Jumping to ISO 27701: Why it helps if you've already got 27001 Certification

Alan Calder, Founder and CEO,
IT Governance

3 June 2021

01 Introduction

02 Protecting data and the law

03 What can a PIMS do for you?

04 The key components of a PIMS

05 Staff awareness and building a security culture

06 The Board and Directors: Documented evidence

07 Contact details

Today's discussion

Protect • Comply • Thrive

Introduction

IT governance

Our Expertise,
Your Peace of Mind

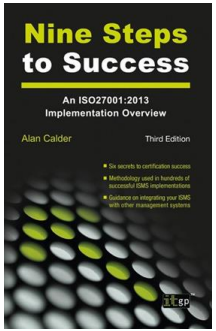
Protect • Comply • Thrive

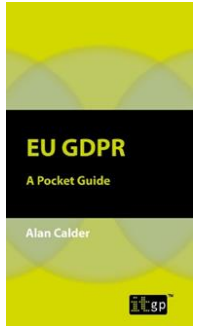
Introduction

Alan Calder, Founder and executive chairman of IT Governance

- IT Governance is the leading global provider of IT governance, risk management and compliance solutions.
- Author of *IT Governance – An International Guide to Data Security and ISO27001/ISO27002* and many other books on cyber security, compliance and governance.

IT Governance has a team of 35 experienced consultants, covering the entire range of GRC disciplines. We typically recruit additional consultants to meet specific project requirements and we are currently increasing the depth of our ICS/OT resource to meet the requirements of our growing CNI consultancy practice.





About IT Governance

Leading global provider of cyber risk and data privacy management solutions.

- We deliver projects all over the world to clients across the spectrum of cyber security and resilience, data privacy, incident response and business continuity.
- Our unique and unrivalled blend of products and services include bespoke and fixed-price consultancy, training, toolkits, software, staff awareness e-learning and penetration testing.
- We pride ourselves on our ability to serve an international customer base and deliver a broad range of integrated, high-quality solutions globally, while meeting the real- world needs of today's organisations, directors and practitioners.
- IT Governance is a subsidiary of GRC International Group plc, focused on delivering IT governance, risk management and compliance solutions.

15 years of experience, 200 employees

IT governance, risk and compliance solutions

More than 12,000 clients across six continents

More than 4,000 training solutions delivered

Group overview

GRC International Group Companies

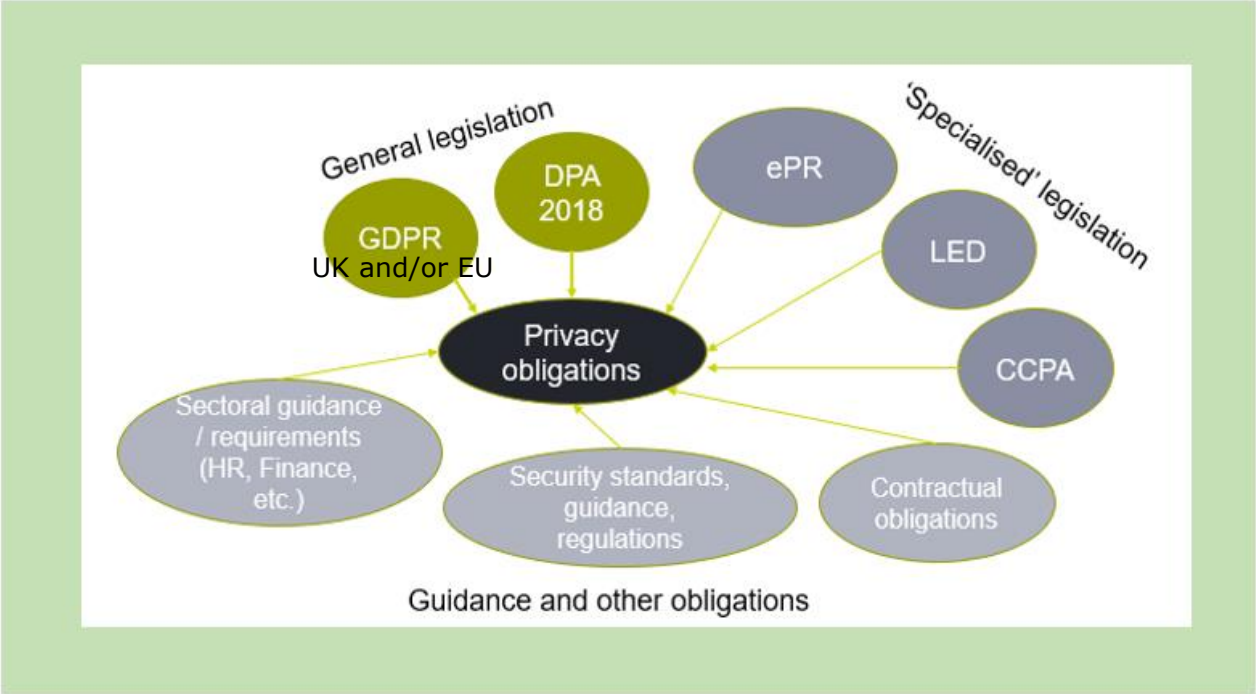
Protecting data and the law

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

The Privacy Universe

Guidance and obligations



Ransomware attacks

Industry reports

61% of organisations have been hit by a ransomware attack over the past 12 months

