How do you secure the data you do not know you have?

April 2021

CERTIFY EY POINT

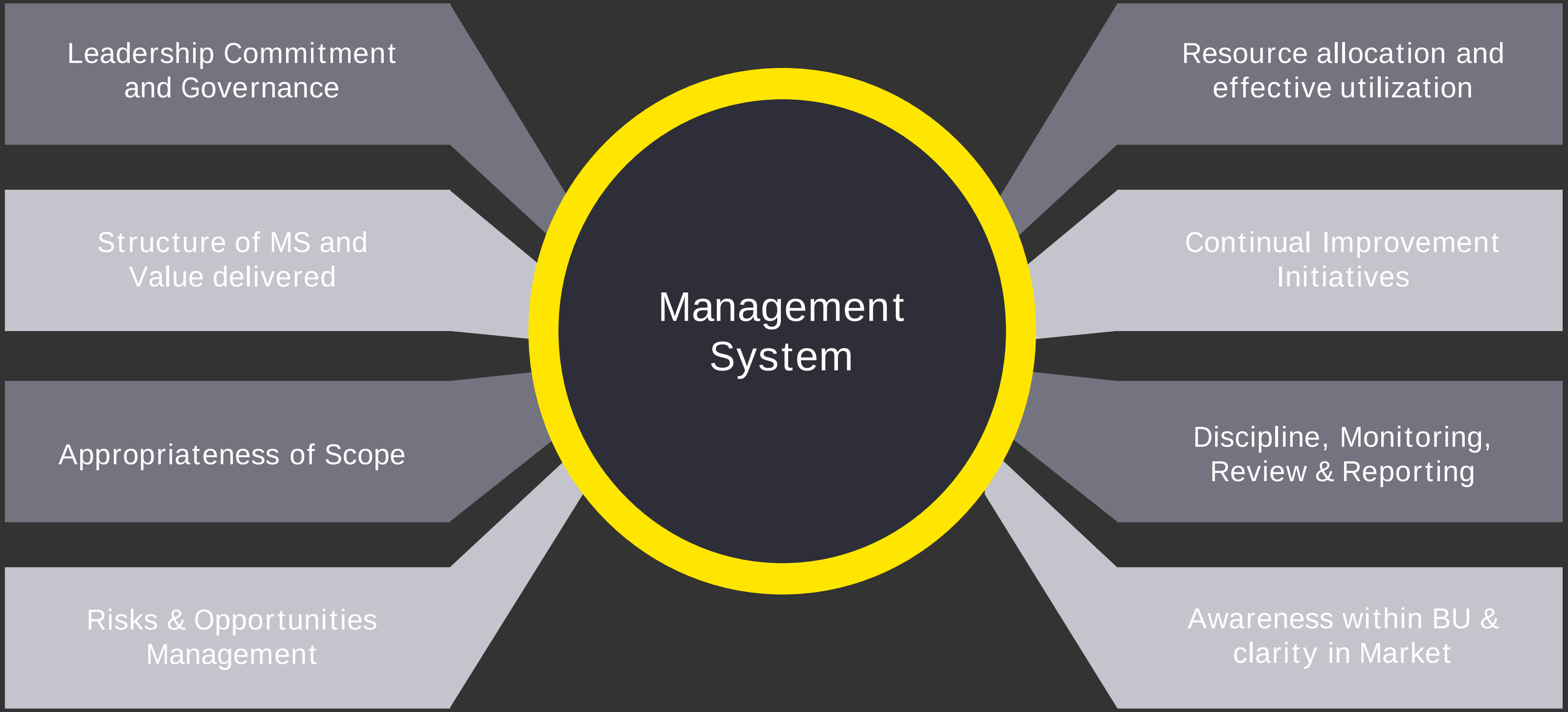
Agenda

1. Setting the scene: Key Concepts
2. Data protection and cyber security through ISO lens
3. Certification

Key Concepts: Management System & Certification

What is a Management System?

