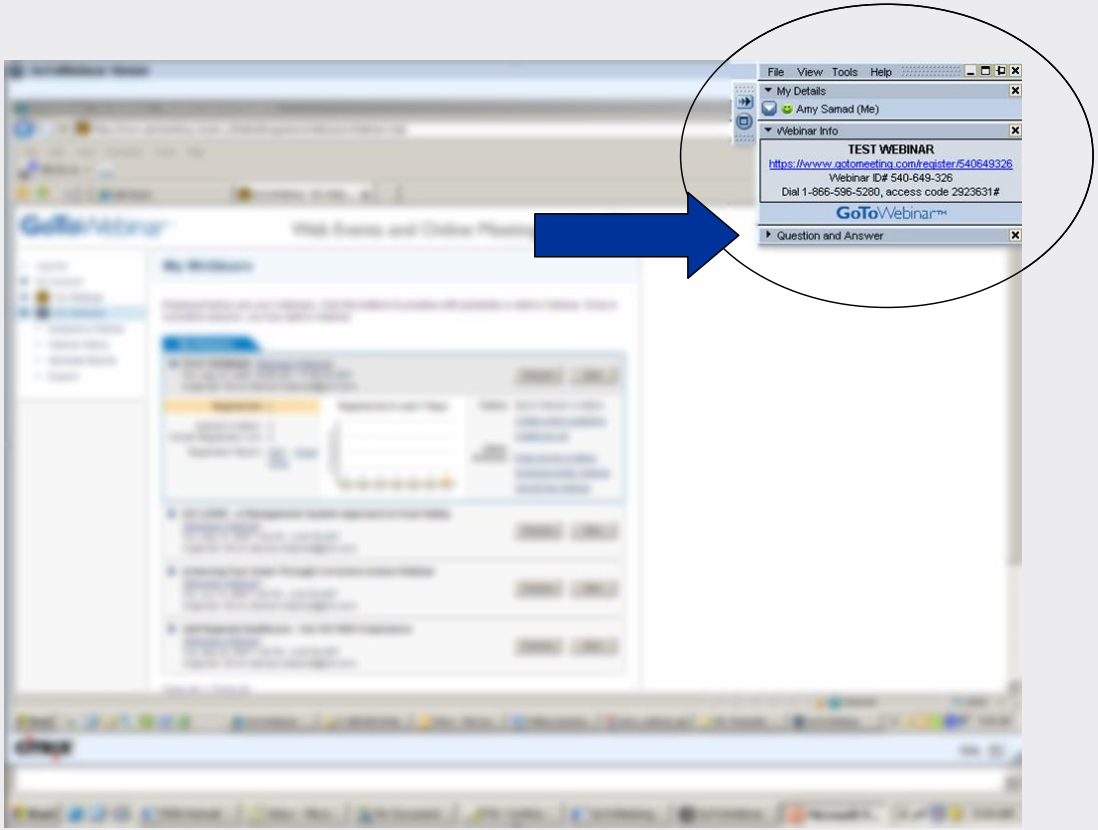
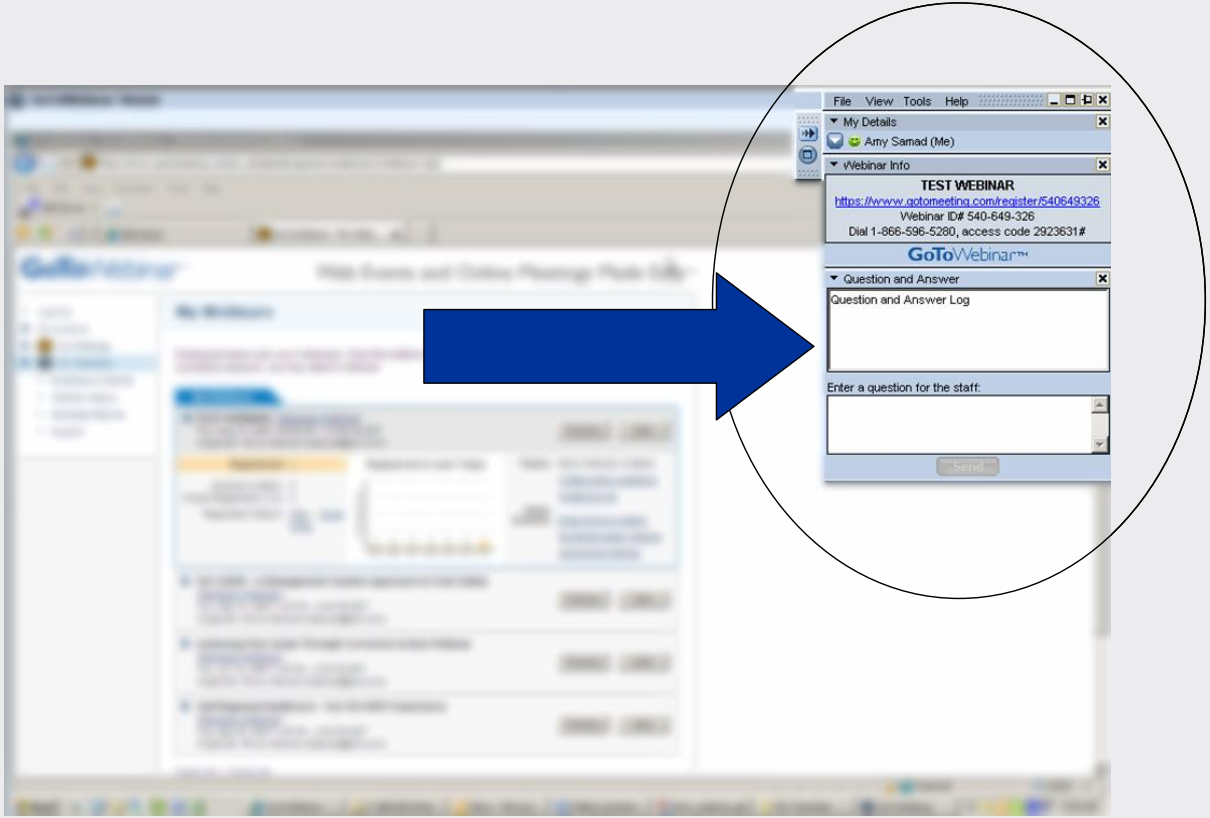
PERRY JOHNSON REGISTRARS, INC.