Mimecast, 2021

31% of organisations have a business continuity plan that covers cyber security

DDCMS, 2021

48% rise in threat volume in the first year of the pandemic

Mimecast, 2021

25% of businesses have cyber security policies that cover home working.

DDCMS, 2021

What does GDPR say?

GDPR Article 24

1. “Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.”

Assessing risk

The ICO advised…

- The ICO has expressly confirmed that when they are notified of a ransomware incident they will immediately begin to look at the organisation's compliance with the GDPR for suspected breaches.
- Organisations should consider the likelihood of risk and, if it were to occur, what would the severity be?
- Risk factors which the ICO will consider include:

Criminal and malicious access

Data exfiltration (which amounts to loss of control)

Detriment to individuals in regards to unavailability

Attacker threats

Speed of access and availability of personal data; and

Permanent loss of personal data i.e. threat actor deleted backups, which results in the loss of the right of access for data subjects.

What can a PIMS do for you?

IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

The privacy compliance framework

Under GDPR, organisations must demonstrate accountability

- A privacy compliance framework links:
  - The governance and internal control framework;
  - The PIMS and ISMS; and
  - The data processing principles.

- Objectives include:
  - Keeping personal data secure (C, I and A);
  - Protecting the rights of data subjects;
  - Compliance with relevant legislation and regulations; and
  - Compliance with customer contracts (SLAs, etc.).

- A PIMS, linked to an ISMS, demonstrates 'technical and organisational measures'

What is ISO 27701?

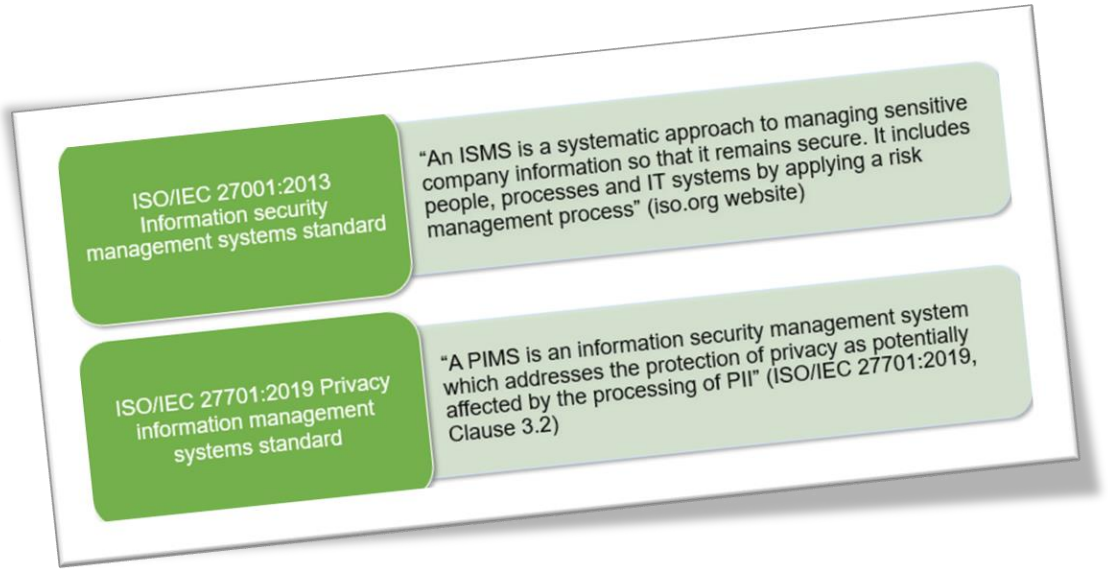
The basics

- ISO/IEC 27701:2019 is a privacy extension to the internationally recognised management system standard for information security, ISO/IEC 27001:2013.
- It is based on the requirements, control objectives and controls of ISO 27001, and includes a set of privacy-specific requirements, controls and control objectives.
- The Standard specifies the requirements for – and provides guidance on establishing, implementing, maintaining and continually improving – a privacy information management system (PIMS).

Personal Information Management Systems

Why organisations need a PIMS to comply with ISO 27701

- While organisations may have already implemented an ISO 27001-compliant ISMS, they may not have included PII in its scope.
- In order 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.