A Management System is an important enabler for an organization to meet its objectives in the most effective way. An effective management system addresses all these factors:



Leadership Commitment and Governance
Structure of MS and Value delivered
Appropriateness of Scope
Risks & Opportunities Management
Management System
Resource allocation and effective utilization
Continual Improvement Initiatives
Discipline, Monitoring, Review & Reporting
Awareness within BU & clarity in Market

What is an ISO Certification?

Certification is a procedure in which an independent party provides written confirmation that a product, process or service is compliant with specified demands.

ISO/IEC JTC 1 is a joint technical committee made up of the International Organization for Standardization and the International Electrotechnical Commission. The committee has released standards against various topics, like Information Security, Business Continuity etc.

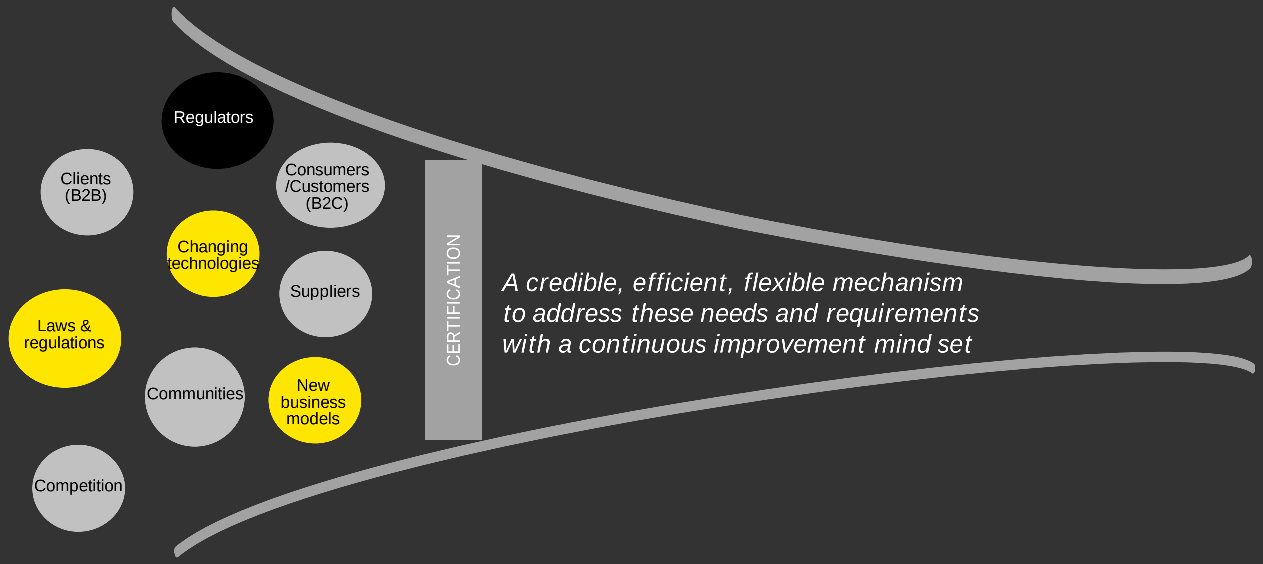
‘’For any organization seeking for improvement, certification should be an outcome/ a result of an effective management system and not the purpose itself’’

Why do organizations get certified?

Building trust in the market is more important than ever. It is becoming more challenging to establish this in a rapidly changing world:

…to create competitive advantage
…to comply with regulations
…to stay in control while maintaining
efficiency and effectiveness

How can certification address this need?



A credible, efficient, flexible mechanism to address these needs and requirements with a continuous improvement mind set