Your journey to ISO 27001: Privacy integration

Alan Calder
Founder, Executive Chairman
IT Governance Ltd.


File View Tools Help
My Details
Amy Samad (Me)
Webinar Info
TEST WEBINAR
https://www.gotomeeting.com/register/540649326
Webinar ID# 540-649-326
Dial 1-866-596-5280, access code 2923631#
GoToWebinar
Question and Answer


File View Tools Help
My Details
Amy Samad (Me)
Webinar Info
TEST WEBINAR
https://www.gotomeeting.com/register/540649326
Webinar ID# 540-649-326
Dial 1-866-596-5280, access code 2923631#
GoToWebinar
Question and Answer
Question and Answer Log
Enter a question for the staff:
Send

Alan Calder

Founder & Executive
Chairman, IT Governance Ltd.

Your journey to ISO 27001 – Privacy integration

October 6, 2022

About IT Governance

The cyber risk and privacy management solutions provider

20 years of experience, 200 employees

IT governance, risk, and compliance solutions

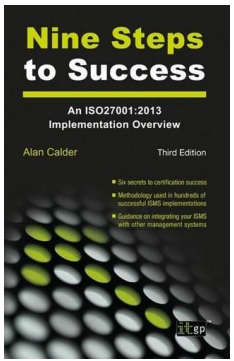
More than 12,000 clients across 5 continents

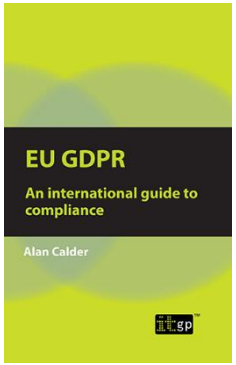
Comprehensive ISO 27001 product and service portfolio

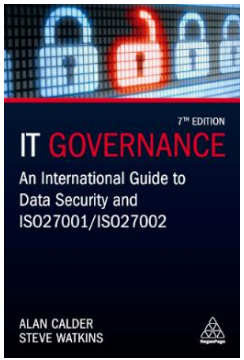
Introduction: Alan Calder

Founder and executive chairman of IT Governance

- Founder and executive chairman of IT Governance, the single source for everything to do with IT governance, cyber risk management, and IT compliance.
- Author of *IT Governance: An International Guide to Data Security and ISO27001/ISO27002* (Open University textbook).







