GIERSCHMANN

Dealing with ISO/IEC 27701 and the GDPR

Square Table, ISACA Netherlands Chapter

25 November 2020,
Markus Gierschmann

Agenda

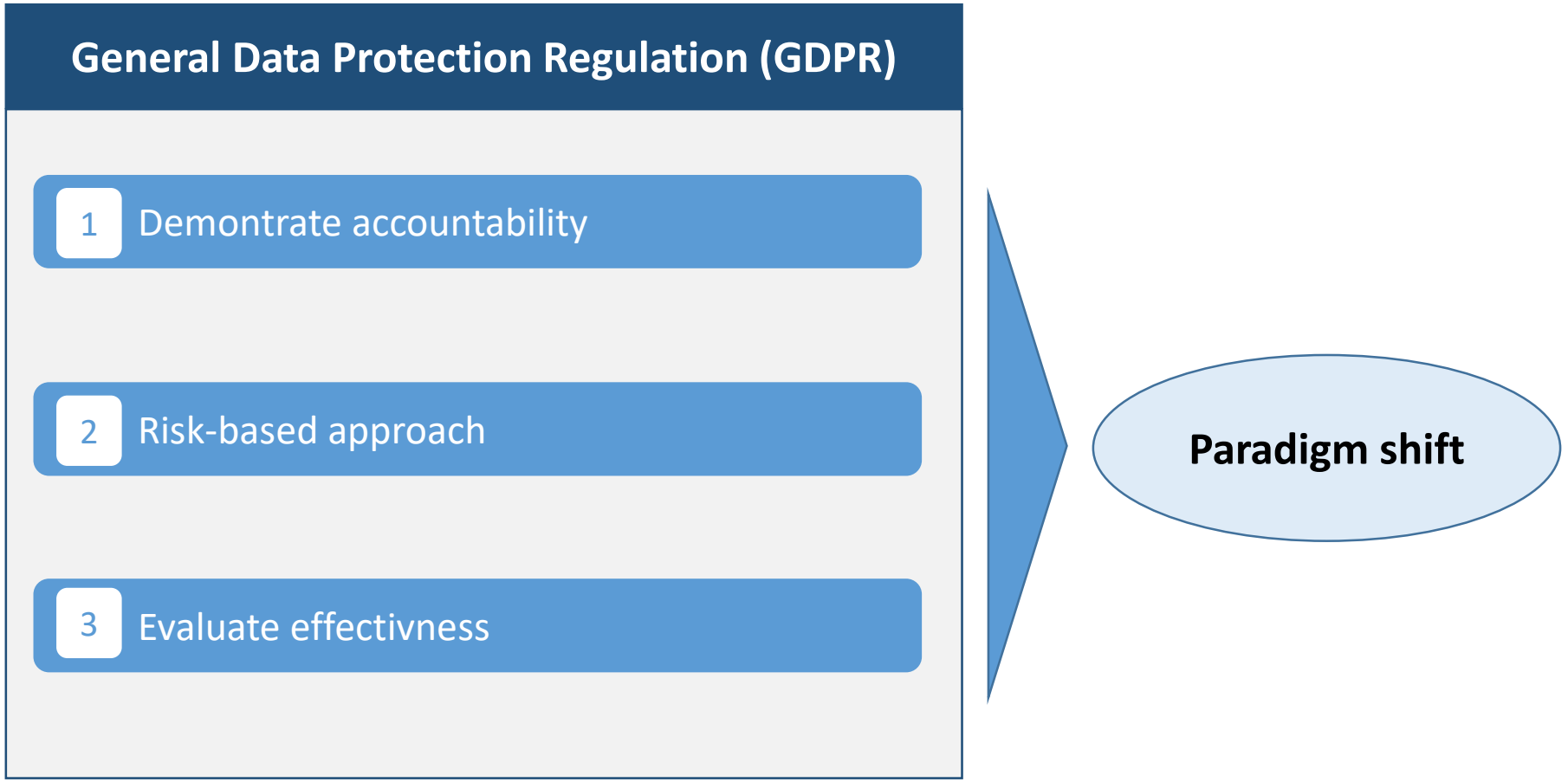
- **GDPR as a game changer**

- International PIMS standard: ISO/IEC 27701

- ISO certification versus GDPR certification

- Outlook: Refinement of ISO 27701 in European Context

Game changer



Accountability = Shifting the burden of proof?

Product liability
in the production

Concept of quality
= perceptible form of state

Process orientation
for repetitive quality assurance
→ PDCA

Quality management system
QMS according to ISO 9001

Accountability
in data protection

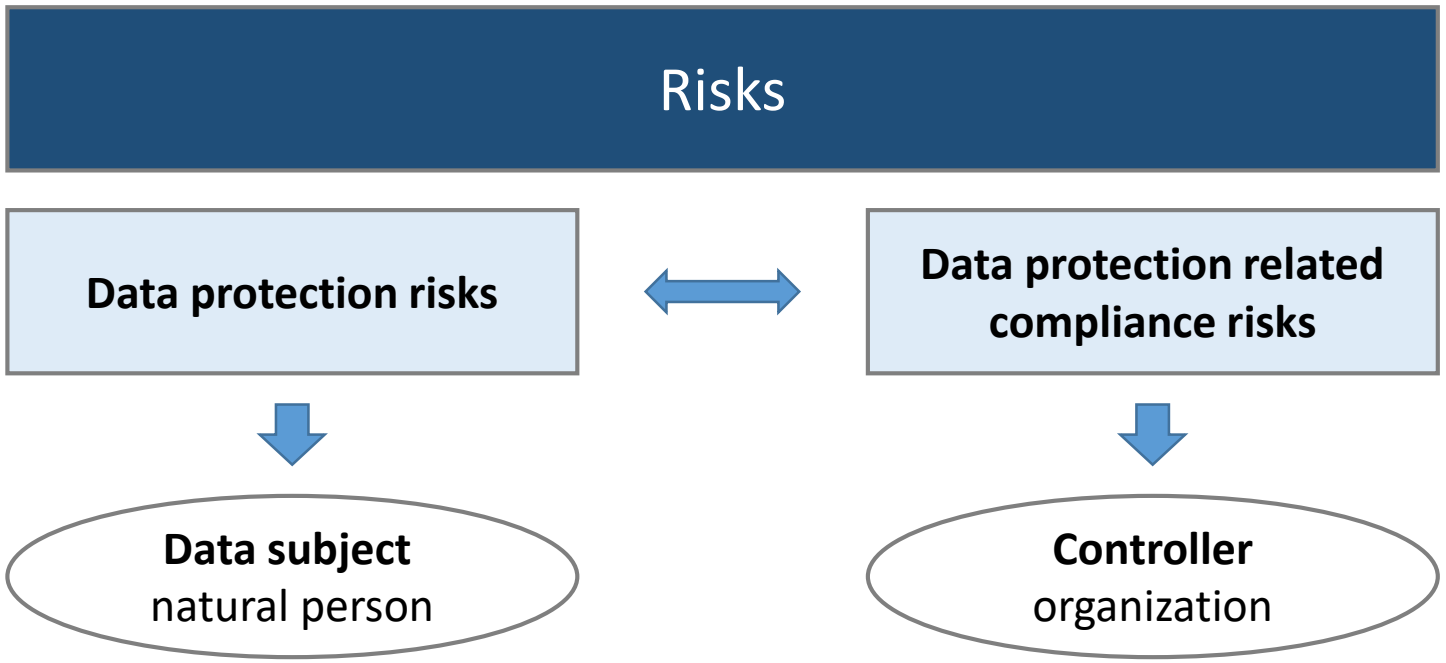
Be able to provide evidence
How responsibility is verifiably perceived