Certification helps to

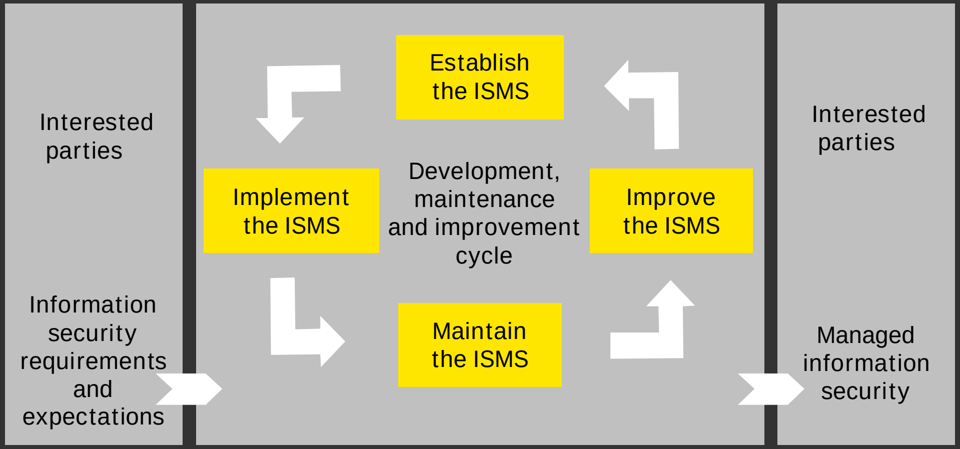
- Build trust and confidence in the market
- Improve performance while at the same time stay ‘’in control’’
- Articulate compliance against regulation and international practices

Data Protection and Cyber Security through ISO lens

ISO/IEC 27001:2013 - a glimpse

Prerequisite for ISO/IEC 27701:2019

- ISO/IEC 27001:2013 provides a common model for implementing and operating an Information Security Management System (ISMS)
- It is not a product or technology driven standard
- It is a comprehensive minimum baseline of information security controls that information security programs shall address in some manner



Interested parties

Information security requirements and expectations

Establish the ISMS

Implement the ISMS

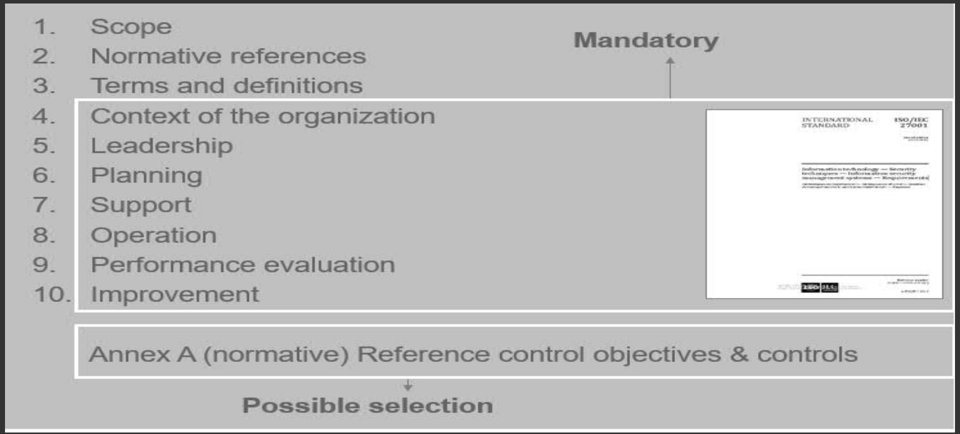
Development, maintenance and improvement cycle

Improve the ISMS

Maintain the ISMS

Interested parties

Managed information security



1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Mandatory

Annex A (normative) Reference control objectives & controls

Possible selection

Augmenting Privacy using Information Security

Personal data** must be secured by means of **'appropriate technical and organizational measures to ensure a level of security'

Access Control *to ensure the appropriate access to the systems and services processing personal data within them.*