Contents

Protect • Comply • Thrive

The importance of integrating privacy into your ISO 27001-compliant ISMS

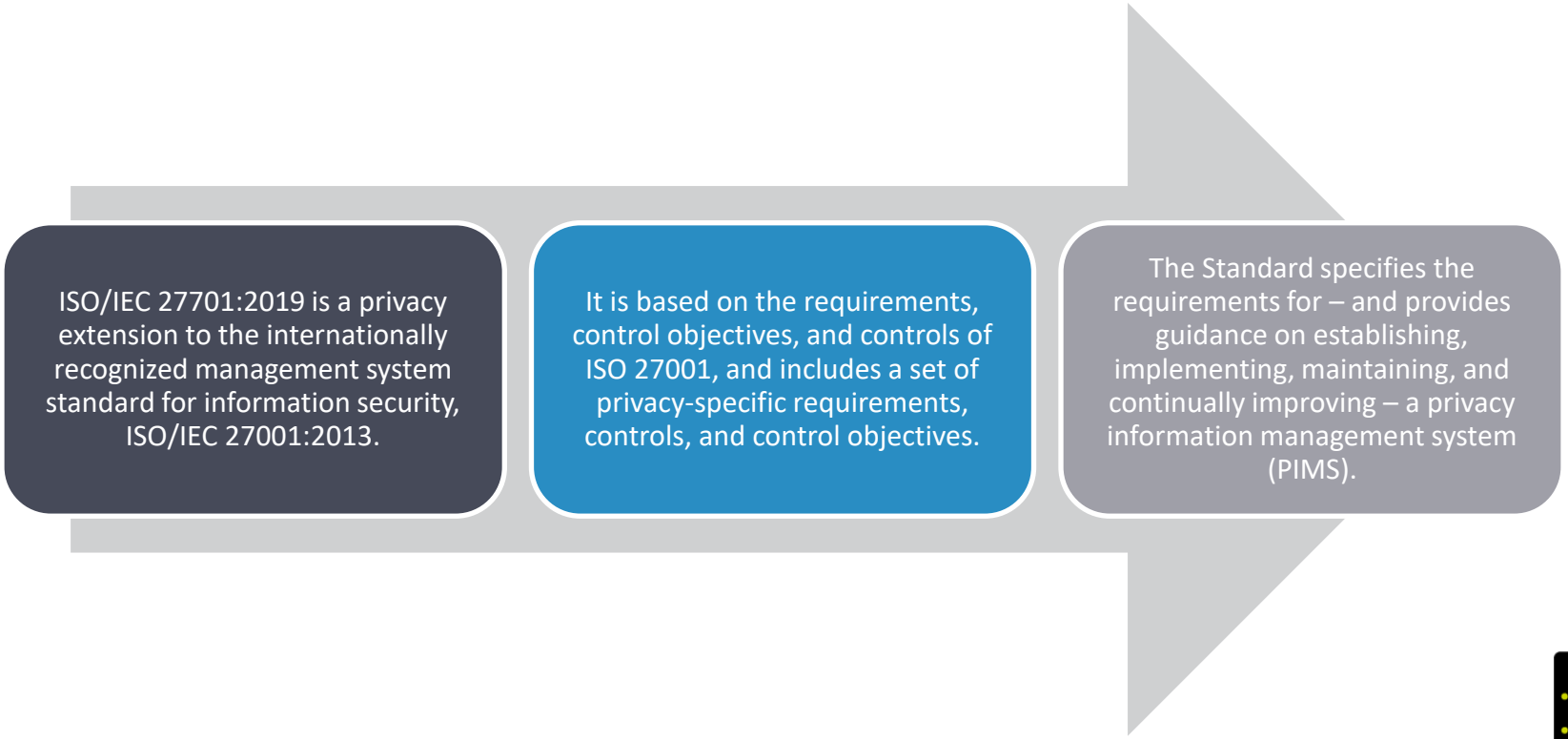
IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Integrating privacy into your ISO 27001-compliant ISMS