„Compliance-Programs“

Regulated certificates
as reliable evidence
→ Harmonisation of the „standards“

Art. 29-Gruppe, WP 173, 2010

Risks for organization and natural person

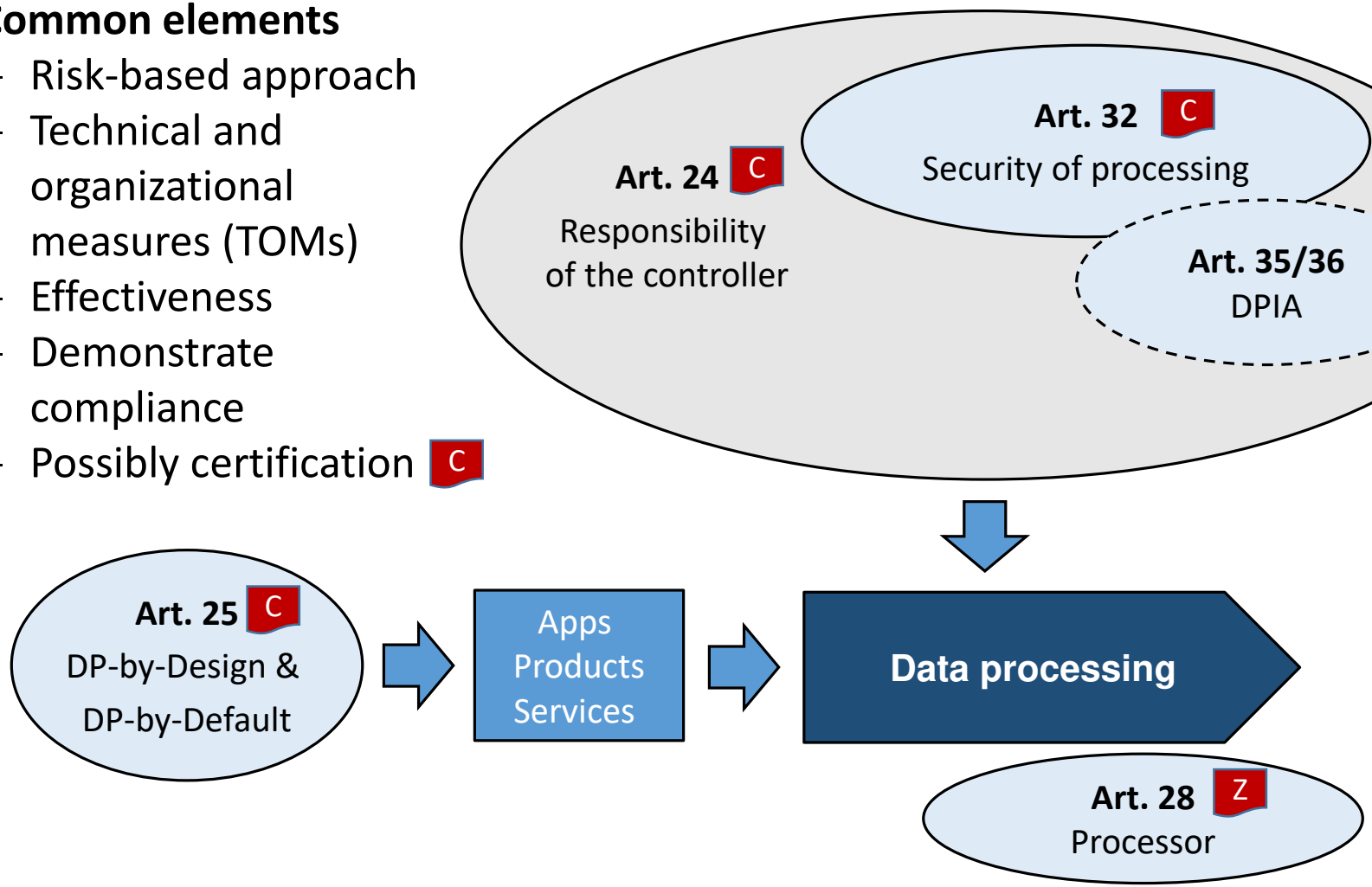


GDPR only considers only risks for the rights and freedoms of natural persons (data subjects); non conformance with regulations/obligations is a compliance risk for controllers.

Risk-based approach

Common elements

- Risk-based approach
- Technical and organizational measures (TOMs)
- Effectiveness
- Demonstrate compliance
- Possibly certification C



„A Privacy Management Program is a must to demonstrate accountability.“

Andrea Jelinek, Vorsitzende EDSA

ICDPPC 2019, Tirana, Albanien

Agenda

- GDPR as a game changer
- **International PIMS standard: ISO/IEC 27701**
- ISO certification versus GDPR certification
- Outlook: Refinement of ISO 27701 in European Context

Privacy Information Management System (PIMS)

INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Privacy Information Management System (PIMS)

ISMS required

No GDPR compliance

No certification according to Art. 42 GDPR


INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

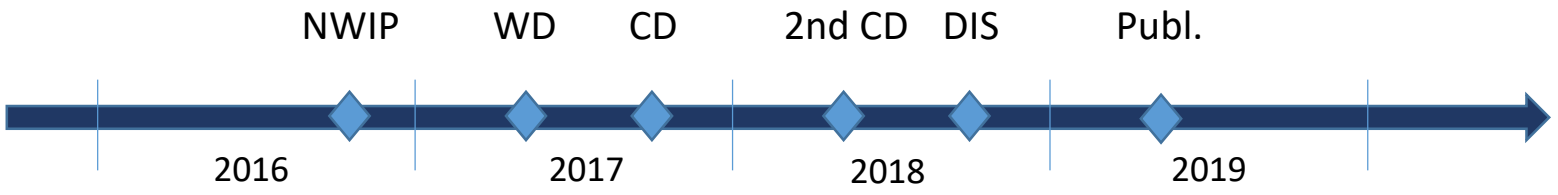
Structured approach

Integrated management system

Global application

Background and development

- ***ISO/IEC meetings and development of ISO-Standard***
  - ***JTC 1/SC 27*** *Information security, cybersecurity and privacy protection*
  - ***WG 5*** *Identity Management & Privacy Technologies*



- ***ISO/IEC 27701****, Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
  - Privacy Information Management System (PIMS) as an extension of an information management system (ISMS)
  - Information security → Information security and privacy

Key design elements

Extension of an ISMS	**PIMS** is an information security management system (ISMS) which addresses the protection of privacy as potentially affected by the processing of PII
PIMS-specific requirements and guidance	Establishing, implementing, maintaining and continually improving a PIMS in the form of an **extension to ISO/IEC 27001 and ISO/IEC 27002** for privacy management within the context of the organization
Extended interpretation of information security	Where "information security" is used in ISO/IEC 27001 or 27002, "**information security and privacy**“ applies instead

Key design elements

5.2.3 Determining the scope of the information security management system

A requirement additional to ISO/IEC 27001:2013, 4.3 is:

When determining the scope of the PIMS, the organization shall include the processing of PII.

NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.