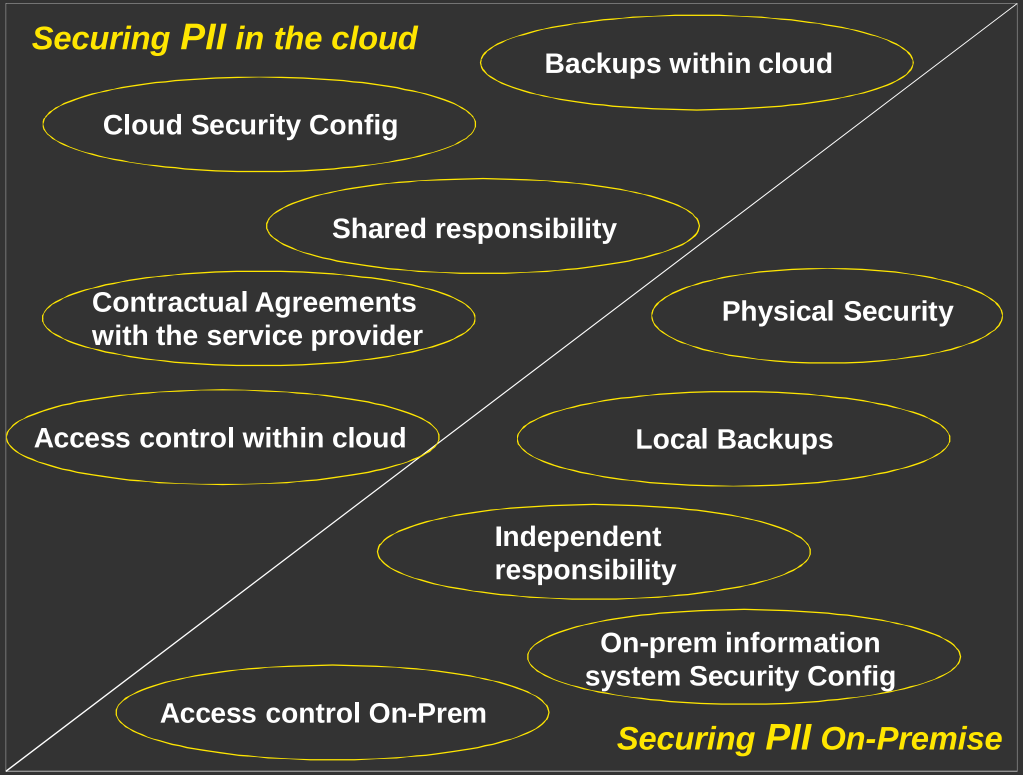
Backups *to restore personal data in a timely manner in the event of a physical or technical incident.*

Cryptography *to enforce measures such as pseudonymisation and encryption to safeguard personal data.*

Data governance *process that identifies all PII or privacy related data, and where it is stored, and the data flow of that data, including what is logged*

Vulnerability scans and tests *to ensure secure configurations of systems and networks that store/ process privacy related information.*

Endpoint protection *to ensure personal data stored/ accessed within end user systems is safeguarded.*



Securing PII in the cloud

- Backups within cloud
- Cloud Security Config
- Shared responsibility
- Contractual Agreements with the service provider
- Access control within cloud

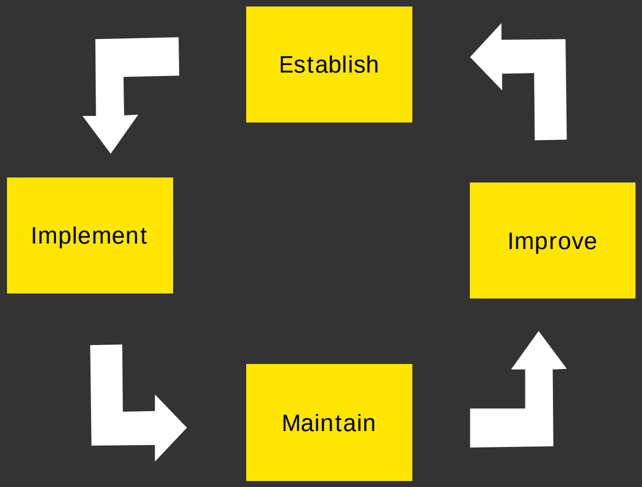
Securing PII On-Premise

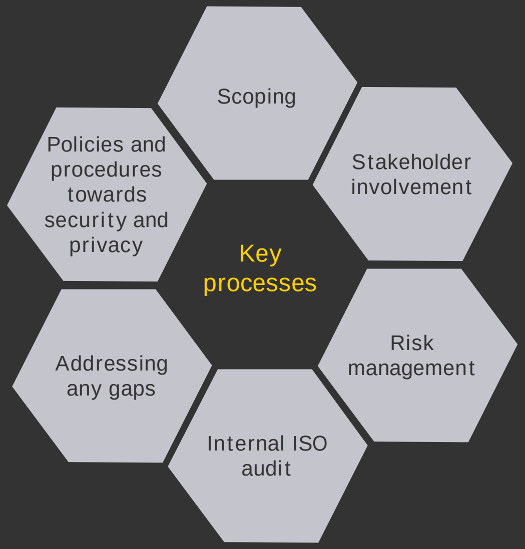
- Physical Security
- Local Backups
- Independent responsibility
- On-prem information system Security Config
- Access control On-Prem