ISO/IEC 27701:2019



ISO 27001 and privacy management

Integrating privacy

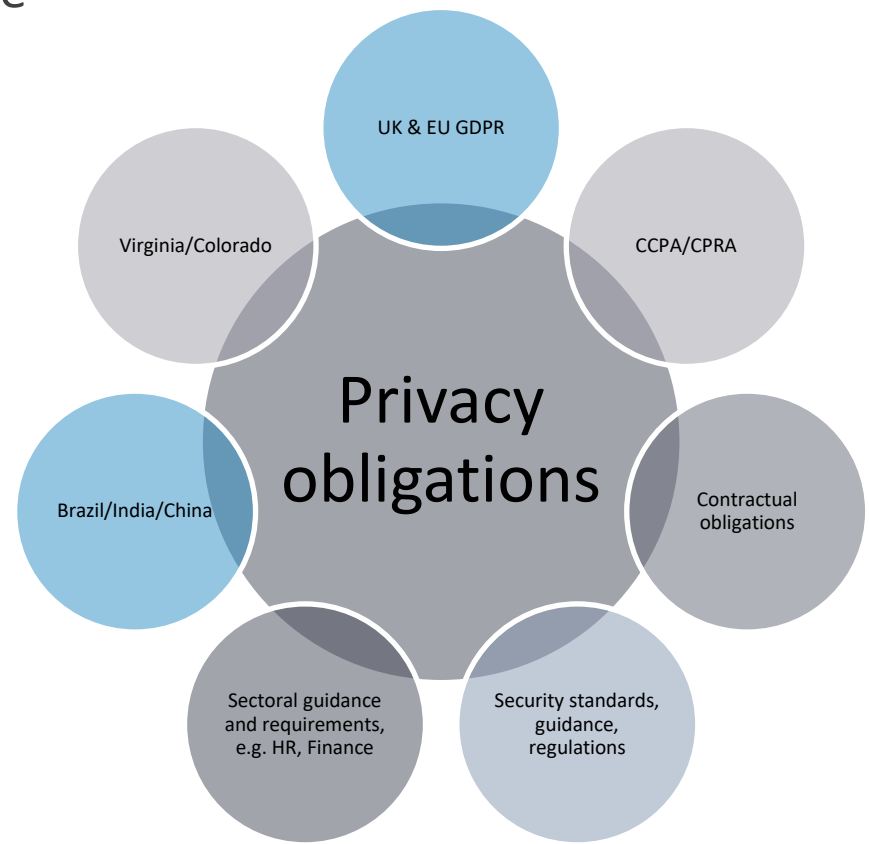
- The EU's General Data Protection Regulation (GDPR), US Laws such as the CCPA and the ongoing growth in data protection laws around the world mean there is an increasing need for a standard or code of conduct to support and demonstrate compliance.

- ISO/IEC 27701 (*Security techniques – Extension to ISO/IEC 27001 and ISO/ IEC 27002 for privacy information management – Requirements and guidelines*)
  - Published in August 2019, it is one of the most comprehensive standards in information security and privacy management
  - It aims to fill the assurance gap and provide a genuinely international approach to data protection as an extension of information security

Why an ISO/IEC privacy management system?

ISO/IEC 27701

The privacy universe



Implementing an ISO 27701-compliant PIMS

The benefits

ISO 27701 implementation and what it means for your business

IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

The link between ISO 27001 (ISMS) and ISO 27701 (PIMS)

Two options

Option A:

- An organization has already implemented an ISMS and wishes to implement a PIMS.

Option B:

- An organization implements an ISMS and a PIMS together as a single implementation project.