Extension of an ISMS	potentially affected by the processing of PII
PIMS-specific requirements and guidance	Establishing, implementing, maintaining and continually improving a PIMS in the form of an **extension to ISO/IEC 27001 and ISO/IEC 27002** for privacy management within the context of the organization
Extended interpretation of information security	Where "information security" is used in ISO/IEC 27001 or 27002, "**information security and privacy**“ applies instead

Key design elements

Extension of an ISMS	**PIMS** is an information security management system (ISMS) which addresses the protection of privacy as
PIMS-specific requirements guidance	the context of the organization
Extended interpretation of information security	Where "information security" is used in ISO/IEC 27001 or 27002, "**information security and privacy**“ applies instead

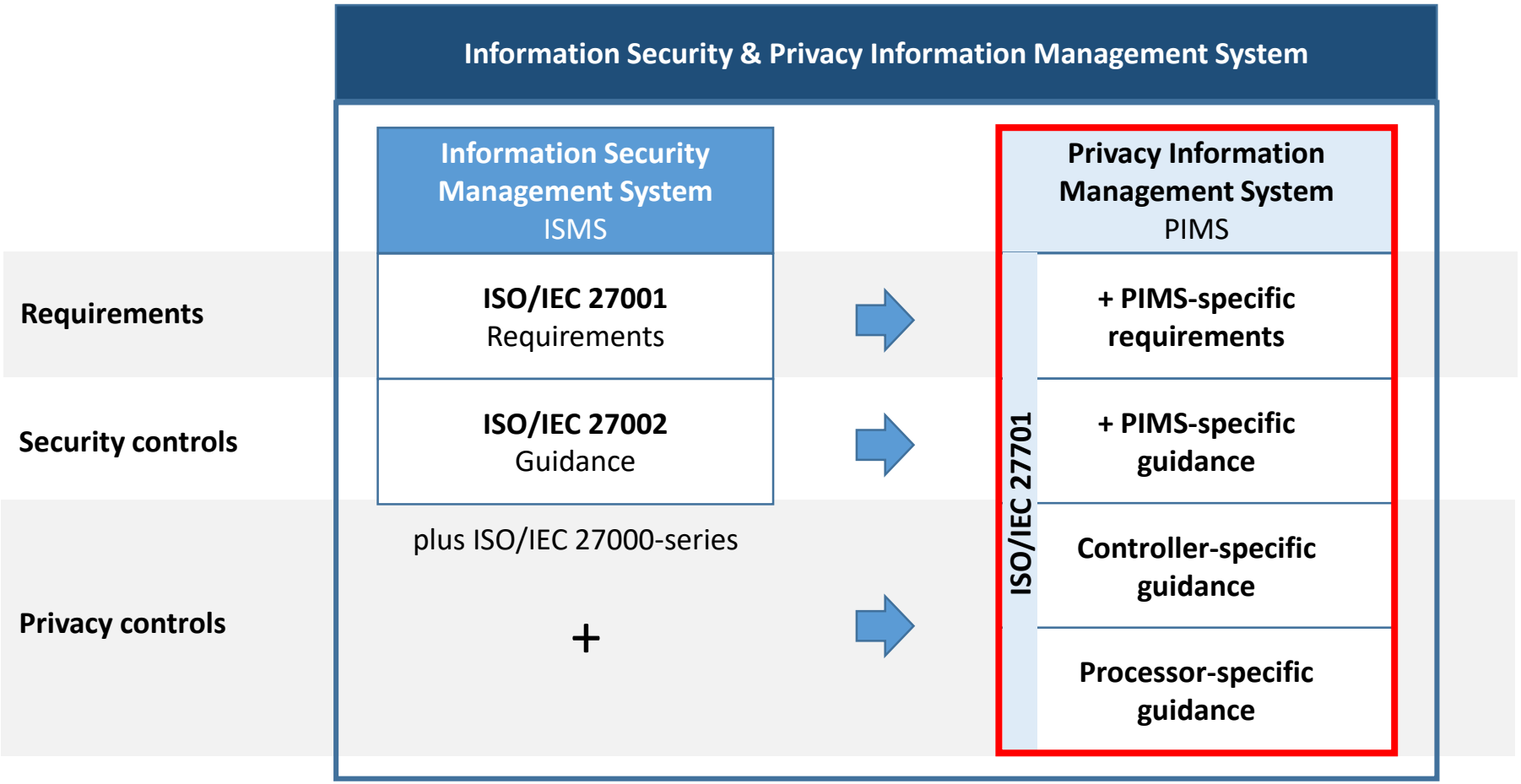
5 PIMS-specific requirements related to ISO/IEC 27001

5.1 General

The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.

NOTE In practice, where "information security" is used in ISO/IEC 27001:2013, "information security and privacy" applies instead (see Annex F).

Structure


Information Security & Privacy Information Management System
Information Security Management System
ISMS
Privacy Information Management System
PIMS
Requirements
ISO/IEC 27001
Requirements
+ PIMS-specific requirements
Security controls
ISO/IEC 27002
Guidance
+ PIMS-specific guidance
plus ISO/IEC 27000-series
Privacy controls
+
Controller-specific guidance
Processor-specific guidance
ISO/IEC 27701

PIMS-specific extension of ISO/IEC 27001

ISO/IEC 27001	Content
1. Context of the organization	1) Organization and its context, 2) Needs and expectations of interested parties, 3) Scope of the ISMS, 4) ISMS
2. Leadership	1) Leadership and commitment, 2) Policy, 3) Organizational roles, responsibilities and authorities
3. Planning	1) Actions to address risks and opportunities, 2) Information security objectives and planning to achieve them
4. Support	1) Resources, 2) Competence, 3) Awareness, 4) Communication, 5) Documented information
5. Operation	1) Operational planning and control, 2) Information security risk assessment, 3) Information security risk treatment
6. Performance evaluation	1) Monitoring, measurement, analysis and evaluation, 2) Internal audit, 3) Management review
7. Improvement	1) Nonconformity and corrective action, 2) Continual improvement

ISO 27701
Additional PIMS-specific requirements
Privacy risk management

PIMS-specific extension of ISO/IEC 27001

ISO/IEC 27001	Content	ISO 27701
1. Context of the organizat	1) Organization and its context, 2) Needs and expectations of	Additional PIMS-specific requirements
2. Leader		
3. Planni		
4. Suppo		
5. Opera		Privacy risk management
6. Perfor evaluatic		
7. Improvement	1) Nonconformity and corrective action, 2) Continual improvement	

5.4.1.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements:

ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows:

The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

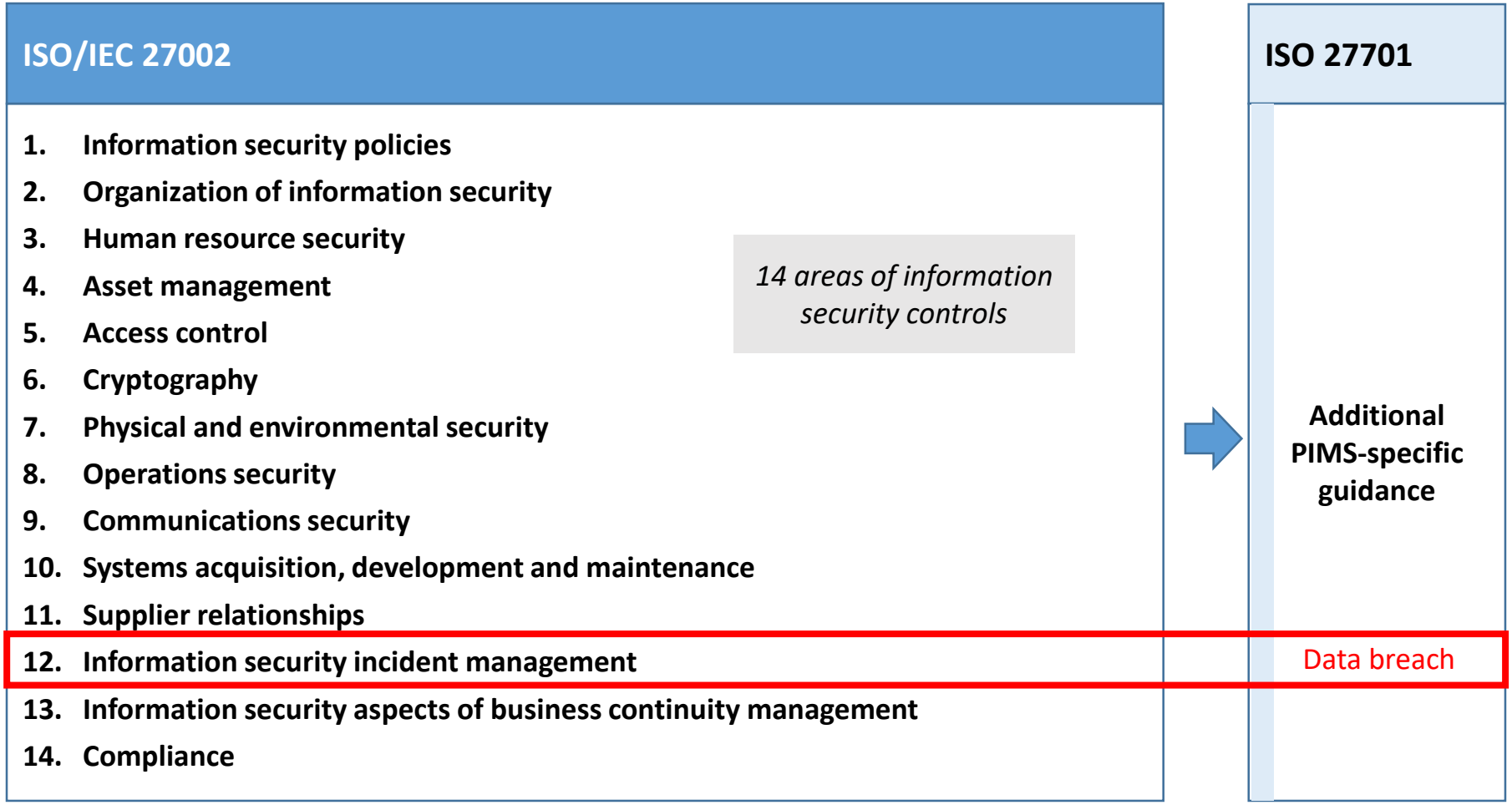
The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.

NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

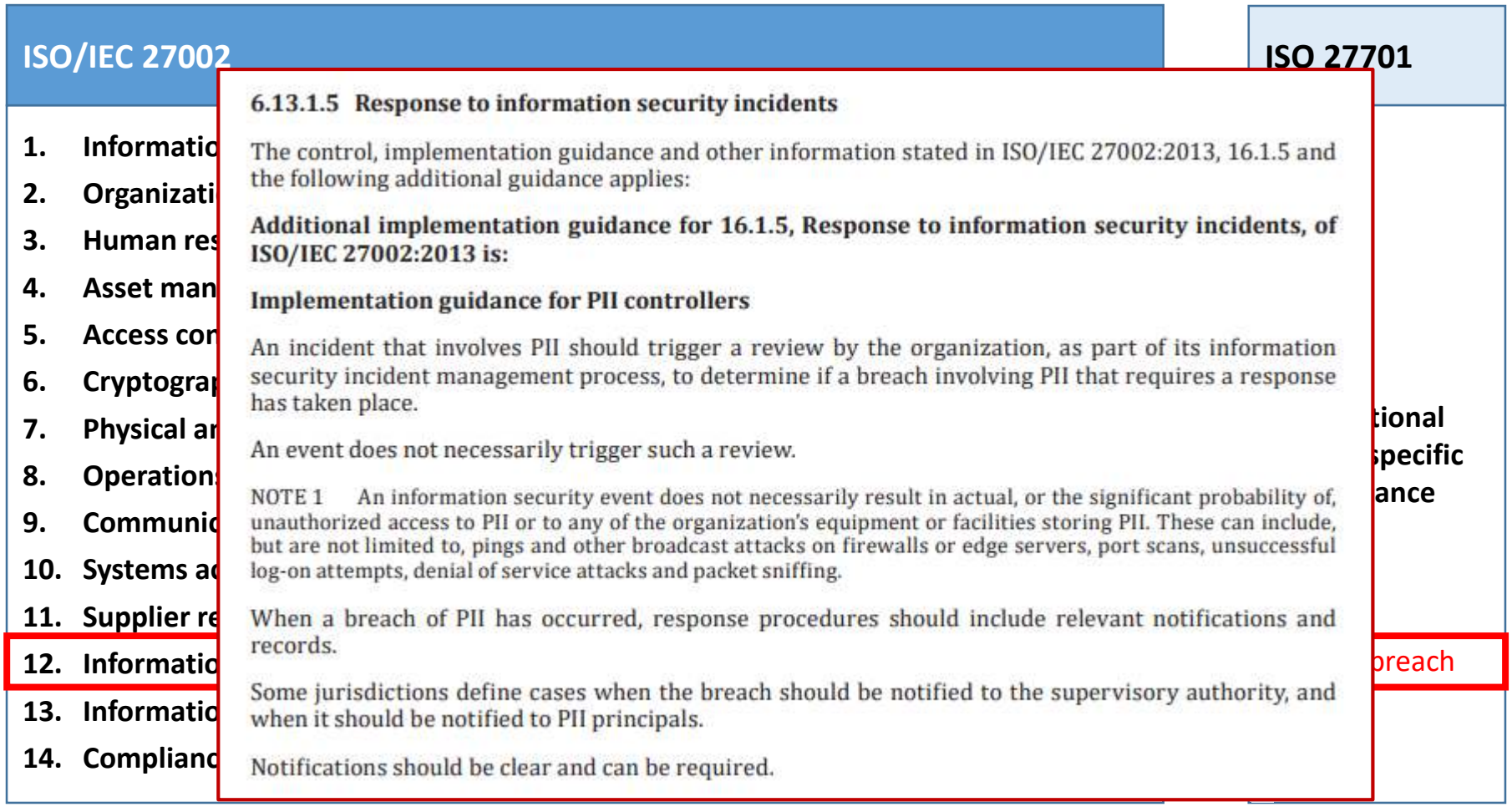
ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows:

The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize.

PIMS-specific extension of ISO/IEC 27002

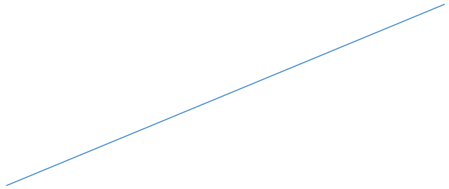


PIMS-specific extension of ISO/IEC 27002



Controller- and processor-specific guidance

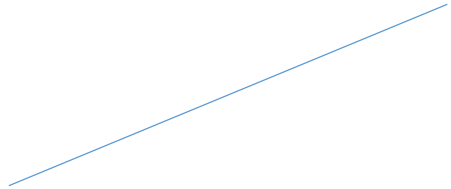
ISO/IEC 27002



Additional ISO/IEC 27002 guidance for PII controller

1. Conditions for collection and processing
2. Obligations to PII principals — Data subject rights
3. Privacy by design and by default
4. PII sharing, transfer, and disclosure

ISO/IEC 27002



Additional ISO/IEC 27002 guidance for PII processor

1. Conditions for collection and processing
2. Obligations to PII principals — Data subject rights
3. Privacy by design and by default
4. PII sharing, transfer, and disclosure

Controller- and processor-specific guidance

ISO/IEC 27002

Additional ISO/IEC 27002 guidance for PII controller

1. **Conditions for collection and processing**
2. **Obligations to PII principals** Data subject rights
3. **Privacy by design and by default**
4. **PII sharing, transfer, and disclosure**

ISO/IEC 27002

7.3.3 Providing information to PII principals

Control

The organization should provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.

Implementation guidance

The organization should provide the information detailed in 7.3.2 to PII principals in a timely, concise, complete, transparent, intelligible and easily accessible form, using clear and plain language, as appropriate to the target audience.

Where appropriate, the information should be given at the time of PII collection. It should also be permanently accessible.