Introducing ISO/IEC 27701:2019

- Released in August 2019. ISO/IEC 27701:2019 is a certifiable privacy extension to ISO/IEC 27001.
- Outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.
- Structure of the standard:
  - PIMS requirements related to ISO/IEC 27001:2013 are outlined in clause 5.
  - PIMS requirements related to ISO/IEC 27002:2013 are outlined in clause 6.
  - PIMS guidance for PII Controllers are outlined in clause 7
  - PIMS guidance for PII Processors are outlined in clause 8
  - The standard further includes the following informative Annex:
    - Annex A lists all applicable controls for PII Controllers
    - Annex B lists all applicable controls for PII Processors
    - Annex C maps ISO/IEC 27701:2019 controls against GDPR
    - Annex D maps ISO/IEC 27701:2019 controls against ISO/IEC 29100
    - Annex E maps ISO/IEC 27701:2019 controls against ISO/IEC 27018
    - Annex F maps ISO/IEC 27701:2019 controls against ISO/IEC 29151

Getting to know the framework





Security and Privacy controls

Privacy controls for PII controllers

Privacy controls for PII Processors

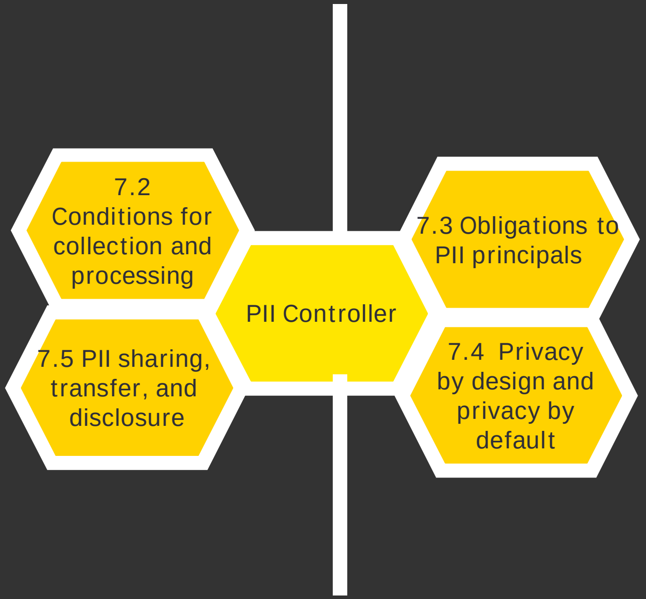
- Extending security policies to include privacy, as applicable.
- Is the organization a PII controller?
- Is the organization a PII processor?

Example control: Controller

Clause 7.2.5

Assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned

Determine the criteria for conducting a PIA, and the elements that are necessary for the completion of a PIA, such as types of PII processed, where the PII is stored and where it can be transferred, and risks and controls pertaining to this PII processing