ISO 27701 requirements

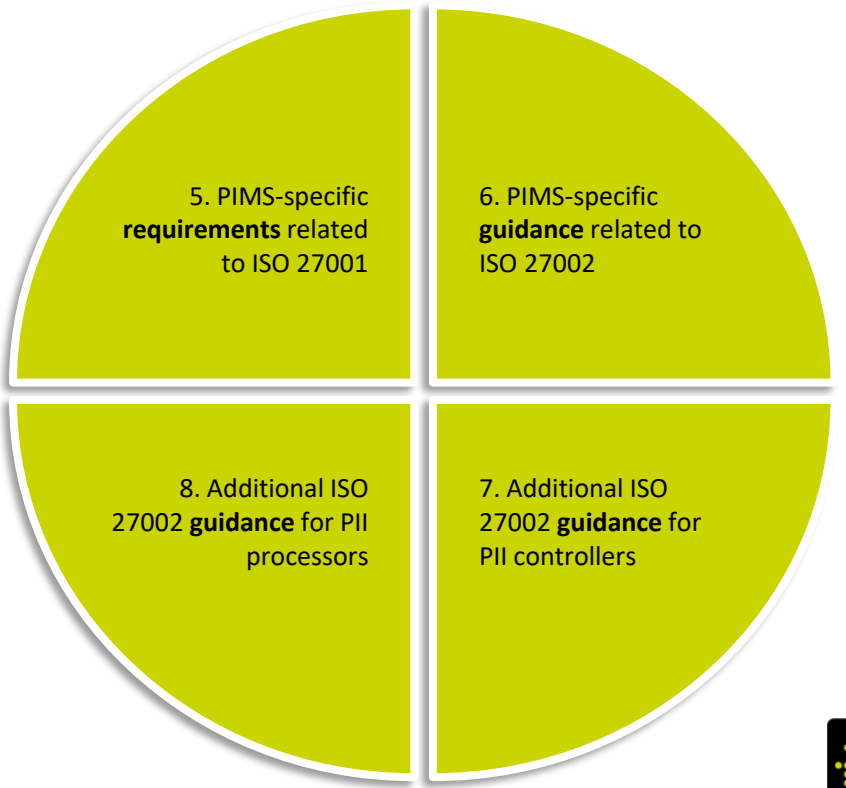
Clauses 5 and 6

- Clause 5.1: The requirements in ISO/IEC 27001:2013 mentioning “information security” should be extended to the protection of privacy as potentially affected by the processing of personally identifiable information (PII).
- Clause 6.1: The guidelines in ISO/IEC 27002:2013 mentioning “information security” should be extended to the protection of privacy as potentially affected by the processing of PII.
- In practice, where “information security” is used in ISO/IEC 27001:2013 and in ISO/IEC 27002:2013, “information security and privacy” applies instead.
- All control objectives and controls should be considered in the context of both risks to information security as well as risks to privacy related to the processing of PII.

Implementation

ISO 27001 & ISO 27701

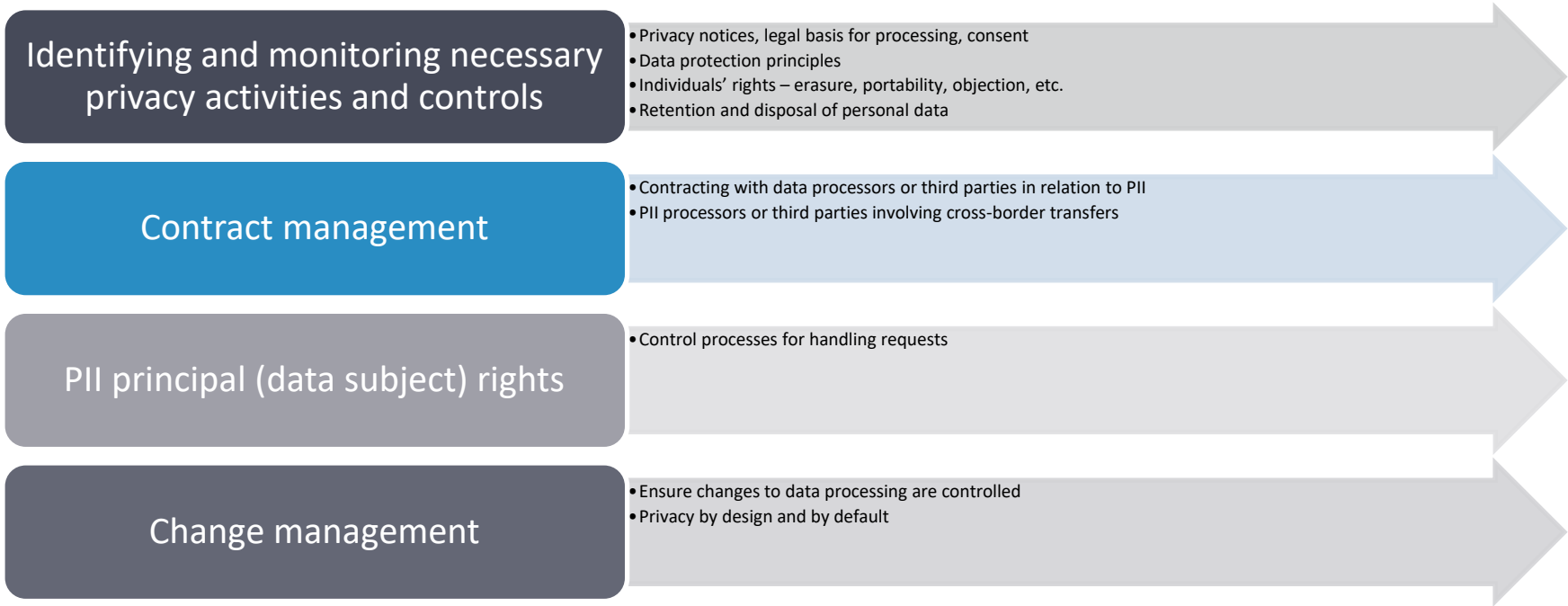
- When considering how and what controls to implement, the organization needs to consider the set of security controls defined in Annex A of ISO 27001:2013, the guidance in ISO 27002:2013, and an additional set of guidance information relating to privacy in Clauses 6, 7, and 8 and in Annexes A and B of ISO 27701:2019.