NOTE Icons and images can be helpful to the PII principal by giving a visual overview of the intended processing.

Controller- and processor-specific guidance

ISO/IEC 27

ontroller

subject rights

8.3.1 Obligations to PII principals

Control

The organization should provide the customer with the means to comply with its obligations related to PII principals.

Implementation guidance

A PII controller's obligations can be defined by legislation, by regulation and/or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion.

Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a contract.

ISO/IEC 27002

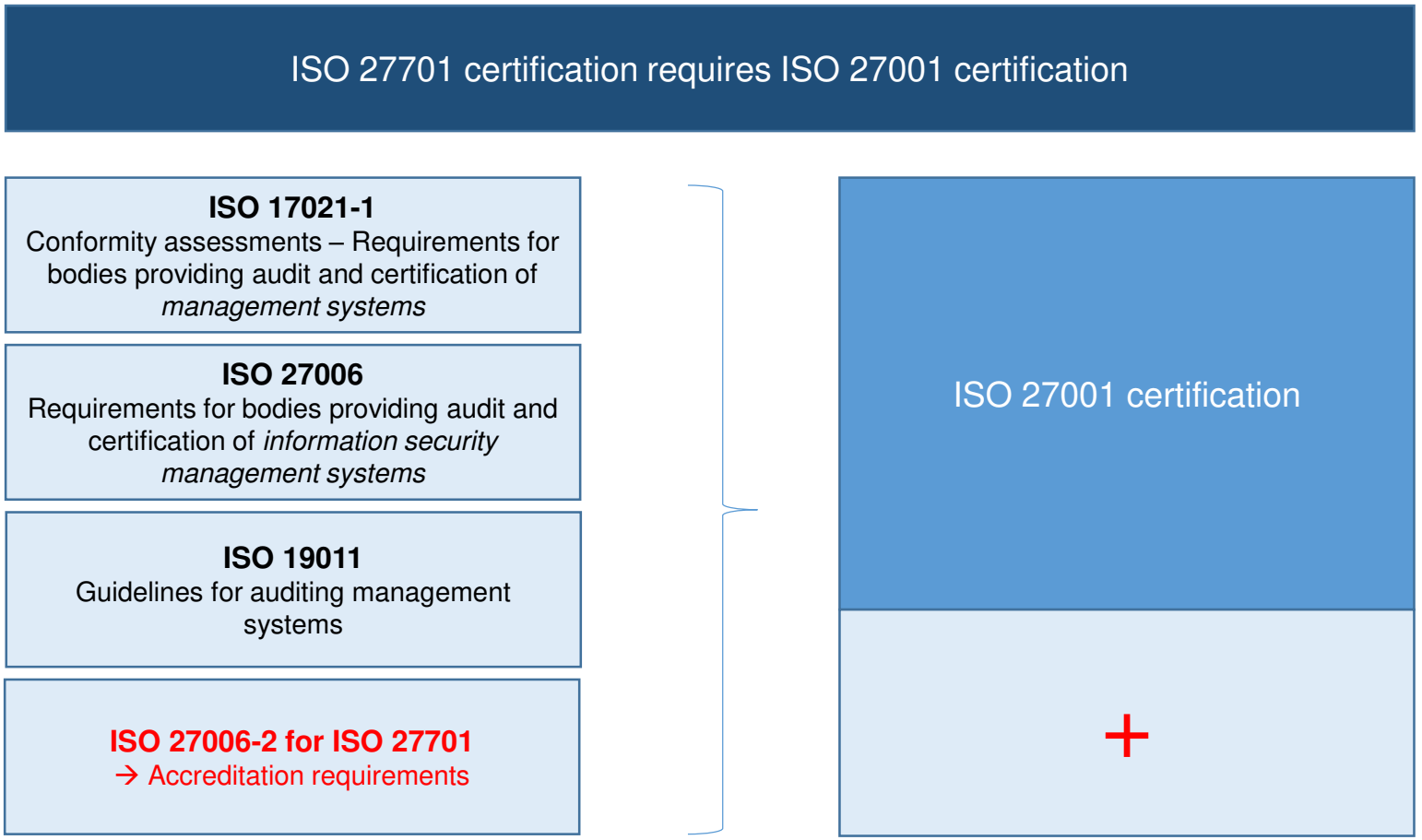
Additional ISO/IEC 27002 guidance for PII processor

1. **Conditions for collection and processing**
2. **Obligations to PII principals** Data subject rights
3. **Privacy by design and by default**
4. **PII sharing, transfer, and disclosure**

Agenda

- GDPR as a game changer
- International PIMS standard: ISO/IEC 27701
- **ISO certification versus GDPR certification**
- Outlook: Refinement of ISO 27701 in European Context

ISO 27701 certification and accreditation



Certification doesn‘t equal certification!

ISO 27001+ certification

≠

Certification according to Art. 42 GDPR

Conformity assessment

Requirements for certification bodies


INTERNATIONAL STANDARD

ISO/IEC 17021-1

First edition 2015-06-15

Certification of management systems

Conformity assessment — Requirements for bodies providing audit and certification of management systems —

Part 1:
Requirements

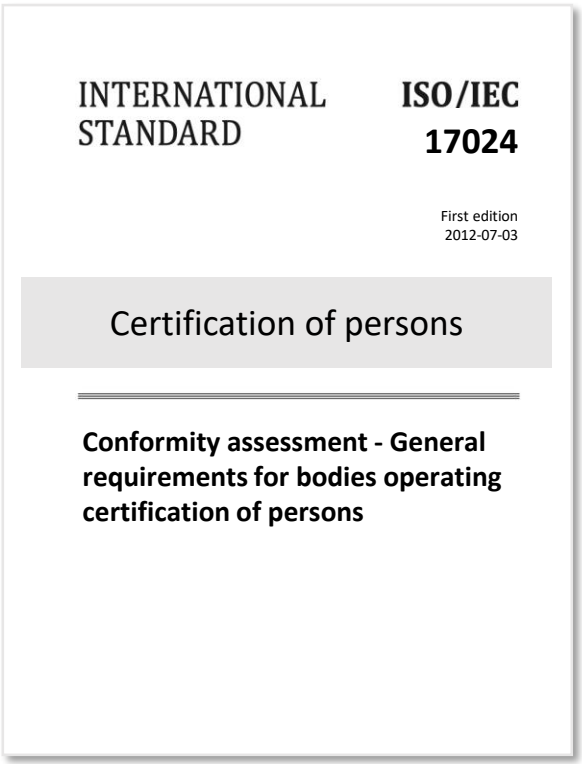

INTERNATIONAL STANDARD

ISO/IEC 17065

First edition 2012-09-15

Certification of products, processes and services

Conformity assessment — Requirements for bodies certifying products, processes and services


INTERNATIONAL STANDARD

ISO/IEC 17024

First edition 2012-07-03

Certification of persons

Conformity assessment - General requirements for bodies operating certification of persons