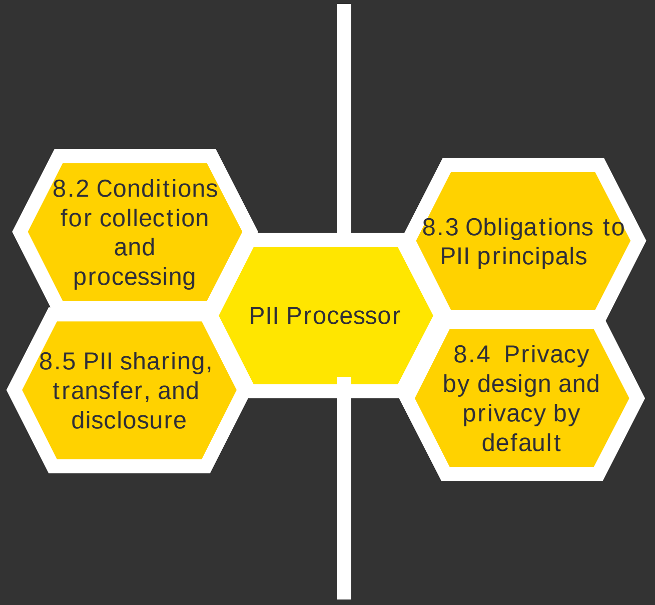

7.2 Conditions for collection and processing
7.3 Obligations to PII principals
PII Controller
7.5 PII sharing, transfer, and disclosure
7.4 Privacy by design and privacy by default

Example control: Processor

Clause 8.2.3

Not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal.

Compliance of PII processors with the customer's contractual requirements should be documented,
especially where marketing and/or advertising is planned. Organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals.


8.2 Conditions for collection and processing
8.3 Obligations to PII principals
PII Processor
8.5 PII sharing, transfer, and disclosure
8.4 Privacy by design and privacy by default

Example regulatory mapping: GDPR

Clause 8.5.8

The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

Mapped GDPR Article 28(2)

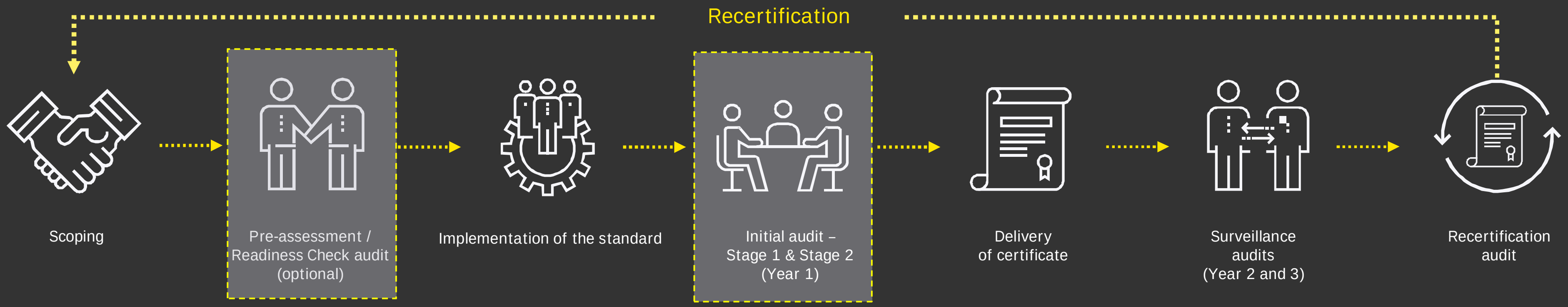
The processor shall not engage another processor without prior specific or general written authorisation of the controller. [2]In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes

Note: The controls framework can also be leveraged for other regulatory requirements, e.g. CCPA, HIPAA

3

Certification Process

Certification process


Recertification

Scoping

Pre-assessment / Readiness Check audit (optional)

Implementation of the standard

Initial audit – Stage 1 & Stage 2 (Year 1)

Delivery of certificate

Surveillance audits (Year 2 and 3)

Recertification audit

Common pitfalls in certification readiness

Right scope – too ambitious or too little

Buy in – Either inadequate executive buy-in or poor roles and responsibilities

Inadequate documentation - – not having the mandatory one's

GRC tooling – Expecting a GRC tool is the solution.

Inadequate integration of the ISO 27701 requirements with existing frameworks

Internal audit – not performing this before the audit.

High on security controls – Focusing only on the Annex A controls doesn't get you the framework in place.

Right competence – failing to establish the right competence

Q&A

Would you like more information? Feel free to reach out to us!

Ayse Yavuz
Ayse.Yavuz@nl.ey.com

Jatin Sehgal
Jatin.Sehgal@nl.ey.com

Thank you!