PIMS and scope

- While organizations may have already implemented an ISO 27001-compliant ISMS, they may not have included PII in its scope.
- To implement a PIMS that complies with the requirements of ISO 27701, the ISMS MUST include PII in its scope.
- Scope needs to be carefully considered and defined before any PIMS implementation project is initiated.

Key components of a PIMS



The structure and controls of ISO 27701 and ISO 27002

IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

ISO/IEC 27001:2013 structure

- Intro
- Application
- Terms and definitions

4. Context of the organization

5. Leadership

6. Planning

7. Support

8. Operation

9. Performance evaluation

10. Improvement

- Annex A – Reference control objectives and controls

ISO/IEC 27701:2019

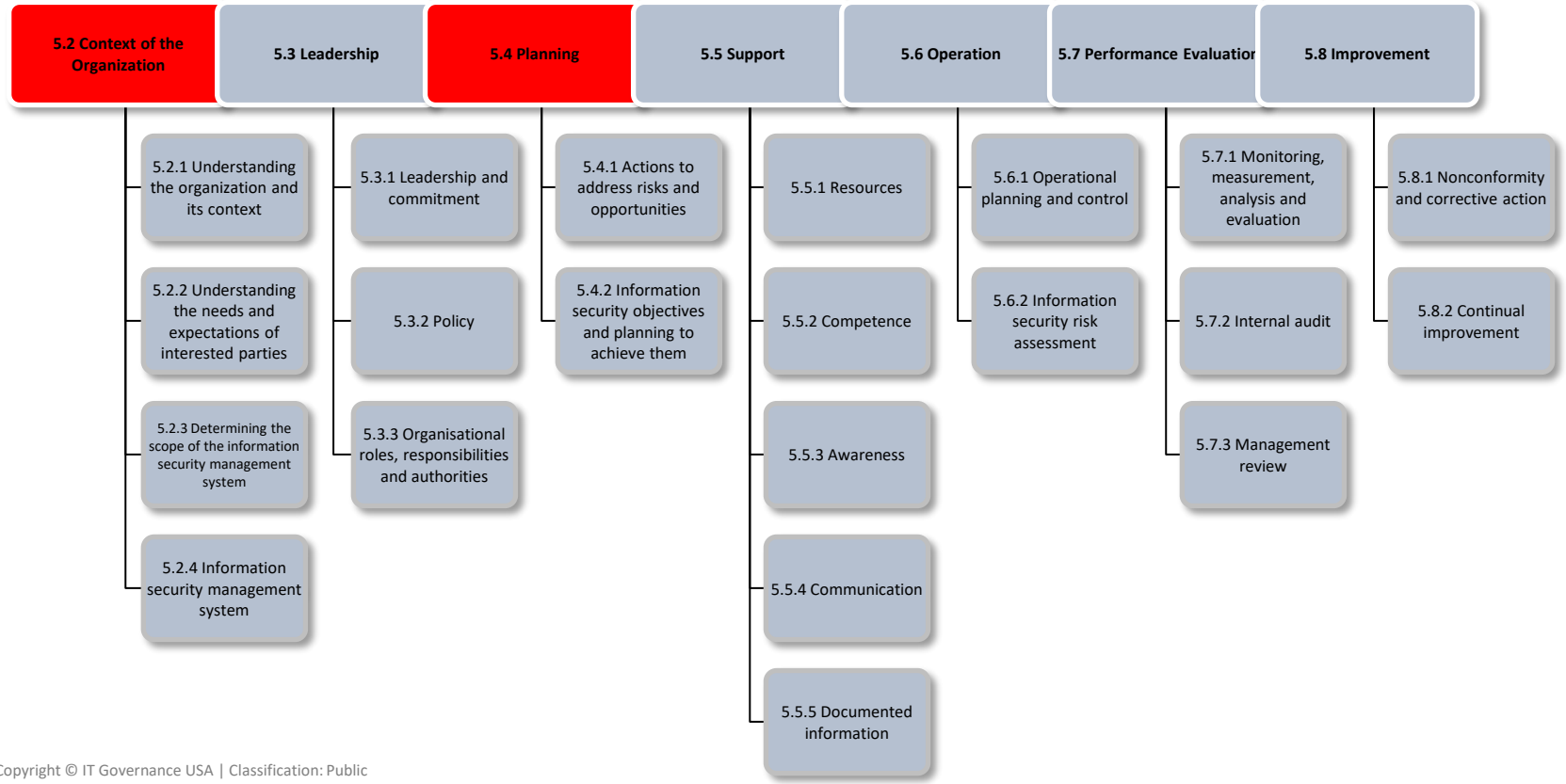
Structure

Clause	Title
1	Scope
2	Normative references
3	Terms and definitions
4	General
5	PIMS-specific requirements related to ISO/IEC 27001
6	PIMS-specific guidance related to ISO/IEC 27002
7	Additional ISO/IEC 27002 guidance for PII controllers
8	Additional ISO/IEC 27002 guidance for PII processors