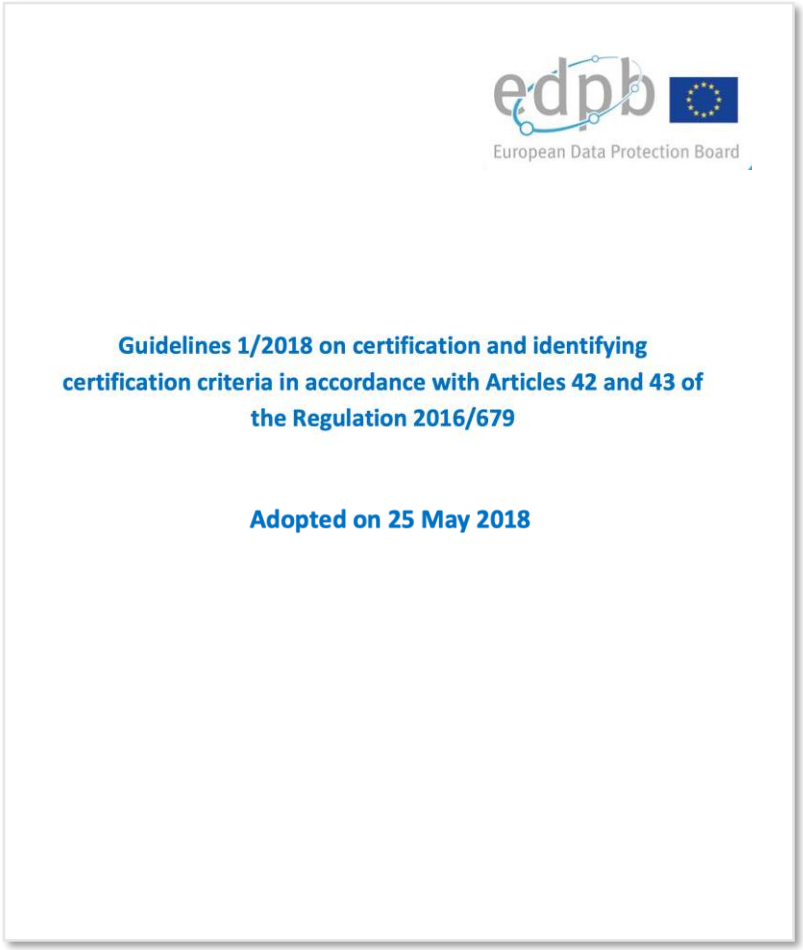
Certification bodies, Art. 43 (1) GDPR

Certification bodies

- **issue and renew certification;**
- are **accredited by** one or both of the following:
  - a) the competent **supervisory authority** or
  - b) the **national accreditation body** named in accordance with
    - Regulation (EC) No. 765/2008,
    - **EN-ISO/IEC 17065/2012** and
    - the **additional requirements** established by the competent supervisory authority.

The naming of the accreditation body shall be in accordance with ISO 17065!

EDPB Guidelines 1/2018



Definition of certification:

Third party conformity assessment (ISO)
or

*"Certification shall refer to **third party attestation related to processing operations by controllers and processors**."*

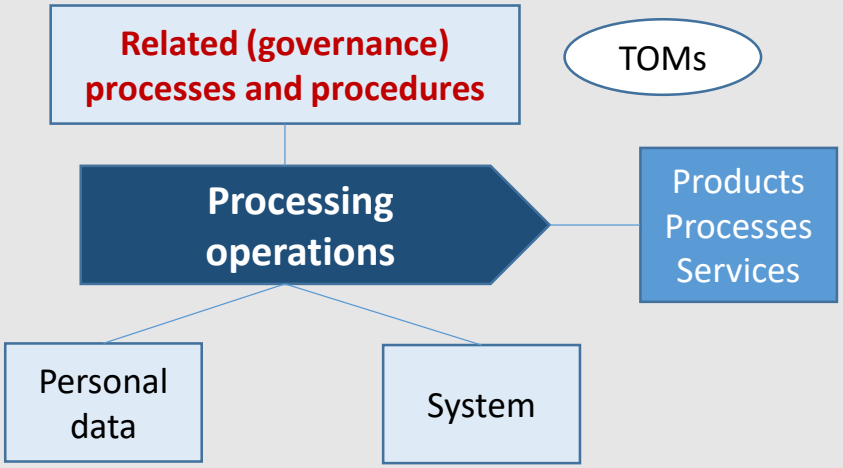
Usage of certification mechanisms:

*"… an **element to demonstrate compliance** with specific obligations of the controllers and processors."*

What can be certified under GDPR?

The EDPB considers that the GDPR provides a broad scope for what can be certified under the GDPR, as long as the focus is on helping demonstrate compliance with this Regulation of processing operations by controllers and processors (Article 42.1).

Processing operations and core components:



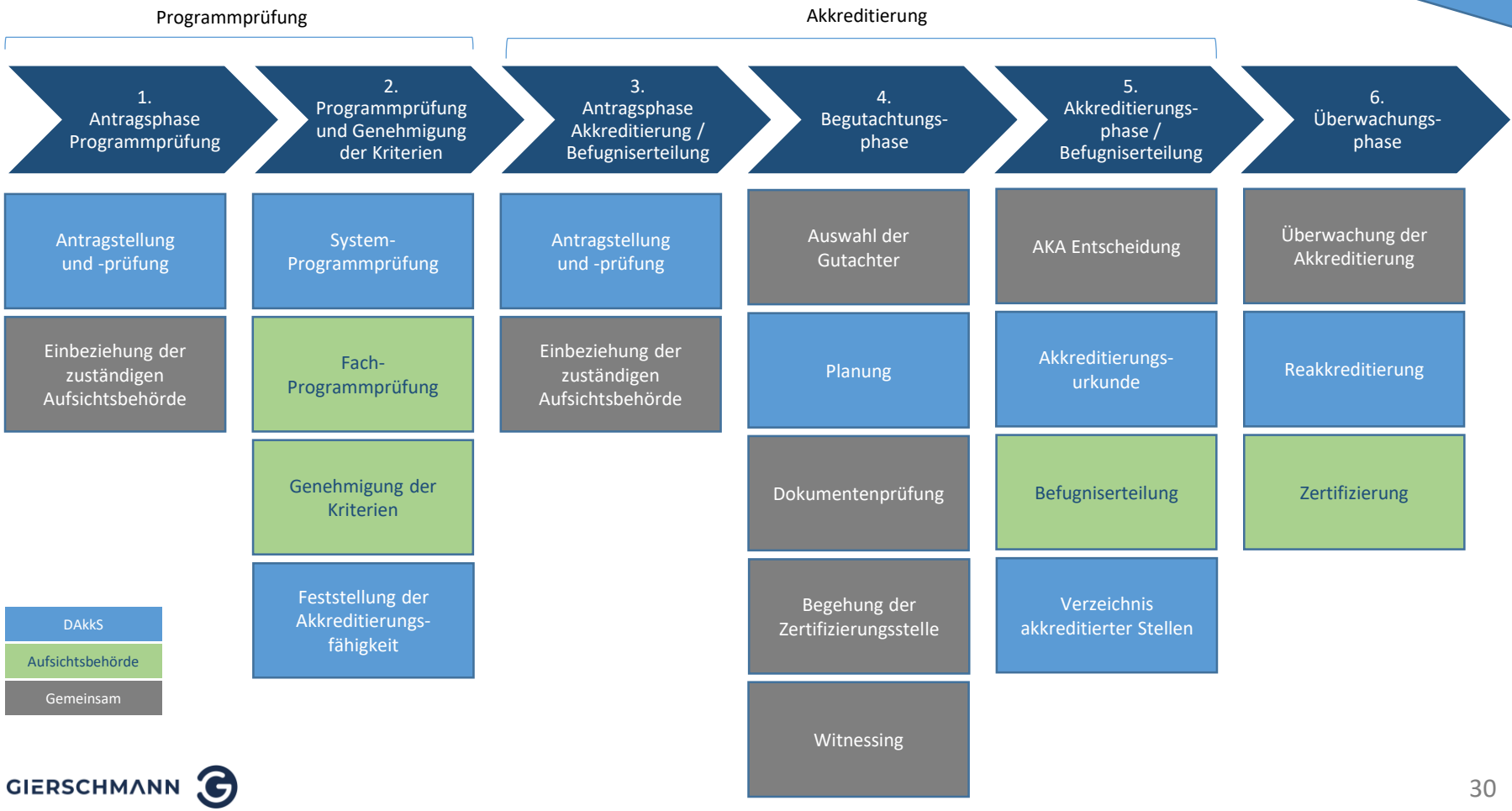
Influencing factors:

1. Organisational / legal structure
2. Who performs the processing
3. IT infrastructure

…, the EDPB considers that the scope of certification under the GDPR is directed to processing operations or set of operations. These may comprise of governance processes in the sense of organisational measures, hence as integral part of a processing operation (e.g. the governance process established for complaints' handling as part of the processing of employee data for the purpose of salary payment).