ISO 27701 requirements and guidelines

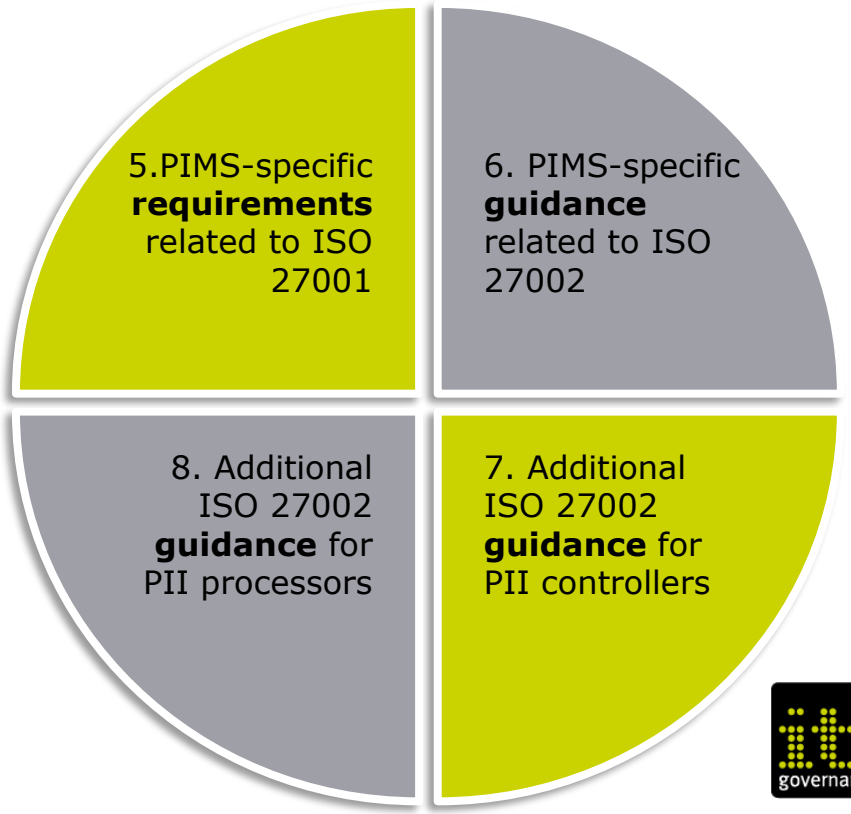
What it means in practice

- 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 PII.
- 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.

Why organisations need to consider ISO 27001 & ISO 27701

The implementation process

When considering how and what controls to implement, the organisation 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.



The key components of a PIMS

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

The key components of a PIMS

Identifying and monitoring necessary privacy activities and controls:

- Privacy notices, legal basis for processing, consent.
- Data protection principles.
- Individuals' rights – erasure, portability, objection, etc.
- Retention and disposal of personal data.

Contract management:

- Contracting with data processors or third parties in relation to PII.
- PII processors or third parties involving cross-border transfers.

PII principal (data subject) rights:

- Control processes for handling requests.

Change management:

- Ensure changes to data processing are controlled.
- Privacy by design and by default.

Staff awareness and building a security culture

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Staff awareness is critical to cyber defence

Persons working under the organisation's control must:

- Be aware of the PIMS policy;
- Understand their contribution; and
- Understand the implications of non-conformance.

Employees with day-to-day responsibilities should:

- Remain informed;
- Be able to demonstrate competence; and
- Receive training (e-learning, face-to-face, etc.).

What evidence is there?

- Training materials
- Records/results
- Certificates
- Communication emails, bulletins, newsletters, intranet, meeting minutes, etc.

The Board and Directors: Documented evidence

IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

ISO 27701 documented evidence

What it means for the Board and Directors

Scope	*A policy that accounts for privacy*	*Risk assessment*	*Risk treatment*
Privacy objectives	*Documented information required by ISO 27001*	*Management review*	*Statement of Applicability*

ISO 27701 documented evidence

PII controller

Purposes for which the PII will be processed	*Lawful bases for PII processing activities*	*The consent process*	*Written contracts with PII processors*	*Legal, regulatory and business obligations to PII principals*
Information to be provided to PII principals	*Handling procedures for PII principal requests*	*PII is accurate, complete and up to date*	*Data minimization objectives*	*Disposal policies and procedures*
	Basis for transfers	*Countries and international organizations to which PII can be transferred*	*Transfers and disclosure records*	

ISO 27701 documented evidence

PII processor

Records related to PII processing

Return, transfer or disposal of PII policy

Countries and international organizations to which PII can possibly be transferred

Disclosures of PII to third parties

Next steps

governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Our ISO 27701 solutions

How we can help you get started

Find out more

Find out more

Find out more

Find out more

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

Like us on Facebook
/ITGovernanceLtd

Follow us on Twitter
/itgovernance

Questions

Protect • Comply • Thrive

Thank you

Protect • Comply • Thrive