Annex	Title
A	PIMS-specific reference control objectives and controls (PII Controllers)
B	PIMS-specific reference control objectives and controls (PII Processors)
C	Mapping to ISO/IEC 29100
D	Mapping to the General Data Protection Regulation
E	Mapping to ISO/IEC 27018 and ISO/IEC 29151
F	How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

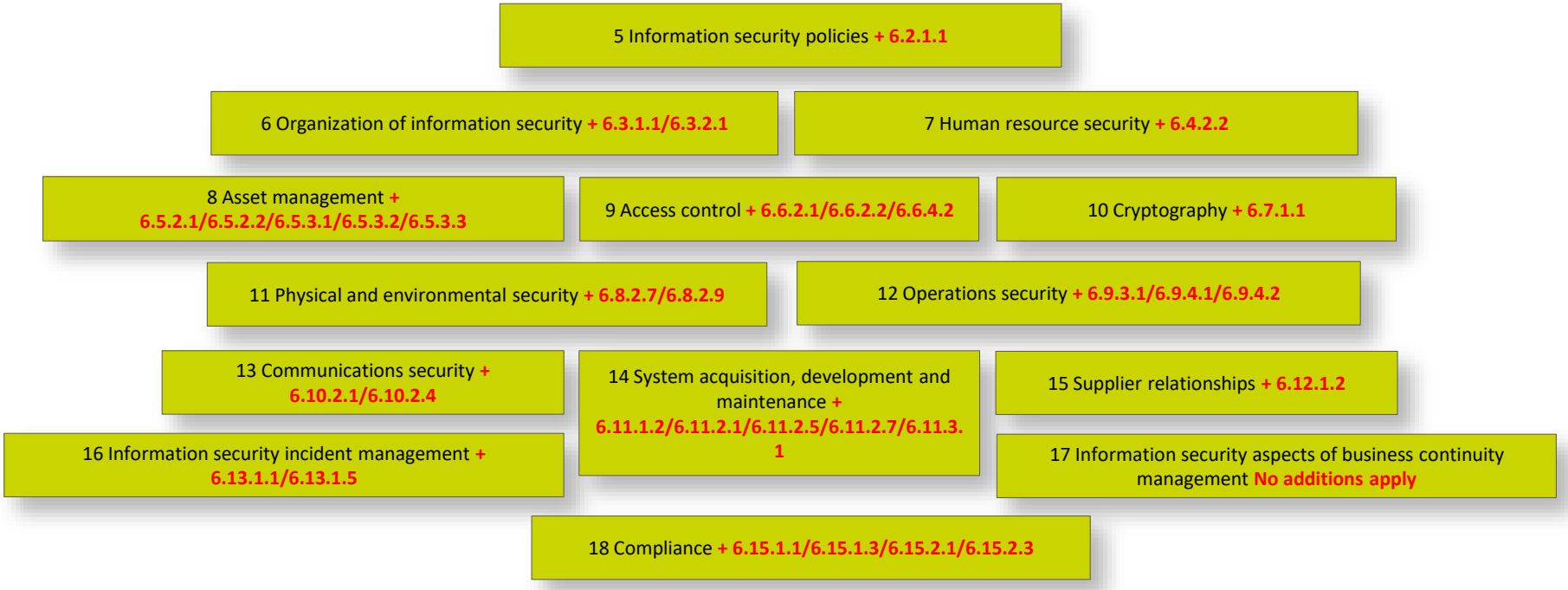
Clause 5

Requirements



Clause 6

Requirements



ISO 27701

Annexes A and B

- In ISO/IEC 27701, there are 31 controls in Annex A and 18 controls in Annex B, each split into 4 identical categories:
    - Conditions for collection and processing
    - Obligations to PII principals
    - Privacy by design and privacy by default
    - PII sharing, transfer, and disclosure
- These are in addition to the controls in Annex A of ISO/IEC 27001.