German accreditation process according to Art. 42, 43 GDPR (Illustrative)

DSK Version 1.0 (15.03.19)



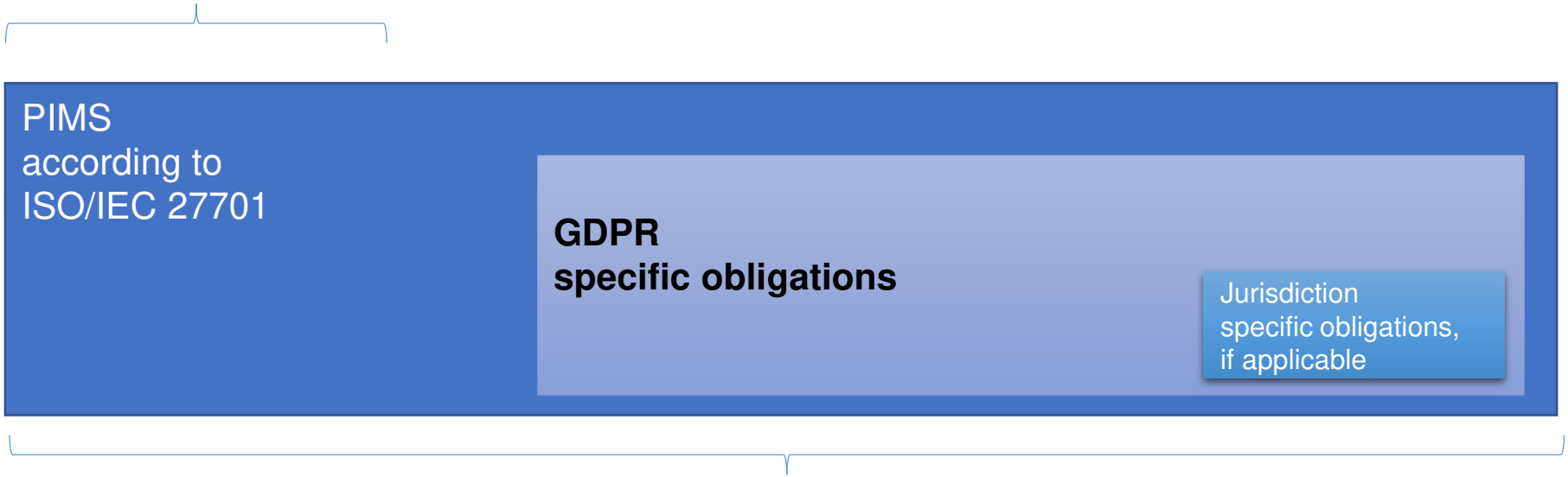
GIERSCHMANN

Agenda

- GDPR as a game changer
- International PIMS standard: ISO/IEC 27701
- ISO certification versus GDPR certification
- **Outlook: Refinement of ISO 27701 in European Context**

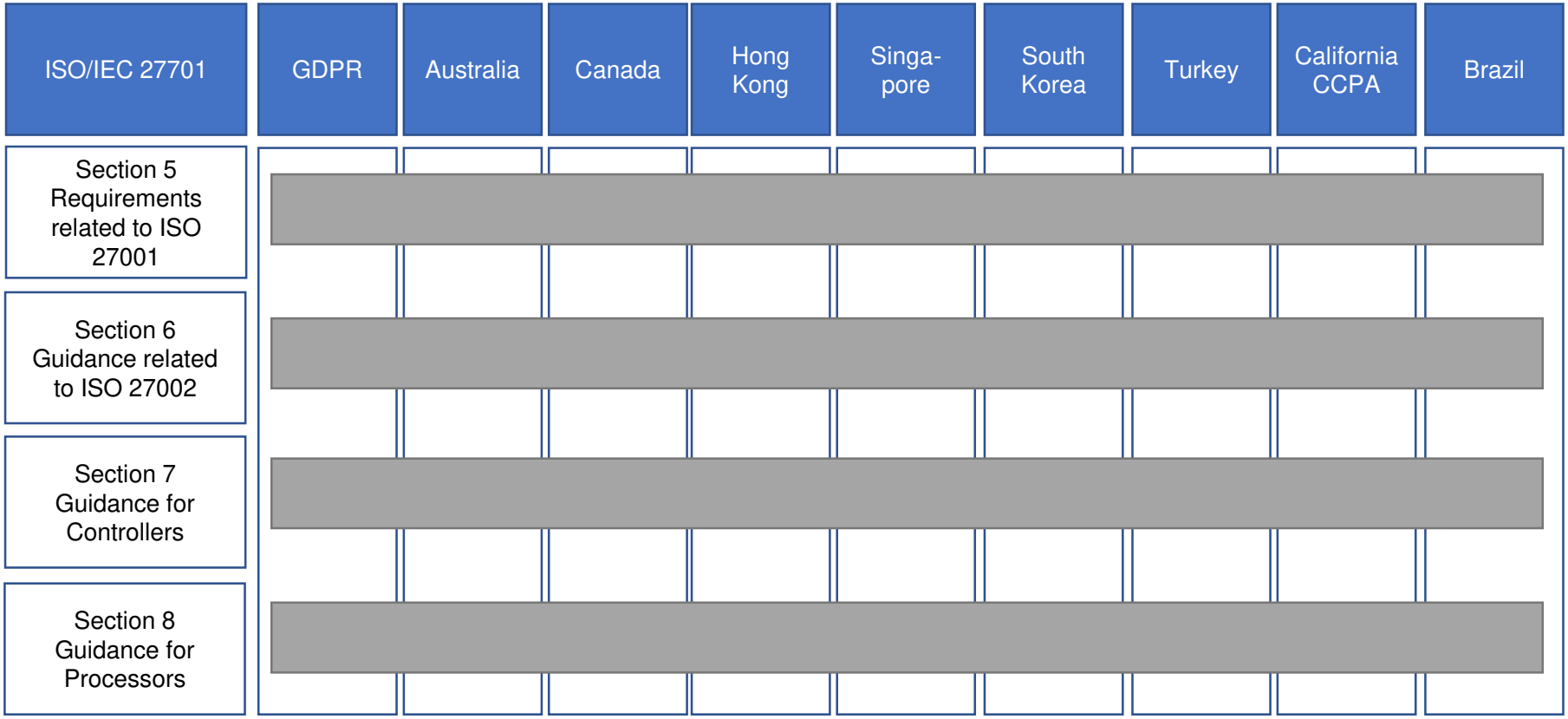
PIMS according to ISO/IEC 27701: An international framework

Generic requirements, which are designed to encompass GDPR requirements, but do not always detail them explicitly → must be further refined in GDPR context



PIMS can be used as a **framework**
in which requirements and obligations of GDPR and
respective jurisdictions can be implemented

Data Protection Mapping Project



Source: https://dataprotectionmapping.z21.web.core.windows.net/#/dashboard

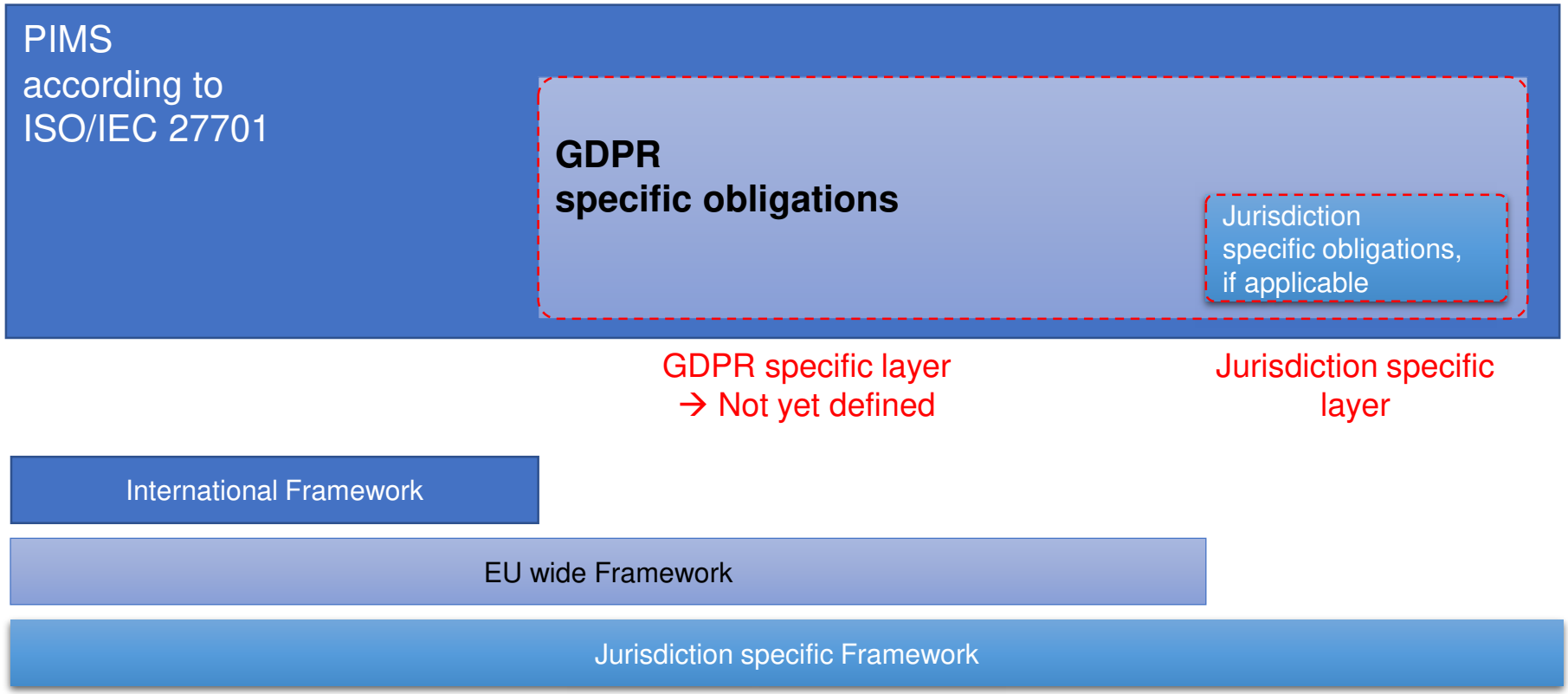
Demonstrate compliance according to GDPR and a certification scheme according to Art. 42 GDPR

GDPR specific PIMS according to ISO/IEC 27701

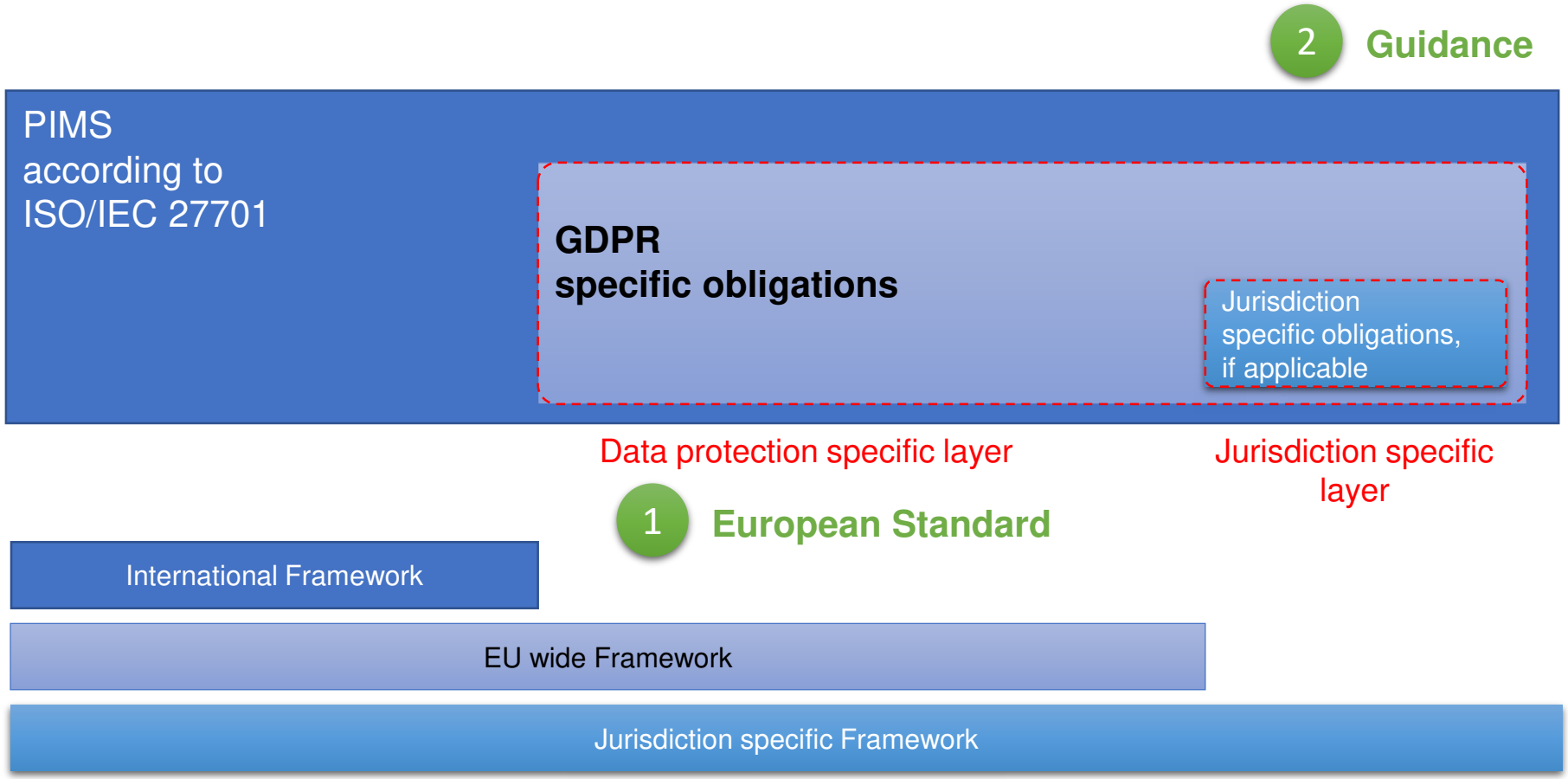
PIMS can be used to demonstrate compliance according to Art. 5(2) GDPR

Certification of PIMS according to ISO 27001+
Certification according to Art. 42 GDPR?

Missing standardized GDPR specific layer



Standardized GDPR specific layer and consistent application



GIERSCHMANN
CONSULTING

Markus Gierschmann
Dipl.-Ing. oec.
Finanzökonom (ebs)
CIPP/E, CIPM

Gierschmann Consulting
Kattjahren 4
22359 Hamburg

T + 49 40 419 239 40
M + 49 175 596 1553

m.gierschmann@gierschmann.com

www.gierschmann.com