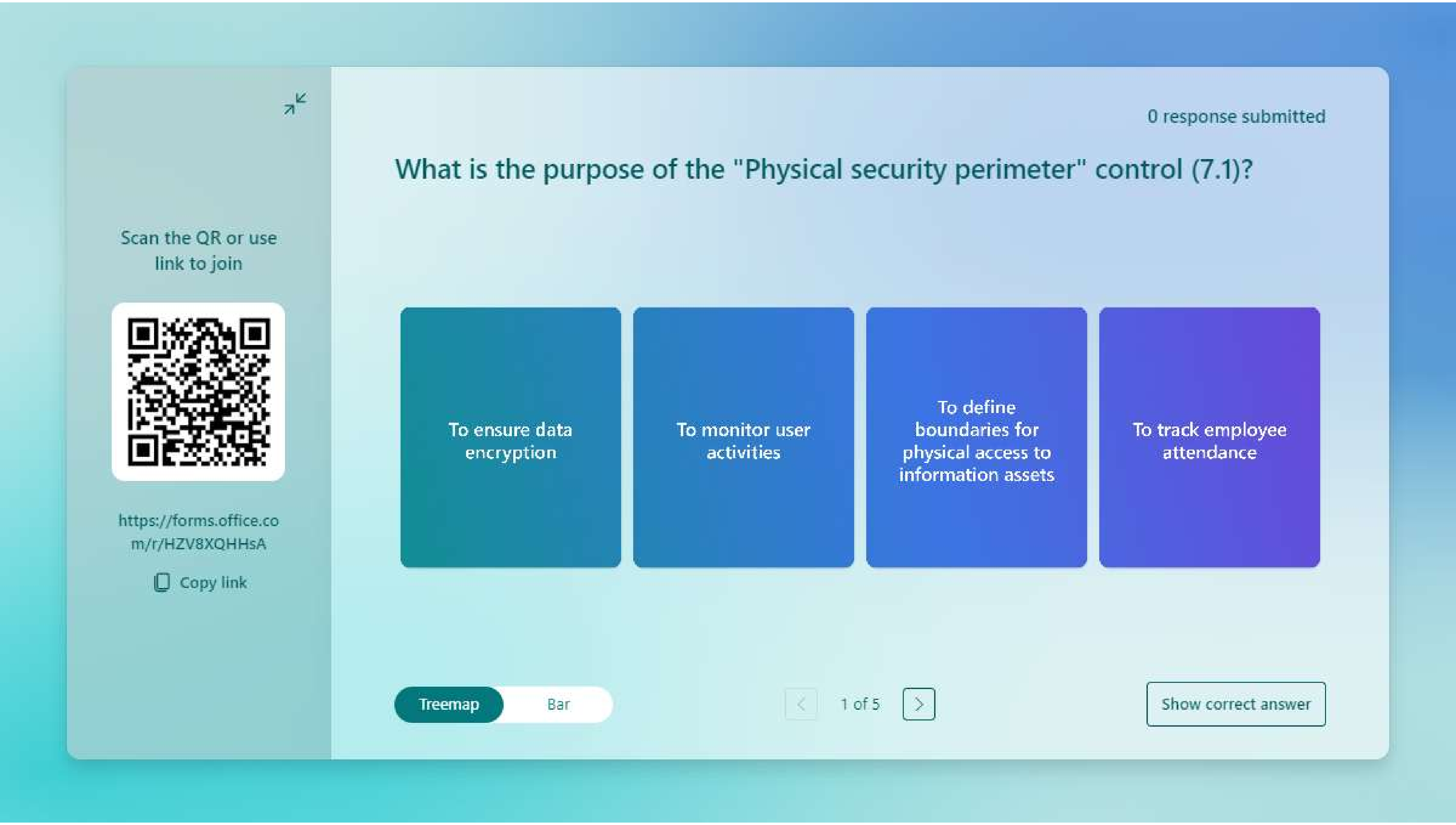
| Physical control | 7.13 | Equipment maintenance |
|---|---|---|
| Maintain equipment correctly to ensure the availability, integrity and confidentiality of information. | | |

- Equipment maintenance should be done **at specified intervals,** in accordance with **specifications** by **authorized personnel.**

# Secure disposal or re-use of equipment

| Physical control | 7.14 | Secure disposal or re-use of equipment |
|---|---|---|
| Verify items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. | | |

- Physically **destroy storage media, encrypt or wipe** any information so that it cannot be retrieved.



Scan the QR or use link to join

https://forms.office.com/r/HZV8XQHHsA

0 response submitted

What is the purpose of the "Physical security perimeter" control (7.1)?

- To ensure data encryption
- To monitor user activities
- To define boundaries for physical access to information assets
- To track employee attendance

# User end point devices

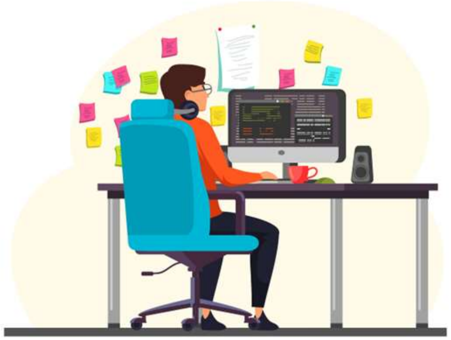
| Technological control | 8.1 | User end point devices |
|---|---|---|
| Protect the information that is stored on, processed by or accessible via user end point devices. | | |

- Consider a **topic-specific policy** on the use of end point devices.
- User **awareness** on security aspects (related to the use of end point devices).
- Establish **BYOD** (Bring Your Own Device) rules and requirements.

# Privileged access rights

| Technological control | 8.2 | Privileged access rights |
|---|---|---|
| Restrict and manage the allocation and use of privileged access rights. | | |

- The uncontrolled allocation of access privileges may lead to security **breaches.**
- Periodically (and in case of significant changes) do a **review** of privileged access rights.



# Information access restriction

| Technological control | 8.3 | Information access restriction |
|---|---|---|
| Restrict access to information and other associated assets in accordance with the topic-specific policy on access control. | | |

- Allow only authorized access to information and prevent unauthorized access.
- Consider **dynamic access management** techniques and processes.

# Access to source code

| Technological control | 8.4 | Access to source code |
|---|---|---|
| Manage appropriately the read and write access to source code, development tools and software libraries. | | |

- Establish **rules** for managing access to program source code.

# Secure authentication

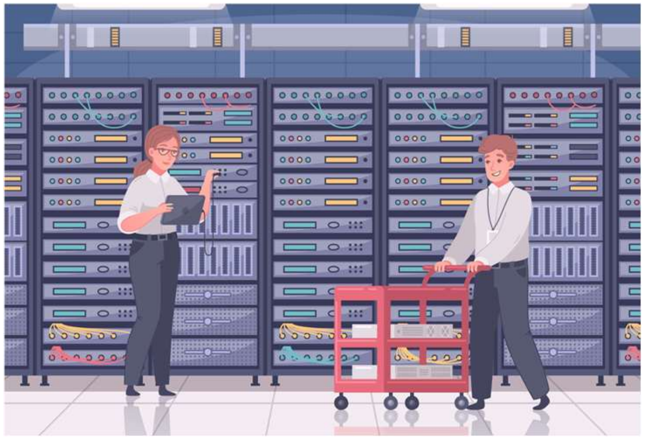
| Technological control | 8.5 | Secure authentication |
|---|---|---|
| Implement secure authentication technologies and procedures based on the information access restrictions and the topic-specific policy on access control. | | |

- **Authenticate users** who request access to information and correlate the **strength of authentication** with the classification of the information to be accessed.

# Capacity management

| Technological control | 8.6 | Capacity management |
|---|---|---|
| Monitor and adjust the use of resources in line with current and expected capacity requirements. | | |

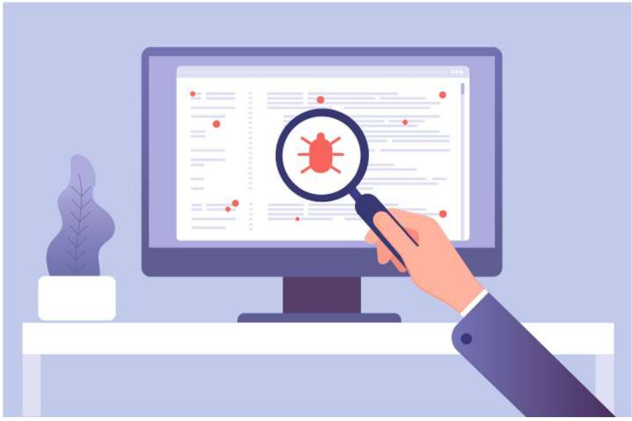
- Maintain **availability,** avoid bottlenecks and support growth.
- **Test** systems and services to confirm there is sufficient capacity for peak periods.
- Document a **capacity plan** for critical systems.



# Protection against malware

| Technological control | 8.7 | Protection against malware |
|---|---|---|
| Protection against malware must be implemented and supported by appropriate user awareness. | | |

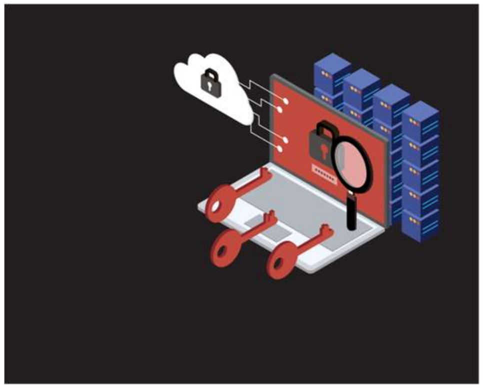
- Prevention and detection software + user awareness + system access rules + change management controls.



# Management of technical vulnerabilities

| Technological control | 8.8 | Management of technical vulnerabilities |
|---|---|---|
| Obtain information about technical vulnerabilities of information systems in use, evaluate exposure to such vulnerabilities and take appropriate measures. | | |

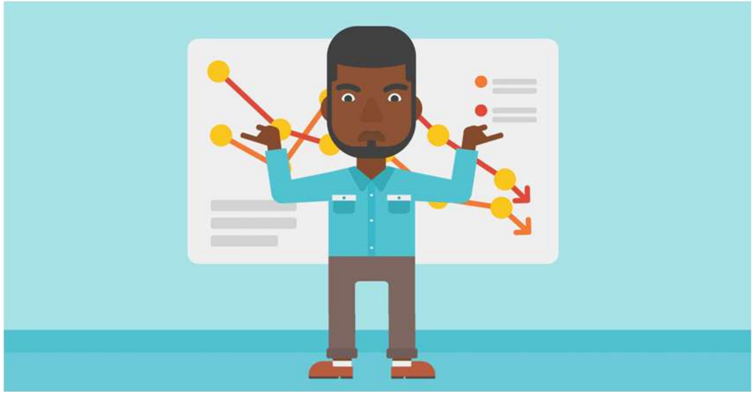
- **Obtain information** from reliable sources about technical vulnerabilities and **address** them, as appropriate.



# Configuration management (New Control)

| Technological control | 8.9 | Configuration management |
|---|---|---|
| Establish, document, implement, monitor and review configurations (including security configurations) of hardware, software, services and networks. | | |

- **Maintain assets** in a desired, consistent state, working as intended with the **appropriate security settings and features.**
- Define **standard templates for security configurations** of hardware, software, networks or services.



# Information deletion (New Control)

| Technological control | 8.10 | Information deletion |
|---|---|---|
| Ensure that information stored on information systems, devices and in any other storage media is deleted when no longer required. | | |

- Consider a **topic-specific policy** on data retention.
- Select an appropriate **deletion method**.
- **Pass** the information deletion requirements to subcontractors and other third parties, as appropriate.

# Data masking (New Control)

| Technological control | 8.11 | Data masking |
|---|---|---|
| Use data masking in accordance with the topic-specific policy on access control and other related topic-specific policies and business requirements, considering the applicable legislation. | | |

- Consider pseudonymization, anonymization and other data masking techniques, depending on the requirements applicable.

# Data leakage prevention (New Control)

| Technological control | 8.12 | Data leakage prevention |
|---|---|---|
| Apply data leakage prevention measures to systems, networks and any devices that process, store or transmit sensitive information. | | |

- **Identify** sensitive information that can be subject to leakage, **monitor** potential data leakage channels, and apply tools to **detect and prevent** data leakage.

# Information backup

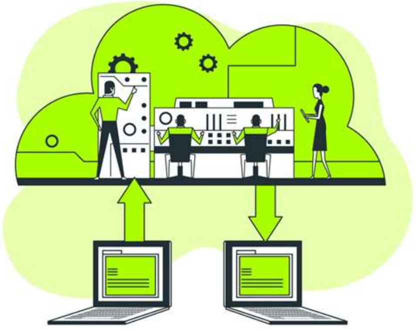
| Technological control | 8.13 | Information backup |
|---|---|---|
| Maintain and regularly test backup copies of information, software and systems, in accordance with the topic-specific policy on backup. | | |

- Establish a **topic-specific policy** on information backup.
- Define requirements for types of backups, frequency or backup storage location(s).

# Redundancy of information processing facilities

| Technological control | 8.14 | Redundancy of information processing facilities |
|---|---|---|
| Implement sufficient redundancy for information processing facilities to meet availability requirements. | | |

- Ensure a similar level of **protection** for redundant components.
- **Test** periodically the functioning of redundant components.



# Logging

| Technological control | 8.15 | Logging |
|---|---|---|
| Produce, store, protect and analyze logs that record activities, exceptions, faults and other relevant events. | | |

- Consider a **topic-specific policy** on logging.
- Ensure sufficient **storage** space and **protection** measures for logs **.**
- **Analyze logs** for indications of compromised security.

# Monitoring activities (New Control)

| Technological control | 8.16 | Monitoring activities |
|---|---|---|
| Monitor networks, systems and applications for anomalous behavior and act, as appropriate, to evaluate potential information security incidents. | | |

- Establish a **baseline** to determine anomalous behavior.
- Decide **what** to monitor and **how.**

# Clock synchronization

| Technological control | 8.17 | Clock synchronization |
|---|---|---|
| Ensure that the clocks of information processing systems used are synchronized to approved time sources. | | |

- Establish a **standard reference time.**

# Use of privileged utility programs

| Technological control | 8.18 | Use of privileged utility programs |
|---|---|---|
| Restrict and control tightly the use of utility programs that can be capable to override system and application controls. | | |

- Control the use of file managers, system diagnostic tools, disk checkers and cleaners, patching tools, etc.

# Installation of software on operational systems

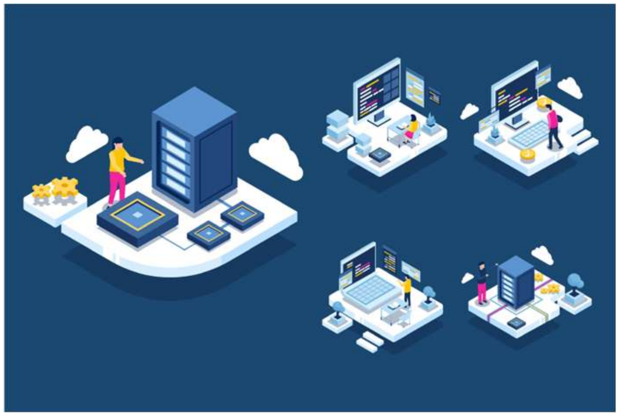
| Technological control | 8.19 | Installation of software on operational systems |
|---|---|---|
| Implement procedures and measures to securely manage software installation on operational systems. | | |

- **Protect** operational systems from the negative consequences that may be associated with the uncontrolled installation of software.

# Network security

| Technological control | 8.20 | Networks security |
|---|---|---|
| Secure, manage and control networks and network devices to protect information in systems and applications. | | |

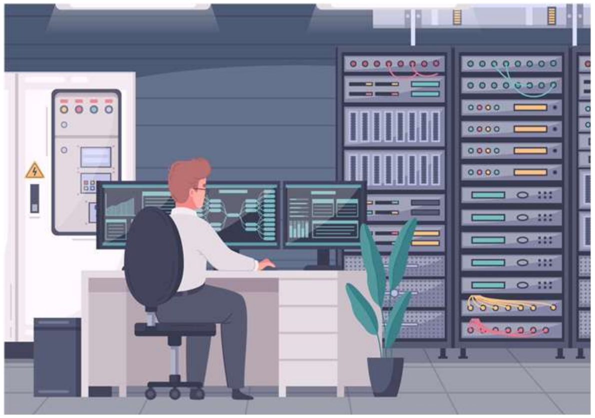
- Assign **responsibilities** for networks security.
- Maintain **up to date documentation** on networks configuration.
- **Protect data** passing through public, wireless and third-party networks.



# Security of network services

| Technological control | 8.21 | Security of network services |
|---|---|---|
| Identify, implement and maintain security mechanisms, service levels and service requirements of network services. | | |

- Ensure that network services providers manage agreed services in a **secure** way.



# Segregation of networks

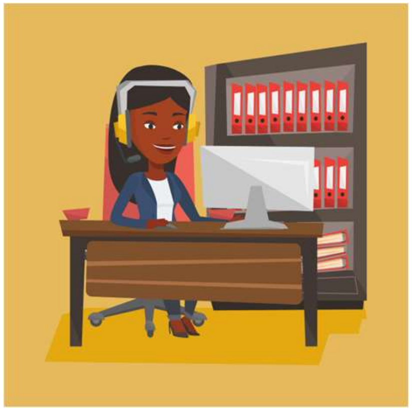
| Technological control | 8.22 | Segregation of networks |
|---|---|---|
| Segregate groups of information services, users and information systems, in the organization’s networks. | | |

- **Split** large networks into separate **domains** and **control the traffic** between the domains.
- Wireless networks require special attention.

# Web Filtering (New Control)

| Technological control | 8.23 | Web filtering |
|---|---|---|
| Access to external websites shall be managed to reduce exposure to malicious content. | | |

- User **awareness** and **technical controls.**
- Establish rules for the **safe and appropriate** use of online resources.



# Use of cryptography

| Technological control | 8.24 | Use of cryptography |
|---|---|---|
| Define and implement rules for the effective use of cryptography, including cryptographic key management. | | |

- Consider a **topic-specific policy** on the use of cryptography to define principles and requirements for using encryption to protect information.
- Establish procedures and methods for the **management of cryptographic keys.**

# Secure development life cycle

| Technological control | 8.25 | Secure development life cycle |
|---|---|---|
| Establish and apply rules for the secure development of software and systems. | | |

- **Information security** should be an **integral part** in the development of software and systems.

# Application security requirement

| Technological control | 8.26 | Application security requirements |
|---|---|---|
| Identify, specify and approve information security requirements when developing or acquiring applications. | | |

- Consider a **risk assessment** focused on the security of applications in use (developed in-house or acquired) and establish appropriate controls.

# Secure system architecture and engineering principles

| Technological control | 8.27 | Secure system architecture and engineering principles |
|---|---|---|
| Establish, document, maintain and apply principles for engineering secure systems to any information system development activities. | | |

- Treat information security as an integral part of every system architecture layer.
- Develop and apply **principles for secure system engineering.**
- Consider **“zero trust”** principles.

# Secure coding (New Control)

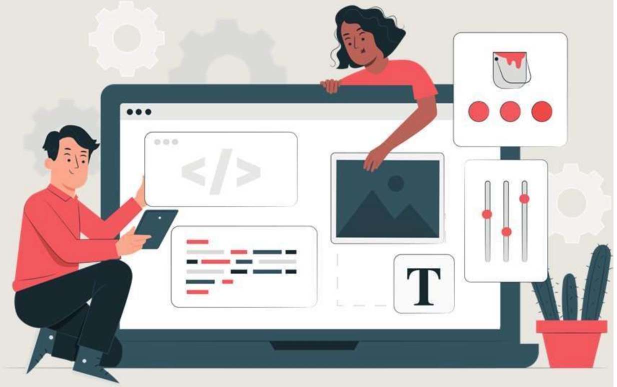
| Technological control | 8.28 | Secure coding |
|---|---|---|
| Apply secure coding principles to software development. | | |

- Ensure that **code is written securely**, so the number of potential security vulnerabilities is reduced.
- Establish controls for **planning and before coding, during coding and after the code has been made operational.**

# Security testing in development and acceptance

| Technological control | 8.29 | Security testing in development and acceptance |
|---|---|---|
| Define and implement security testing processes in the development life cycle. | | |

- Validate through testing that **information security requirements have been met.**



# Outsourced development

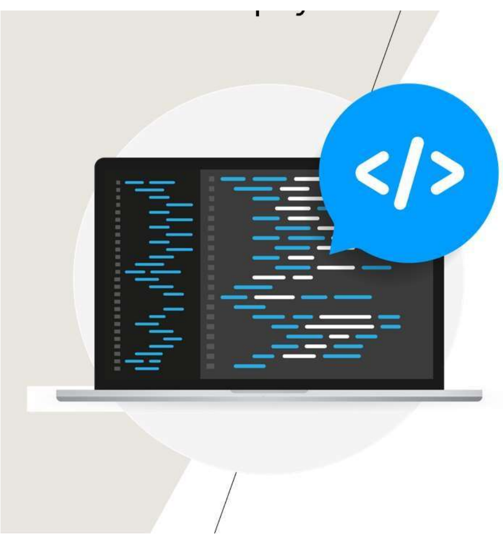
| Technological control | 8.30 | Outsourced development |
|---|---|---|
| Direct, monitor and review the activities related to outsourced system development. | | |

- Consider and address the **risks** related to the **product** (obtained from outsourced development arrangements) as well as the risks in relation to the **provider** of outsourced development.

# Separation of development, test and production environments

| Technological control | 8.31 | Separation of development, test and production environments |
|---|---|---|
| Separate and secure the development, testing and production environments. | | |

- Main objective is to **protect the production environment.**
- Consider the physical or virtual separation of environments.



# Change management

| Technological control | 8.32 | Change management |
|---|---|---|
| Changes to information processing facilities and information systems shall be subject to change management procedures. | | |

- **Procedures** to control changes should be documented and applied.
- The procedures should cover aspects like the planning of changes, authorization, communication, testing, implementation, fall back arrangements or records to be kept.

# Test information

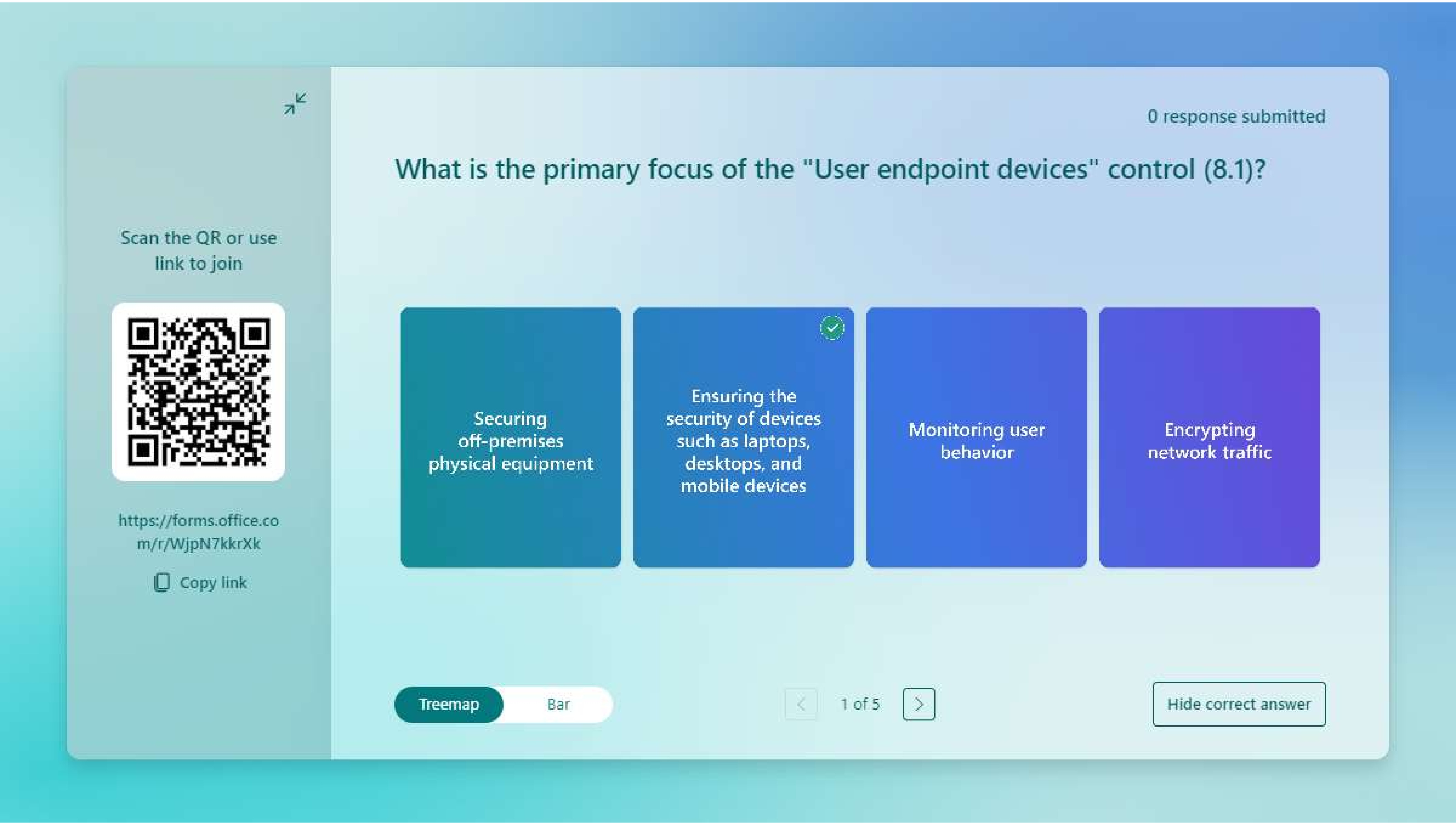
| Technological control | 8.33 | Test information |
|---|---|---|
| Select, protect and manage appropriately test information. | | |

- Operational information used for testing should remain **confidential.**
- **Sensitive data** should not be copied to development or testing environments.

# Protection of information systems during testing

| Technological control | 8.34 | Protection of information systems during audit testing |
|---|---|---|
| Plan and agree audit tests and other assurance activities that involve the assessment of operational systems between the tester and appropriate management. | | |

- Reduce the **impact** that audits and other assurance activities may have on operational systems and business processes.



0 response submitted

What is the primary focus of the "User endpoint devices" control (8.1)?

- Securing off-premises physical equipment
- Ensuring the security of devices such as laptops, desktops, and mobile devices ✓
- Monitoring user behavior
- Encrypting network traffic

Scan the QR or use link to join

https://forms.office.com/r/WjpN7kkrXk

# ISO/IEC 27001 Certifications for organizations

- Obtained after passing an **audit**.
- Valid for **3 years** with annual **surveillance audits**.
- Can be **suspended** or **withdrawn**.
- Visit Us: https://www.qualityasia.in/contact.php

QUALITY ASIA

# Audits: Definition, Principles, and Types

# Audit

- "Systemic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled."

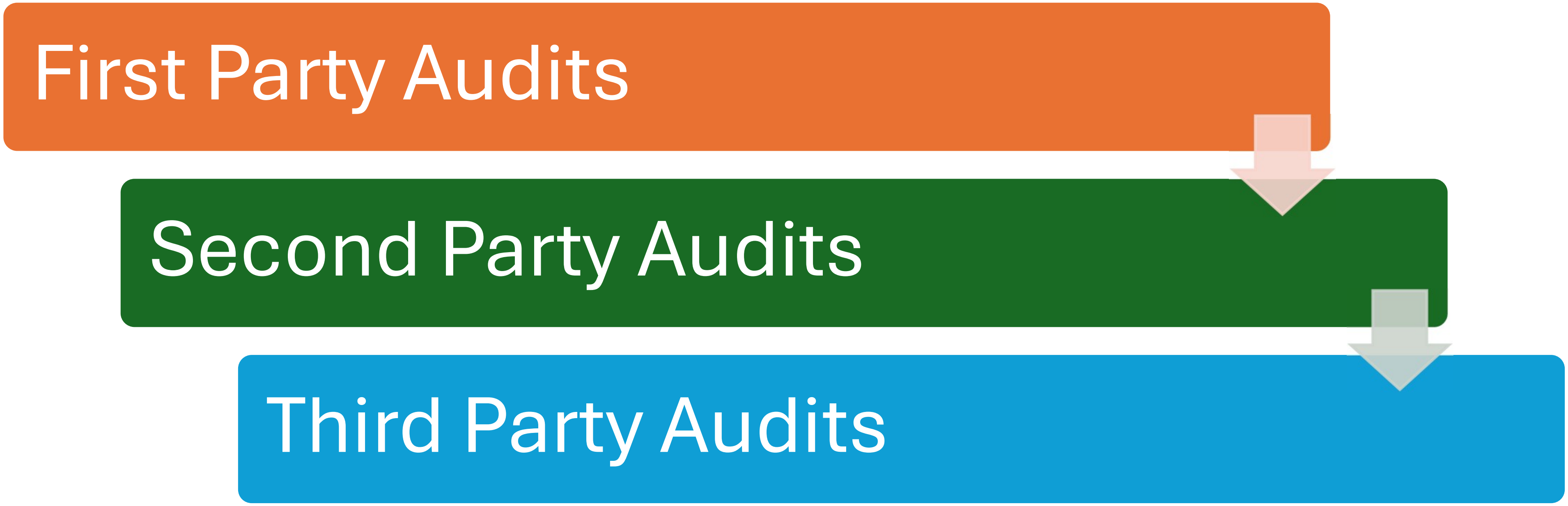
- Alternative Definitions:
  - Impartial documented activity
  - Follows written checklists and documentation
  - Uses examination of audit evidence to determine the existence of objective evidence
  - Verifies that applicable processes of a QMS have been identified  and are effectively controlled.

# Reasons for Conducting Audits

- To examine the Food Safety Management System for Improvements
- To ensure ISO 22000, and all other standards, are being complied with.
- To determine compliance or non-compliance
- To meet regulatory requirements
- To enable certification

# Effective Audits - Requirements

- Timely access to facilities, documents and personnel, including top management
- Defined auditing procedures
- Support/involvement of management
- Competent audit team
- Impartial and objective audit team



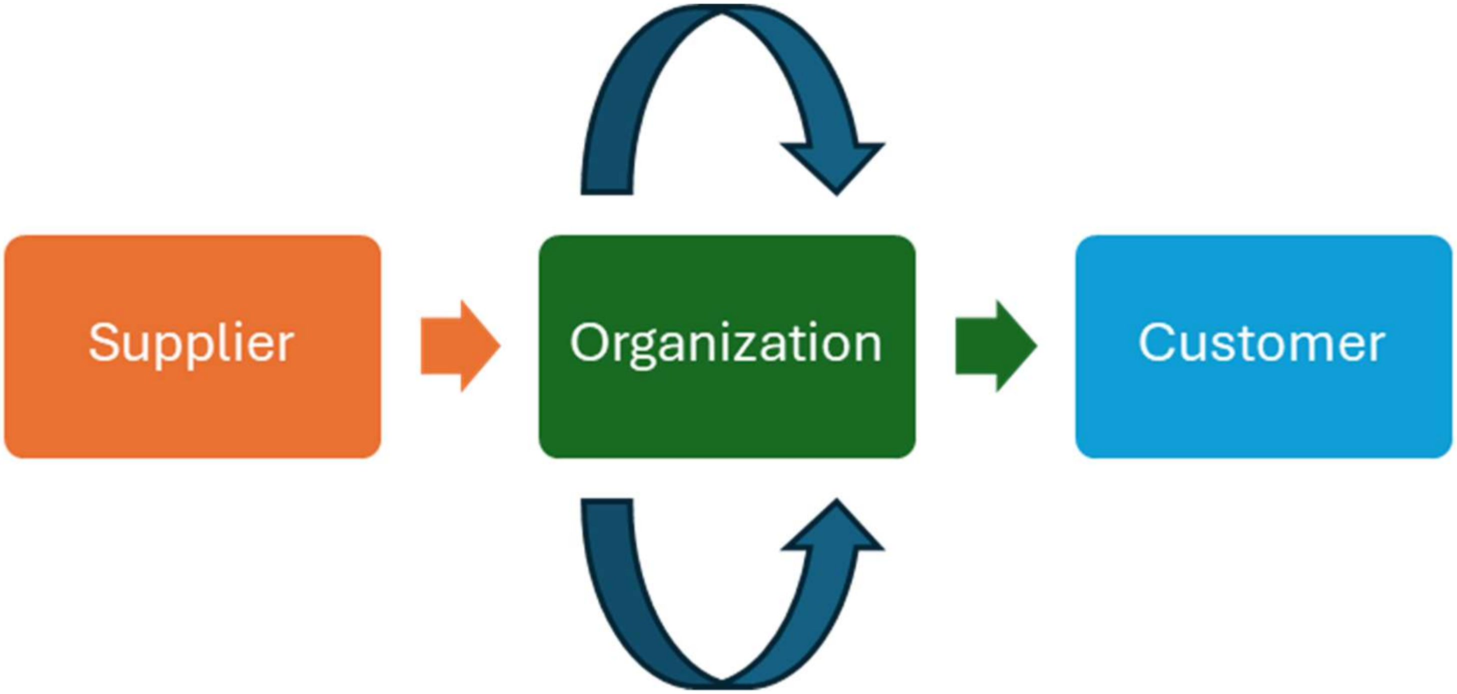
First Party Audits

Second Party Audits

Third Party Audits

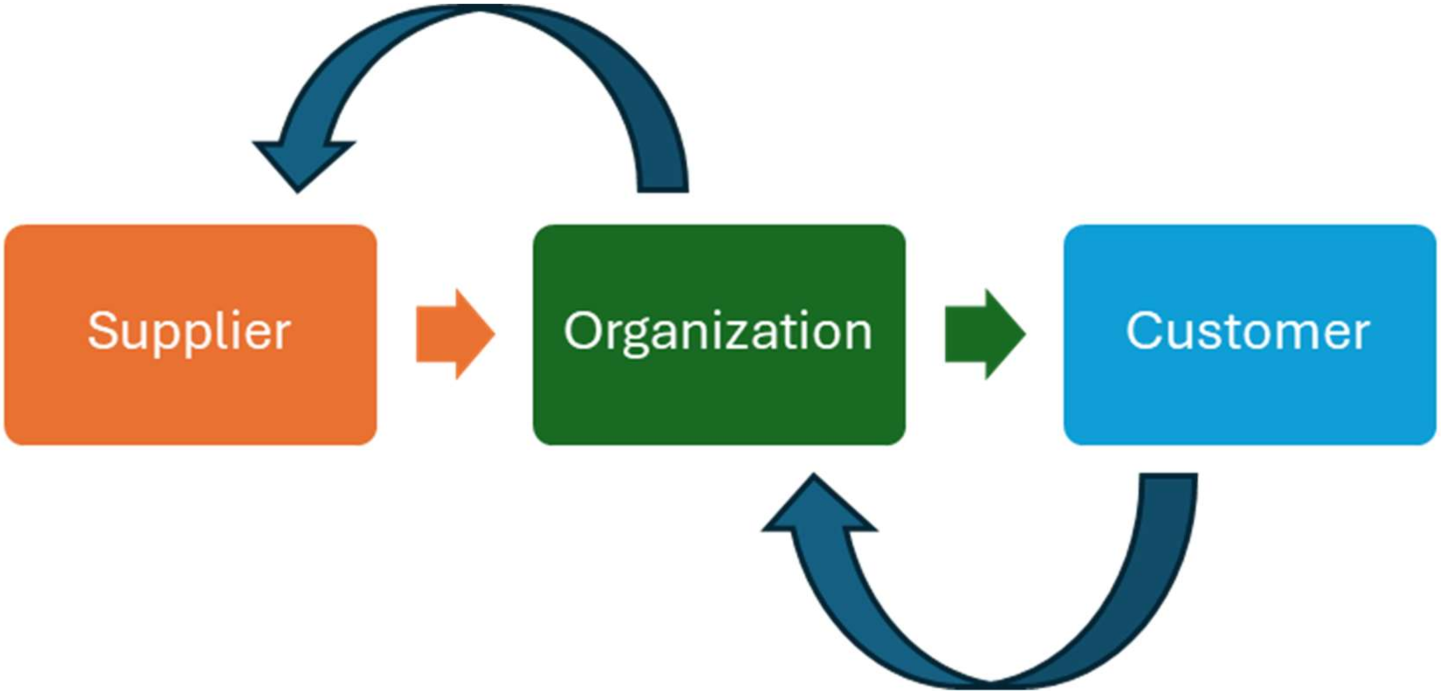
# First Party Audit

- Internal audits
- Performed within an organization
- Auditors have no vested interest in the area being audited



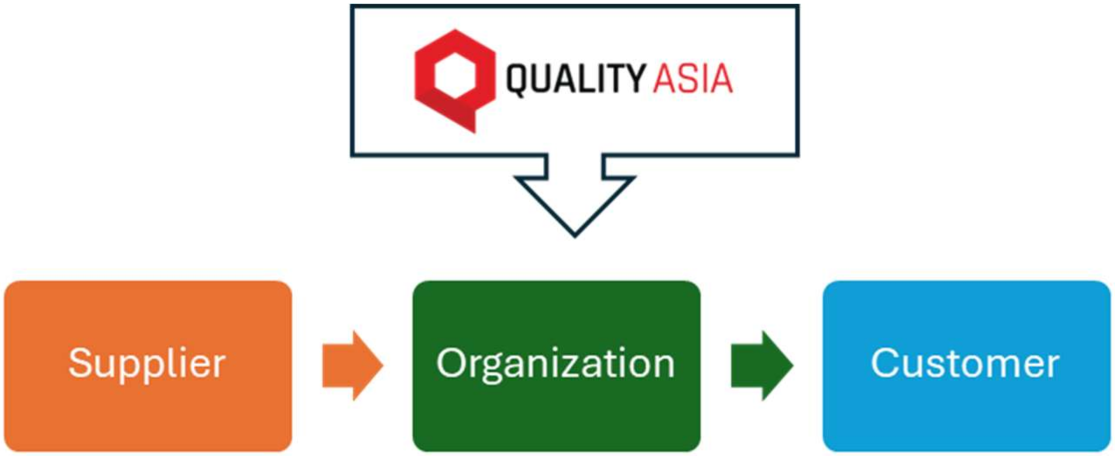
# Second Party Audit

- Performed by Customers on suppliers
- Before or after awarding a contract



# Third Party Audit

- Performed by an audit organization independent of the customer-supplier relationship
- Free from any conflict of interest



## Audit participants

Client – Organization or person requesting the audit

Auditor – A Person who conducts the audit

Auditee – Organization or individual being audited

# Client, responsible for..

- Initiates audit
- Determines audit purpose and scope
- Provide resources
- Receives the audit report
- Determine the report distribution

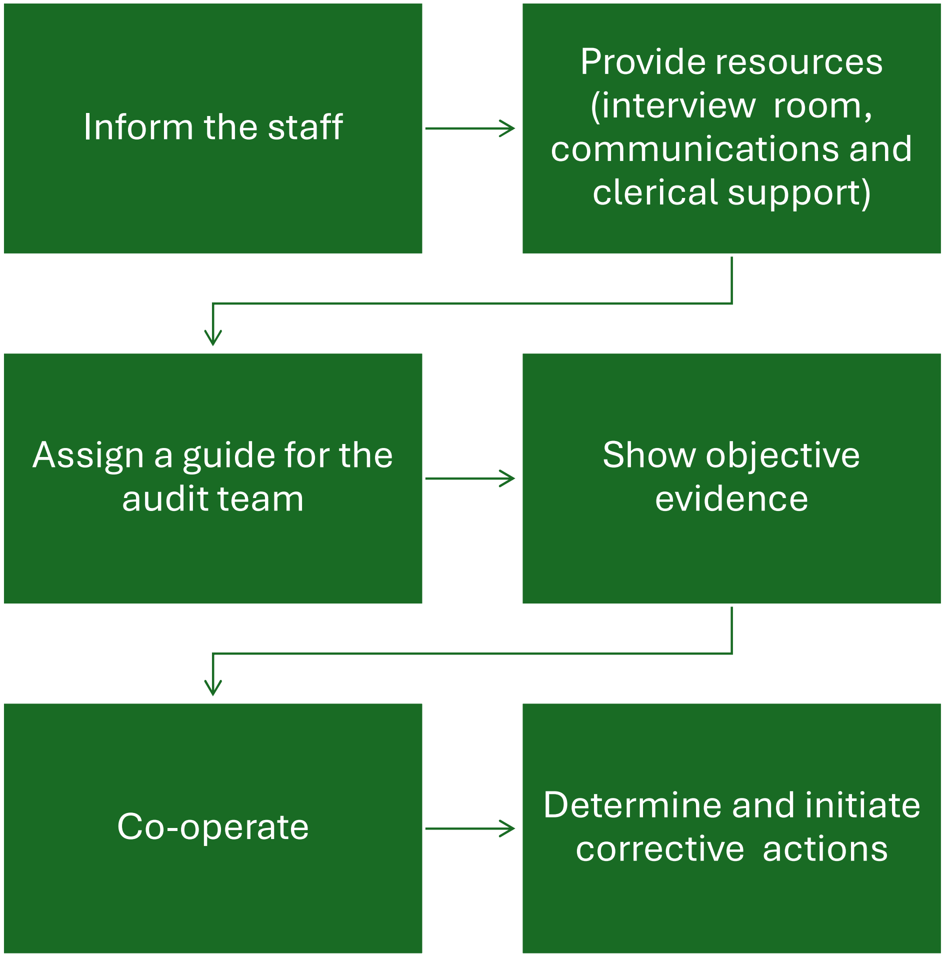
# Auditor, responsible for…

- Understand the purpose, scope and audit criteria.
- Plans the audit
- Perform the audit
- Collect audit evidences
- Analyze audit evidences
- Reports the audit
- Follows up the action on audit findings

# Lead auditor, responsible for…

- Balance the strength and weaknesses of team members
- Manage the audit process
- Represent the audit team
- Lead the audit team
- Prepare and complete the audit report

# Auditee, responsible for…



Inform the staff

Provide resources (interview room, communications and clerical support)

Assign a guide for the audit team

Show objective evidence

Co-operate

Determine and initiate corrective actions

# Audit participants - 2

Technical Expert – a person who provides specific knowledge or expertise to the audit team.

Observer – a person who accompanies the audit team but does not audit.

Guide – a person appointed by the auditee to assist the audit team.

# Phases of an Audit

## Phases of an Audit

- Planning
- Preparation
- Performance
- Reporting and Follow Up

## Planning the Audit Stage

- Frequency and timing
- Responsibility
- Criteria
- Scope
- Methods
- Duration

QUALITY ASIA

# Planning Internal Audits

| | |
|---|---|
| **Frequency and timing:** | Based on status and importance |
| **Responsibility:** | Competent auditor with technical knowledge |
| **Criteria:** | Organization’s own procedures, specifications, documents, etc.<br>Internal Standards e.g., ISO 22000:2018 |
| **Scope:** | A process<br>An area of the company, e.g. distribution, Quality control, servicing |
| **Duration** | Depends on the size of the scope |

# Planning Second Party Audits

| | |
|---|---|
| **Frequency and timing:** | As determined by the organization |
| **Responsibility:** | Competent auditor with technical knowledge |
| **Criteria:** | Contractual obligations<br>Organization’s management system<br>ISO 22000 or other agreed standards |
| **Scope:** | The entire facility<br>An area of the company, e.g. a product line |
| **Duration** | Depends on the size of the scope |

# Planning third Party Audits

**Frequency and timing:**

- As determined by the accreditation

**Responsibility:**

- Qualified auditor with technical knowledge & experience

**Criteria:**

- ISO 45001 or other standards

**Scope:**

- Entire organization
- Management system operations as defined by applicable standard

**Duration**

- Depends on accreditation requirements

# Audit Procedure

- External audits are usually agreed in advance with the auditee and carefully planned, however ‘unannounced audits’ may be carried out by the Certification Bodies or Customers and their representatives as a policy or when there is some justification for such an audit

# Activities Prior to the Audit

- Create audit program and audit plan and notify the auditee

- Arrange audit logistics

- Prepare audit checklist

QUALITY ASIA

# Audit preparation

Notify person to be audited and agree to a date and time

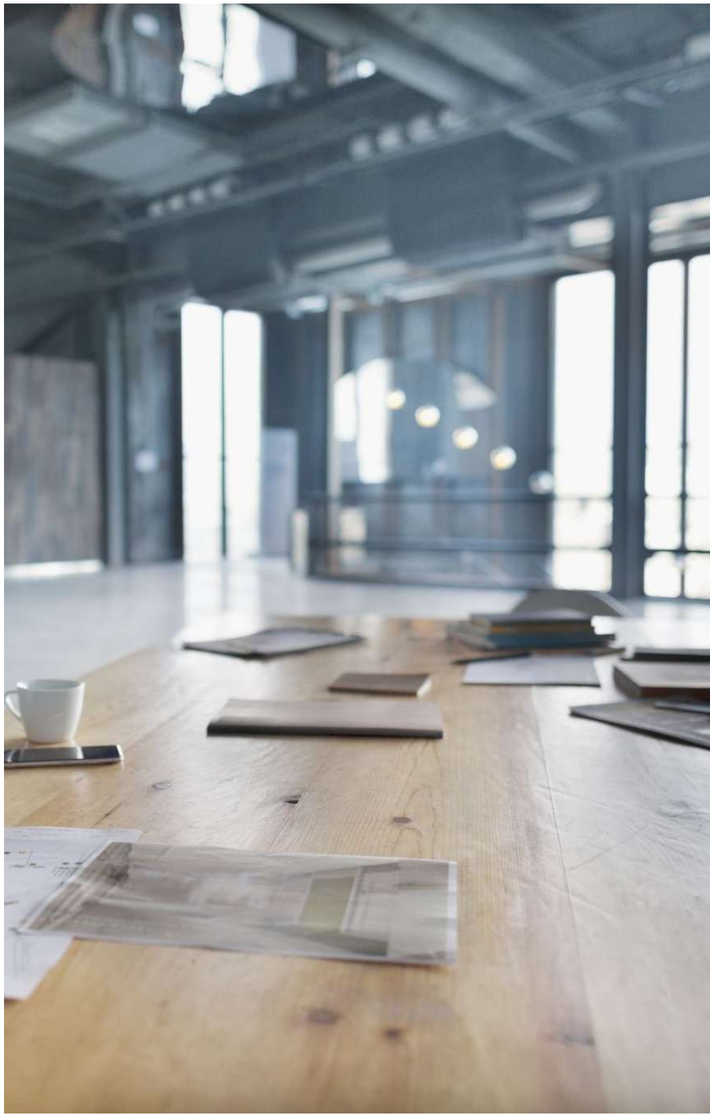
Review documents: procedures, forms, previous reports, corrective action requests, work instructions, etc.

Prepare/review/update checklists

Brief auditor/team

# Arrange for Audit Logistics

- Travel and accommodation
- Safety and security considerations
  - Personal Protective Equipment (PPE)
  - Location and/or Camera Permit
- Need for a Guide
- Translators
- Facilities
  - Working area, conference room, internet, printer, tea/coffee and working lunch



# Audit Checklist

## The Checklist

- To be used as a working document and as a record
- Tool to audit company processes, not standard
- Should follow the natural process of the organization

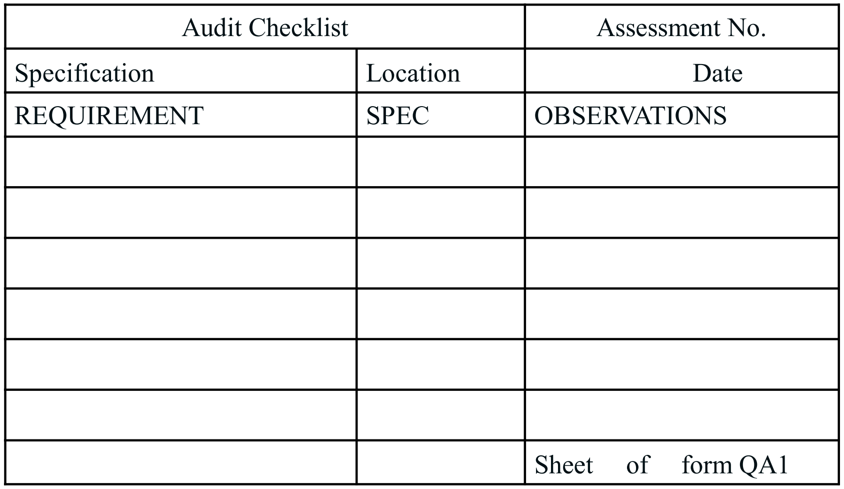
## The Purpose of the Checklist

- To provide guidance to the auditor
- To ensure that the audit scope is covered (processes, activities)
- To reinforce the objectives and scope of the audit
- To act as a record

## Risks of the Checklist

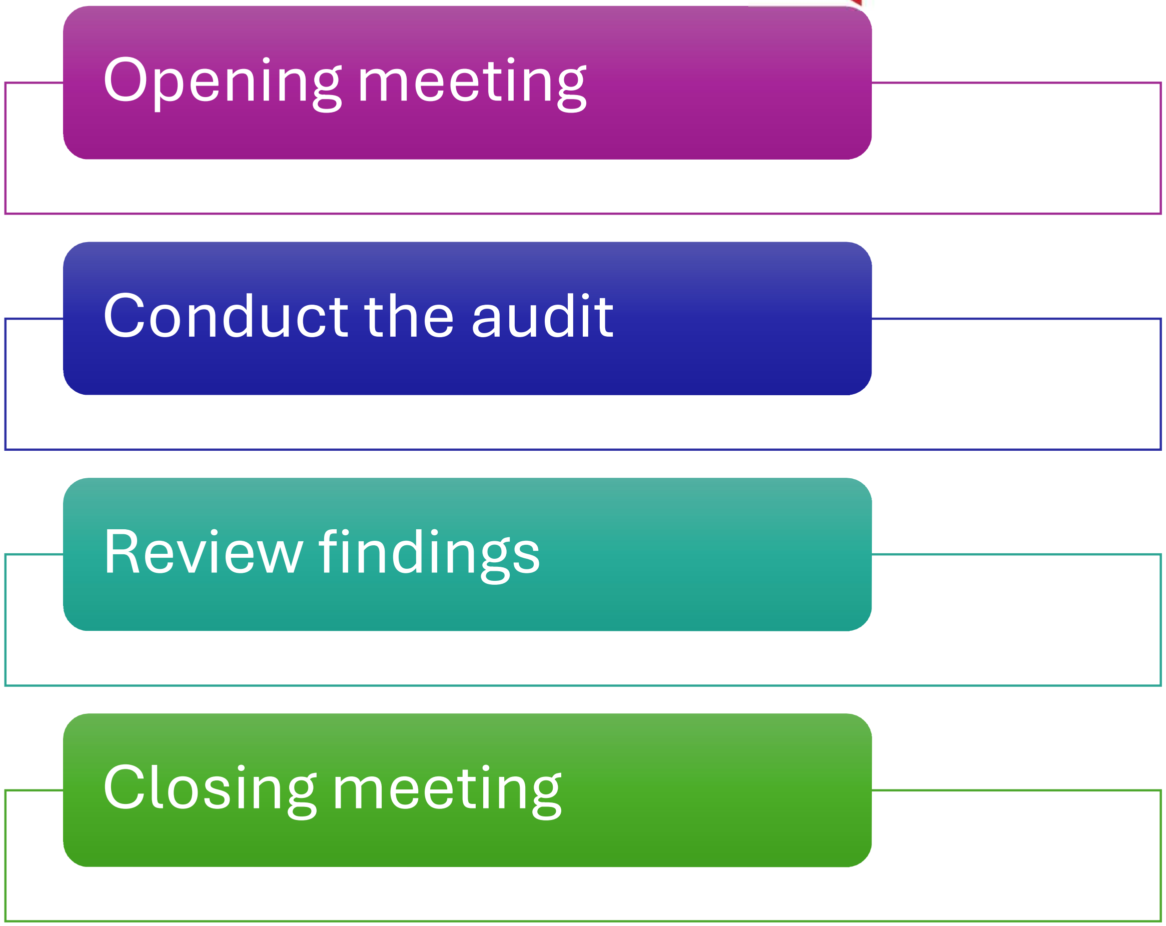
- Too focused on a single area
- Insufficient information included to evaluate conformance in interviews
- Not customized to reflect company's practices

# Sample Checklist



| | | |
|---|---|---|
| Audit Checklist | | Assessment No. |
| Specification | Location | Date |
| REQUIREMENT | SPEC | OBSERVATIONS |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | Sheet of form QA1 |

# Audit Performance



- Opening meeting
- Conduct the audit
- Review findings
- Closing meeting

# Opening Meeting

- Introduce auditors or audit team
- Discuss audit scope and process
- Explain reporting and follow-up procedures
- Necessary for:

  a) Good communication

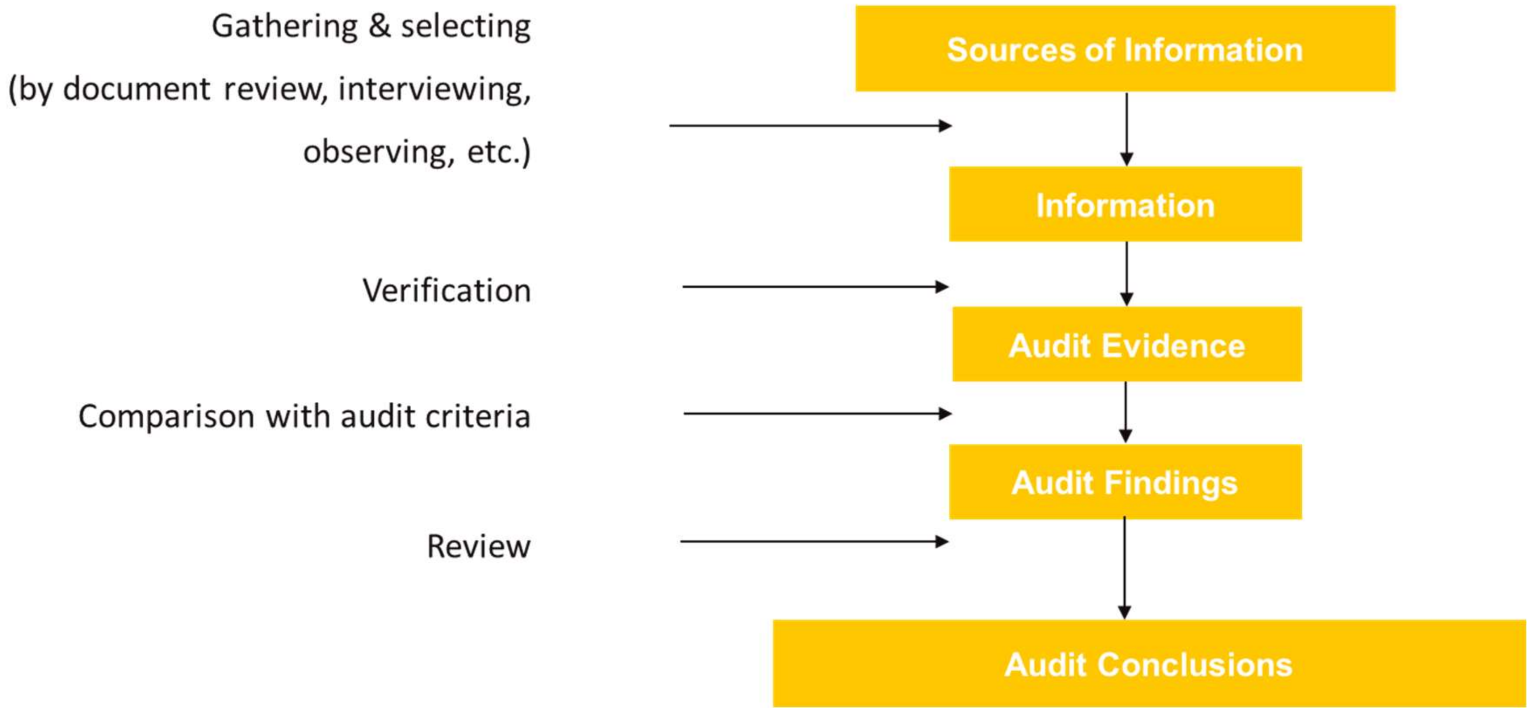
  b) Co-operation

  c) Openness

# The Auditor must:

- Deal with top management
- Understand the key issues in the organization
- Focus on the critical processes
- Audit for business improvement
- Meet the area representative first
- Always talk to those performing the task
- Explain the purpose of the visit
- Be calm, polite, reassuring
- Never talk down
- Never act superior
- Speak clearly and carefully

# The Auditor Process



Gathering & selecting (by document review, interviewing, observing, etc.)

Verification

Comparison with audit criteria

Review

Sources of Information

Information

Audit Evidence

Audit Findings

Audit Conclusions

# Obtaining objective (audit) Evidence

May be gathered from:

- Interviews with people
- Observation of activities
- Interactions between functions, activities, processes
- Measurement of processes and programs
- Documents/records
- Data summaries, reports from other sources (e.g., customer feedback)

- People:
  - Does anyone understand the systems and documentation?
  - Are the employees competent?
  - Is there co-operation?
  - Are there any system problems?

# Obtaining objective (audit) Evidence (Continued)

- Observation of activities
  - Are the processes efficient? Effective?
  - Are things in logical sequence?
  - Are the interactions between processes defined?
  - What is the significance of links between processes?
  - Can inputs and outputs be identified?

- Measurement of processes and programs
  - Capacity of processes
  - Product measurement
  - Accuracy
  - Dependability
  - Cycle times
  - Resource utilization
  - Productivity

# Obtaining objective (audit) Evidence (Continued)

Documents/records

- Issue status?
- Complete and concise?
- Condition?
- Legibility?
- Identity?
- Approval?
- Availability?

Data summaries

- Customer feedback
- Vendor analysis
- Internal Audits
- Financial measurements
  - Preventive, appraisal and failure cost analysis (Cost of quality)
  - Cost of nonconformity

# Examine objective Evidence

**Examine:**

- Documents/data
  - Fully complete
  - Accurate data
  - Check for authorization
  - Review analysis of data
- Physical Evidence
- Environmental Conditions

**Establish:**

- Extent of conformity/nonconformity
- Nature for nonconformity
- Sample: According to the amount and variety of evidence

# Use the Checklist

- To record conformity/nonconformity
- To track where you are and manage time
- To control the pace of the audit and manage auditee personalities
- To ensure all areas are covered
- To make notes for follow-up in other areas
- For future reference

# Questioning Techniques

Who?

What?

When?

Where?

Why?

How?

QUALITY ASIA

# Controlling the Audit

- Insist that people being questioned answer for themselves
- Do as little talking as possible
- Do not let others dictate the pace
- Rephrase misunderstood questions
- Give compliments
- Say, “Thank you”
- Be aware of hidden agendas and emotional blackmail

# Some Basic Issues

- Establish that the company is demonstrating control over the operation
- Involve management in the audit process
- Observe work progression when possible
- Evaluate physical objective evidence
- Examine inputs and outputs
- Make comprehensive notes

# Some Basic Rules

Seek verification

- Do not assume people will lie, but seek to verify statements if necessary

Do not accept pre-prepared samples

- Choose your own

# General Principles of Auditing

- **Integrity** – the foundation of professionalism
- **Fair presentation** – the obligation to report truthfully and accurately
- **Due professional care** – the application of diligence and judgment in auditing
- **Confidentiality** – security of information
- **Independence** – the basis for the impartiality of the audit and objectivity of the audit conclusions
- **Evidence-based approach** – the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process

# Auditor’s Personal Attributes

**Ethical** – Fair, truthful, sincere, honest and discreet

**Open-minded** – willing to consider alternative ideas or points of view

**Diplomatic** – tactful in dealing with people

**Observant** – actively observing physical surroundings and activities

**Perceptive** – aware of and able to understand situations

**Versatile** – able to readily adapt to different situations

**Tenacious** – persistent and focused on achieving objectives

**Decisive** – able to reach timely conclusions based on logical reasoning and analysis

**Self-reliant** – able to act and function independently whilst interacting effectively with others

QUALITY ASIA

# General knowledge and skills of Management System Auditors

- Audit principles, procedures and methods
- Management system and reference documents
- Organizational context
- Applicable legal and contractual requirements and other requirements that apply to the auditee
- Discipline and sector-specific knowledge and skills of management system auditors

# Generic Knowledge and Skills of Audit Team Leaders

Audit team leaders should be able to:

- Balance the strengths and weaknesses of the individual audit team members
- Develop a harmonious working relationship among the audit team members.
- Plan audits and effectively use audit resources
- Manage the uncertainty of achieving audit objectives
- Protect the health and safety of the audit team members including compliance with the requirements
- Organize and direct the audit team members
- Provide direction and guidance to auditors-in-training
- Prevent and resolve conflicts as necessary
- Represent the audit team
- Lead the audit team to reach the audit conclusions
- Prepare and complete the audit report

# Good Practices for Auditors

- Introduce self and/or audit team
- Ensure agenda is understood
- Keep to agenda
- Keep control of the audit and time
- Avoid arguments
- Listen
- Keep records
- Remain polite, calm, professional

# Audit Review

- Conduct a private review when the audit is finished
- Interim or “end of the day” reviews (or both) may be appropriate
- Review and complete checklists
- Study and compare notes (team)
- List nonconformities

# Analyzing Results

Review if:

- The deficiency is an isolated error or a breakdown of a system
- Auditee is aware of the problem
- The deficiency has been reported before

# Closing Meeting

- Explain/discuss the findings
- Obtain agreement
- State overall degree of conformity
- Mention the positive points

| Internal audits | Second party audits | Third party audits |
|---|---|---|
| • Informal<br>• Constructive<br>• System improvement | • Contracts at stake<br>• Reports used as future reference<br>• More emotional situation than first party audit meeting<br>• Be prepared to be challenged | • Contracts at stake<br>• Reports used as future reference<br>• More emotional situation than first party audit meeting<br>• Be prepared to be challenged |

# Non-conformance management in first party audits

- **Identification**: Auditors identify non-conformities against the organization’s internal procedures or ISO requirements.
- **Recording**: Non-conformances are documented in the audit report.
- **Corrective Action**: The organization takes corrective actions to address root causes and prevent recurrence.
- **Verification**: Follow-up audits or reviews ensure actions are implemented effectively.
- **Purpose**: Improve internal systems, ensure compliance, and prepare for external audits.

# Non-conformance management in second party audits

- **Identification**: Non-conformities against agreed terms, product specifications, or food safety requirements are identified.
- **Reporting**: Issues are communicated to the supplier formally.
- **Corrective Action**:
  - The supplier is required to provide a Corrective Action Plan (CAP) within a specified timeline.
  - Actions include root cause analysis, corrective measures, and preventive actions.
- **Verification**: Follow-up audits or supplier reviews are performed to verify corrections.
- **Purpose**: Ensure suppliers meet contractual obligations and quality standards.

# Non-conformance management in third party audits

- **Identification**: Non-conformities are classified as:
  - Major: Systematic failures or high-risk non-compliance.
  - Minor: Isolated issues that don’t pose significant risk.
- **Reporting**: Non-conformities are included in the audit report and communicated to the auditee.
- **Corrective Action**:
  - Auditees must submit an action plan with root cause analysis, corrective actions, and preventive measures.
  - A timeline is set to resolve major non-conformities (often 30-90 days).
- **Verification**:
  - Major non-conformities require evidence submission and/or re-audit.
  - Minor non-conformities are checked during the next surveillance audit.
- **Purpose**: Achieve certification, regulatory compliance, or demonstrate conformity to standards.

# Nonconformance Statement

A short statement describing the nonconformity including:

- What - The issue in question

  (a statement of nonconformity)

- Why - What the statement is raised against?

  (the requirement, or specific reference to the requirement)

- Objective Evidence - The objective evidence found

  (the objective evidence observed that supports statement of nonconformity)

# Nonconformance report

- Used to report non-conformity audit findings
- Must be factual
- Must be understandable and traceable
- Raise non-compliances on completion of an audit
- Allow the auditee to implement corrective action prior to the closing meeting
- The auditee is requested to sign signifying an understanding and acceptance of the non-compliance

# Wording of NC report

- It is important when preparing and wording NC-Report's to take care and ensure it is justified
- Failure to achieve clear information will invite challenge of the findings at the closing meeting
- This will be particularly important in areas where the emphasis has changed with respect to the requirements in order that they will be clearly understood, i.e.
  - Management Commitment
  - Competence
  - Communication
  - Continual Improvement

# Example of Nonconformance Statement

- **A statement of nonconformity:**
  - The organization's employees lacked adequate awareness of information security policies and procedures, resulting in a failure to comply with security requirements.
- **The requirement, or specific reference to the requirement:**
  - ISO 27001:2022 Clause 7.3 Awareness : "Persons doing work under the organization’s control shall be aware of:
    - the information security policy;
    - their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance;
    - the implications of not conforming with the information security management system requirements.“
- **The objective evidence observed that supports statement of nonconformity:**
  - During employee interviews, it was found that several team members in the operations department were unaware of the organization's information security policy, including procedures for identifying and reporting security incidents. No evidence of recent awareness training for these employees was available.

# Audit Reporting

The audit report should include:

- Auditors, contracts, scope
- Overall conclusions
- Deficiencies, observations, supporting objective evidence
- Follow-up details

Exclude from Report:

- Confidential information given in interviews
- Matters not raised or discussed at the closing meeting
- Subjective opinions – use only verifiable facts / objective evidence
- Ambiguous statements
- Antagonistic words or phrases

# Audit Reporting

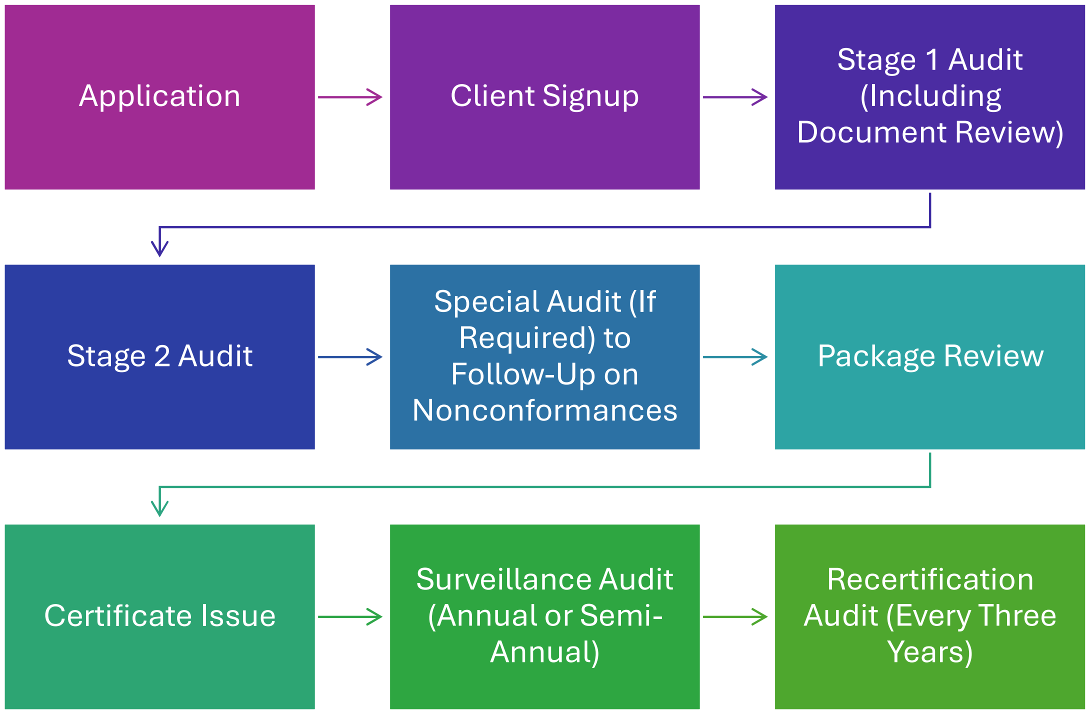
- Description of audit aim, purpose and scope
- Number of non-compliances and summary of audit findings
- Description of good points and any main concerns
- Description of the identified opportunities for improvement
- Recommendations made because of audit findings

# Audit Follow-Up

- Verify that action(s) are implemented
- Ensure short- and long-term effectiveness
- Record follow-up details & objective evidence reviewed
- Sign off forms

QUALITY ASIA

# Registration Process Flow



Application

Client Signup

Stage 1 Audit (Including Document Review)

Stage 2 Audit

Special Audit (If Required) to Follow-Up on Nonconformances

Package Review

Certificate Issue

Surveillance Audit (Annual or Semi-Annual)

Recertification Audit (Every Three Years)

# Certifications and Internal Auditor Trainings offered

- We offered certifications and internal auditor training for -
  - ISO 9001 (QUALITY MANAGEMENT SYSTEMS)
  - ISO 14001 (ENVIRONMENT MANAGEMENT SYSTEMS)
  - ISO 45001 (OCCUPATIONAL HEALTH & SAFETY MANAGEMENT SYSTEMS)
  - ISO 50001 (ENERGY MANAGEMENT SYSTEMS)
  - ISO 27001 (INFORMATION SECURITY MANAGEMENT SYSTEMS)
  - ISO 22000 (FOOD SAFETY MANAGEMENT SYSTEMS)
  - ISO 13485 (MEDICAL DEVICES QUALITY MANAGEMENT SYSTEMS)
  - ISO 26000 (SOCIAL ACCOUNTABILITY MANAGEMENT SYSTEMS)

QUALITY ASIA

QUALITY ASIA

# Our Accreditation

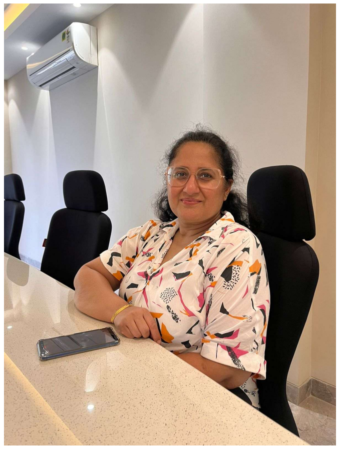
- At Quality Asia Certifications, our commitment to excellence is validated through our prestigious accreditations.
- We are proud to be recognized by leading national and international accreditation body, including **NABCB (National Accreditation Board for Certification Bodies), IAF Accredited** ensuring the highest standards of quality and compliance.
- Our accreditations reflect our rigorous adherence to industry standards and our dedication to providing reliable and trustworthy certification services. These credentials are a testament to our expertise and our unwavering commitment to delivering value to our clients.
- Proud BNI (Business Network International) Member

MEMBER OF MULTILATERAL IAF RECOGNITION ARRANGEMENT

NABCB
QM-085

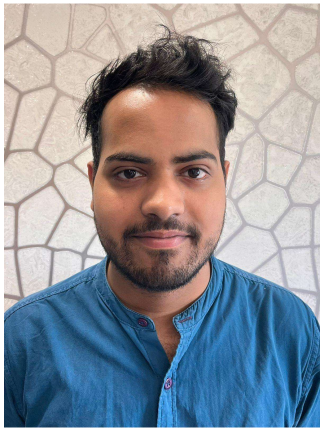
QUALITY ASIA

# LEADERSHIP TEAM

| |  | | |
|---|---|---|---|
| **Mr Atul Suri** | **Mrs. Seema Suri** | **Mr Samarth Suri** | **Ms Palak Ahuja** |
| **Lead Auditor & Reviewer** | **Director - Accreditations** | **Managing Director** | **GM - Certifications** |
| Responsible for Leading Teams of Auditors and Establishing Excellence in Auditing Operations | Responsible for Maintaining Accreditation Status and Heading Audit Review and Certification Decision Process | Responsible for Marketing & Promotions, and ensuring Right Visibility of the Certification Body | Responsible for Heading and Managing Certification and Operations and Ensuring Client Success through Certifications |

QUALITY ASIA

# CORE TEAM

| | | | |
|---|---|---|---|
| |  | | |
| **Mr Parveen Singh Negi** | **Mr Sagar Mahour** | **Team of Auditors** | **Team of Executives** |
| **Business Development Head** | **Quality Assurance Officer** | | |
| Responsible for Heading Sales Teams and Ensuring Customer Acquisition in the Most Ethically Right Manner | Responsible for compliance with accreditation standards, manages documentation and audits, assists in training programs, and supports marketing and operational excellence initiatives. | Responsible for Conducting Ethical and Quality Rich Audits, enabling Organizations to Understand and Upgrade their Systems and Processes | Responsible for Managing the Shows behind the scenes |

QUALITY ASIA

# Training Information and Evaluation

**Training Material** will be provided to you through mail.

**Training Evaluation**, a google form link is provided to you through mail.

**Training Feedback** is the part of the Training evaluation form, please provide your valuable feedback.

QUALITY ASIA

# Quality Asia School and Free Training program updates…

- **Quality Asia School: Explore comprehensive training programs on various ISO standards: [https://www.qualityasia.in/qasia-school.php](https://www.qualityasia.in/qasia-school.php)**

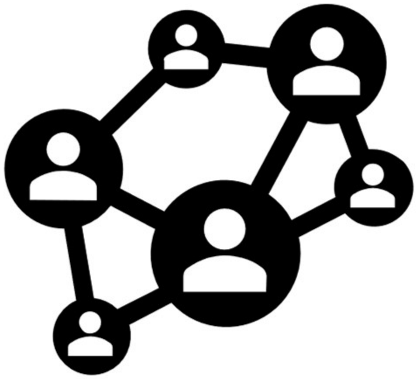
- **Join our WhatsApp channel for convenient access to live training sessions: [https://whatsapp.com/channel/0029VamtSmnJ93wcEDIsrT1Z](https://whatsapp.com/channel/0029VamtSmnJ93wcEDIsrT1Z)**

- **Free Internal Auditor Training Calendar: Explore upcoming training sessions on various ISO standards, including ISO 14001, on our website: [https://www.qualityasia.in/training-calendar.php](https://www.qualityasia.in/training-calendar.php)**

# Join us on…

QUALITY ASIA

- Follow and Connect with Quality Asia Certifications: Stay updated on our latest news and training programs by following us on Social media:
  - Instagram: https://www.instagram.com/qualityasia/
  - LinkedIn: https://www.linkedin.com/company/quality-asia/mycompany/
- Quality Asia YouTube Channel: Subscribe for insights and educational videos on ISO standards and auditing practices: https://www.youtube.com/@QualityAsia



# Thank You.