How NIST and SOC 2 support ISO 27001 implementation

IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

SOC 2

Introduction

Created by the American Institute of Certified Public Accountants (AICPA)

Provides assurance to customers about the security of your organization's information systems

Contains five "trust service principles":

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

Focuses on services and the people, processes, and technology that support them

Key similarities

SOC 2 and ISO 27001

Third-party assessors

Both frameworks call for an independent third party to do the external audit

Customer trust

Both help win new business and retain existing customers

International recognition

Both are internationally recognized standards

Information security

Both frameworks are meant to effectively implement controls that secure data and information

Key differences

SOC 2 and ISO 27001

ISO 27001

- Scope – establishment and maintenance of an ISMS
- Applicability – early stages of adoption in the U.S.

SOC 2

- Scope – requires security controls to be enforced, does not focus on creation of a management system, focuses on service first
- Applicability – early stages of adoption outside the U.S.

Key differences (continued)

SOC 2 and ISO 27001

ISO 27001

- Third-party assessor – a recognized accredited certification body must do external audit, third-party audit
- Certification – certification is received following a successful external audit

SOC 2

- Third-party assessor – can only be performed by a licensed Certified Public Accountant (CPA), second-party audit
- Certification – no certification, an attestation report is given

Key differences (continued)

SOC 2 and ISO 27001

ISO 27001

- Sector – any organization/sector looking to implement information security best practice
- Renewal time frame – certification valid for three years with regular check-ins

SOC 2

- Sector – prevalent in SaaS companies; companies that own service delivery
- Renewal time frame – the SOC 2 report must be renewed annually as a complete audit

NIST

Privacy Framework

- In 2020, NIST released the Privacy Framework, the latest in a series of guidelines that are designed to help organizations better protect their sensitive information.
- The Privacy Framework is structured similarly to the NIST Cybersecurity Framework (CSF) but focuses on the identification and management of privacy risks.
- Organizations that have already implemented the CSF will therefore have a head start when it comes to the Privacy Framework – particularly as the former touches on data privacy.
- The Privacy Framework is much more in-depth, and worth following if you're serious about securing your organization, keeping stakeholders satisfied, and meeting cybersecurity laws such as the CPRA and EU GDPR.

Practical solutions to integrate privacy into your ISMS

IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

How IT Governance USA can help

Our solutions

Learn how to extend an ISO 27001-compliant ISMS to cover privacy information management.

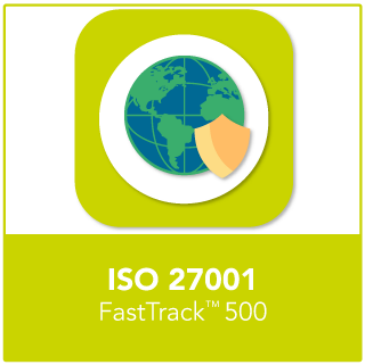
Find out more

This tool lists all the requirements from ISO 27701:2019, against which you can assess your current state of compliance and prioritize work areas.

Find out more

Extend your ISMS to cover data protection and privacy with our FastTrack™ service.

Find out more



A fixed-priced consultancy package designed to help organizations with between 20 and 500 employees achieve ISO 27001 certification readiness in an agreed time frame.

Find out more

Questions

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive


Thank you

Get in touch

Contact details

United Kingdom

Visit our website
www.itgovernance.co.uk

Email us
servicecentre@itgovernance.co.uk

Call us
+44 (0)333 800 7000

Join us on LinkedIn
/company/it-governance

Follow us on Twitter
/ITGovernanceLtd

Like us on Facebook
/ITGovernance

Europe

Visit our website
www.itgovernance.eu

Email us
servicecentre@itgovernance.eu

Call us
+353 (0) 1 695 0411

Join us on LinkedIn
/company/it-governance-europe-ltd

Follow us on Twitter
/itgovernanceeu

Like us on Facebook
/ITGovernanceEU

United States

Visit our website
www.itgovernanceusa.com

Email us
servicecenter@itgovernanceusa.com

Call us
+1 877 317 3454

Join us on LinkedIn
/company/it-governance-usa-inc

Follow us on Twitter
/ITGovernanceUSA

Like us on Facebook
/ITG_USA

Upcoming Webinars

[e-Stewards V.4.1 Overview]
August 15, 2022 – 1:00 pm ET
Speaker: Austin Matthews, PJR EHS Program Manager

[FSSC 22000: A Food Safety Management System for Packaging Manufacturers]
August 16, 2022 – 11:00 am ET
Speaker: Jacqueline Southee, NA Representative FSSC

[IATF Common Audit Report Application (CARA) and Remote Auditing]
August 17, 2022 – 11:00 am ET
Speaker: Joseph Krolikowski, PJR QMS Program Manager

Find more upcoming webinars at PJR.com/Webinars

PERRY JOHNSON REGISTRARS, INC.

Questions

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive