Free ISO 27701:2019 Internal Auditor Training

From Quality Asia Certifications Private Limited

QUALITY ASIA

Structure of the Course

- Introduction
- Revision and History
- Important Concepts
- Clause 1-3 Scope, Normative References, Terms, Definitions and abbreviations
- Clause 4 General
- Clause 5 PIMS-specific related requirement from ISO 27001
- Clause 6 PIMS-specific related guidance from ISO 27002
- Clause 7 Additional ISO 27002 guidance for PII Controllers
- Clause 8 Additional ISO 27002 guidance for PII Processors
- Impact on Organization and Auditors
- Internal Auditing

Objectives of the course

- Gain a clear understanding of the clauses and privacy controls of ISO/IEC 27701:2019.
- Interpret the requirements for PII Controllers and Processors in the organization's context.
- Understand how to assess the effectiveness of a PIMS in managing privacy risks.
- Learn internal auditing principles, techniques, and practices as per ISO 19011:2018 guidelines.
- Support the organization in strengthening its privacy compliance and continual improvement.

Trainer Introduction

- **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

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

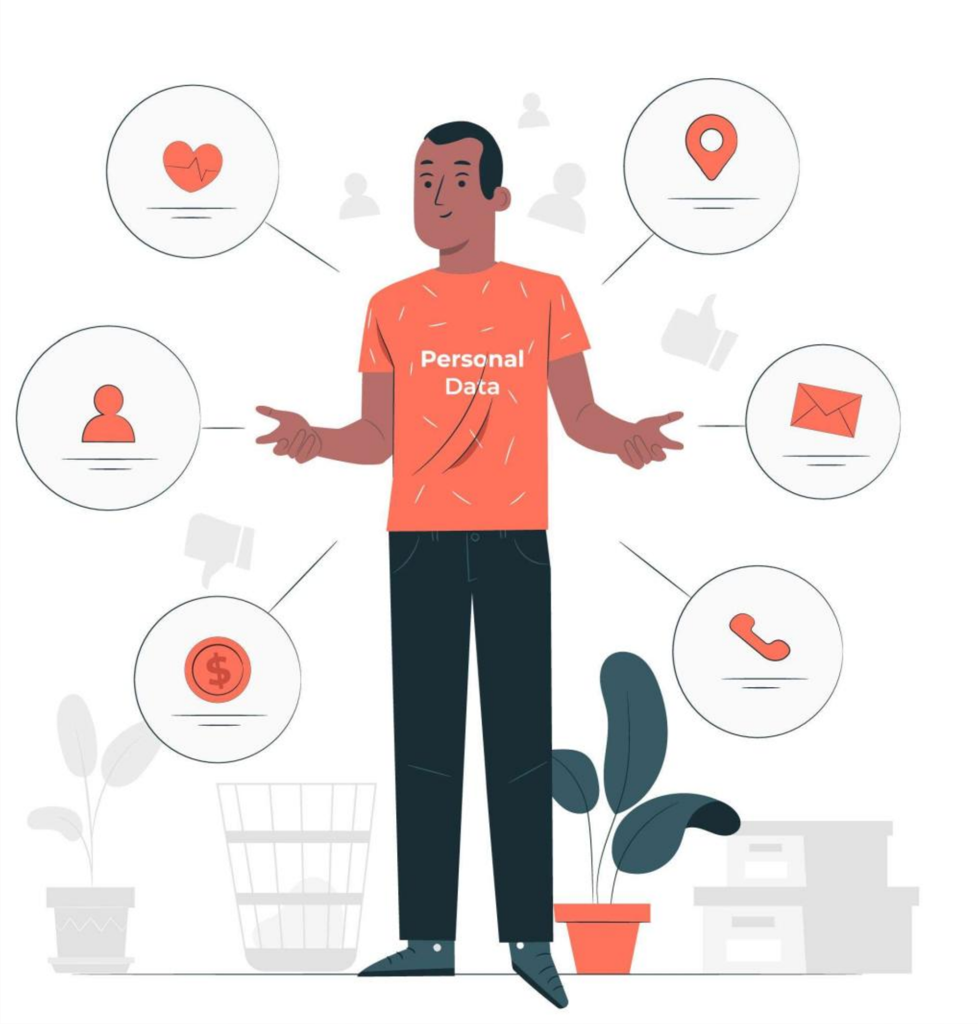
We offer a focused training session on a different ISO standard each month, ensuring continuous learning and up-to-date knowledge for your team.

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.



ISO/IEC 27701 Privacy Information Management System

About ISO/IEC 27701

About ISO/IEC 27701

- Requirements for a PIMS (Privacy Information Management System)
- Extension for privacy of ISO/IEC 27001
- For any organization (PII controller or processor)
- Aligned with the GDPR Other related standards: ISO/IEC 29100; ISO/IEC 29151; ISO/IEC 29134 ...

ISO/IEC 27701

Includes all requirements and controls (114) in ISO/IEC 27001 with some privacy additions

+

Controls for PII controllers and PII processors

- Section 1 - Introduction
- Section 2 – Overview of ISO/IEC 27001 requirements
- Section 3 – Overview of information security controls in ISO/IEC 27001
- **Section 4 – Controls for PII controllers**
- **Section 5 – Controls for PII processors**

Basic privacy elements

Actors (ISO/IEC 29100:2011)

PII principals

Persons who provide personal data for processing

PII controller

Determines the purpose and means of PII processing

PII processor

Carries out processing of PII on behalf of the controller and according to its instructions

Joint PII controller

PII controller that determines purpose and means of processing jointly with one or more PII controllers

PII Controller or PII Processor ?

- … not always easy to decide

- An organization can be both PII controller and PII processor
- ***but not for the same processing activity***

PII & PII Processing ?

PII Processing

- Operation or set of operations performed on personally identifiable information, that can be automated or not
- *(collection, recording, structuring, storage, alteration, retrieval, consultation, use, dissemination, combination, erasure, destruction)*

PII is...

- Acc. to ISO/IEC 29100: any information that (a) can be used to identify a PII principal to whom the information relates; or (b) is, or might be, directly or indirectly linked to a PII principal
- Acc. to the GDPR: any information relating to an identified or identifiable natural person

Overview of privacy principles

Consent & choice

The persons should have the choice whether to allow PII processing or not

Purpose, legitimacy and specification

The purpose of processing must comply with the law and be communicated to PII principals

Collection limitation

Data collected must be limited to what is strictly necessary for the purpose

Data minimization

Minimize PII processed and third parties with access to PII

Use, retention and disclosure limitation

PII used only for specified purpose, retained only as needed for purpose

Accuracy and quality

PII must be accurate, complete, up-to-date, adequate and relevant for purpose

Overview of privacy principles

Openness, transparency and notice

PII principals receive sufficient, clear and easy to access information

Individual participation and access

PII principals should be able to access and review PII, as permitted by the law

Accountability

The organization shall take the responsibility for the PII processing

Information security

There should be controls in place to protect the confidentiality, integrity and availability of data

Privacy compliance

Controls, audits, verifications to ensure PII processing meets requirements

Relationship with the GDPR

ISO/IEC 27701

International standard applicable regardless of jurisdiction

More general requirements that must be considered in the context of the local legislation

Its application if voluntary

GDPR

Applicable for organizations located in the EU and organizations from outside the EU that process personal data of EU citizens

Its application is mandatory

PII (Personally Identifiable Information	=	Personal data
PII Principal	=	Data subject
PII Controller/ Processor	=	Data Controller/ Processor

Major Data Protection Laws Related to PII

GDPR (General Data Protection Regulation) – European Union

- **Applies to:** Organizations processing data of EU residents (even outside EU)
- **Key Principles:**
  - Lawfulness, fairness, transparency
  - Purpose limitation, data minimization
  - Accuracy, storage limitation, integrity & confidentiality
- **Notable Requirements:**
  - Consent management
  - Data subject rights (access, rectification, erasure, portability)
  - DPO appointment (in certain cases)
  - Breach notification within 72 hours
  - Fines up to **€20 million or 4% of global turnover**

DPDP Act 2023 (Digital Personal Data Protection Act) – India

- **Applies to:** Personal data processing in India and offshore if related to Indian users
- **Key Provisions:**
  - Clear consent requirements
  - Data Fiduciary and Data Principal roles (similar to controller/principal)
  - Right to access, correction, and grievance redressal
  - Data Protection Board of India for enforcement
- **Penalty:** Up to **₹250 crore** for non-compliance

CCPA / CPRA – California, USA

- **Applies to:** Businesses with consumers in California meeting revenue or data threshold
- **Key Features:**
    - Right to know, delete, opt-out of sale
    - Introduced **Sensitive Personal Information** category
    - Data minimization and purpose limitation
    - Enforcement by California Privacy Protection Agency

Other Emerging & Notable Frameworks

- **LGPD (Brazil)** – Similar to GDPR, includes data protection officer, consent, data subject rights
- **PIPEDA (Canada)** – Privacy law for commercial organizations
- **PDPA (Singapore, Thailand, Malaysia)** – Sector-neutral, consent-based framework with enforcement

Introduction to the DPDP Act, 2023

- Enacted: **11th August 2023**, India
- Objective: To **protect personal data** of individuals and **regulate data processing** by Data Fiduciaries
- Applicability:
  - Applies to **digital personal data** in India
  - Also applies to **processing outside India** if it relates to goods/services to individuals in India
- The Digital Personal Data Protection (DPDP) Act, 2023 marks India's formal entry into the global landscape of modern data governance. Unlike previous regulations, it shifts the focus from mere compliance to accountability, placing clear obligations on businesses while empowering individuals with enforceable rights over their digital footprint. Understanding and adhering to the DPDP Act is crucial for all entities that handle personal data within India or process the data of Indian citizens, regardless of the geographical location.

Why a data protection act is needed in India

- With the rapid growth of digital technologies and online services, the collection and processing of personal data has become increasingly prevalent. Prior to the DPDP Act, India lacked a comprehensive privacy law. While the Supreme Court of India recognized the right to privacy as a constitutionally protected right in 2017, the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) had limitations.
- The DPDP Act aims to fill this crucial gap by providing a comprehensive legal framework for data protection in India. Furthermore, there was a lack of clarity regarding individuals' legal rights regarding their personal data and a lack of accountability for organizations processing this data. The DPDP Act establishes the Data Protection Board of India (DPB) to enforce the law and hold organizations accountable, thereby empowering individuals with greater control over their personal data.

Status, applicability, and scope of the DPDP Act

- The DPDP Act applies to the processing of digital personal data within India where the data is collected online or offline and is subsequently digitized. It also has extraterritorial application, extending to the processing of digital personal data outside of India if such processing is related to offering goods or services to individuals within India. This means organizations based outside India but targeting the Indian market will also need to comply with the DPDP Act.

Exclusions from the DPDP Act

- **Personal or Domestic Use -** Data processed by individuals for personal or household purposes (e.g., phone contacts, home videos).
- **Non-Automated / Manual Data -** Offline records not digitized or processed by automated means.
- **Publicly Available Personal Data -** Data made public by the Data Principal or under a legal obligation.
- **Offline Personal Data -** Physical records not intended to be digitized (e.g., handwritten forms stored in files).
- **Law Enforcement / National Security -** Exempt for data processed under sovereign or legal obligations.
- **Journalistic, Literary, or Artistic Purposes -** Content created for freedom of expression in media and art.

Key principles and definitions

Key principles	Explanation
Lawfulness	This principle dictates that personal data must be processed in a manner that is lawful, fair, and transparent to the individuals concerned. This implies that processing must have a legal basis, be conducted in good faith, and provide individuals with clear information about how their data is being handled.
Purpose Limitation	This principle mandates that personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those original purposes. This means that organizations must clearly define why they are collecting personal data and can only use it for those stated reasons, unless a new purpose is compatible with the original purpose.
Data Minimization	This principle emphasizes that personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. Organizations should only collect and retain the personal data that is strictly required to fulfill the specified purposes.

Key principles and definitions

Key principles	Explanation
Accuracy	This principle requires that personal data is accurate and kept up to date where necessary. Data Fiduciaries have an obligation to make reasonable efforts to ensure the accuracy and completeness of personal data.
Storage limitation	This principle stipulates that personal data should be retained only as long as necessary to fulfill the purposes for which it was processed. Data Fiduciaries must erase personal data when the Data Principal withdraws consent or when it is reasonable to assume the specified purpose is no longer being served, unless retention is necessary for compliance with any law. For government entities, storage limitation may not always apply.
Integrity and Confidentiality	This principle necessitates that personal data is processed in a manner that ensures appropriate security, protecting against unauthorized or unlawful processing, accidental loss, destruction, or damage through suitable technical and organizational measures. Data Fiduciaries are responsible for implementing reasonable security safeguards to prevent personal data breaches.

Key definitions of the DPDP Act

Term	Definition
Personal Data	Any data about an individual who is identifiable, directly or indirectly (e.g., name, phone, address, location, ID, employee codes).
Digital Personal Data	Personal data in digital form, whether originally collected digitally or digitized later.
Data Principal	The individual to whom personal data relates, including parents/guardians in the case of children or differently abled persons.
Processing	Any operation on personal data—collection, recording, storage, sharing, erasure—performed through automated or partly automated means.
Data Fiduciary	Any entity that determines the purpose and means of processing. Must issue notices, obtain consent, ensure accuracy/security, and report breaches.
Data Processor	An entity that processes personal data on behalf of a Data Fiduciary, under its instructions.
Significant Data Fiduciary (SDF)	Designated by the Central Government based on sensitivity/volume of data. Must appoint: - Data Protection Officer (DPO) in India - Independent data auditor - Conduct DPIAs
Consent Manager	A registered entity that helps Data Principals give, manage, and withdraw consent across platforms.
Personal Data Breach	Any unauthorized access, processing, loss, or disclosure of personal data that affects its confidentiality, integrity, or availability. Must be reported to DPB and affected individuals.

Obligations of Data Fiduciaries under the DPDP Act

- **Lawful Processing of Personal Data**
  - Must process data **only for lawful purposes**
  - Consent-based or for **legitimate uses** such as:
    - Voluntary data sharing by the individual
    - Public interest, medical emergencies, employment, licenses, etc.
- **Providing Notice**
  - **Clear, concise, and accessible notice** before collection
  - Must include:
    - What data is collected
    - Purpose of collection
    - Data Principal rights
    - Language: English + any of the 22 scheduled languages (as per user choice)
- **Obtaining Valid Consent**
  - Must be **explicit, informed, and verifiable**
  - Children (<18 yrs): **Parental/legal guardian consent** required
  - **Deemed consent** in limited scenarios (legal obligation, vital interest, etc.)

Obligations of Data Fiduciaries under the DPDP Act

- **Right to Withdraw Consent**
  - Data Principals can withdraw consent **anytime**
  - Fiduciaries must provide **simple opt-out mechanisms**
- **Cessation of Processing**
  - Processing must **stop** post consent withdrawal unless:
    - Required by law
    - Covered under a legal exemption
- **Security Safeguards**
  - Must implement **reasonable security measures**
  - Prevent:
    - Unauthorized access
    - Disclosure, destruction, or breach
  - Include audits, encryption, and breach preparedness
- **Data Breach Notification**
  - **Immediate intimation** to:
    - **Data Protection Board**
    - **Affected individuals**

Obligations of Data Fiduciaries under the DPDP Act

- **Erasure of Personal Data**
  - Data must be deleted:
    - After purpose is fulfilled
    - Or on consent withdrawal
- **Exemptions** apply (e.g., legal retention by govt.)
  - **Grievance Redressal Contact Info**
  - Publish contact details for Data Principals to raise concerns
- **Grievance Redressal Mechanism**
  - Set up **responsive grievance systems**
  - Expected turnaround: **7 days** (or as per future rules)
- **Children’s & Disability Data Handling**
  - No **behavioral tracking** or **targeted ads**
  - Consent through lawful guardian is mandatory

QUALITY ASIA

Additional Obligations for Significant Data Fiduciaries (SDFs)

- **SDF Status: Assigned based on:**
  - Volume/sensitivity of data
  - Risk to Data Principal rights
  - Impact on national interest or sovereignty
- **Extra Obligations:**
  - Appoint a **DPO based in India**
  - Appoint an **Independent Data Auditor**
  - Conduct **Periodic DPIAs** (Data Protection Impact Assessments)
- **Goal:** Greater accountability for high-risk entities

Rights of Data Principals under the DPDP Act

Rights	Explanation
Right to Access Information	• Know what personal data is being collected, the **purpose**, and with whom it is being shared. • Right to receive **clear and comprehensive notice** before data collection. • Data Fiduciaries must explain **how the data is processed**.
Right to Correction and Erasure	• Request correction of inaccurate or incomplete data. • Request deletion of data when the purpose is fulfilled or consent is withdrawn. • Includes the "right to be forgotten", limiting future disclosure or processing.
Right to Nomination	• Appoint another person to exercise rights **in case of death or incapacity**. • Ensures data rights are protected beyond the individual's direct control.

Rights of Data Principals under the DPDP Act

Rights	Explanation
Right to Grievance Redressal	• File complaints with the Data Protection Board of India (DPB). • Data Fiduciaries must: • Provide grievance contact details • Respond within 7 days or less
Right to Object	• Object to data processing under specific circumstances. • Data Fiduciaries must respect objections unless legitimate overriding grounds exist.
Right to Be Forgotten	• Covered under erasure rights. • Individuals can limit the disclosure of their personal data once it's no longer necessary or consent is withdrawn.
Right to data portability	• Earlier drafts included this right, but it is not part of the final Act. • No legal provision allows Data Principals to transfer their personal data between services.

Understanding the Role of DPIAs (Data Protection Impact Assessments)

What is a DPIA?

- A Data Protection Impact Assessment is a process to identify and assess privacy risks to individuals' personal data.
- Mandated for Significant Data Fiduciaries (SDFs) under the DPDP Act.
- Considered a best practice for any high-risk data processing activity.

When is a DPIA Needed?

- Use of new technologies
- Large-scale processing of sensitive data
- Activities that may result in discrimination or harm
- Processing that poses a high risk to the rights/freedoms of Data Principals

Steps to Conduct a DPIA

- **Describe the Processing Operation**
  - Detail the nature, scope, purpose, and context of personal data use.
  - Include what data is collected, how long it’s retained, and who accesses it.
- **Assess Necessity & Proportionality**
  - Is the data relevant, adequate, and not excessive?
  - Aligns with the principle of data minimization.
- **Identify Risks to Data Principals**
  - Analyze potential impacts on confidentiality, integrity, or availability.
  - Evaluate likelihood and severity of harm.
- **Mitigate or Manage the Risks**
  - Define measures to eliminate or reduce privacy risks.
  - Document risk mitigation, acceptance, or transfer decisions.

Managing Consent under the DPDP Act

- **Valid Consent must be:**
    - Free, specific, informed, unconditional, and unambiguous
    - Provided through a clear affirmative action
- **Pre-Consent Notice:**
    - Organizations must give clear, accessible privacy notices before collecting data
    - Notices must include:
        - What data is being collected
        - Purpose of use
        - How to exercise rights and file complaints
- **Blanket Consent Not Allowed:**
    - Consent must be purpose-specific
    - No bundled or generalized consent for multiple uses
- **Consent Withdrawal:**
    - Must be as easy as giving consent
    - Organizations must:
        - Record consent details
        - Allow simple opt-out
        - Track withdrawals

Managing Consent under the DPDP Act

- **Re-evaluation of Data Practices:**
  - Review and realign data collection and processing activities with consent principles
- **Timely Rights Fulfillment:**
  - Ensure clear procedures and timely responses to requests for access, correction, and erasure
- **Access Requests:**
  - Verify identity of Data Principal
  - Provide:
    - Summary of data being processed
    - Processing purposes and activities
    - Recipients of the data

Managing Consent under the DPDP Act

- Correction Requests:
  - Allow Data Principals to request:
    - Rectification of inaccurate/misleading data
    - Completion or updating of data
- Erasure Requests:
  - Must delete personal data upon withdrawal of consent
  - Retain only if legally required
- Set up dedicated channels, trained staff, and identity verification processes
- Maintain clear records to support compliance and timely resolution of Data Principal requests

Data Protection Board of India

- Independent body for enforcement
- Can:
  - **Receive complaints**
  - Conduct **inquiries and investigations**
  - Impose **penalties** (up to ₹250 crore per instance)
- Also oversees **voluntary undertakings**

Penalties Under the DPDP Act

- Breach of obligations: up to ₹250 crore
- Failure to report breach: ₹200 crore
- Failure to safeguard children's data: ₹50 crore
- Non-compliance with Data Principal rights: ₹10,000 (individuals)

Benefits of implementing ISO/IEC 27701

- Reduces complexity
- Generates documentary evidence
- Tailored to PII controllers and processors
- Maps to GDPR and various frameworks
- Provides assurance and confidence

Key terms and alternative terms

Terms as used in ISO/IEC 27701	Alternative term
Privacy information management system (PIMS)	Personal information management system (PIMS)
Personally identifiable information (PII)	Personal data
PII principal	Data subject
Privacy by design	Data protection by design
Privacy by default	Data protection by default
PII controller	Controller
PII processor	Processor

Key terms & Definitions

Term	Definition
Personally identifiable information (PII)	any information that (a) can be used to establish a **link between the information and the natural person** to whom such information relates, or (b) is or can be **directly or indirectly linked to a natural person**
Privacy information management system (PIMS)	information security management system which addresses the protection of privacy as potentially affected by the processing of PII
PII principal	natural person to whom the personally identifiable information (PII) relates
PII controller	privacy stakeholder (or privacy stakeholders) that **determines the purposes and means for processing personally identifiable information (PII)** other than natural persons who use data for personal purposes

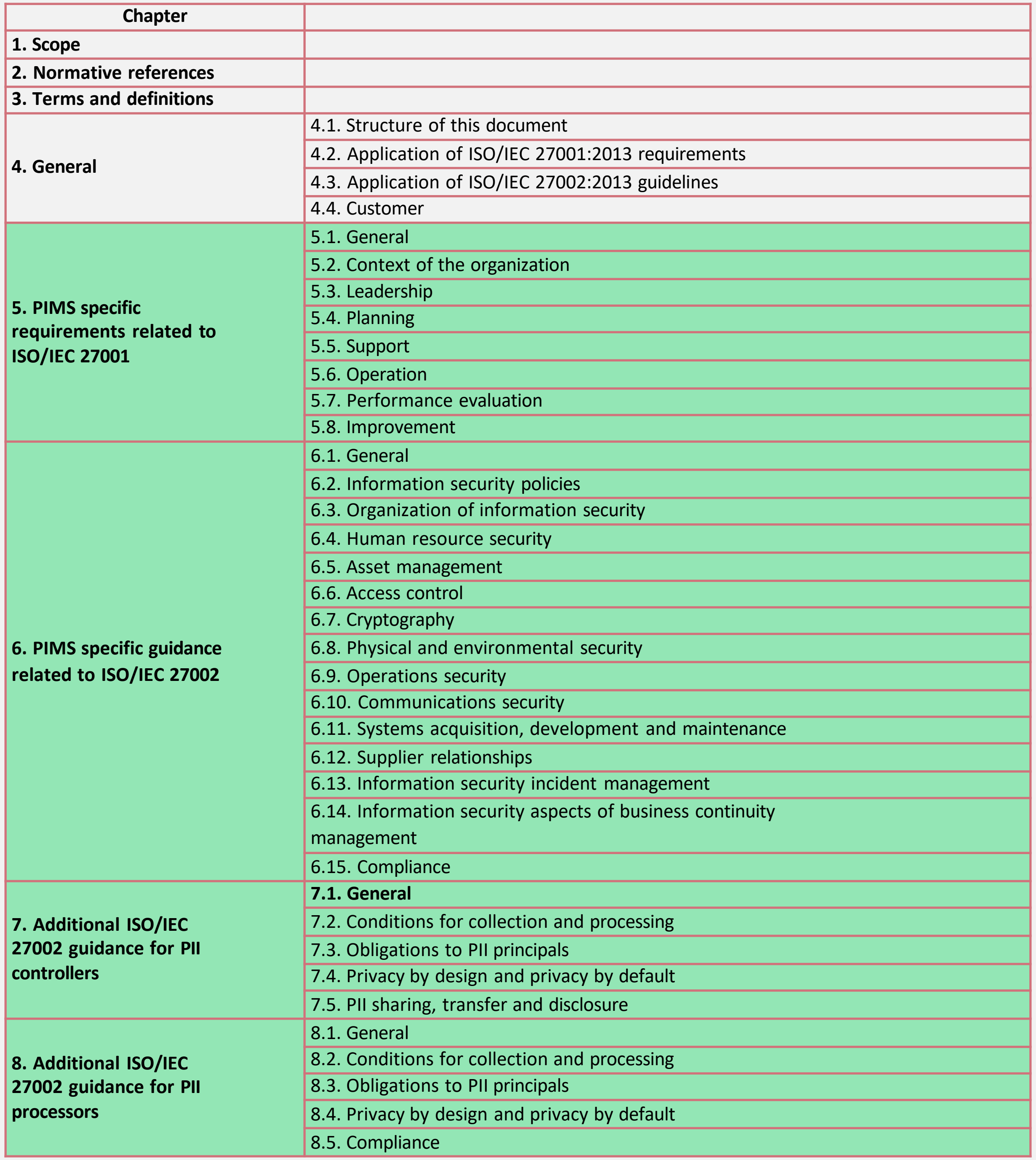
Key terms & Definitions

Term	Definition
PII processor	privacy stakeholder that **processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller**
privacy risk	effect of uncertainty on privacy
privacy impact assessment (PIA) privacy risk assessment	overall process of identifying, analyzing, evaluating, consulting, communicating and planning the treatment of **potential privacy impacts** with regard to the processing of **personally identifiable information**, framed within an **organization's broader risk management framework**

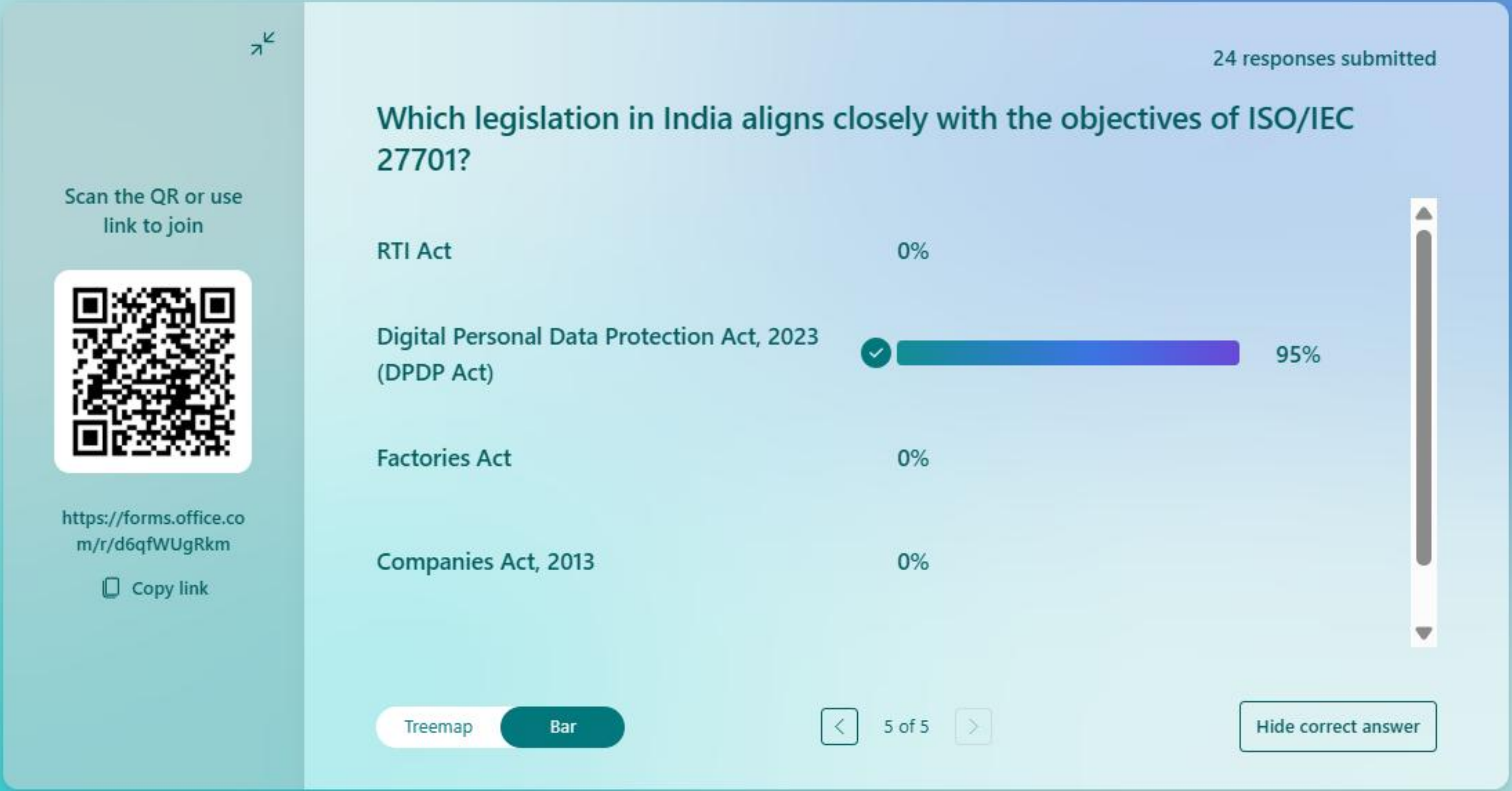
PIMS Plan, Do, Check, Act cycle

PLAN
DO
Continual
Improvement
ACT
CHECK

The structure of ISO/IEC 27701



Chapter	
1. Scope	
2. Normative references	
3. Terms and definitions	
4. General	4.1. Structure of this document
	4.2. Application of ISO/IEC 27001:2013 requirements
	4.3. Application of ISO/IEC 27002:2013 guidelines
	4.4. Customer
5. PIMS specific requirements related to ISO/IEC 27001	5.1. General
	5.2. Context of the organization
	5.3. Leadership
	5.4. Planning
	5.5. Support
	5.6. Operation
	5.7. Performance evaluation
	5.8. Improvement
6. PIMS specific guidance related to ISO/IEC 27002	6.1. General
	6.2. Information security policies
	6.3. Organization of information security
	6.4. Human resource security
	6.5. Asset management
	6.6. Access control
	6.7. Cryptography
	6.8. Physical and environmental security
	6.9. Operations security
	6.10. Communications security
	6.11. Systems acquisition, development and maintenance
	6.12. Supplier relationships
	6.13. Information security incident management
	6.14. Information security aspects of business continuity management
	6.15. Compliance
7. Additional ISO/IEC 27002 guidance for PII controllers	**7.1. General**
	7.2. Conditions for collection and processing
	7.3. Obligations to PII principals
	7.4. Privacy by design and privacy by default
	7.5. PII sharing, transfer and disclosure
8. Additional ISO/IEC 27002 guidance for PII processors	8.1. General
	8.2. Conditions for collection and processing
	8.3. Obligations to PII principals
	8.4. Privacy by design and privacy by default
	8.5. Compliance



Scan the QR or use link to join

https://forms.office.com/r/d6qfWUgRkm

24 responses submitted

Which legislation in India aligns closely with the objectives of ISO/IEC 27701?

RTI Act		0%
Digital Personal Data Protection Act, 2023 (DPDP Act)	✓	95%
Factories Act		0%
Companies Act, 2013		0%

Clause 4 - General

Clause No.	Clause Name
4.1.	Structure of the document
4.2.	Application of ISO/IEC 27001:2013 requirements
4.3.	Application of ISO/IEC 27002:2013 guidelines
4.4.	Customer

4.1. Structure of this document

- This standard extends ISO/IEC 27001 and ISO/IEC 27002 to include privacy management, focusing on the protection of Personally Identifiable Information (PII).
- Clause 5 and 6 provide PIMS-specific requirements and guidance aligned with ISO/IEC 27001 and 27002, respectively.
- Clause 7 and 8 introduce additional controls for PII controllers and PII processors.
- Annexes A–B list specific control objectives; C–F provide mappings to related standards like ISO 29100, GDPR, ISO 27018.
- This structure enables seamless integration of privacy into existing ISMS frameworks.

4.2. Application of ISO/IEC 27001:2013 requirements

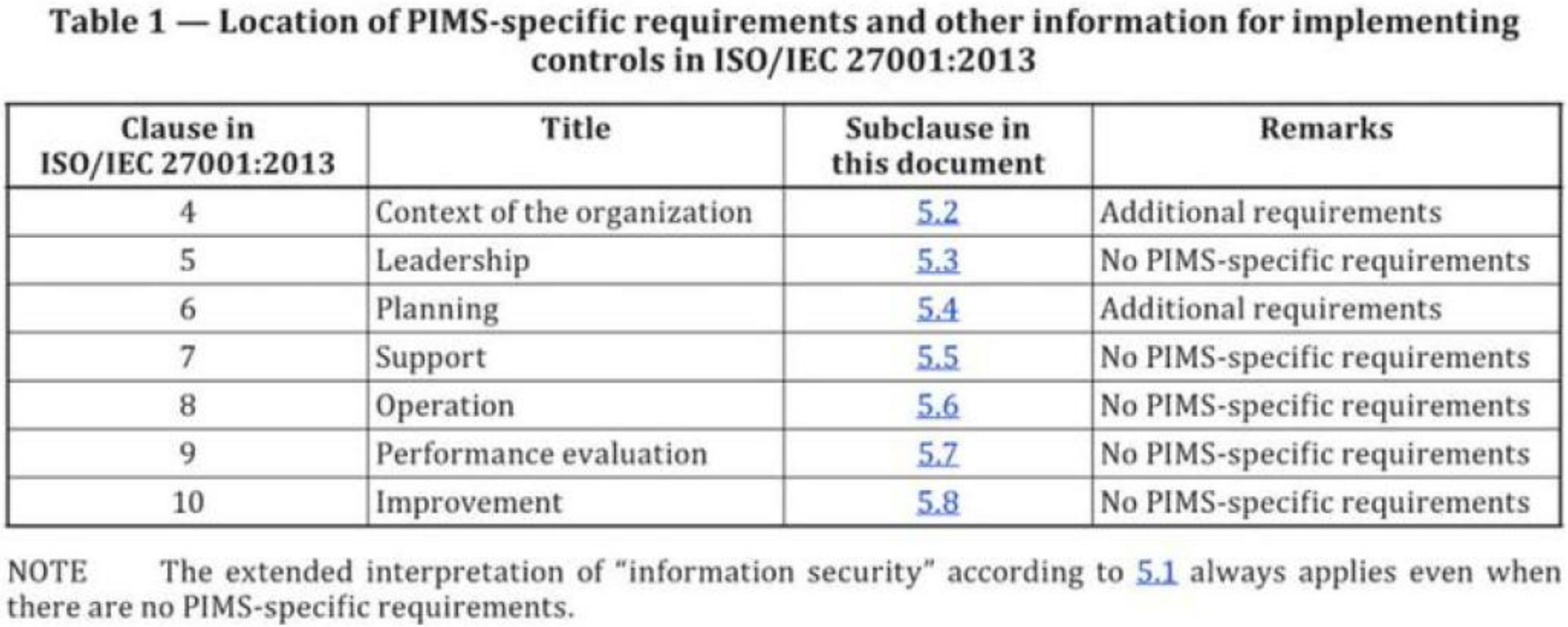


Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

4.3. Application of ISO/IEC 27002:2013 guidelines

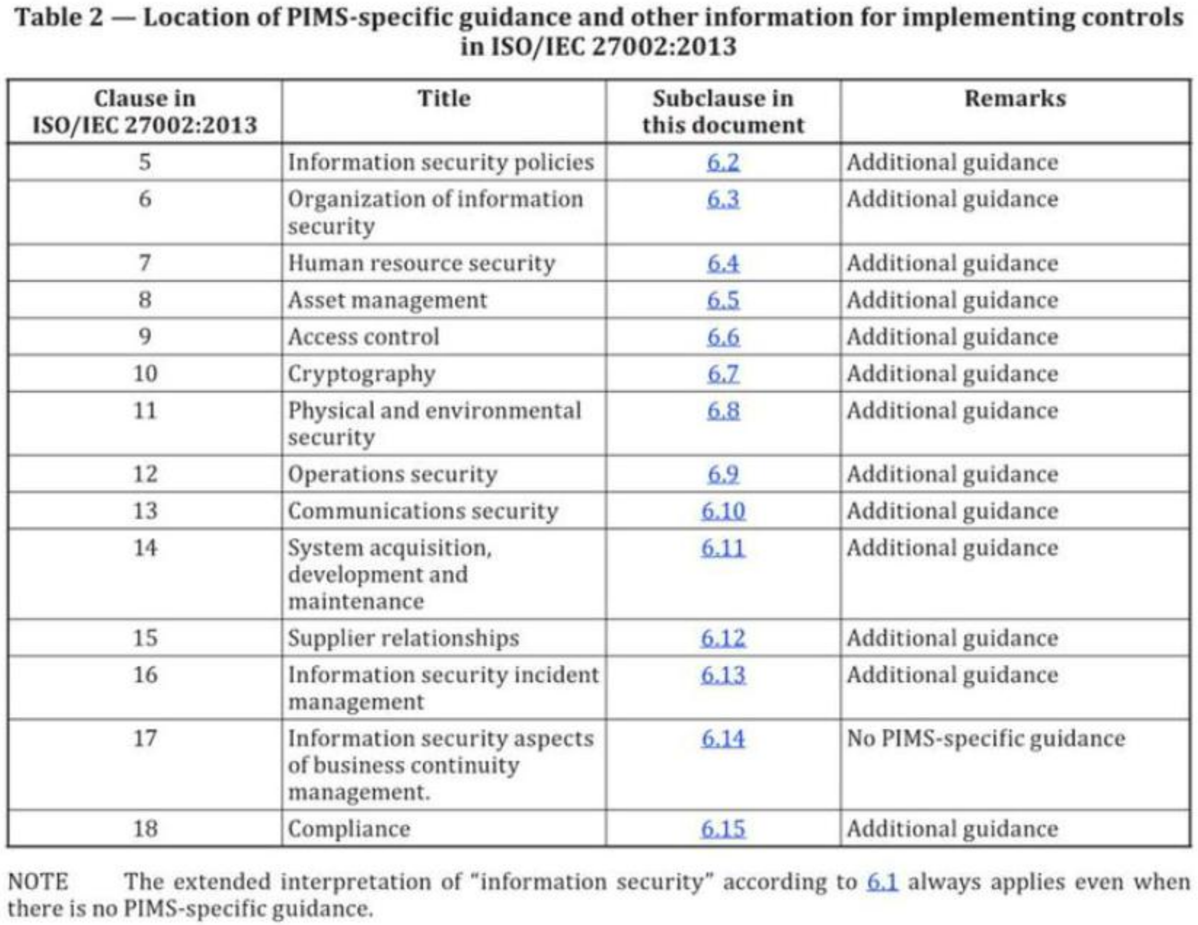


Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013

Clause in ISO/IEC 27002:2013	Title	Subclause in this document	Remarks
5	Information security policies	6.2	Additional guidance
6	Organization of information security	6.3	Additional guidance
7	Human resource security	6.4	Additional guidance
8	Asset management	6.5	Additional guidance
9	Access control	6.6	Additional guidance
10	Cryptography	6.7	Additional guidance
11	Physical and environmental security	6.8	Additional guidance
12	Operations security	6.9	Additional guidance
13	Communications security	6.10	Additional guidance
14	System acquisition, development and maintenance	6.11	Additional guidance
15	Supplier relationships	6.12	Additional guidance
16	Information security incident management	6.13	Additional guidance
17	Information security aspects of business continuity management.	6.14	No PIMS-specific guidance
18	Compliance	6.15	Additional guidance

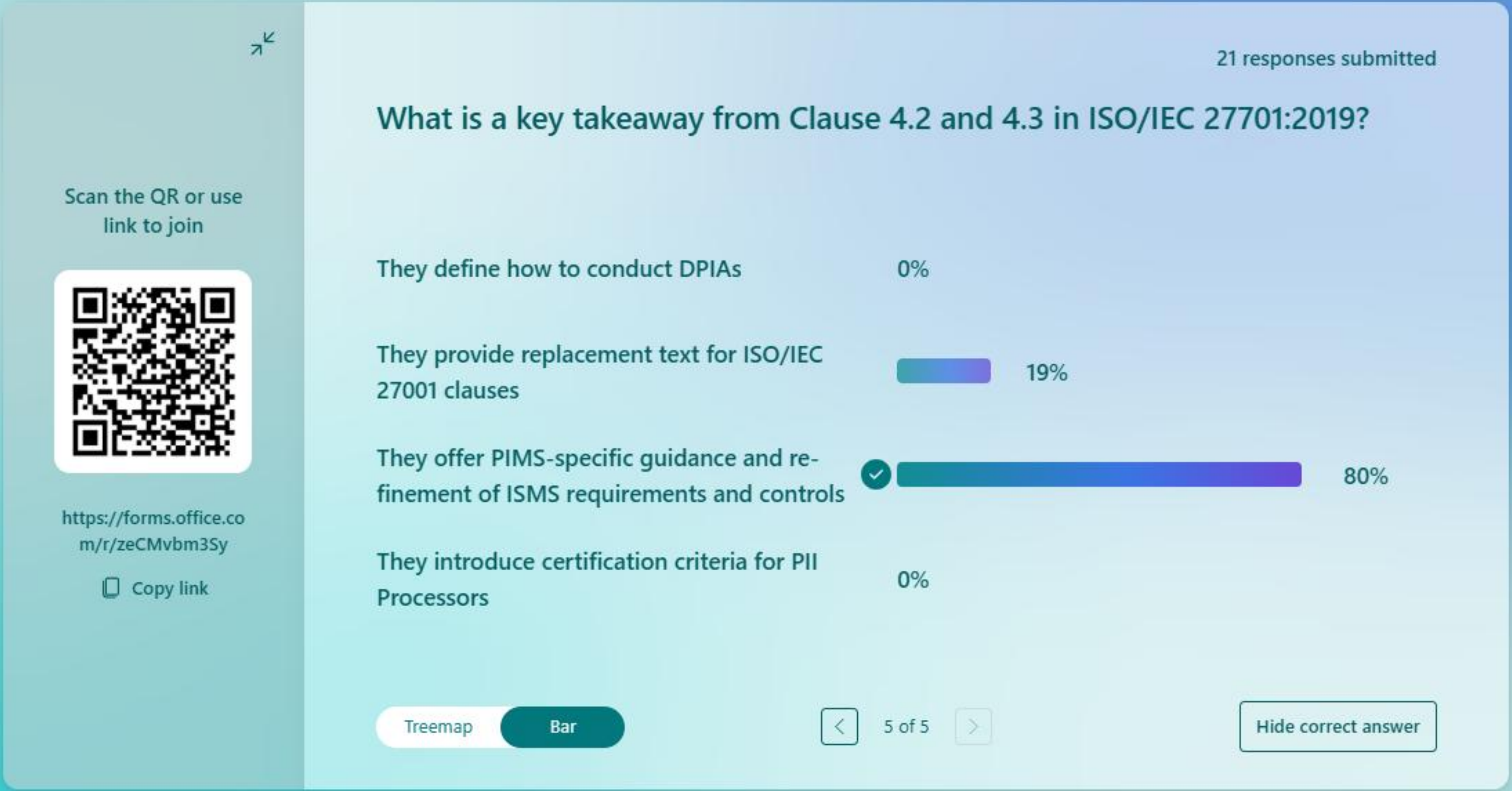
NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

4.4. Customer

- The term **"customer"** is contextual and depends on the role of the organization in the PII processing chain.

Types of Customers:

- **(a)** An organization with a contract with a **PII controller** *(e.g., the end customer of the controller; can also be a joint controller)*
- **(b)** A **PII controller** with a contract with a **PII processor** *(e.g., customer of the processor)*
- **(c)** A **PII processor** contracting a **PII sub-processor** *(e.g., customer of the sub-processor)*



Scan the QR or use link to join

https://forms.office.com/r/zeCMvbm3Sy

21 responses submitted

What is a key takeaway from Clause 4.2 and 4.3 in ISO/IEC 27701:2019?

They define how to conduct DPIAs		0%
They provide replacement text for ISO/IEC 27001 clauses		19%
They offer PIMS-specific guidance and refinement of ISMS requirements and controls	✓	80%
They introduce certification criteria for PII Processors		0%

Clause 5 - PIMS specific requirements related to ISO/IEC 27001

Clause No.	Clause Name
5.1.	General
5.2.	Context of the organization
5.3.	Leadership
5.4.	Planning
5.5.	Support
5.6.	Operation
5.7.	Performance evaluation
5.8.	Improvement

5.1. General

- The term **"information security"** in ISO/IEC 27001:2013 must be **extended to include privacy protection** — specifically the protection of **Personally Identifiable Information (PII)**.
- All controls and requirements in ISO/IEC 27001 should be applied with a **dual focus**:
  - **Information Security**
  - **Privacy of PII subjects**
- Wherever **"information security"** appears in ISO 27001, read it as: **"Information Security and Privacy"**

5.2. Context of the organization

- The organization must determine its role:
  - As a **PII Controller**, **Joint PII Controller**, and/or **PII Processor**.
- Identification of **external and internal issues** relevant to the purpose of the organization and its PIMS (Privacy Information Management System)
- Examples of Relevant Factors
  - Applicable privacy legislation
  - Relevant regulations and judicial decisions
  - Internal governance, policies, and procedures
  - Administrative and contractual requirements
- If the organization acts as both controller and processor, each role must be evaluated separately with distinct controls.

5.2. Context of the organization

The organization must **identify interested parties** that have:

- Interests or responsibilities in relation to **PII processing**
- This includes **PII principals** (data subjects)

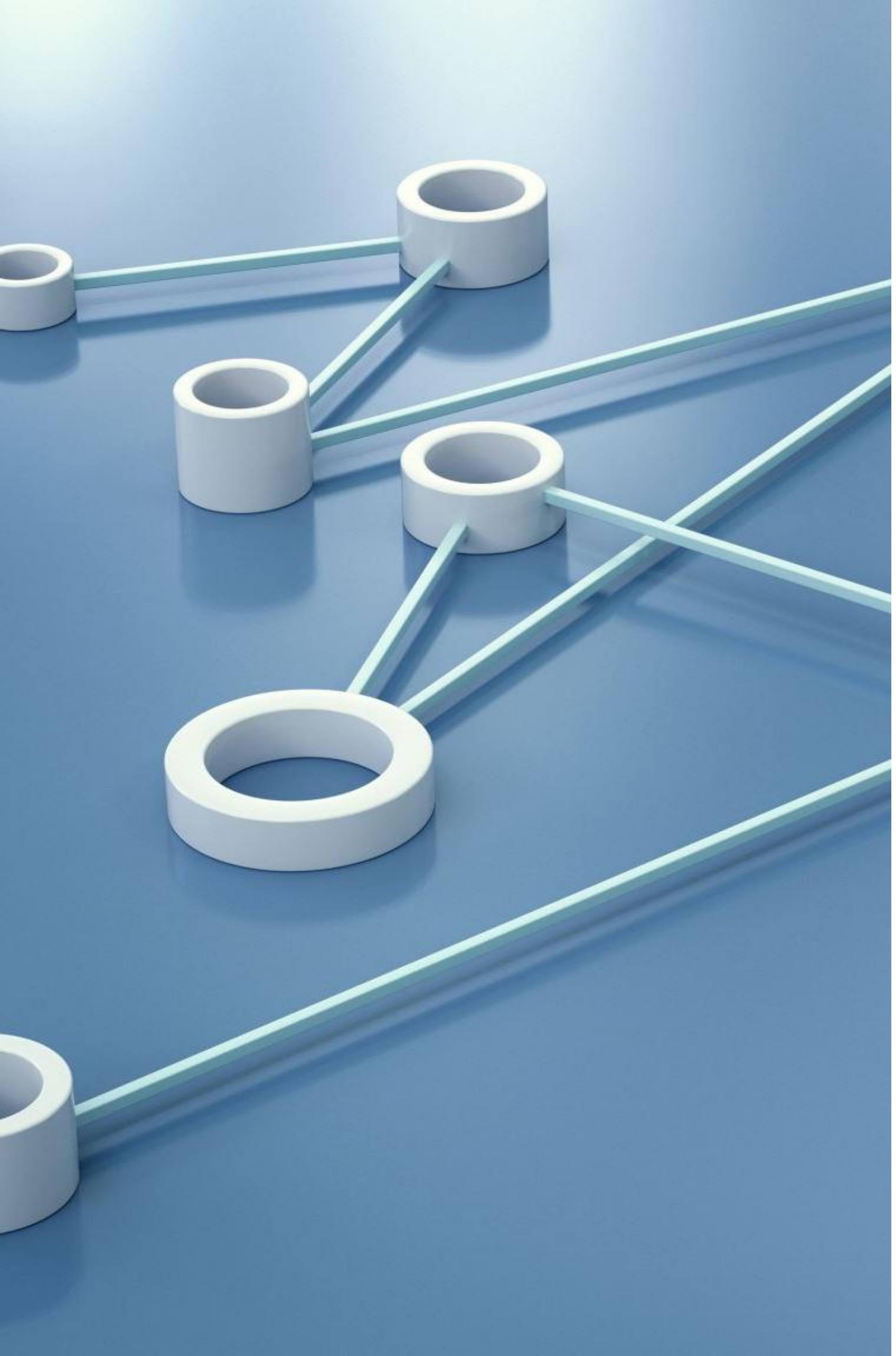
Examples of Interested Parties

- Customers (see Cl. 4.4)
- Supervisory authorities
- Other PII controllers
- PII processors and subcontractors

5.2. Context of the organization

When defining the **scope of the PIMS**, the organization must ensure it:

- **Includes the processing of PII** (Personally Identifiable Information)



5.2. Context of the organization

- **Establish, implement, maintain, and continually improve** a **Privacy Information Management System (PIMS)**

5.3. Leadership

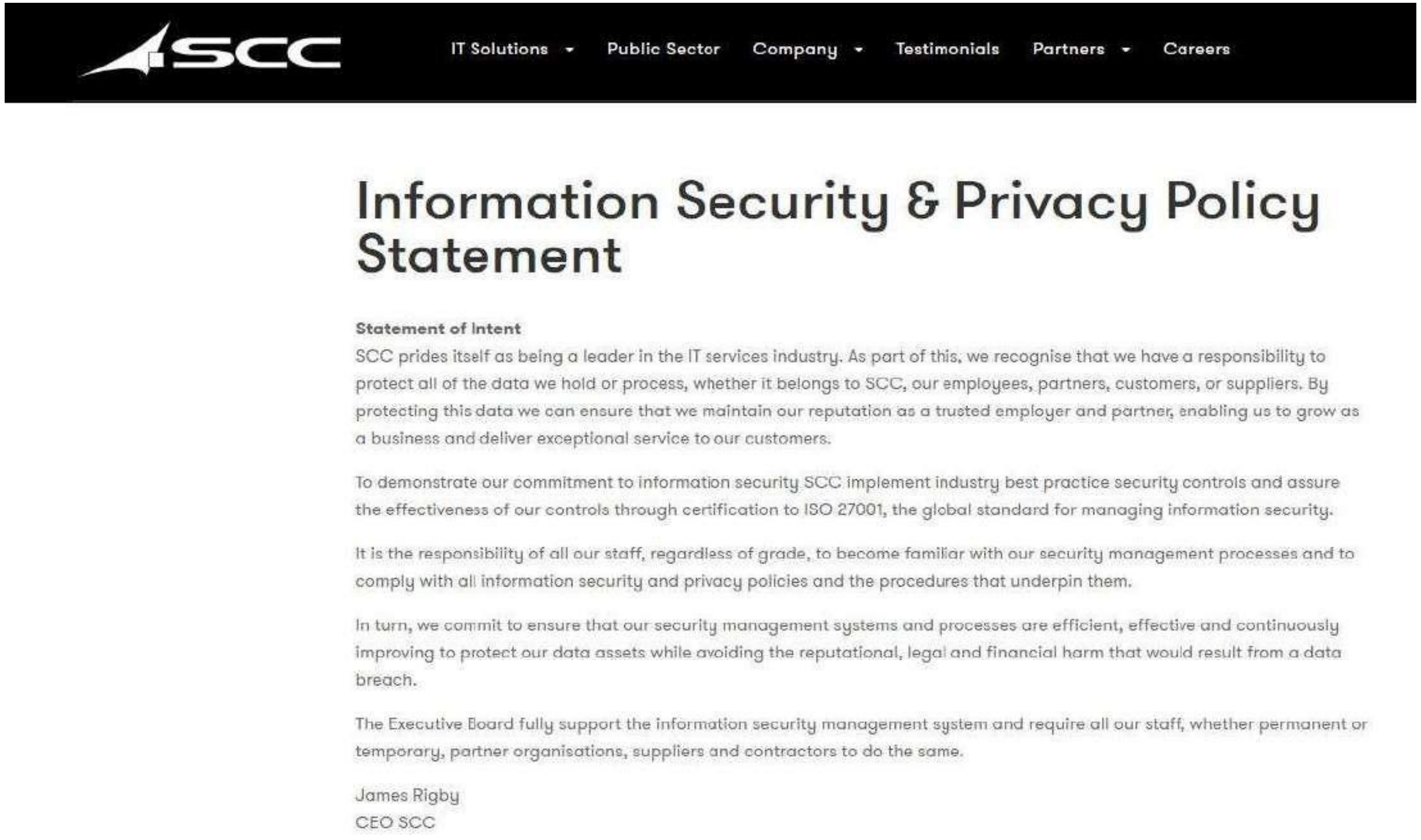
- No specific privacy additions, the requirements of ISO/IEC 27001 apply
- The top management of the organization must show support for the management system

QUALITY ASIA

Policy on information security and privacy

- Written
- Communicated
- Available to interested parties (as appropriate)

Sample Policy



Information Security & Privacy Policy Statement

Statement of Intent

SCC prides itself as being a leader in the IT services industry. As part of this, we recognise that we have a responsibility to protect all of the data we hold or process, whether it belongs to SCC, our employees, partners, customers, or suppliers. By protecting this data we can ensure that we maintain our reputation as a trusted employer and partner, enabling us to grow as a business and deliver exceptional service to our customers.

To demonstrate our commitment to information security SCC implement industry best practice security controls and assure the effectiveness of our controls through certification to ISO 27001, the global standard for managing information security.

It is the responsibility of all our staff, regardless of grade, to become familiar with our security management processes and to comply with all information security and privacy policies and the procedures that underpin them.

In turn, we commit to ensure that our security management systems and processes are efficient, effective and continuously improving to protect our data assets while avoiding the reputational, legal and financial harm that would result from a data breach.

The Executive Board fully support the information security management system and require all our staff, whether permanent or temporary, partner organisations, suppliers and contractors to do the same.

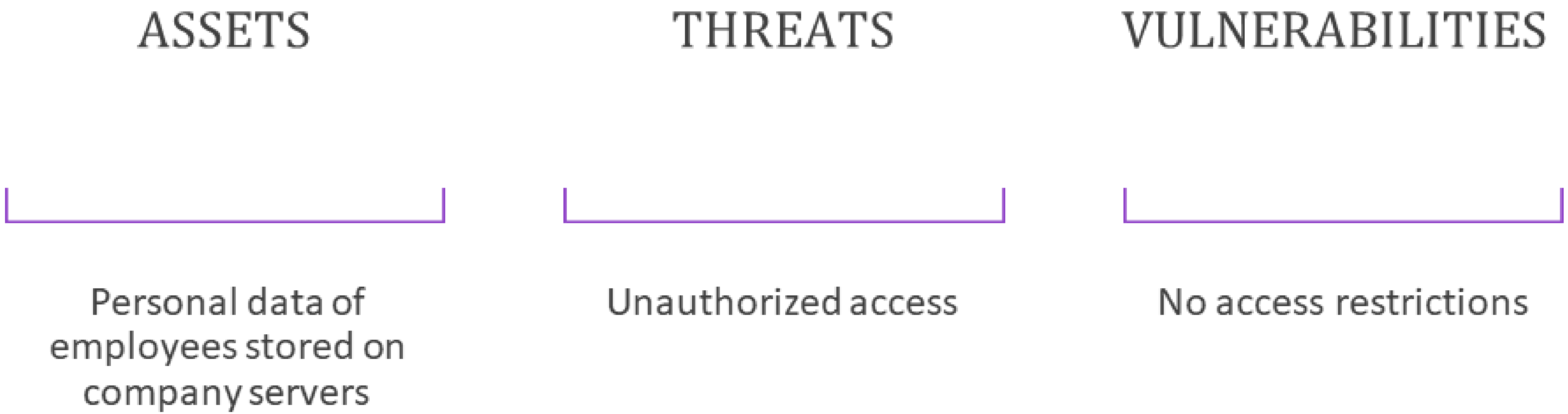
James Rigby
CEO SCC

Organization roles, responsibilities and authorities

- No specific privacy additions, the requirements of ISO/IEC 27001 apply
- Responsible to ensure that the management system conforms to requirements
- **DPO (Data Protection Officer)** – required by the GDPR in certain circumstances.

5.4. Planning - Risk assessment and treatment

- The organization shall define and apply a risk assessment process (including risks related to PII processing)



ASSETS	THREATS	VULNERABILITIES
Personal data of employees stored on company servers	Unauthorized access	No access restrictions

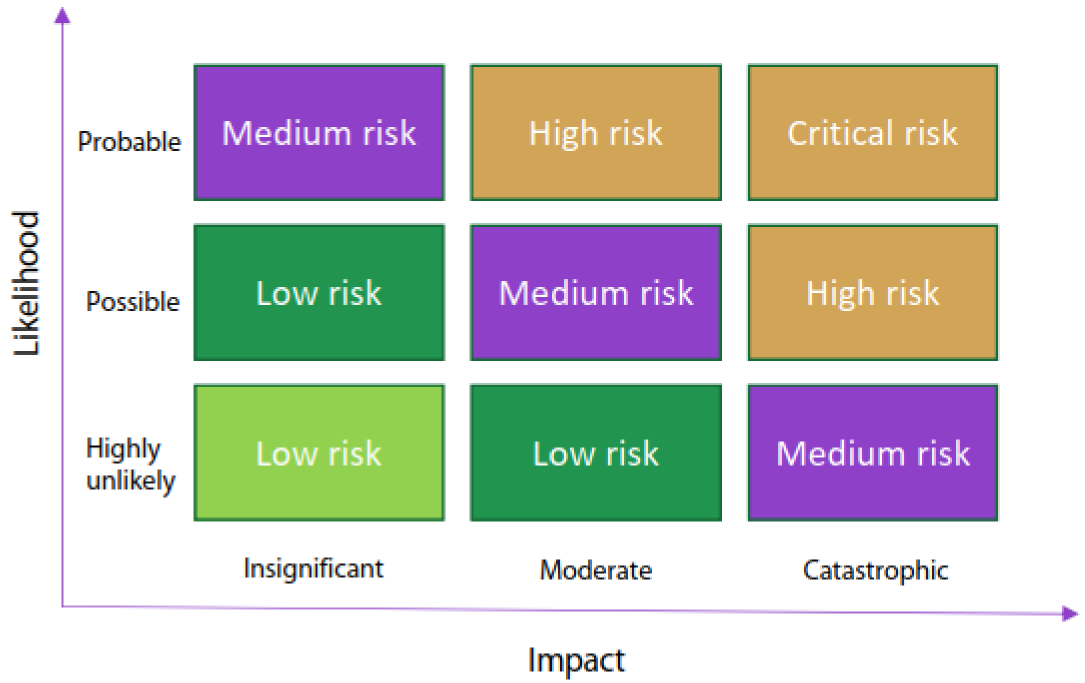
Information Security Risk Assessment

Organizations must:

- Use **information security risk assessment** for confidentiality, integrity, and availability.
- Apply **privacy risk assessment** for risks to **PII processing**.
- Ensure both types of risks are **consistently managed** and **interlinked**.
- Assess consequences for **both the organization and PII principals** if risks materialize.

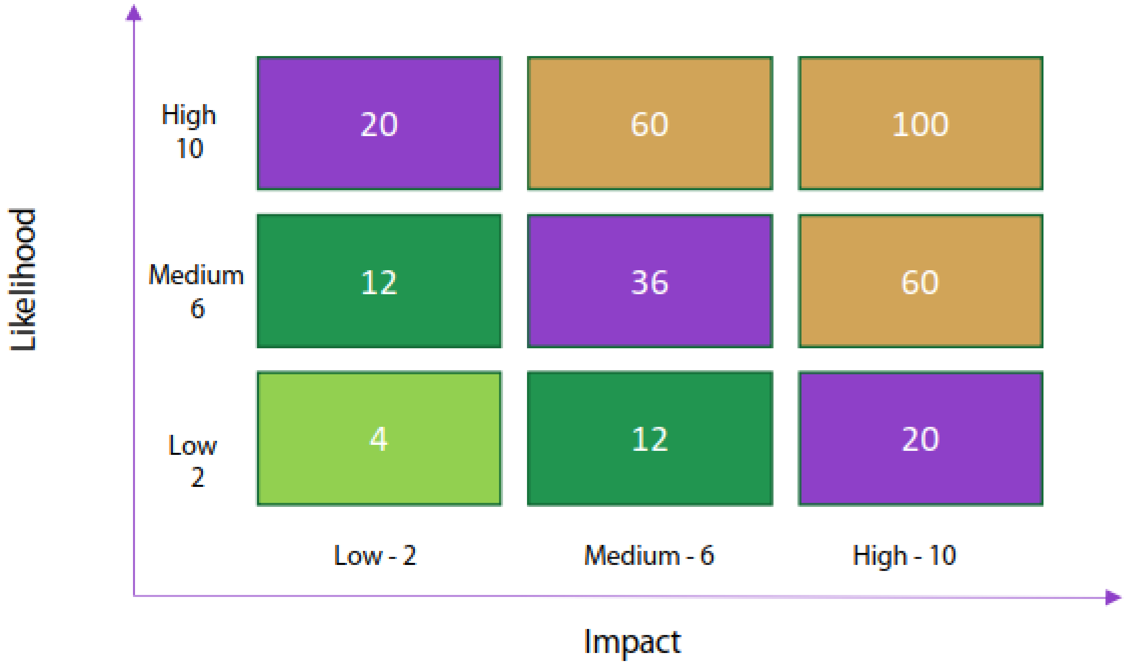
Qualitative vs. Quantitative Risk Assessment

Qualitative Risk Assessment



Likelihood	Insignificant	Moderate	Catastrophic
Probable	Medium risk	High risk	Critical risk
Possible	Low risk	Medium risk	High risk
Highly unlikely	Low risk	Low risk	Medium risk

Quantitative Risk Assessment



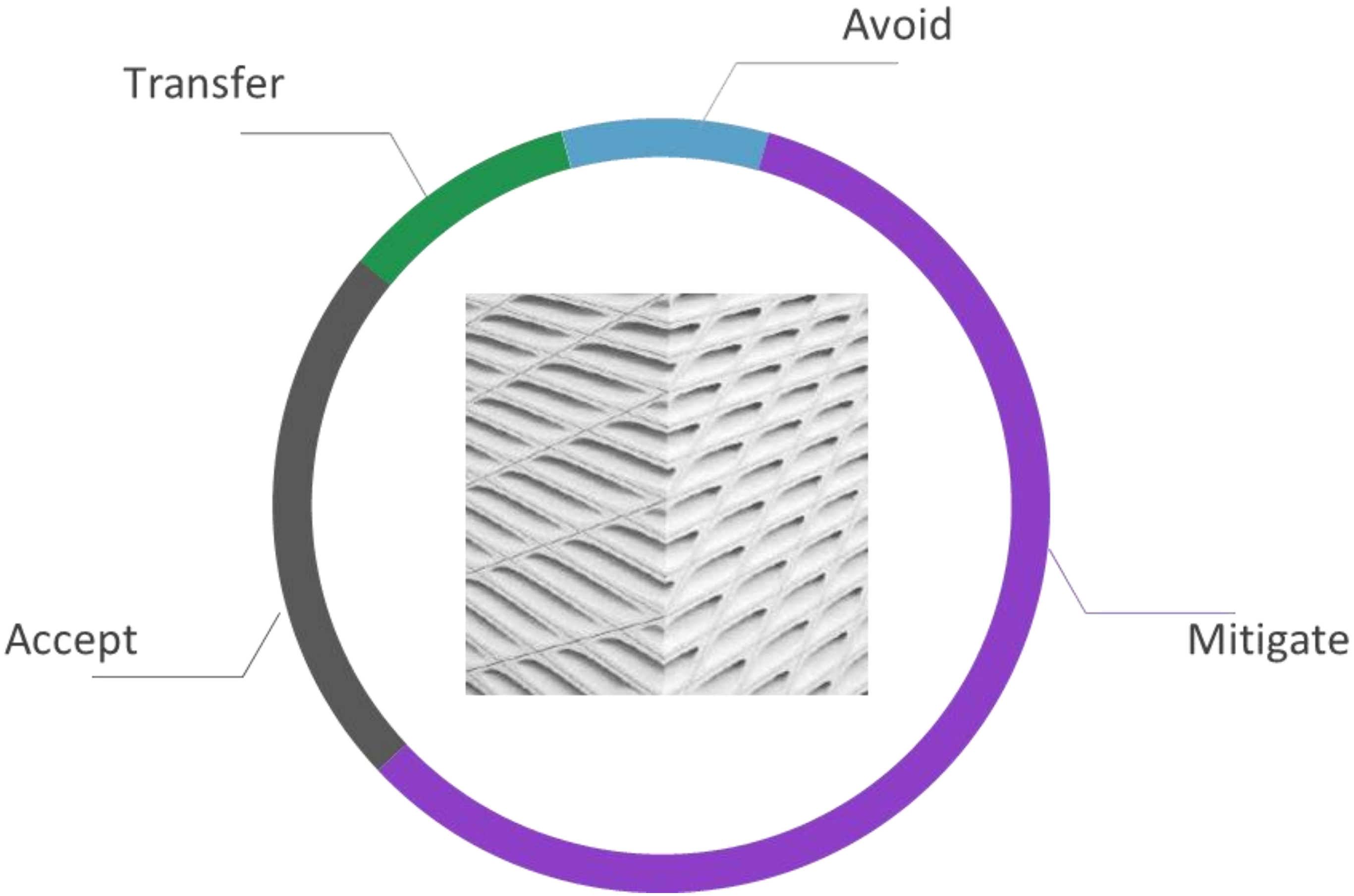
Likelihood	Low - 2	Medium - 6	High - 10
High 10	20	60	100
Medium 6	12	36	60
Low 2	4	12	20

Risk owners

Information Security Risk Treatment (PIMS-specific)

- This clause builds upon ISO/IEC 27001:2013 Clause 6.1.3 by introducing privacy-specific considerations in the risk treatment process.
- The organization must compare selected controls from:
  - ISO 27001 Annex A
  - ISO 27701 Annex A (for PII Controllers)
  - ISO 27701 Annex B (for PII Processors)
- The purpose is to ensure that no necessary controls are omitted, especially those protecting PII.

Risk treatment



Statement of applicability

- Includes the security controls from ISO/IEC 27001 + the applicable privacy controls of ISO/IEC 27701 + other control (if considered appropriate).

- **Should be revised whenever things change.**

Objectives and planning to achieve them

- The organization shall establish information security and privacy objectives at relevant functions and levels.
- There should be plans for the achievement of objectives (what will be done, who will be responsible, resources, when the objectives will be completed...)
- Objectives shall be documented, and their achievement must be monitored.

5.5. Support

No specific privacy additions, the requirements of ISO/IEC 27001 apply

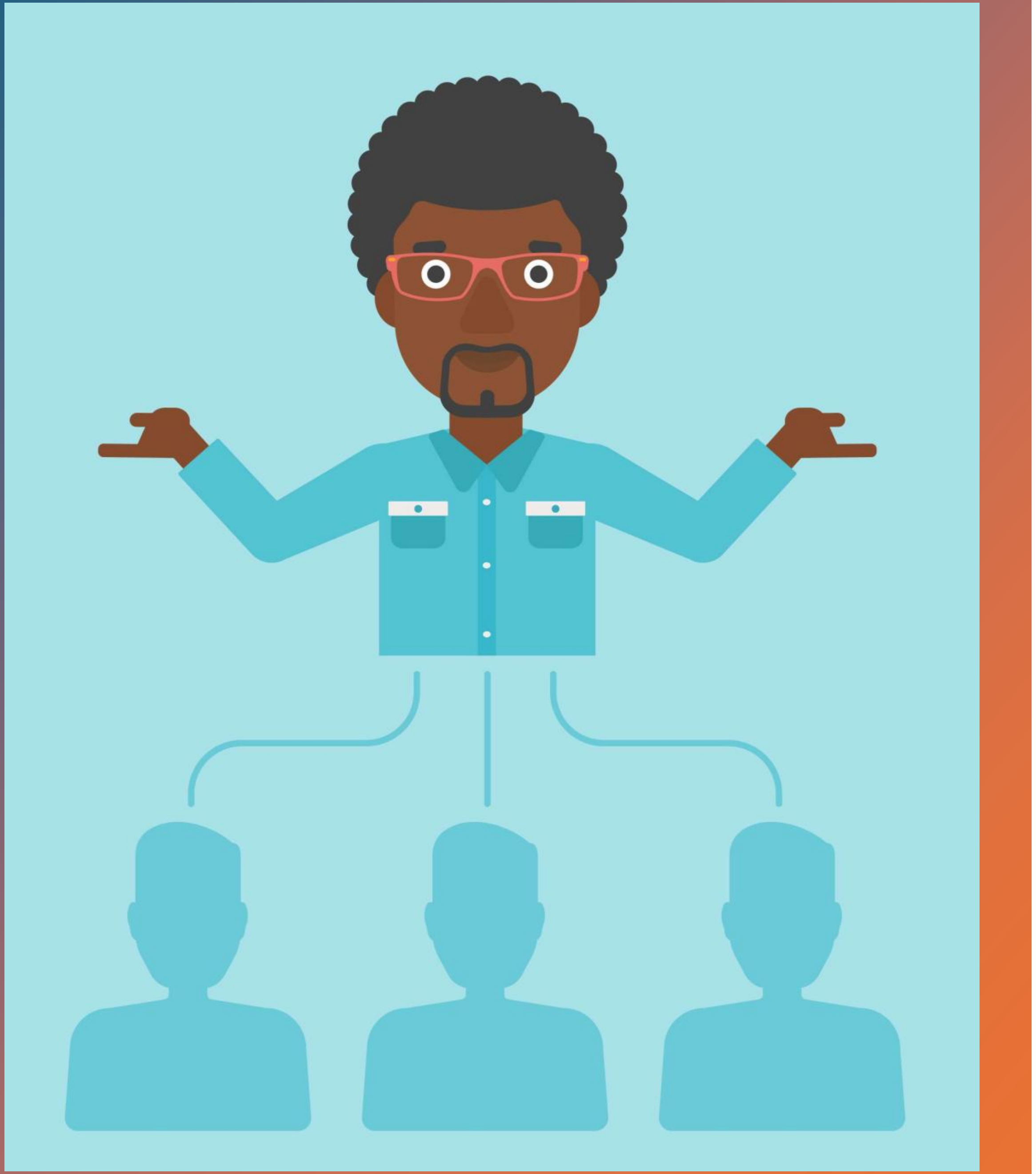
Resources

- Top management should provide the resources required for the establishment, the implementation, the maintenance and improvement of the management system.

Competence

- Identify competence needs
- Ensure people have the required competence
- Retain documented evidence of competence

Education + training + experience



Awareness

- Meant to ensure that people in the organization **understand** the importance of **complying** with security and privacy requirements, the **potential impact** of a data breach and how everyone **contributes** to the management system

Communication

- External and internal communication processes

Internal communication

Company staff should be informed about privacy aspects

External communication

With customers, PII principals, business partners, authorities...

Documented information (procedures, policies, manuals, regulations…)

- Mandatory docs (i.e. Risk assessment, SoA, Privacy and Information Security policy, objectives, MS scope…)
- Not mandatory but needed docs (i.e. procedures, policies, etc)

QUALITY ASIA

Controls for documented information:

- Format
- Review and approval
- Distribution
- Protection
- Revision
- Retention
- Disposition

5.6. Operation

- No specific privacy additions, the requirements of ISO/IEC 27001 apply

Implement the Risk treatment plan

Keep the risk assessment up to date

Plan and control changes

5.7. Performance evaluation

- No specific privacy additions, the requirements of ISO/IEC 27001 apply

Determine what to monitor and measure

+

responsibilities

Retain documented information

Internal audit

- Conduct internal audits of the management system at planned intervals

- Establish an internal audit programme
- For each internal audit document an audit plan (to include at least scope, criteria, objectives)
- Consider competence and objectivity of auditors
- Document findings and conclusions in the audit report

Management review

- Management review meetings shall take place at planned intervals

- Participants include top management, those responsible for the management system, different other positions

- The meeting discusses a number of topics and generates output data

5.8. Improvement

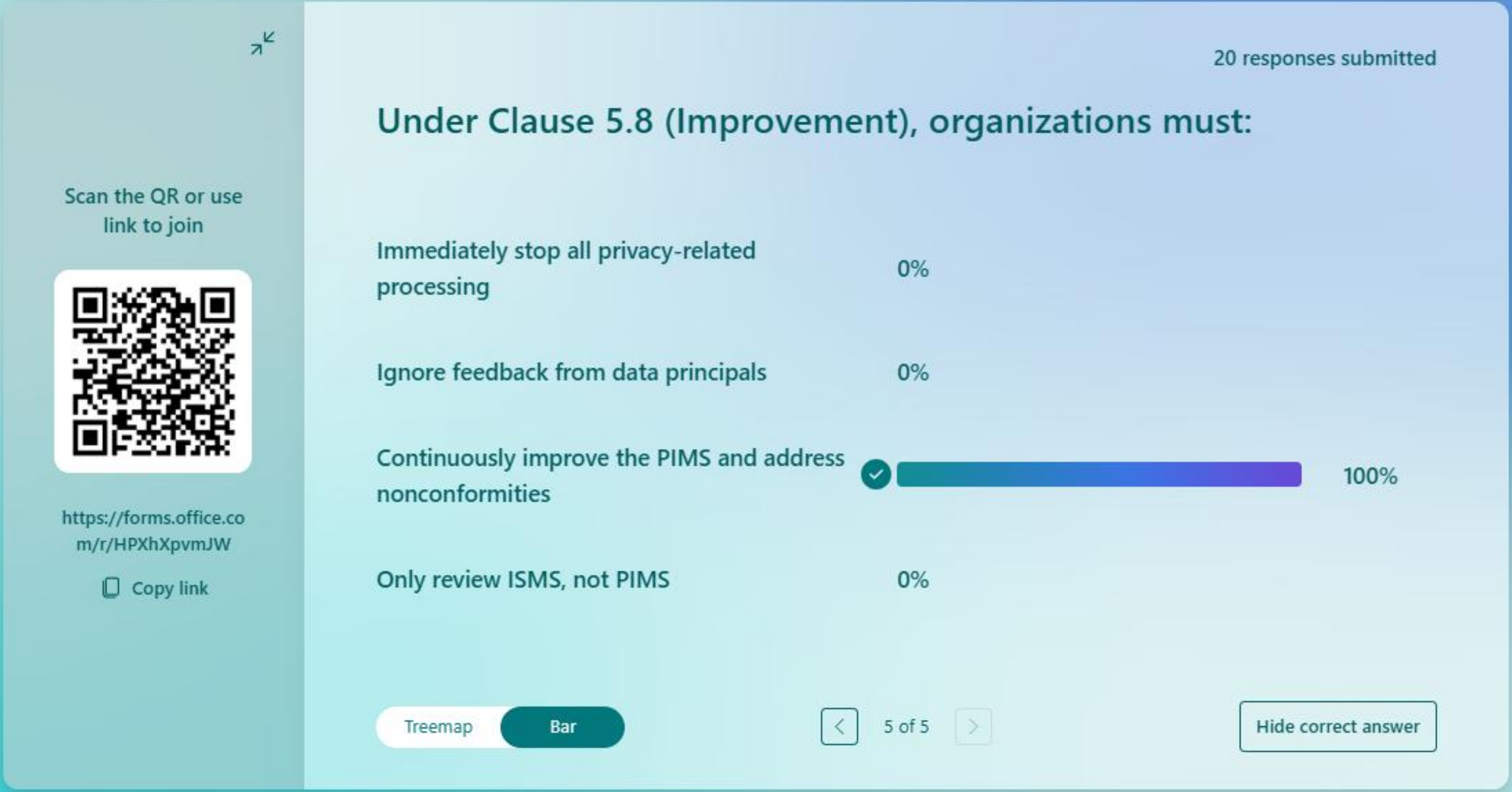
- No specific privacy additions, the requirements of ISO/IEC 27001 apply

Nonconformity
a non-fulfilment of a requirement

- Identify the nonconformity
- React to control the nonconformity and deal with the consequences
- Investigate to identify causes
- Implement corrective actions to ensure a similar situation does not happen again

Improvement

The organization shall act to continually improve its management system



Scan the QR or use link to join

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

Copy link

20 responses submitted

Under Clause 5.8 (Improvement), organizations must:

Immediately stop all privacy-related processing 0%

Ignore feedback from data principals 0%

Continuously improve the PIMS and address nonconformities ✓ 100%

Only review ISMS, not PIMS 0%

Clause 6 - PIMS specific guidance related to ISO/IEC 27002

Clause No.	Clause Name
6.1.	General
6.2.	Information security policies
6.3.	Organization of information security
6.4.	Human resource security
6.5.	Asset management
6.6.	Access control
6.7.	Cryptography
6.8.	Physical and environmental security
6.9.	Operations security
6.10.	Communications security
6.11.	Systems acquisition, development and maintenance
6.12.	Supplier relationships
6.13.	Information security incident management
6.14.	Information security aspects of business continuity management
6.15.	Compliance

6.1. General

- The guidelines in ISO/IEC 27002:2013 that mention "information security" must be extended to include:
- Protection of privacy, specifically in the context of processing of PII (Personally Identifiable Information)
- Where “information security” appears in ISO 27002, read it as:
  ➤ **“Information security and privacy”** (See Annex F)
- All control objectives and controls must address:
  - **Security risks**, and
  - **Privacy risks** related to **PII processing**

6.2. Information security and privacy policies

- Their purpose is to provide management direction and support for information security and privacy.
- This can be done through:
    - Separate privacy policies, or
    - Augmented information security policies
- Supported by lower-level policies that must also address the processing of PII (e.g. mobile devices, access control, cryptography, backup…)

6.2. Information security and privacy policies

- The organization should formally state its **support and commitment** to:
  - Complying with **PII protection laws and regulations**
  - Adhering to **contractual obligations** with partners, subcontractors, and third parties (customers, suppliers, etc.)
- Policies must be **periodically reviewed and updated**
- Ensure alignment with evolving:
  - **PII protection legislation**
  - **Organizational roles** (Controller or Processor)

6.3.1. Organization of information security and privacy – Internal organization

One or several persons shall be responsible for privacy related issues (e.g. DPO)

Can be outsourced

Independent

Sufficient independence to perform the tasks

Expertise

In data protection legislation and be involved in PII processing related issues

Responsibility

Informs top management and employees on their obligations and communicates with authorities

- Define and allocate roles and responsibilities relevant for information security and privacy and segregate conflicting duties.

Information Security Roles and Responsibilities

Organizations must:

- **Appoint a designated contact** for handling **PII-related inquiries**:
  - For **PII controllers**: A contact for **PII principals (data subjects)**
  - For general use: A contact for **customers or external parties**
- Assign responsible individuals to **develop, implement, and maintain**:
  - A **privacy governance program**
  - Compliance with **applicable privacy laws and regulations**

Responsibilities of the Designated Person:

- Act **independently**, reporting directly to senior management
- Manage all **PII processing–related matters**
- Be an expert in **data protection law and practice**
- Serve as a **point of contact for supervisory authorities**
- Educate employees and top management on **PII-related obligations**
- Provide guidance for **Privacy Impact Assessments (PIAs)**

Note: This role may align with a **Data Protection Officer (DPO)** in jurisdictions where required.

Segregation of duties

- Avoid a single person having total control and prevent conflicts of interests.

6.3.2. Mobile devices – Additional Requirement

- The use of mobile devices shall not lead to a compromise of PII processed.
- A policy for the use of mobile devices should be established + BYOD policy

Teleworking
(work arrangement that allows the employee to perform work-related tasks from home or another convenient location)

- Establish a policy for teleworking
- Authorize teleworking locations

6.4. Human resources security

Screening of candidates

Consider PII processing involved

Contractual agreements

Address confidentiality

Training

Train employees on security and privacy

Disciplinary process

Applicable for security and privacy breaches

Exit interview

Understand and remind obligations

Access rights

Remove access rights

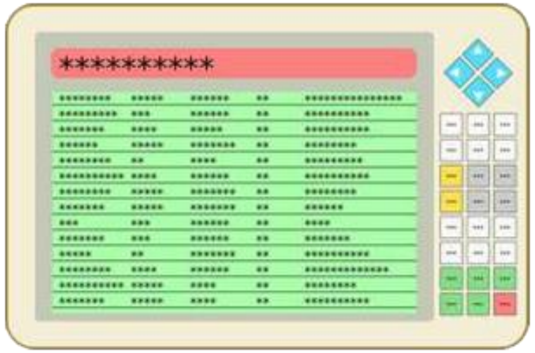
6.4.2.2. Information security awareness, education and training

Organizations must **enhance awareness and training programs** to include **privacy-specific risks and responsibilities**, especially for those handling **Personally Identifiable Information (PII)**.

Training should cover:

- **Incident reporting awareness**
- **Consequences of privacy/security breaches**, including:
  - For the **organization**: legal penalties, loss of business, reputational harm
  - For **staff members**: disciplinary action
  - For **PII principals**: emotional, physical, or material impact

6.5. Asset management



Inventory of assets

Asset – anything that has value to the organization

Asset ownership and acceptable use Assets should be "owned"

Purpose of ownership: assign responsibility for protecting the assets

Acceptable use policies

Information classification and labelling

The organization should develop an information classification scheme

Confidential

Restricted

Internal use

Public

PII should be explicitly included in the classification scheme

Labelling information

6.5.2.1. Classification of Information – Additional Requirement

The organization's **information classification system** must:

- **Explicitly include PII** (Personally Identifiable Information)
- Integrate PII classification into the overall **data classification scheme**

Helps identify:

- **What types of PII** are being processed (e.g., sensitive, financial, biometric)
- **Where the PII is stored**
- **Which systems** it flows through

6.5.2.2. Labelling of information – Additional requirement

The organization must ensure that all **personnel under its control**:

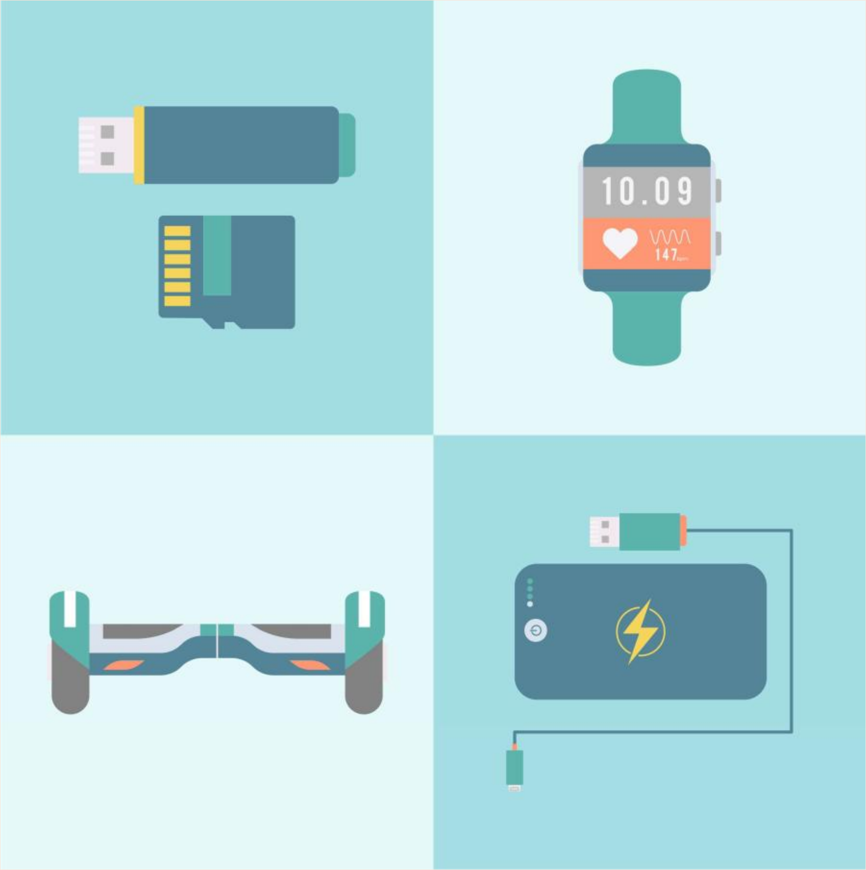
- Understand the **definition of PII (Personally Identifiable Information)**
- Can **identify and label** information that qualifies as PII

Media handling

- Controls for removable media if used for storing or transferring PII
- Document all use of removable media or devices used to store **PII**
- Prefer **encrypted** physical media/devices for PII storage
- Use **unencrypted** media only when unavoidable — apply **compensating controls** (e.g., tamper-evident packaging)

Removable media taken outside the organization:

- Is prone to **loss**, **damage**, or **unauthorized access**
- **Encryption** adds a critical layer of protection for PII



6.5.3.2. Disposal of media – Additional requirement

When **removable media** containing **PII (Personally Identifiable Information)** is disposed of, the organization must:

- Implement **secure disposal procedures**
- Ensure **previously stored PII** is **unrecoverable and inaccessible**

Documentation Requirement:

- Disposal procedures must be included in the organization's **documented information**
- These procedures must be **executed consistently** and **auditable.**

6.5.3.3. Physical media transfer – Additional requirement

When **physical media containing PII** is transferred (incoming or outgoing), organizations must:

- Implement a **tracking system** to log:
  - Type of media
  - Sender and recipient (authorized parties)
  - Date and time of transfer
  - Number of physical media units

Security Measures:

- Use **encryption** wherever possible to protect data
- Data must be accessible **only at the destination**, not in transit
- Physical media should **not leave the premises** without:
  - **Authorization procedures**
  - Controls ensuring **only authorized personnel** can access PII.

6.6. Access control

Access control policy

Principles (e.g. need to know, need to use)

Provide access rights (including priviledged rights)

Remove access

6.6.2.1. User registration and de-registration – Additional requirement

Organizations must ensure that:

- **User registration/de-registration procedures** cover systems and services that **process PII**
- These procedures address situations such as:
  - **User account compromise**
  - **Inadvertent disclosure** of registration credentials
  - **Corruption or loss** of user control data

6.6.2.1. User registration and de-registration – Additional requirement

Security Enforcement:

- **Deactivated or expired user IDs** must not be reused on systems handling PII
- Only **authorized, registered users** should have access to systems processing personal data

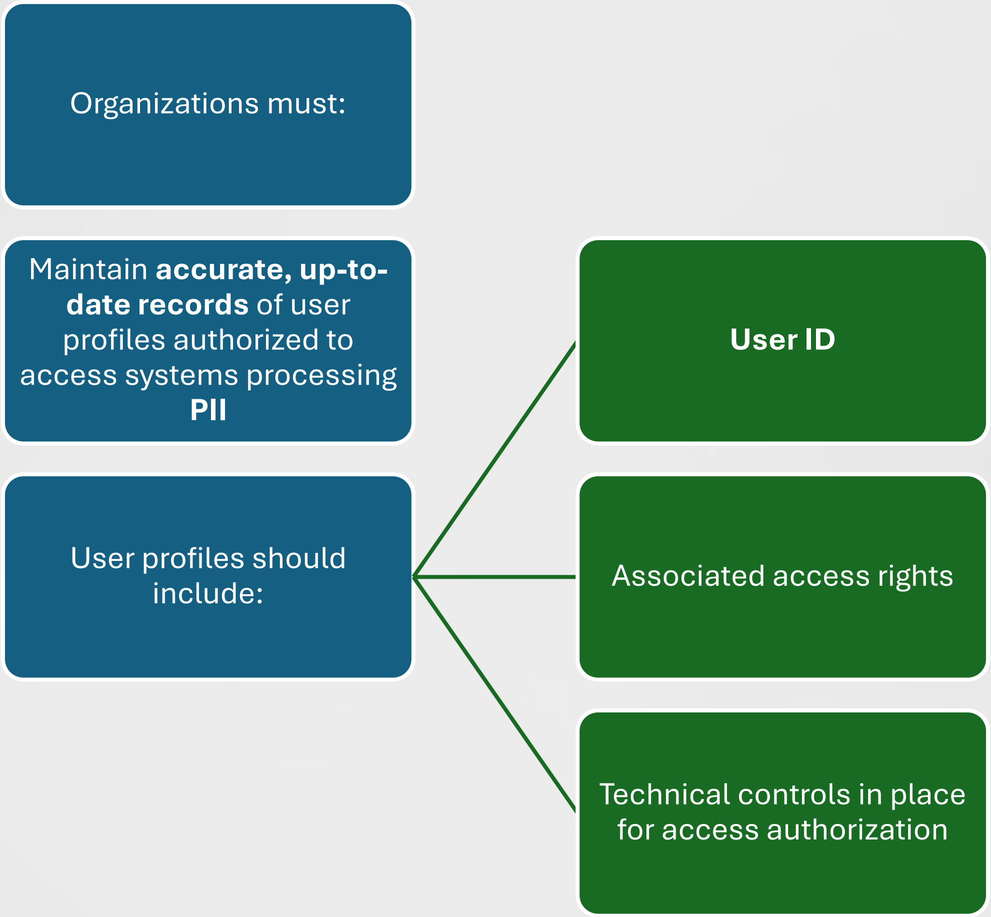
For PII Processing Services:

- If PII processing is offered as a **service**, the **customer** may manage user IDs
- In such cases, responsibilities must be clearly outlined in the **documented agreement**

Jurisdictional Compliance:

- Some regions may require **regular checks** for unused credentials
- Organizations must ensure **local legal compliance** for PII-related user access systems

6.6.2.2. User Access Provisioning



Organizations must:

Maintain **accurate, up-to-date records** of user profiles authorized to access systems processing **PII**

User profiles should include:

- **User ID**
- Associated access rights
- Technical controls in place for access authorization

Purpose of Individual Access IDs:

- Ensure systems can:
  - Identify **who accessed** PII
  - Track **what actions** (additions, deletions, modifications) were performed
- Supports **accountability** and **security auditing**

PII Processing as a Service:

- If the organization provides **PII processing as a service**:
  - The **customer** may manage access
  - The organization must offer tools to **assign, manage, or revoke** access as required.

Privileged access rights

- Restricted
- Automatic expiration
- Assigned to a different user ID
- Granted by the asset owner

6.6.4.2 – Secure Log-on Procedures – Additional requirement

When **requested by the customer**, the organization must:

- **Provide secure log-on capabilities** for any user accounts under the customer's control
- Ensure that systems handling **PII** accessed by customer-managed accounts are protected using:
    - **Authentication controls**
    - **Access validation mechanisms**
    - **Secure login protocols**

Passwords

- Define the process to generate passwords
- Educate users
- Verify users' identity

Access control

Utility programs

Limit their use

Access to source code

Restrict access to source code of programs

6.7. Cryptography

- The decision to use cryptography for PII protection should be in line with the results of the Privacy Impact Assessment

Policy

Document a policy on the use of cryptographic controls

Inform

Inform the customer

Key management

Control cryptographic keys from generation to destruction

6.7.1.1 – Policy on the Use of Cryptographic Controls - Additional guidance

Organizations must:

- Use **cryptography** to protect certain types of **PII** (e.g., health data, ID numbers, passport data) where required by **jurisdictional law**
- Inform **customers**:
  - **When and how** cryptographic controls are applied to protect PII
  - What **capabilities** are available to help customers implement their own encryption measures
- Cryptographic use may be **mandated by law** in certain regions

6.8. Physical and environmental security

Security perimeters

Entry controls

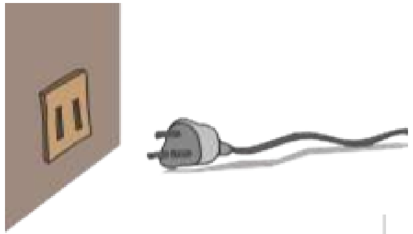
External and environmental threats

Delivery and loading areas

Equipment

- Protect the equipment against environmental threats
- Position equipment so that risks are minimized
- Maintain equipment adequately
- Authorization for taking equipment off-premises
- Clear desk and clear screen policy
- Secure disposal

Utilities and cabling



Supporting utilities

Inspect and test supporting utilities

Cabling security

Cables must be protected against interception, interference and damage

6.8.2.7 - Secure Disposal or Re-use of Equipment – Additional guidance

Organizations must ensure that:

- When **storage devices are reassigned or disposed of**, any previously stored **PII must not be accessible**
- Technical controls must be applied to prevent **unauthorized recovery of data**

Risk Context:

- Deleting PII does **not guarantee** that it is unrecoverable
- Performance limitations may **prevent complete erasure**
- This poses a risk of **unintended PII access** by subsequent users

Implementation Guidance:

- Devices should be treated as **containing PII by default**
- Use secure disposal techniques:
  - Cryptographic erasure
  - Overwriting
  - Physical destruction (e.g., shredding or degaussing)

6.8.2.9 - Clear Desk and Clear Screen Policy - Additional guidance

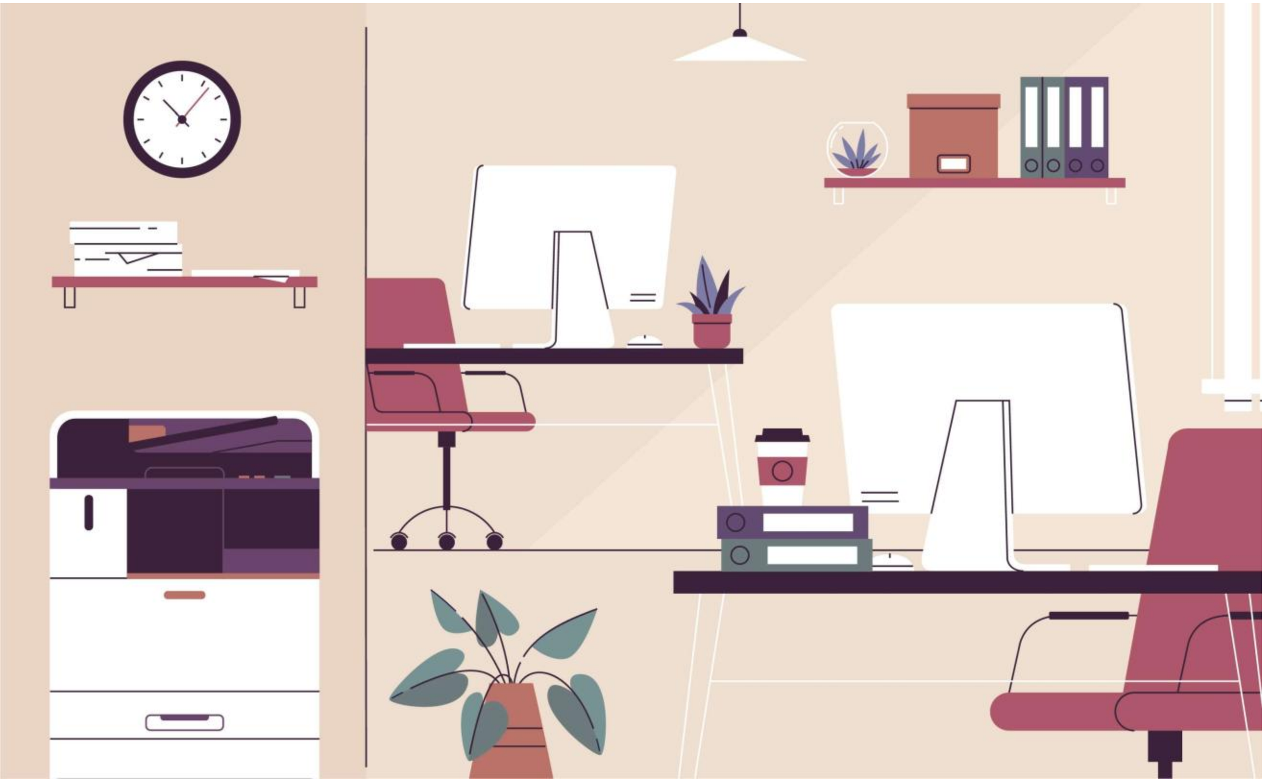
Organizations should:

- **Limit the creation of hardcopy documents** containing **PII**
- Only generate physical PII documents that are **strictly necessary** for the **defined processing purpose**

Purpose of the Control:

- Prevent **unauthorized access** to PII left on desks or screens
- Reduce risk of **PII exposure** in shared or open work environments

Implementation Measures:



- Apply **clear desk** practices:
  - Lock away PII-related documents when not in use
- Apply **clear screen** practices:
  - Log off or lock screens when unattended

6.9. Operations security

Document operating procedures

Control changes

Capacity management

Separate development, testing and operational environments

Protect against malware

6.9.3. Backup – Additional guidance

Backup policy

Supplementary ISO/IEC 27701 requirements

- Document requirements for PII backup, recovery and restoration
- Inform customers on PII backup and restoring capacity
- Keep logs of PII backup restoration

Backup & Restore Responsibilities

- If the organization offers **backup/restore services**, it must:
  - Clarify **capabilities and scope** of PII restoration
  - Identify **who is responsible** for backup-related decisions
- Maintain a **PII restoration log** including:
  - Name of the responsible person
  - Description of restored PII

Risk and Integrity Controls:

- Where **PII must be restored**, systems must:
  - **Ensure integrity** of PII data
  - Trigger processes to **notify** and **resolve issues** involving PII or its principals

6.9.4.1 – Event Logging – Additional guidance

Organizations must establish a **process to review event logs** for systems handling **PII**, using:

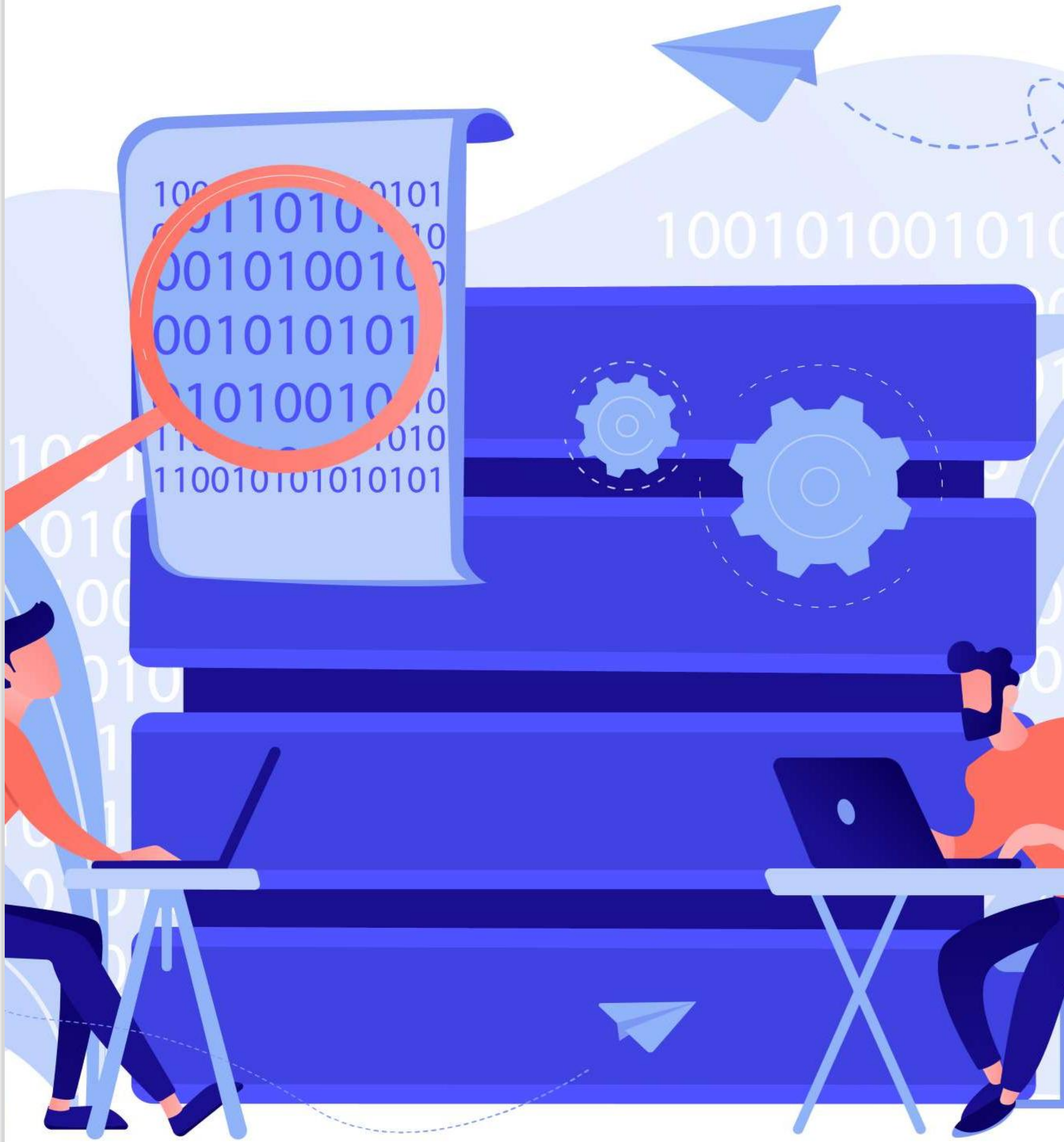
- **Automated monitoring** and alerting, or
- **Manual review** at scheduled intervals

What to Record in Event Logs (if PII is involved):

- **Who** accessed the data
- **When** and **which PII principal's** data was accessed
- **What changes** (additions, deletions, modifications) were made
- **Reason for the event** if applicable

Shared Services / Cloud Providers:

- Define and document **roles and responsibilities** between service providers
- Address agreements on **log access and usage rights**



Logging and monitoring

Produce logs and review the regularly

- Keep logs of access to PII
- Make sure customers have access only to logs related to their activities
- Review logs
- Protect logs
- Define log retention periods and delete logs automatically
- Synchronize clocks

6.9.4.2 – Protection of Log Information – Additional guidance

- Log information (e.g., for monitoring or diagnostics) may contain **PII** and must be protected accordingly.

Implement **access controls** to ensure logs are:

- Accessed only by authorized personnel
- Used only for their intended purpose
- Put in place **automated procedures** to:
  - **Delete** or **de-identify** logs
  - In line with defined **retention schedules**

Control of operations security

Control software installation

Be informed on vulnerabilities

6.10. Communication security

Network security management

- Network controls (procedures, responsibilities, activity monitoring, access restriction…)
- Agree service and security levels with suppliers and monitor their services
- Network segregation (segmentation)
- Monitor the effectiveness of controls implemented

Information transfer

Maintain the security and privacy of information exchanged inside the organization and with external parties

- Policies and procedures for information exchange
- Agreements on information transfer
- Electronic messaging
- Confidentiality and non-disclosure agreements

6.10.2.1 – Information Transfer Policies and Procedures – Additional guidance

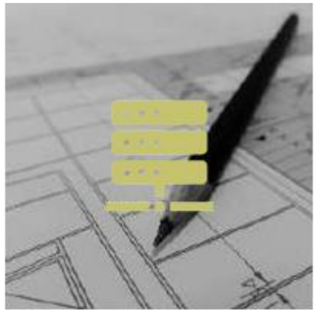
designed by freepik

- The organization should define procedures to ensure that **PII processing rules** are:
  - Enforced **both within and outside** the system, where applicable
- Applies to any form of **data movement**—internal, external, automated, or manual

6.10.2.4 – Confidentiality or Non-disclosure Agreements – Additional guidance

- All individuals under the organization's control with access to PII must:
  - Be bound by a **confidentiality obligation**
  - The agreement should specify the **duration** of the obligation
- For **PII Processors**:
  - The organization must ensure that **employees and agents comply** with internal policies and procedures regarding **data handling and protection**

6.11. System acquisition, development and maintenance



Security and privacy requirements

To be considered in the acquisition of new systems and enhancement of existing ones.

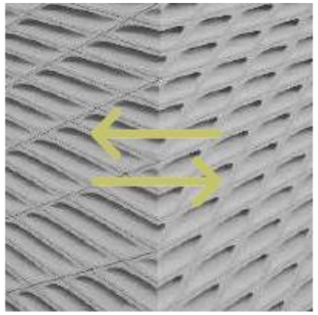
Information on public networks

Protect the information transmitted through public networks (also internet). PII should be encrypted.

Software development

Document and apply a secure development policy. Privacy by design and privacy by default.

6.11. System acquisition, development and maintenance



Control changes

Changes to the software development process shall be controlled

Modifications to software packages

The organization should restrict modifications to vendor supplied software

Software testing

Avoid using PII for software testing purposes

6.11.1.2 – Securing Application Services on Public Networks – Additional guidance

- Organizations must ensure that **PII transmitted over untrusted networks** is **encrypted** during transmission.

Untrusted Networks Include:

- The **public internet**
- Any external network **not under the organization’s operational control**

6.11.2.1 – Secure Development Policy – Additional guidance

Development policies must incorporate **privacy-by-design** and **privacy-by-default** principles, ensuring that:

- **PII protection** is embedded into system design and development processes
- The design addresses **obligations to PII principals** and complies with **legal/regulatory requirements**

Development Policies Should Address:

- **PII protection guidance** and implementation of **privacy principles** throughout the SDLC
- PII risk assessment outputs and **Privacy Impact Assessment (PIA)** inputs during design (see **Clause 7.2.5**)
- **PII protection checkpoints** aligned with project milestones
- Required **privacy and PII knowledge** for development teams
- A design approach that **minimizes PII processing by default**

6.11.2.5 – Secure Systems Engineering Principles – Additional guidance

Key Requirement:

Systems and components related to **PII processing** must be designed with:

- **Privacy by Design**
- **Privacy by Default**
- Facilitation of controls for **PII Controllers (Clause 7)** and **PII Processors (Clause 8)**

Design Objective:

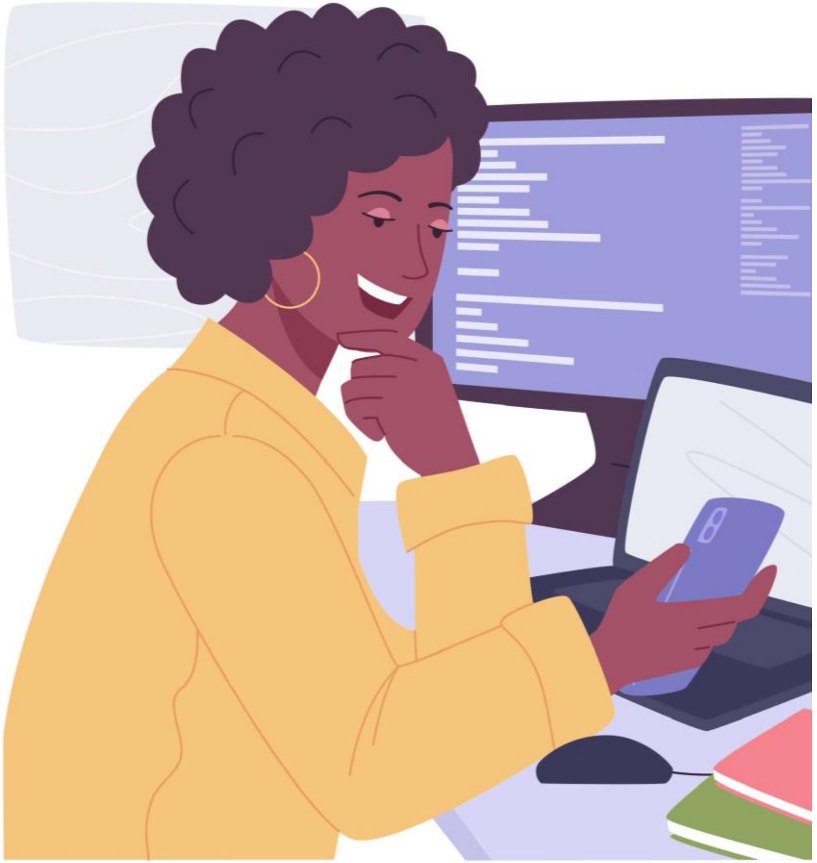
- Ensure that PII collection and processing is:
  - **Purpose-limited**
  - **Minimized to necessity**
  - **Compliant with privacy impact analysis** (see Clause 7.2)

If required by jurisdiction, systems must:

- **Automatically delete** PII after the defined retention period
- Be designed to **support automated deletion**

6.11.2.7 – Outsourced Development – Additional guidance

- When **outsourcing development**, organizations must apply the **same principles** of:
  - **Privacy by Design**
  - **Privacy by Default**
- These principles must be **embedded into outsourced systems** just as they would be in internal development.
- Ensures that **third-party developers** also uphold privacy expectations and legal requirements, protecting PII even outside the organization’s direct control.



6.11.3.1 – Protection of Test Data – Additional guidance

- **PII should not be used** for testing purposes.
- Organizations should use **false or synthetic PII** instead.

If Using Real PII for Testing:

- Only if unavoidable, implement:
  - **Technical and organizational controls** equivalent to those used in production
- Apply a **risk assessment** to identify and apply suitable **mitigating measures**

QUALITY ASIA

6.12. Supplier relationships

Suppliers can have a significant impact on security and privacy

Policy

Security and privacy policy applicable for supplier relationships

Contracts

Include in contracts security and privacy requirements

Supply chain

Ask suppliers to propagate security and privacy requirements

Monitor

Monitor supplier performance and control changes

6.12.1.2 – Addressing security within Supplier agreements – Additional guidance

Organizations must define in supplier agreements:

- Whether **PII is processed**
- The **technical and organizational security measures** the supplier must implement
- Requirements that align with the organization's **information security** and **PII protection obligations** (Refer to Clauses **7.2.6** and **8.2.1**)

Supplier Agreement Should Cover:

- **Allocation of responsibilities** across:
  - The organization
  - Its partners
  - Suppliers
  - Third parties (e.g., customers, subcontractors)
- **Mechanisms to ensure compliance** with legal and regulatory requirements
- **Provision for independent audits** and evidence of compliance

Contracts with suppliers must **explicitly state** that:

- PII shall be processed **only per the organization's instruction**

6.13. Incident management

- Procedures to prepare and deal with incidents
- Responsibilities for incident management
- Training and awareness
- Assess events
- Respond to incidents
- Identify source
- Learn from incidents

PII breach

An incident that leads to access to PII

- Legislation may require PII breach notification
  - to relevant authorities
  - to PII principals
  - to customer (controller)

Some countries require **specific breach response procedures**, including:

- **Mandatory notifications** within a specified timeframe
- Demonstrated **compliance readiness**

6.13.1.1 – Responsibilities and Procedures – Additional guidance

As part of the **incident management process**, organizations must:

- Define **responsibilities and procedures** for:
    - **Identifying** and **recording** breaches involving **PII**
    - **Notifying** affected parties and authorities of such breaches

Deal with incidents

Maintain records of incidents

Incident Report -

- Description and consequences
- Time
- Who reported
- To whom
- What has been done
- Notifications
- Consequences

Learn from incidents

6.13.1.5 – Response to Information Security Incidents – Additional guidance

Implementation Guidance for PII Controllers:

- Any incident involving **PII** must trigger a **review** to determine if it constitutes a **PII breach**.
- If a breach has occurred, the response should:
  - Include **clear notification** and **recordkeeping**
  - Follow **jurisdictional rules** on timing and authority notification

Notification Should Include:

- Contact point for details
- Description and likely consequences
- Scope of the breach (records & individuals)
- Steps taken or planned to resolve
- Status of PII (lost, disclosed, altered, unavailable)

6.13.1.5 – Response to Information Security Incidents – Additional guidance

Implementation Guidance for PII Processors:

- Breach notification duties should be defined **in contracts**
- PII processors must notify controllers **without undue delay**
- Contracts must define:
  - **Notification process**
  - **Information provided to controllers**
  - **Timelines for notification**

In case of a breach:

- Keep records with similar details as for PII controllers
- Ensure customer is notified if PII is compromised
- In some jurisdictions, processors may need to notify **regulatory authorities** directly

6.14. Information security and privacy aspects of business continuity

Business Continuity

- Information security and privacy aspects should be integrated into the business continuity arrangements
- Refer - ISO 22301 – Business continuity management systems

Business impact analysis

Plans, procedures, responsibilities

Testing and improvement

Redundancy

Review availability requirements and implement redundancy as needed

6.15. Compliance

- Identify requirements that the organization shall comply to (i.e. legislation, contractual requirements, etc.)

COPYRIGHT

Intellectual property rights

Protection of records

Cryptography

6.15.1.1 – Identification of Applicable Legislation and Contractual Requirements – Additional guidance

- Organizations must identify **legal obligations and sanctions** related to **PII processing**
- This includes:
  - **Fines or penalties** from supervisory authorities
  - Other **contractual risks** due to non-compliance

In some jurisdictions, ISO/IEC 27701 can serve as a **contractual framework** between:

- The organization and the **customer**
- Outlining roles and responsibilities for **privacy**, **security**, and **PII protection**

6.15.1.3 – Protection of Records – Additional guidance

- Organizations must retain **current and historical records** of:
  - Privacy policies
  - Related procedures
- These may be required for:
  - **Customer dispute resolution**
  - **Regulatory investigations**
- Keep **previous versions** of documents as per the **defined retention schedule**

6.15.2.1 – Independent Review of Information Security – Additional guidance

- When acting as a **PII processor**, and if **individual customer audits** are:
  - **Impractical**, or
  - Could **increase security risks**,
    → The organization should provide **independent evidence** of implemented security controls.

What to Provide to Customers:

- Before and during the contract period:
  - **Transparent, independent audit results**
  - Evidence showing compliance with internal **policies and procedures**
  - Audit conducted by a **recognized body** chosen by the organization

QUALITY ASIA

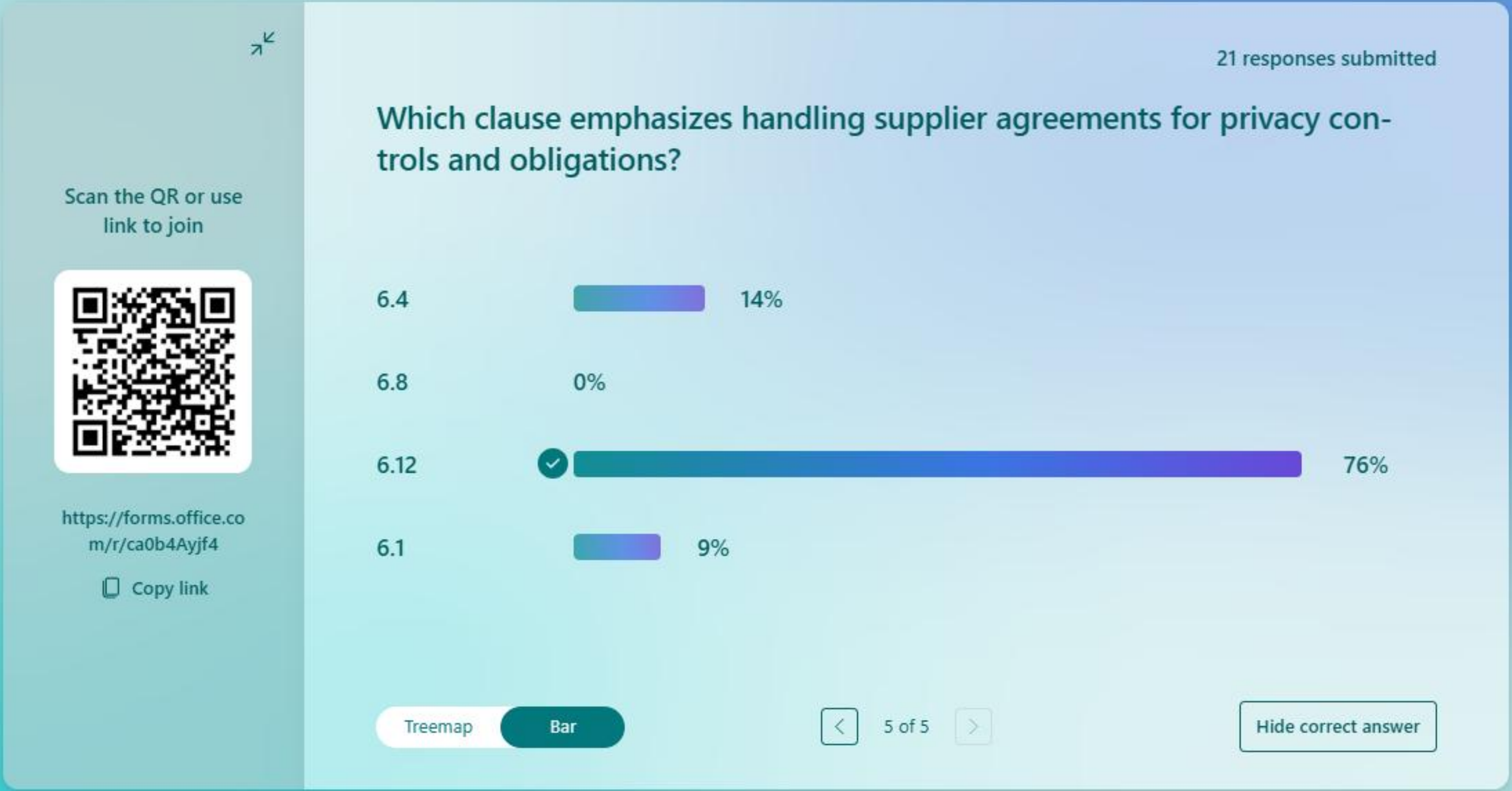
6.15.2.3 – Technical Compliance Review – Additional guidance

Organizations must conduct **technical reviews** of:

- Tools and components used for **PII processing**
- Their **compliance with security policies and standards**

Review Methods May Include:

- **Ongoing Monitoring**
  - Ensure that **only permitted PII processing** is occurring
- **Penetration or Vulnerability Testing**
  - Especially on **de-identified datasets**
  - Simulate attacks to validate that **de-identification methods** meet policy and regulatory requirements



Scan the QR or use link to join

https://forms.office.com/r/ca0b4Ayjf4

Copy link

21 responses submitted

Which clause emphasizes handling supplier agreements for privacy controls and obligations?

6.4	14%
6.8	0%
6.12 ✓	76%
6.1	9%

Clause 7 - Additional ISO/IEC 27002 guidance for PII controllers

Clause No.	Clause Name
7.1.	General
7.2.	Conditions for collection and processing
7.3.	Obligation to PII principals
7.4.	Privacy by design and privacy by default
7.5.	PII sharing, transfer and disclosure

QUALITY ASIA

7.2. Purpose and lawful basis

- Identify, document and communicate the purpose of PII processing.
- PII principals must be informed clearly about the purpose of PII processing.

7.2.2. Lawful basis

- Determine, document and comply with the lawful basis for PII processing, considering the purpose identified.

- Possible options:
  - Consent
  - Performance of a contract
  - Legal obligation
  - Vital interests of PII principals or other natural persons
  - Public interest task
  - Legitimate interest

Consent

Obtain and record consent

Obtain and record consent

Consent is one of the legal basis for PII processing.

Document when and how consent is obtained

Freely given	PII principal is not pressured or influenced
Specific	To the purpose of the processing
Unambiguous and explicit	Requires an action from the PII principal

Privacy Impact Assessment

Detect and evaluate the risks arising from the processing of PII and implement controls

- Systematic and extensive evaluation of personal aspects that is based on automated processing, producing legal effects on PII principals
- Large scale processing of special PII categories (e.g. health data, data related to the racial or ethnic origin, genetic or biometric data, data about the sexual orientation of natural persons, trade-union membership data, political opinions, religious or philosophic beliefs)
- Systematic monitoring of a publicly accessible area on a large scale.

? Is a PIA required?

Privacy Impact Assessment

ISO/IEC 29134:2017 – Methodology for the PIA

1. Team

Setting up a team

2. Plan

Prepare a plan

3. Describe

Describe what is being assessed (PII, principals, purposes, assets, subcontractors…)

Privacy Impact Assessment

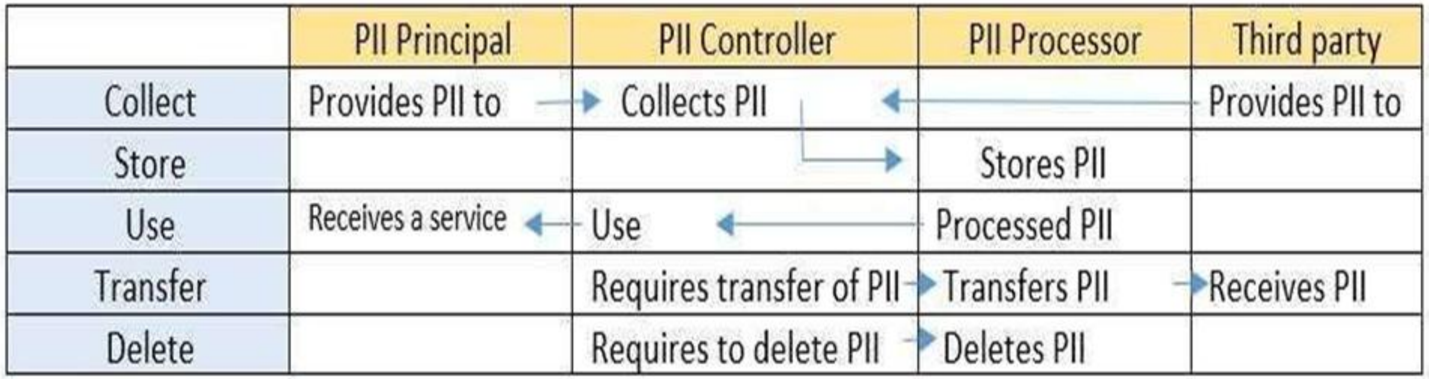
ISO/IEC 29134:2017 – Methodology for the PIA

4. Stakeholders

Identify stakeholders and if possible obtain their feedback

5. Information flows

Identify information flows



	PII Principal	PII Controller	PII Processor	Third party
Collect	Provides PII to	Collects PII		Provides PII to
Store			Stores PII	
Use	Receives a service	Use	Processed PII	
Transfer		Requires transfer of PII	Transfers PII	Receives PII
Delete		Requires to delete PII	Deletes PII	

QUALITY ASIA

Privacy Impact Assessment

ISO/IEC 29134:2017 – Methodology for the PIA

- unauthorized access or modification of PII;
- PII theft or loss;
- excessive collection;
- inappropriate or unauthorized linking of PII;
- failure to consider rights of PII principals;
- insufficient information;
- change or extend processing purpose without informing PII principals;
- processing without required consent;
- sharing PII without consent;
- excessive/ unnecessary retention…

6. Privacy risks

Identify privacy risks

Privacy Impact Assessment

ISO/IEC 29134:2017 – Methodology for the PIA

7. Analyze risks

Estimate impact and likelihood

Impact estimation		
Level of impact	Estimated consequences	Examples
Negligible	PII principals are not affected at all or there are small inconveniences that PII principals should be able to overcome without any problem	Annoyances, time spent to re-enter information into the system
Limited	Significant inconveniences that the PII principals should be able to overcome despite a few difficulties	Denial of access to a service, extra costs, fear, lack of understanding
Significant	The PII principals should be able to deal with the consequences but with serious difficulties	Blacklisting by banks, property damage, loss of employment
Maximum	PII principals suffer significant or irreversible consequences which they may not overcome	Inability to work, death or long-term psychological or physical ailments

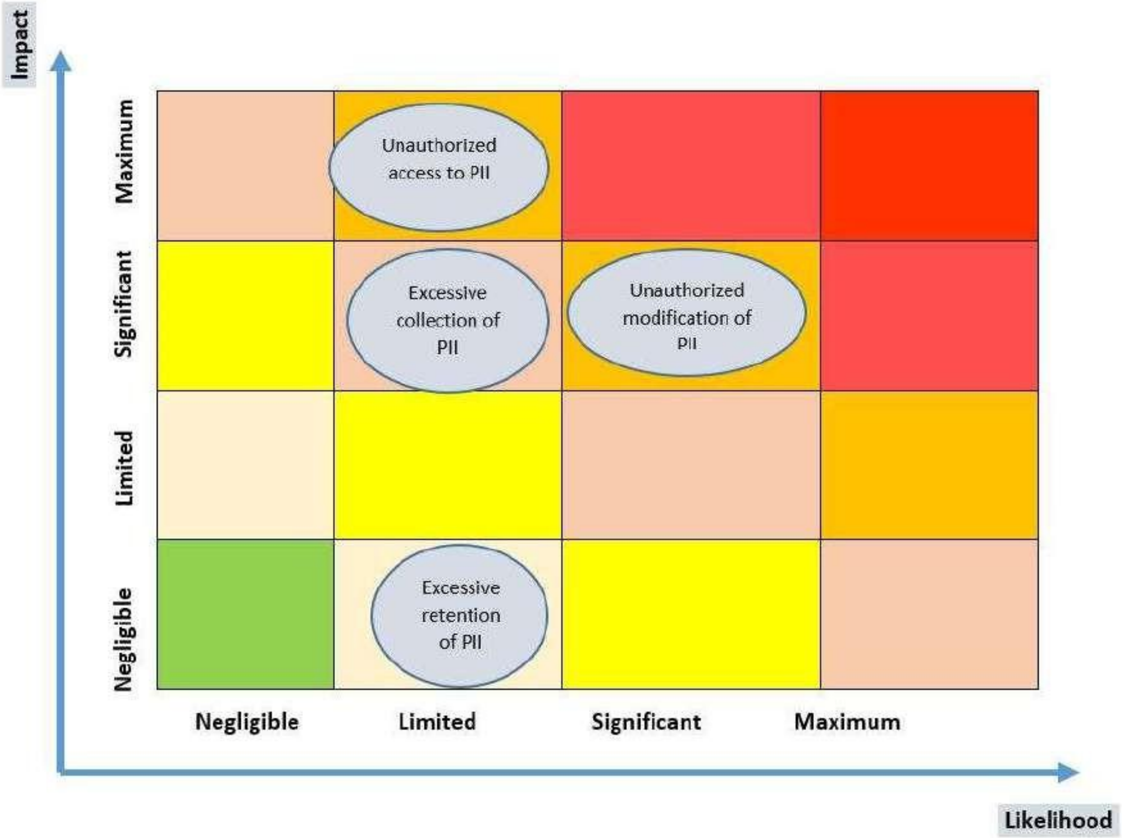
Likelihood estimation	
Likelihood level	Estimated likelihood
Negligible	It does not seem possible to happen given the controls in place
Limited	It appears to be difficult to happen
Significant	It appears to be possible
Maximum	It is likely to happen

Privacy Impact Assessment

ISO/IEC 29134:2017 – Methodology for the PIA

8. Assess risks

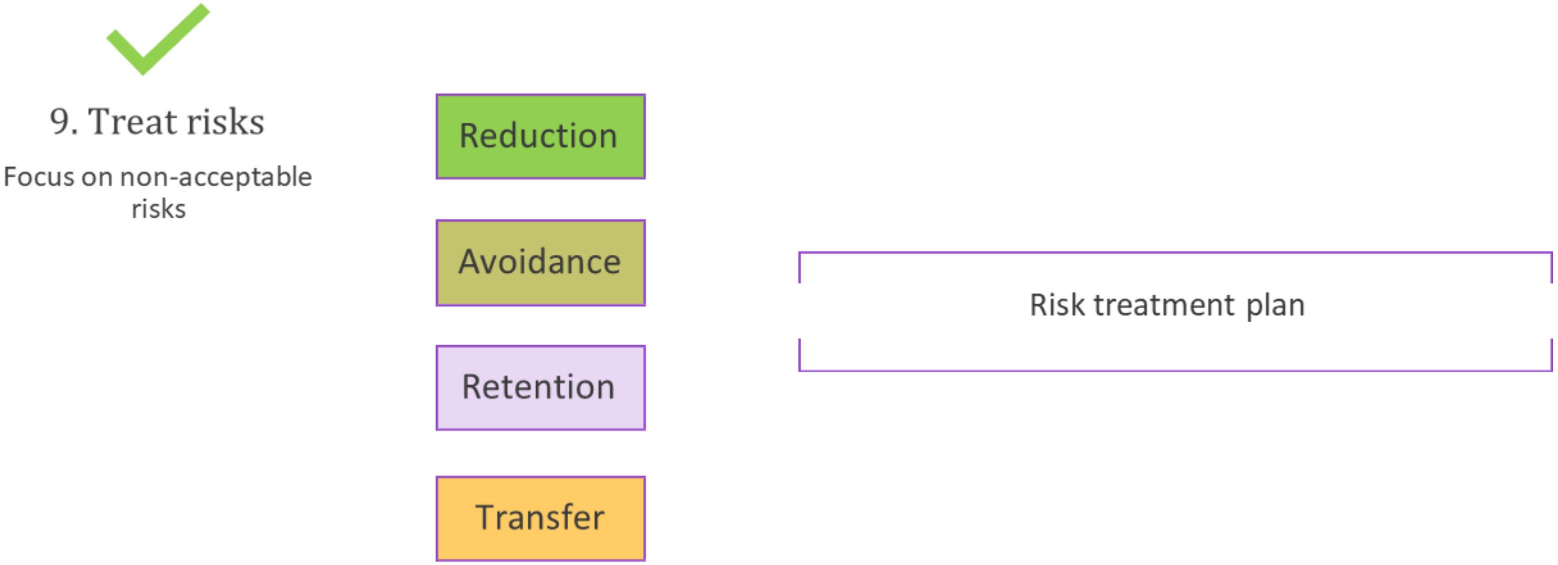
Combine impact and likelihood



	Negligible	Limited	Significant	Maximum
Maximum		Unauthorized access to PII		
Significant		Excessive collection of PII	Unauthorized modification of PII	
Limited				
Negligible		Excessive retention of PII		

Privacy Impact Assessment

ISO/IEC 29134:2017 – Methodology for the PIA



9. Treat risks

Focus on non-acceptable risks

Reduction

Avoidance

Retention

Transfer

Risk treatment plan

Privacy Impact Assessment

ISO/IEC 29134:2017 – Methodology for the PIA

- Information on the organization
- Compliance obligations
- Scope of the PIA
- Purpose of the PIA
- Who and when conducted the PIA
- Types of PII collected and processed
- Description of processing activities
- Legal jurisdiction
- Methodology for the PIA
- Threshold for non-acceptable risks
- Risk map
- Risk treatment plan
- Conclusions, decisions, recommendations

✓

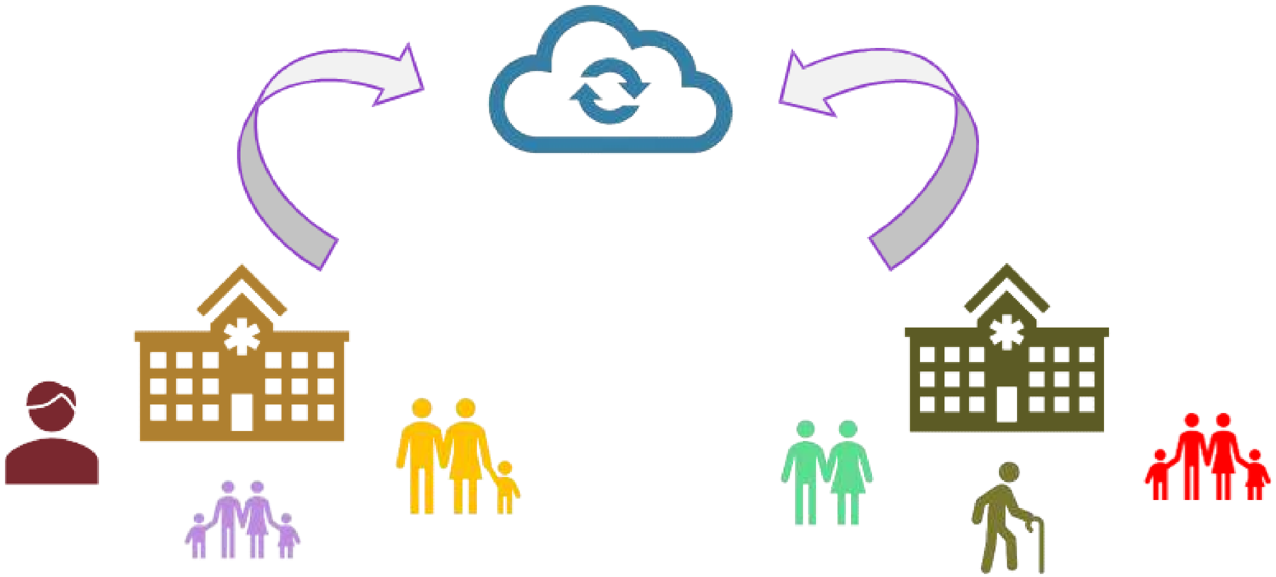
10. PIA report

Generate the report

Contracts with PII processors

Contracts

- The PII controller should sign contracts with all PII processors it uses.
- Contracts should require PII processors to implement the controls in ISO/IEC 27701



Joint PII controller
Two or more organizations acting as PII controllers

Joint controller agreement:

- Parties
- Purpose of data sharing
- PII processed
- Processing activities
- Roles and responsibilities
- Data breach management
- Retention and disposal of PII
- Obligations to PII principals
- Contact point
- Failure to fulfil the agreement

Records related to PII processing

Maintain records in secure conditions

- Inventory of processing activities
  - Type
  - Purpose
  - PII processed
  - PII principals
  - Recipients
  - Security
  - PIA

7.2. Obligations to PII principals Legislation, regulations, contracts…

Determine and fulfill obligations

- Identify obligations to PII principals
- Provide the means to meet the obligations
- Provide a contact point to PII principals

Determine information to PII principals

- Purpose and lawful basis
- Contact
- How was PII obtained
- Legal obligations
- Transfer and recipients of PII
- Retention
- Automated processing
- Rights of PII principals and obligations of the PII controller
- How a complaint can be lodged

7.3. Obligations to PII principals

Providing information to PII principals

- Clear and easy to access
- Concise, complete and provided in a timely manner
- Provide a contact point to PII principals

Providing mechanisms to withdraw or modify consent

- Communicate to PII principals
- Define response time to requests
- Record requests
- Stop processing once consent is withdrawn
- Communicate requests to all parties involved

Providing mechanisms to object to PII processing

- According to applicable legislation

7.3. Obligations to PII principals

Access, correction and/ or erasure

- Provide information to PII principals
- Mechanisms for correcting PII at the request of PII principal
- Allow PII principals to have PII
- deleted

Obligations to inform third parties

- Adequate communication
- Allocate responsibility

Providing copy of PII processed

- Provide a copy of PII processed upon request *(check legislation for requirements about format)*
- Transfer a copy of PII to another organization at the request of PII principal (if possible)

7.3. Obligations to PII principals

Handling requests

Document how requests are handled (e.g. response times, fees, responsibilities, process...)

Automated decision making

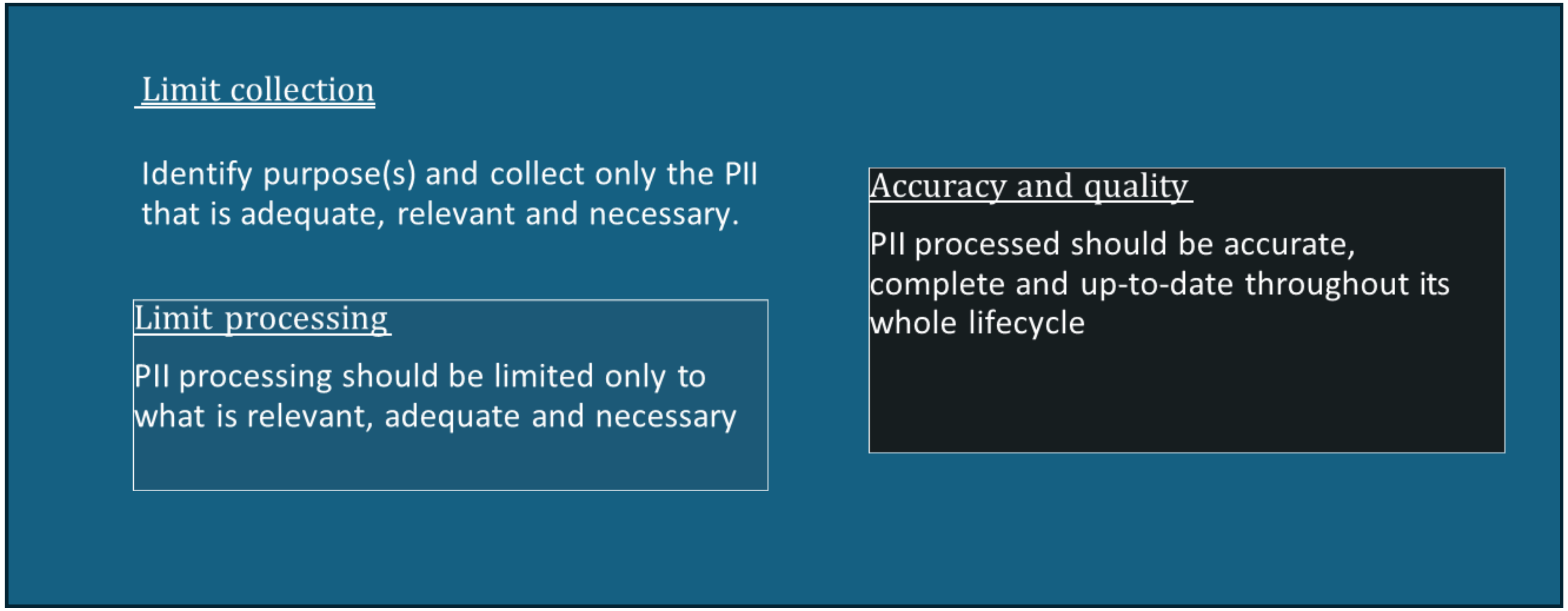
A decision based exclusively on automated means (without human intervention)

Identify legal requirements

(e.g. notification of PII principal, right to object and require human intervention)

7.4. Privacy by design and privacy by default

- Collection and processing of PII is limited only to what is necessary for the purposes of processing



Limit collection

Identify purpose(s) and collect only the PII that is adequate, relevant and necessary.

Limit processing

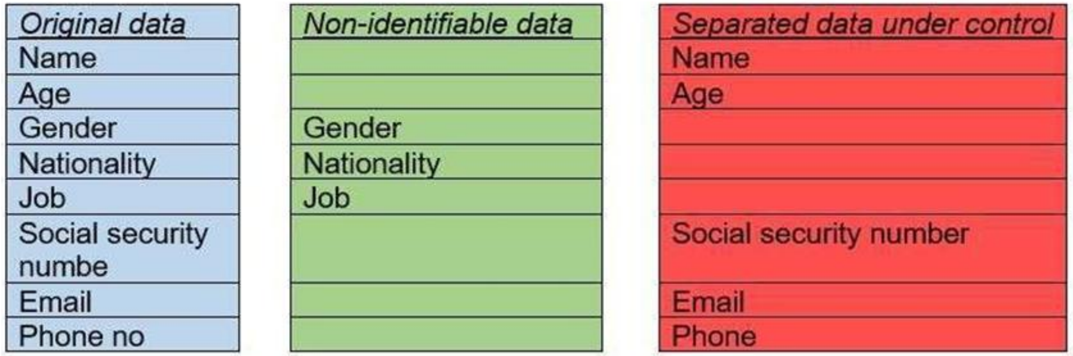
PII processing should be limited only to what is relevant, adequate and necessary

Accuracy and quality

PII processed should be accurate, complete and up-to-date throughout its whole lifecycle

7.4. Privacy by design and privacy by default

- PII minimization objectives
- Data minimization – processing should only use as much personal data as it needs in order to achieve the purpose.
- Data pseudonymization
- PII cannot be attributed to a specific PII principal without additional information



Original data	*Non-identifiable data*	*Separated data under control*
Name		Name
Age		Age
Gender	Gender	
Nationality	Nationality	
Job	Job	
Social security numbe		Social security number
Email		Email
Phone no		Phone

Scrambling: CRISTIAN ⟶ STIIRACN

7.4. Privacy by design and privacy by default

Data anonymization

PII is irreversibly altered so the PII principal can no longer be identified directly or indirectly

data masking, data generalization, adding noise to data ...

The de-identification techniques used should be in line with the results of the Privacy Impact Assessment

7.4. Privacy by design and privacy by default

De-identification and deletion at the end of processing

When not needed for processing PII should be deleted or de-identified

Temporary files

Delete temporary files as soon as they are not needed for the processing

Retention

Keep PII for the shortest period possible to serve the purpose

Disposal

Choose an adequate disposal method

PII transmission controls

Secure PII transmitted and ensure it reaches destination

7.5. PII sharing, transfer, and disclosure
Identify basis for PII transfers between jurisdictions

- Comply to the applicable legislation
  - Data transfers outside the EU under the GDPR:
  - Adequacy decisions
  - Safeguards (e.g. Standard Contractual Clauses, Binding Corporate Rules, certification mechanisms)
  - PII principal information and consent

7.5. PII sharing, transfer, and disclosure

QUALITY ASIA

Countries and international organizations to which PII can be transferred

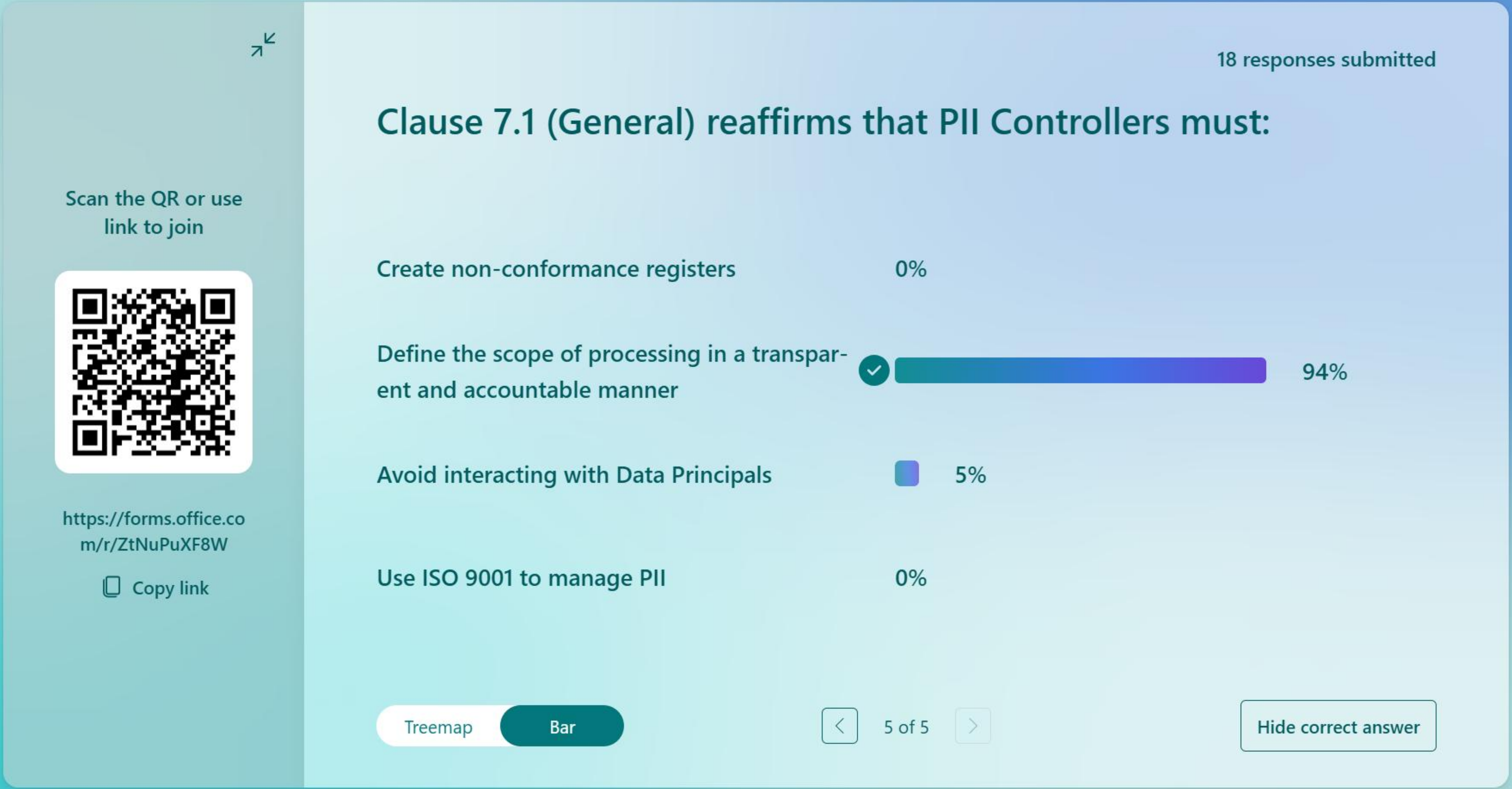
Document and make available to customers the countries and international organizations to which PII can be transferred

Records of transfers of PII

Keep records of PII transfers and cooperate with third parties

Records of PII disclosure to third parties

Maintain records of PII disclosures to third parties (register)



Scan the QR or use link to join

https://forms.office.com/r/ZtNuPuXF8W

18 responses submitted

Clause 7.1 (General) reaffirms that PII Controllers must:

Create non-conformance registers		0%
Define the scope of processing in a transparent and accountable manner	✓	94%
Avoid interacting with Data Principals		5%
Use ISO 9001 to manage PII		0%

Clause 8 - Additional ISO/IEC 27002 guidance for PII processors

Clause No.	Clause Name
8.1.	General
8.2.	Conditions for collection and processing
8.3.	Obligation to PII principals
8.4.	Privacy by design and privacy by default
8.5.	PII sharing, transfer and disclosure

8.2. Conditions for collection and processing

Customer agreement

The contract with the customer should specify the role of the organization in providing assistance

Organization's purposes

PII processing only for purposes specified by the customer and according to its instructions

Marketing and advertising use

Do not use PII for marketing and advertising in the absence of PII principal consent

8.2. Conditions for collection and processing

Infringing instruction

Inform the customer about processing instructions that could be infringing the legislation

Customer obligations

Provide the information needed to meet obligations

Records related to PII processing

Keep records to demonstrate that obligations are fulfilled

8.3. Obligations to PII principals

- Objective: ensure that PII principals receive appropriate information about the processing and that any other obligations towards them are met.

Support the customer in meeting his obligations to PII principals

8.4. Privacy by design and privacy by default

Temporary files

Delete, destroy or otherwise dispose of temporary files as soon as they are not needed for the processing

PII transmission controls

Secure PII transmitted according to the contract or the instructions of the customer

Return, transfer or disposal of PII

Document and make available to customers a policy on retention and disposal of PII at the end of processing

8.5. PII sharing, transfer and disclosure

Transfers

Basis for PII transfers between jurisdictions

Inform the customer on the basis for transferring PII to other jurisdictions so the customer can object.

Countries and international organizations

Document and communicate to the customer the countries and international organizations where PII can be transferred during normal operation

8.5. PII sharing, transfer and disclosure

Disclosure

Records of PII disclosures

Record all PII disclosures (what, to whom, when)

Notification of disclosure requests

Inform the customer on PII disclosure requests

Legally binding PII disclosures

Reject any PII disclosure request that is not legally binding and consult with the customer

8.5. PII sharing, transfer and disclosure

Subcontractors

Disclosure of subcontractors used to process PII

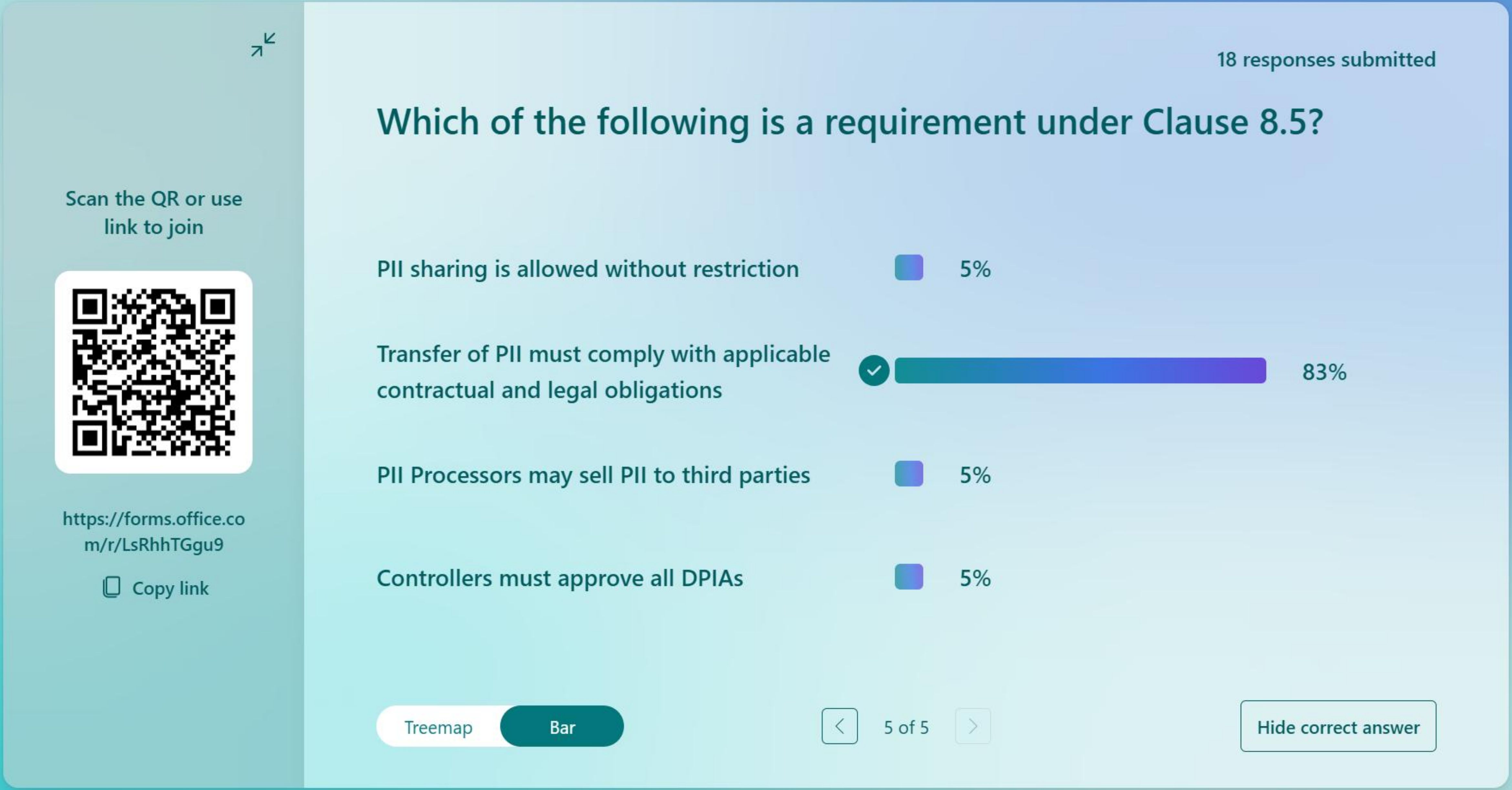
Inform the customer on subcontractors and countries where PII can be transferred

Engagement of a subcontractor to process PII

Obtain an authorization from the customer before subcontracting PII processing

Change of subcontractor to process PII

Obtain the authorization from the customer for changing subcontractors



Scan the QR or use link to join

https://forms.office.com/r/LsRhhTGgu9

18 responses submitted

Which of the following is a requirement under Clause 8.5?

PII sharing is allowed without restriction 5%

✓ Transfer of PII must comply with applicable contractual and legal obligations 83%

PII Processors may sell PII to third parties 5%

Controllers must approve all DPIAs 5%

5 of 5

Certification to ISO/IEC 27701

- ISO/IEC 27701 is a certifiable extension to ISO/IEC 27001 for establishing a Privacy Information Management System (PIMS).

Who Can Get Certified?

- Organizations that:
  - Are already **ISO/IEC 27001 certified**
  - Process PII as **Controllers, Processors, or both**
  - Have implemented the additional **PIMS controls** from ISO/IEC 27701
- Certification is typically issued by an accredited certification body **after successful PIMS audit**, building upon ISO/IEC 27001.

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 AIMS have been identified and are effectively controlled.

Reasons for Conducting Audits

- To examine the Privacy Information Management System for Improvements
- To ensure ISO 27701, and all other standards, are being complied with.
- To determine compliance or non-compliance
- To meet regulatory requirements
- To enable certification

QUALITY ASIA

Effective Audits - Requirements

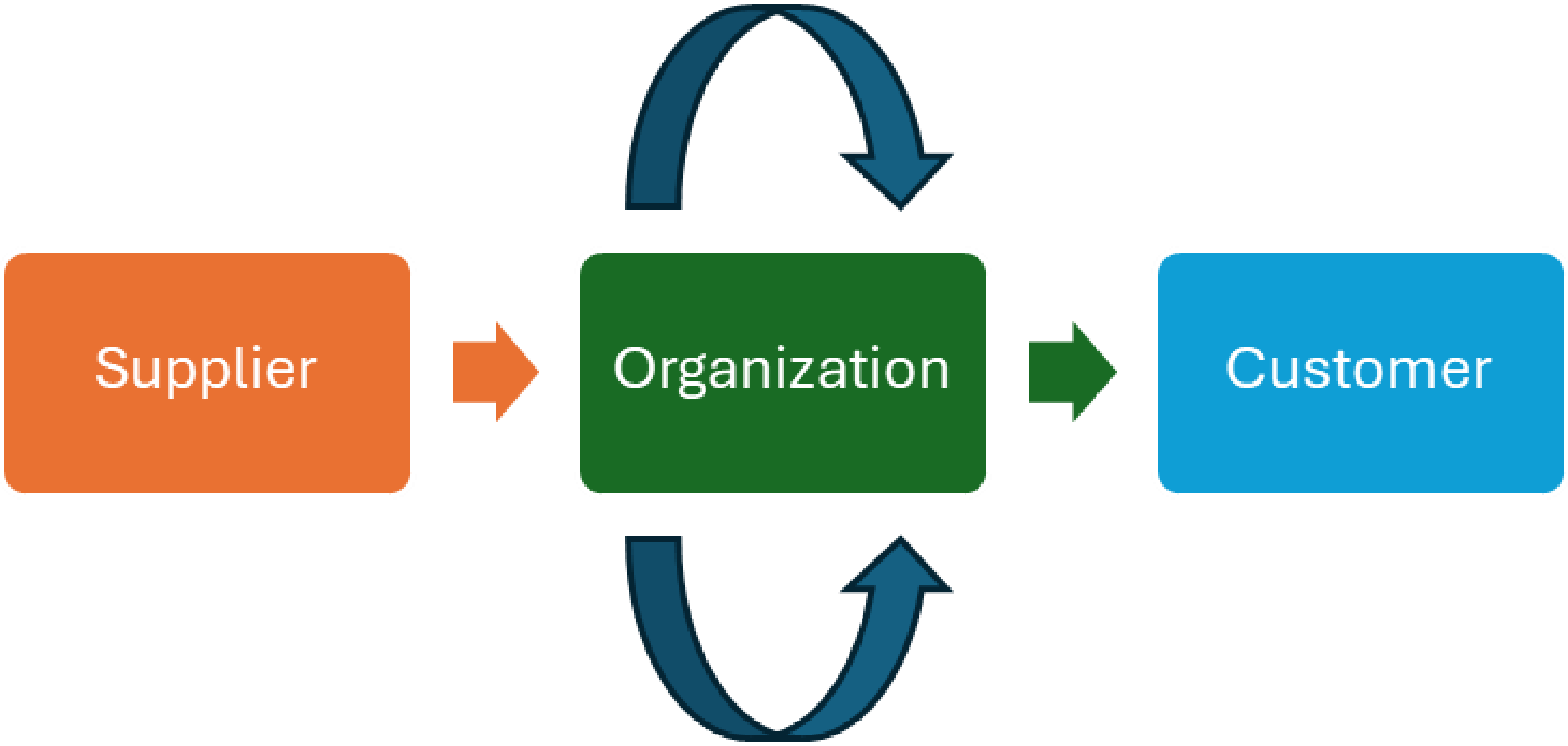
- Timely access to facilities, documents and personnel, including top management
- Defined auditing procedures
- Support/involvement of management
- Competent audit team
- Impartial and objective audit team

Type of Audit

- 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



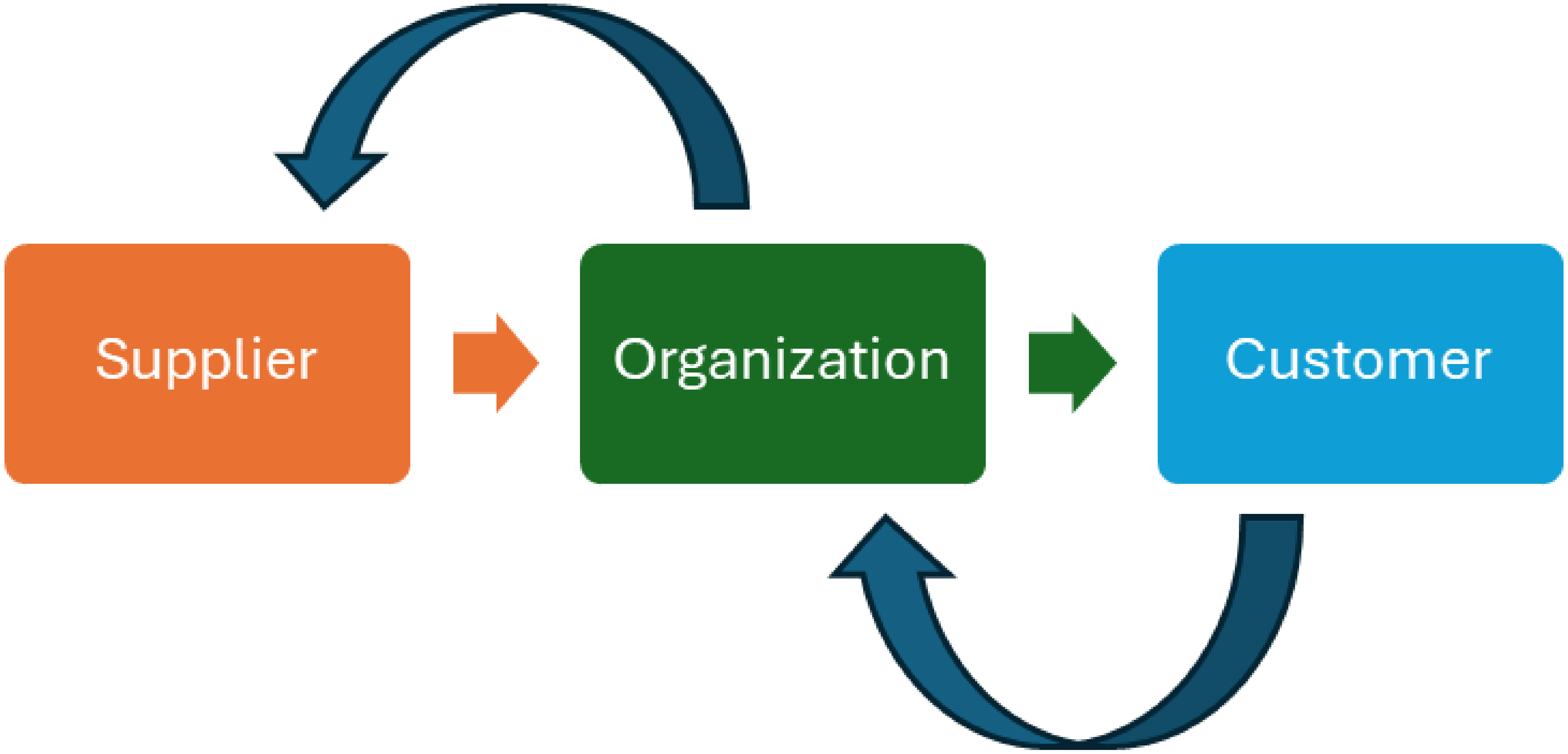
Supplier

Organization

Customer

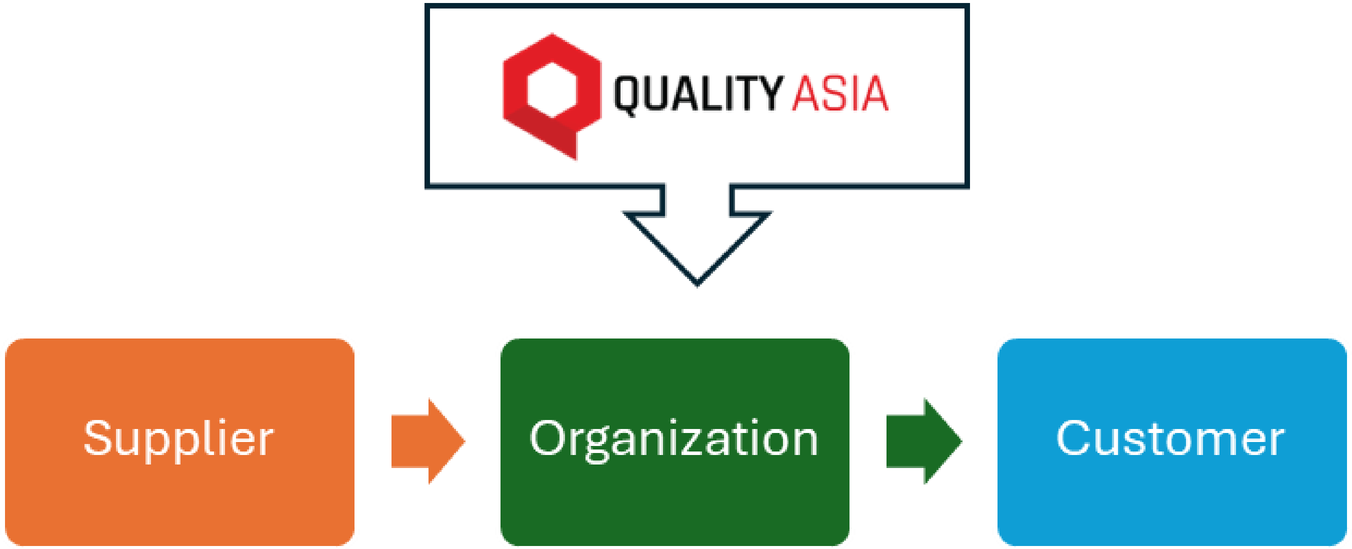
Second Party Audit

- 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

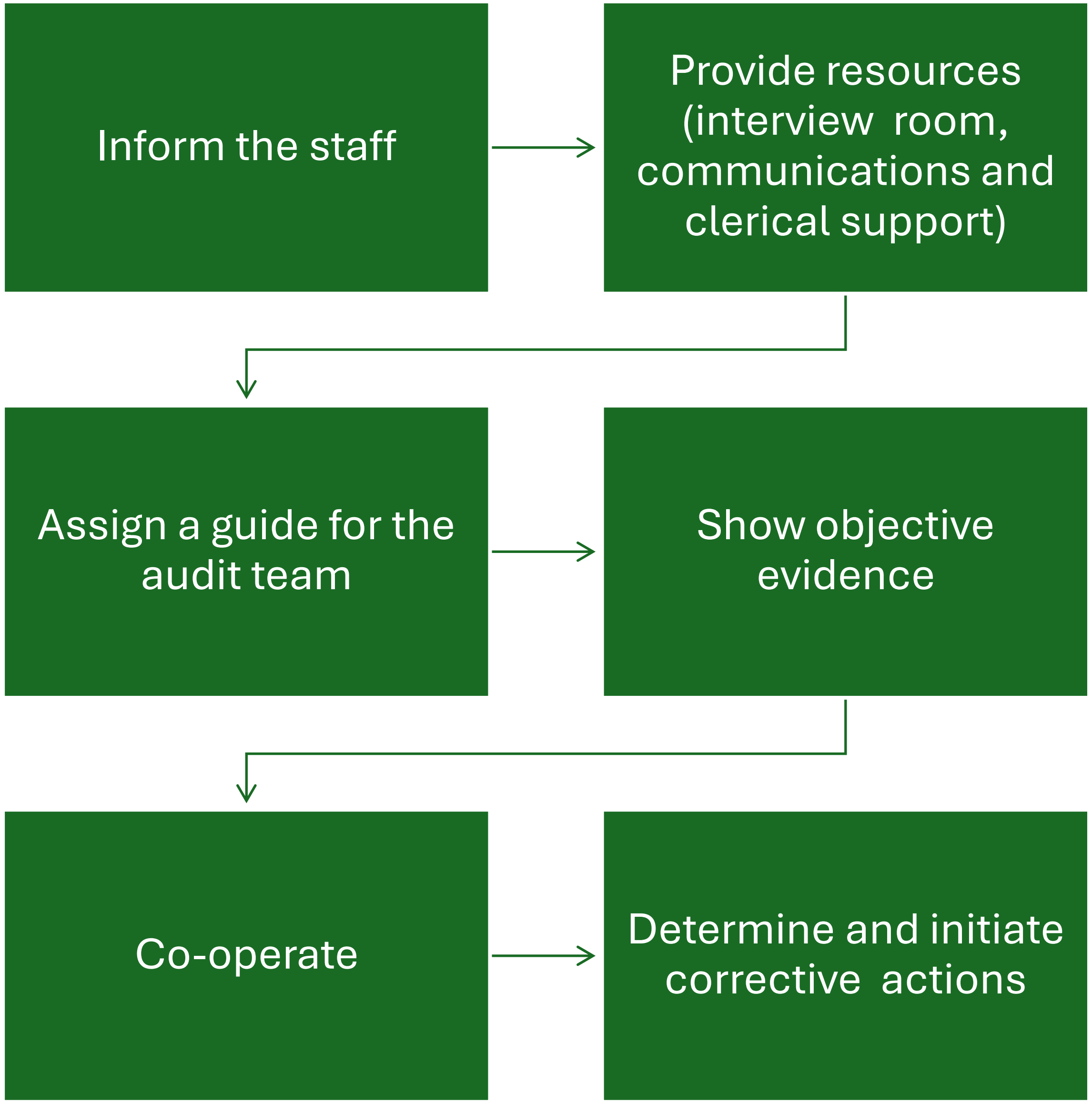
Auditor, responsible for…

- 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

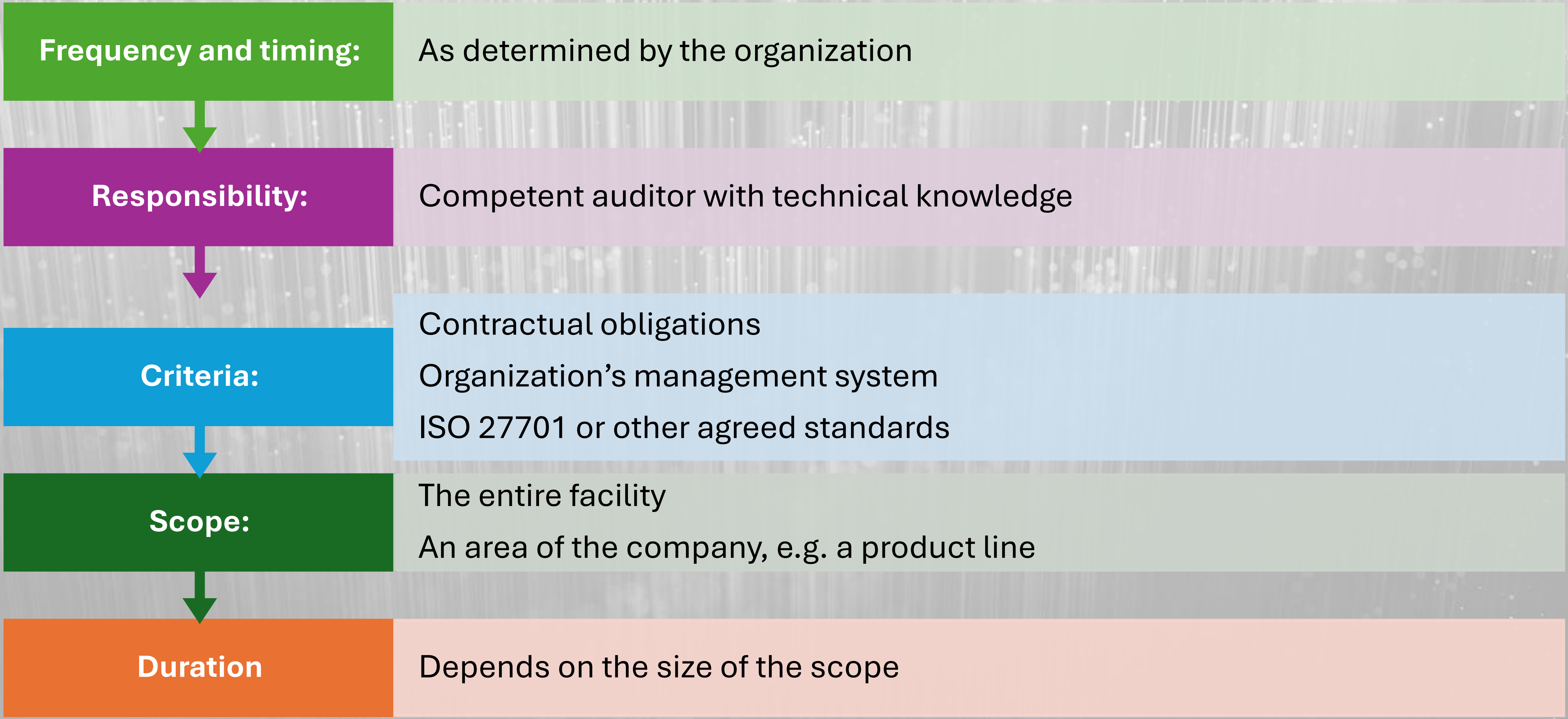
Planning the Audit Stage

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

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. Internal Standards e.g., ISO 27701:2019
Scope:	A process 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 Organization’s management system ISO 27701 or other agreed standards
Scope:	The entire facility 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 27701 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

Audit preparation

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

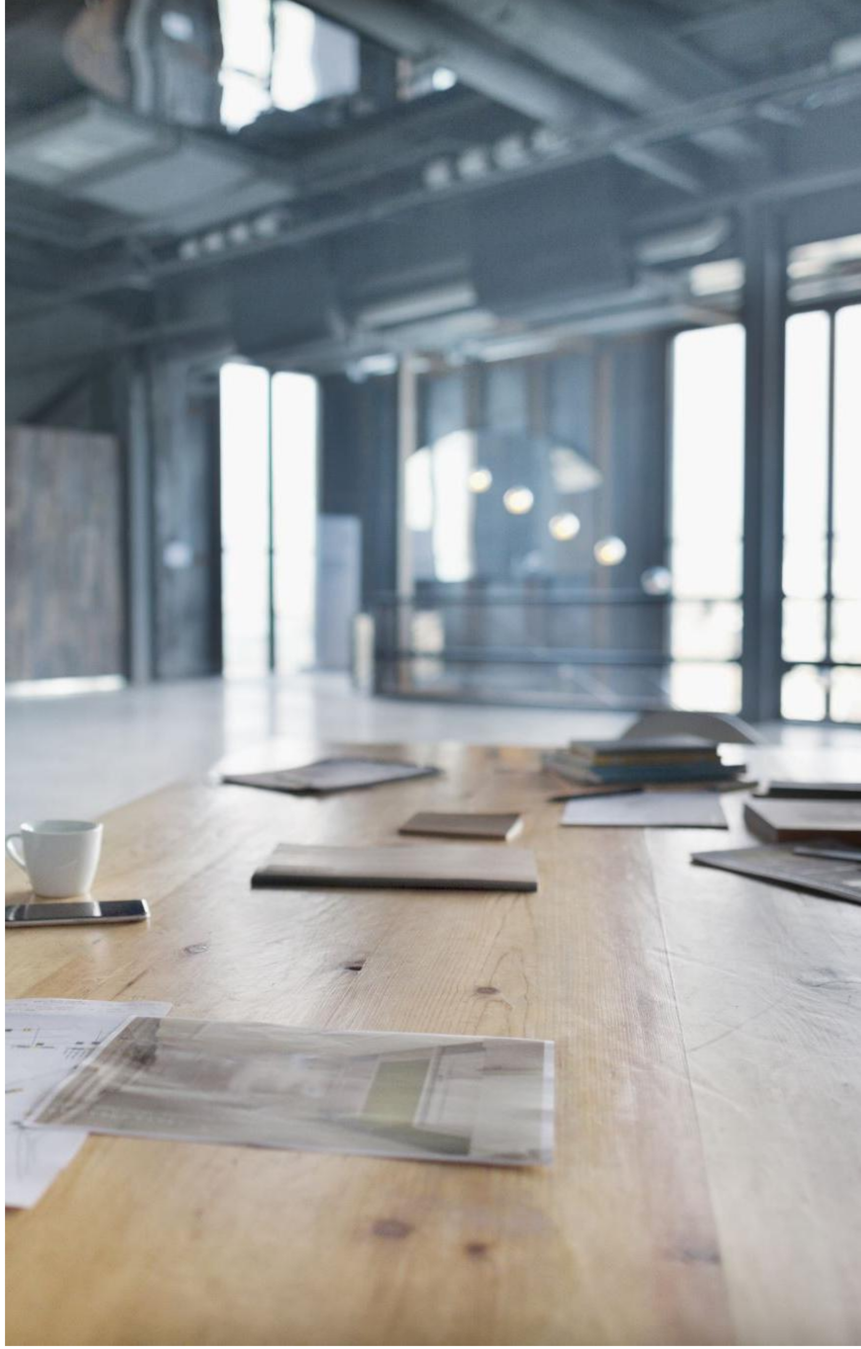
Review documents: procedures, forms, previous reports, corrective action requests, work instructions, etc.

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

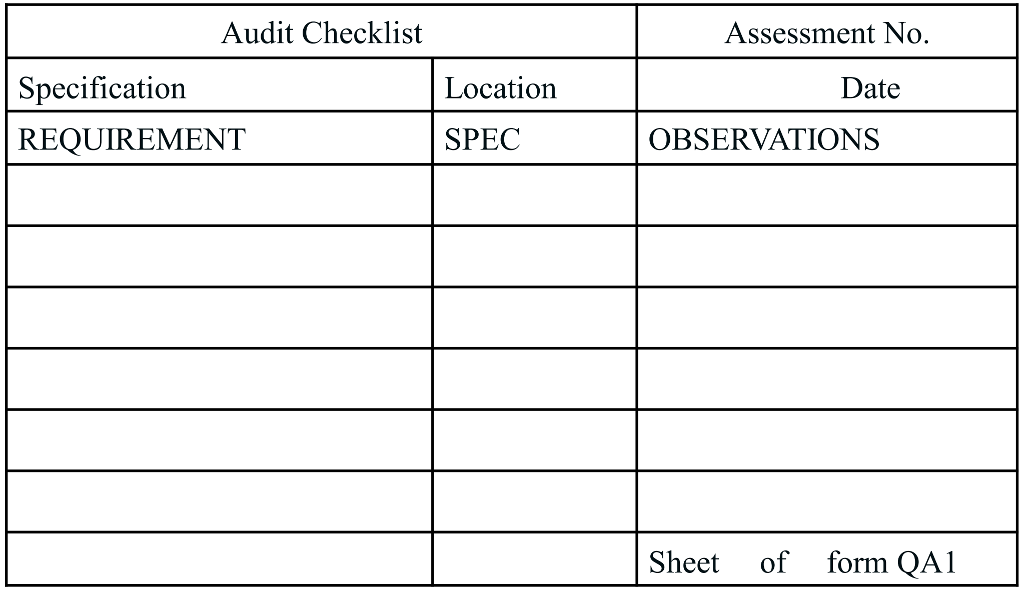
The Purpose of the Checklist

- 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

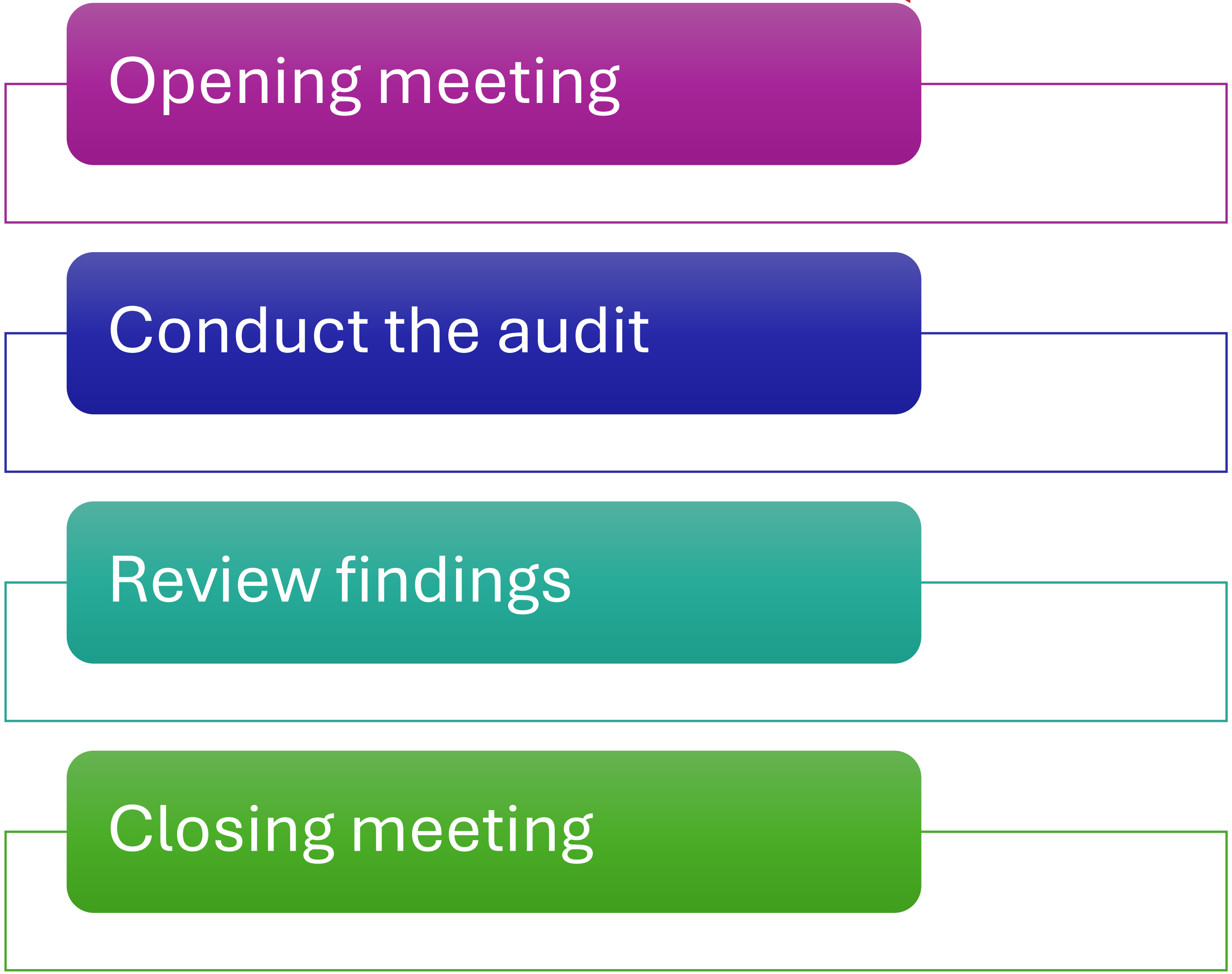
- Too focused on a single area
- Insufficient information included to evaluate conformance in interviews
- Not customized to reflect company's practices

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

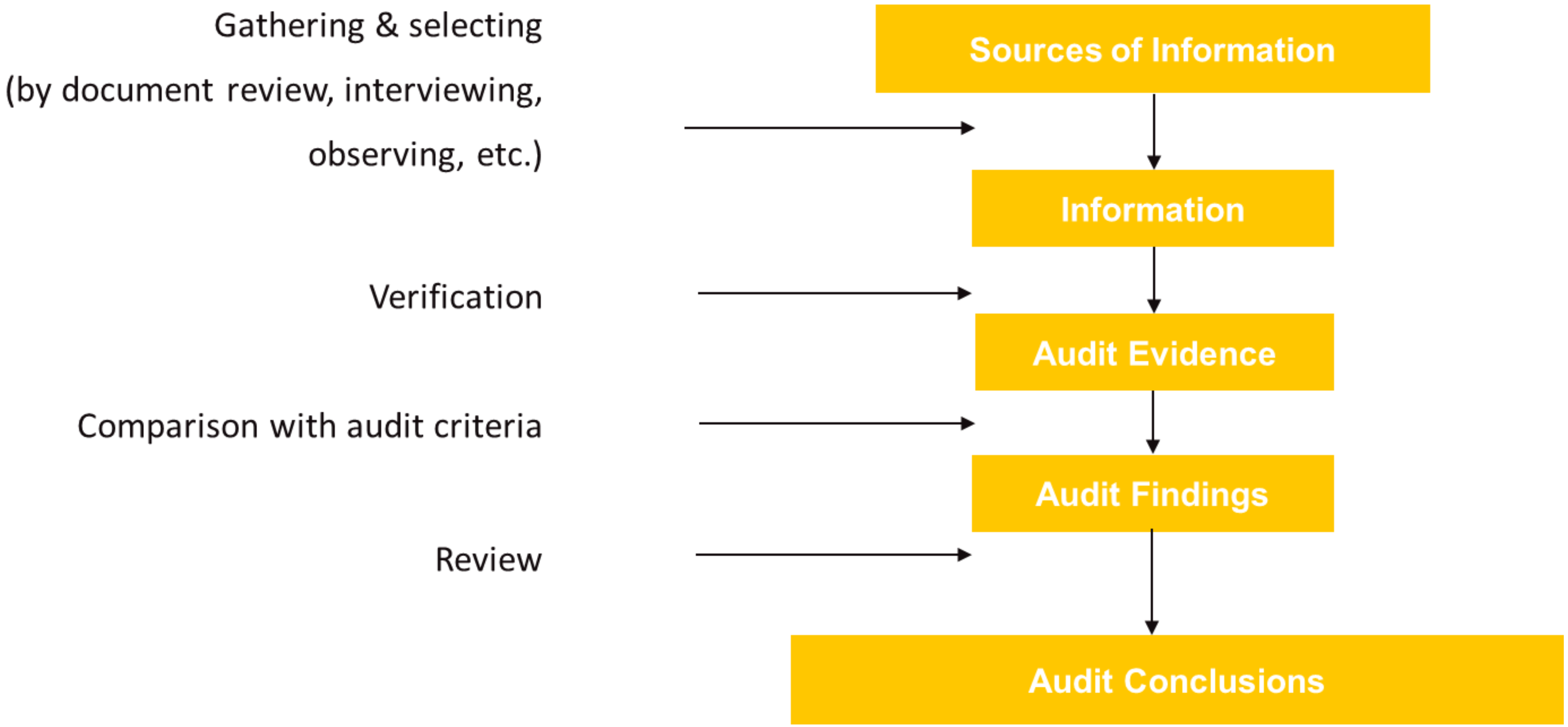
b) Co-operation

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

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 • Constructive • System improvement	• Contracts at stake • Reports used as future reference • More emotional situation than first party audit meeting • Be prepared to be challenged	• Contracts at stake • Reports used as future reference • More emotional situation than first party audit meeting • 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 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 the Privacy Information Management System (PIMS) policies and procedures, leading to ineffective handling of PII-related risks and responsibilities.
- **The requirement, or specific reference to the requirement:**
  - ISO/IEC 27701:2019 – Clause 7.3 (for PII Controllers) / 8.3 (for PII Processors):
  - "Persons working under the organization’s control shall be aware of:
    - The organization’s PII protection policies
    - Their roles in supporting compliance
    - The implications of not conforming to privacy management requirements"
- **The objective evidence observed that supports statement of nonconformity:**
  - During employee interviews, it was found that several team members handling personal data were unaware of the PIMS policy or related data protection procedures. No documented records of PIMS awareness training or communication could be provided during the audit.

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

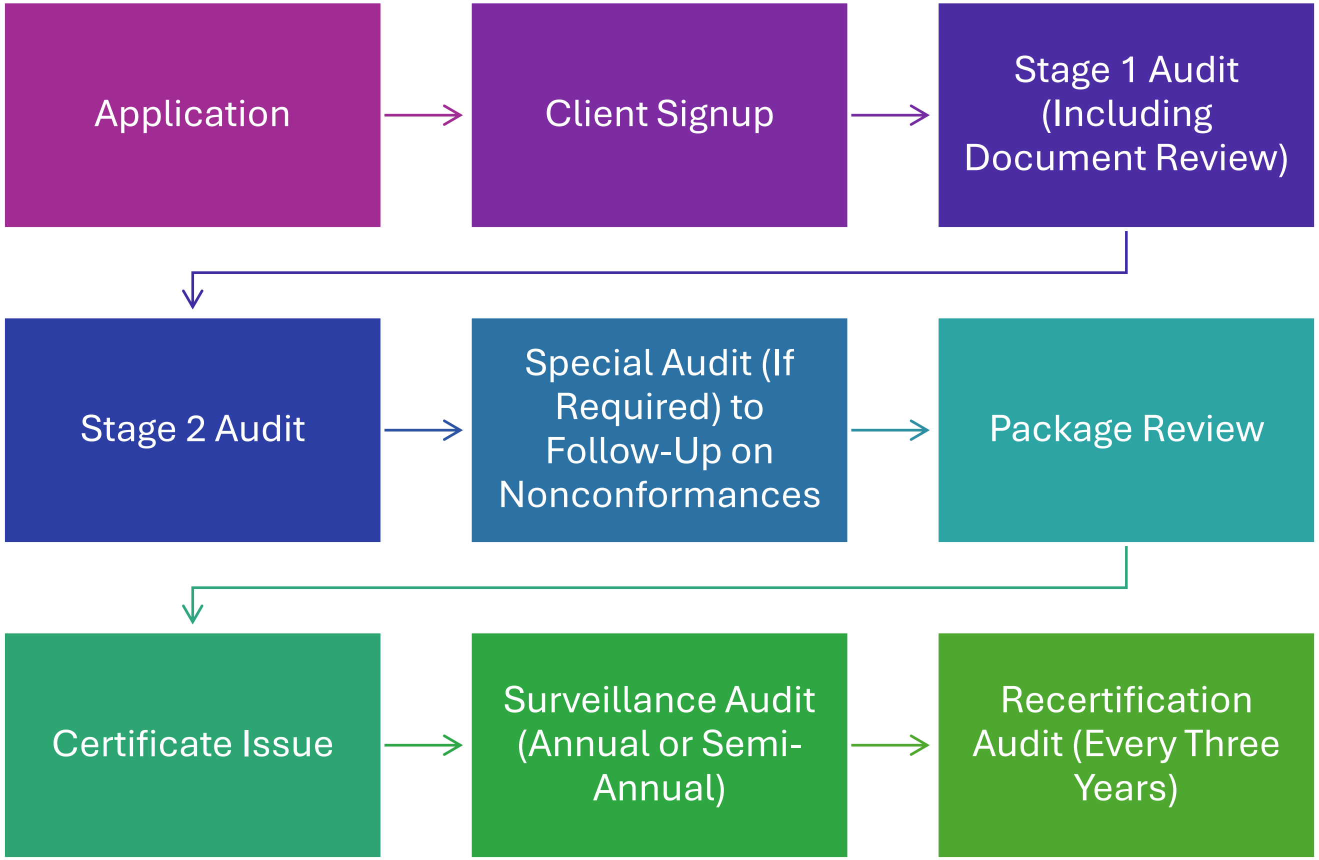
- Description of audit aim, purpose and scope
- Number of non-compliances and summary of audit findings
- Description of good points and any main concerns
- Description of the identified opportunities for improvement
- Recommendations made because of audit findings

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 offer 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)
  - ISO 42001 (ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEM)
  - ISO 27701 (PRIVACY INFORMATION MANAGEMENT SYSTEM)

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

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 School and Free Training program updates…

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

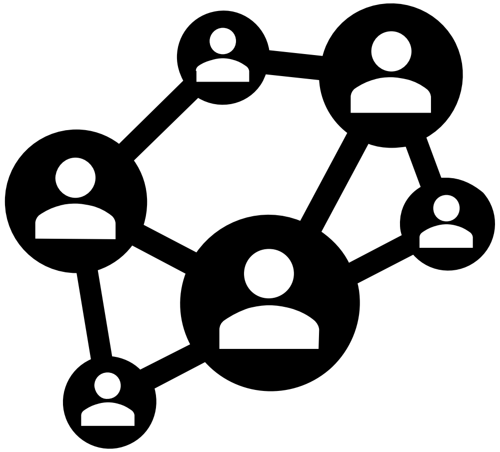
- **Join our WhatsApp channel for convenient access to live training sessions: https://whatsapp.com/channel/0029VamtSmnJ93wcEDIsrT1Z**

Next Upcoming Training Schedule

Training Name	Standard Name	Date	Registration Link
ISO 22301 IA Training Program	Business Continuity Management System (BCMS)	29-June-2025	https://forms.gle/sz3hPnXPUDqkoTnU7
ISO 20000-1 IA Training Program	IT Service Management Systems (ITSMS)	27-July-2025	https://forms.gle/Tzad2KZCs8RmVaWj7

Join us on…

- 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.