Our expertise,
your peace of mind

Privacy Integration - Empowering your ISO 27001 ISMS with ISO 27701 and Europrivacy certification

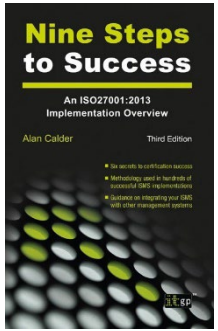
Alan Calder, Founder and Executive Chairman, IT Governance

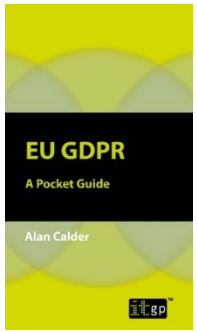
September 2, 2023

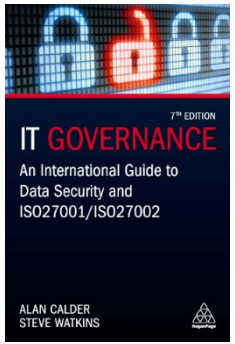
Introduction: Alan Calder

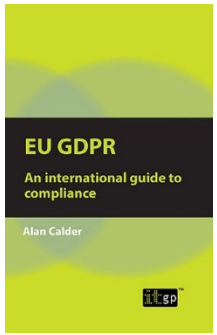
Founder and executive chairman of IT Governance

- 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).









About IT Governance

The cyber risk and privacy management solutions provider

20 years of experience, 200 employees

IT governance, risk and compliance solutions

Comprehensive GDPR and Privacy product and service offering

Comprehensive ISO 27001 product and service offering

IT Governance's Partnership with Perry Johnson Registrars

An ISO 27001 implementation and certification partnership

ISO 27001 Implementation Experts

IT Governance partners with Perry Johnson Registrars (PJR) and provides organisations with expert ISO 27001 implementation services

Certification Authority

IT Governance handles ISO 27001 implementation projects, while Perry Johnson Registrars independently certifies management system compliance, ensuring a seamless process for clients.

Our expertise, your peace of mind

Successfully carried out more than

2,000

projects to help organisations prepare and maintain their ISO 27001 and/or GDPR compliance.

More than

1,600

cyber security projects delivered

Successfully issued more than

7,000

Cyber Essentials certifications

More than

1,100

organisations use our governance, risk and compliance software

Agenda

01 The benefits of implementing ISO 27701 as a privacy extension to ISO 27001.

02 Key considerations when scoping an ISO 27701 implementation project.

03 Effective strategies for gaining support from top management and securing the necessary budget and resources for the integration process.

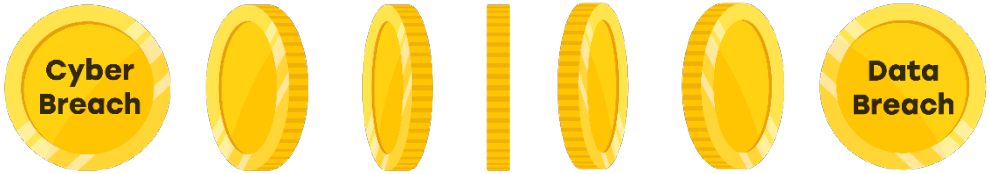
04 Leveraging Europrivacy certification for GDPR compliance and strengthening your organisation's security posture in the EU market.

05 Practical steps and solutions to help organisations navigate the entire integration process, from detailed gap analysis to policy development and training.

06 Live Q&A

The benefits of implementing ISO 27701 as a privacy extension to ISO 27001

Cyber security vs Data protection



- Personal data, including names, addresses, and financial information, remains a prime target for cybercriminals due to its high value on the black market.
- Recent major breaches, like the Alibaba Data Breach in July 2022, affecting 1.1 billion users, highlight the urgency for strong data protection measures.
- The ongoing MOVEit hack, which began in May this year, is poised to be recorded as one of the most extensive and successful cyberattacks in history. So far It has impacted over 1,000 organisations and 60 million individuals, leading to the exposure of critical personal information, including social security numbers, banking details, and health records.
- Integrating ISO 27001 and ISO 27701 is vital for comprehensive security, covering both general information security and specific safeguards for personal data compliance.

What is ISO 27701?

Implementing ISO 27701 as an extension of your ISMS

- ISO/IEC 27701:2019 is a privacy extension to the international information security management standard, ISO/IEC 27001 (ISO/IEC 27701 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines).

- ISO 27701 specifies the requirements for – and provides guidance for establishing, implementing, maintaining and continually improving – a PIMS (privacy information management system).

- ISO 27701 is based on the requirements, control objectives and controls of ISO 27001, and includes a set of privacy-specific requirements, controls and control objectives.

How do ISO 27001 and ISO 27701 integrate with each other?

Implementing ISO 27701 as an extension of your ISMS

- ISO 27001 establishes the requirements for an ISMS (information security management system) that takes a risk-based approach to security, covering people, processes and technology.
- Certification to ISO 27001 provides stakeholders with assurance that data is being secured appropriately.
- Organisations that have implemented ISO 27001 can use ISO 27701 to extend their security efforts to cover privacy management, including the processing of PII (personally identifiable information), which can help them demonstrate compliance with data protection laws such as the GDPR or State-level privacy laws.
- Organisations without an ISMS can implement ISO 27001 and ISO 27701 together as a single implementation project.

Benefits of ISO 27701 as a privacy extension to ISO 27001

Implementing ISO 27701 as an extension of your ISMS

Comprehensive Privacy Framework

Legal and regulatory compliance

Third-party assurance and risk reduction

Efficient privacy management and data protection

Improve structure and focus

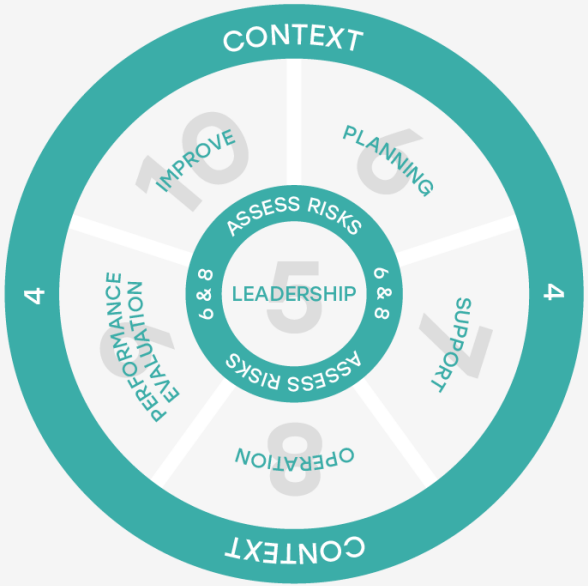
Reduce the need for supplier/regulatory audits

Obtain independent assurance on your security and privacy management

ISMS Overview

ISO 27001 MANAGEMENT SYSTEM CLAUSES

1, 2 & 3	Scope, normative references, and terms and definitions.
4	Internal and external issues that may be relevant to the organisation and to achieving the ISMS objectives. Includes confirming interested parties and scope.
5	How top management will support the ISMS by creating roles and measures to implement and monitor it. Includes developing an information security policy aligned to business objectives.
6	How the organisation creates actions to address risks. Includes setting information security objectives.



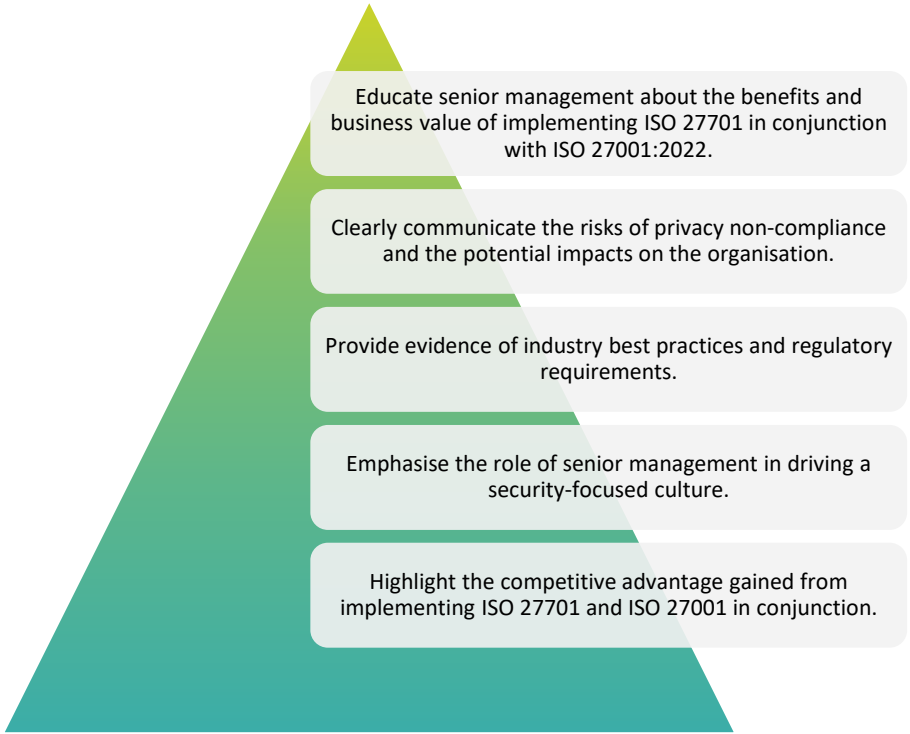
Securing the right resources, people and infrastructure to manage and maintain the ISMS.	7
How the plans and processes will be executed, including documentation that needs to be produced.	8
How the organisation will monitor, measure, analyse and evaluate the ISMS.	9
Corrective action and continual improvement requirements.	10

ISO 27001 and ISO 27002

- ISO 27001 and ISO 27002 standards have been updated to 2022 versions, reflecting current best practices in information security.
- ISO 27701 currently remains at the 2019 version. The ISO/IEC 27701 standard's updated draft was published in early January 2023. This will now go through a ballot stage before a final draft and a completed article are developed.
- Despite the version disparity, it's worth noting that utilising the mapping in ISO 27002, which links the 2013 and 2022 versions, allows for a straightforward integration of ISO 27701:2019 clauses into the 2022 standards.
- This mapping process facilitates the alignment of ISO 27701:2019 with the updated 2022 standards, ensuring a comprehensive and up-to-date approach to privacy and information security.

Key considerations when scoping an ISO 27701 implementation project

Strategies for scoping an ISO 27701 implementation project



Scoping your ISO 27701 & ISO 27001:2022 project

Scoping your ISO 27701 & ISO 27001:2022 project

ISO 27701 control mappings

As well as providing privacy-specific requirements, controls and control objectives for controllers and processors, ISO 27701 includes annexes that map them to:

ISO 29100

Information technology – Security techniques – Privacy framework

ISO 29151

Information technology – Security techniques – Code of practice for personally identifiable information protection

ISO 27018

Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Note: It also contains an annex that maps its requirements and controls to the GDPR's requirements, so ISO 27701 can be used as a GDPR compliance guide by data controllers and processors.

For instance, data controllers' obligations for meeting data subjects' rights under the GDPR are covered by ISO 27701's controls covering obligations to PII principals.

Strategies for gaining support from top management and securing the necessary budget and resources for the integration process

Board commitment and senior management support

ISO 27701 as an extension to ISO 27001:2022 requires active engagement and support from senior management.

Senior management’s commitment is vital for resource allocation, decision-making and implementation success.

Demonstrates the organisation's commitment to privacy management as part of information security.

Sets the tone for a culture of security awareness and accountability.

Enables the allocation of necessary resources and budgets for the transition project.

Increases the likelihood of successful implementation and long-term compliance.

Demonstrate GDPR compliance with ISO 27701 and ISO 27001

- ISO 27701 and ISO 27001 will help you meet GDPR and other privacy requirements and show that you have the necessary security measures in place to protect personal data and uphold data subjects' rights.

- Article 42 of the GDPR discusses data protection certification mechanisms and data protection seals and marks.

- It is possible to achieve independently accredited certification to ISO 27001 – and by extension ISO 27701 if you implement its controls – which will demonstrate to stakeholders and regulators that your organisation is following international best practice when it comes to securing personal data/PII.

ISO 27001/27701 Certification

Commit
Management commit from an informed position

Design and implement ISMS to:

- Fulfil requirements of customers and stakeholders
- Deliver continual improvement
- Meet information security objectives and mitigate business risks
- Comply with regulations, legislation & industry mandates
- Manage information assets

Information Security Management System + Privacy Management Integration

Internal Audit

Certification
Stage 1 and Stage 2 audits by Accredited Certification Body

CAV (continual assessment visits) 'check-up'

Leveraging Europrivacy certification for GDPR compliance and strengthening your organisation’s security posture in the EU market.

What is Europrivacy™/®?

The European Data Protection Seal

- Europrivacy is the first GDPR (General Data Protection Regulation) certification mechanism recognised by the EDPB as the European Data Protection Seal, as defined by Article 42 of the Regulation, in all EU .
- It enables organisations to demonstrate that their data processing activities comply with the EU GDPR and relevant national and international regulations.
- The Europrivacy certification scheme was developed through the European Research Programme Horizon 2020, and co-funded by the European Commission and Switzerland.
- It was approved by the EDPB (European Data Protection Board) as the European Data Protection Seal on 10 October 2022.
- It is managed and continually updated by the ECCP (European Centre for Certification and Privacy) in Luxembourg and its International Board of Experts in data protection, with the support of official partners such as the Italian Institute for Privacy and Data Valorisation.

Who needs Europrivacy certification?

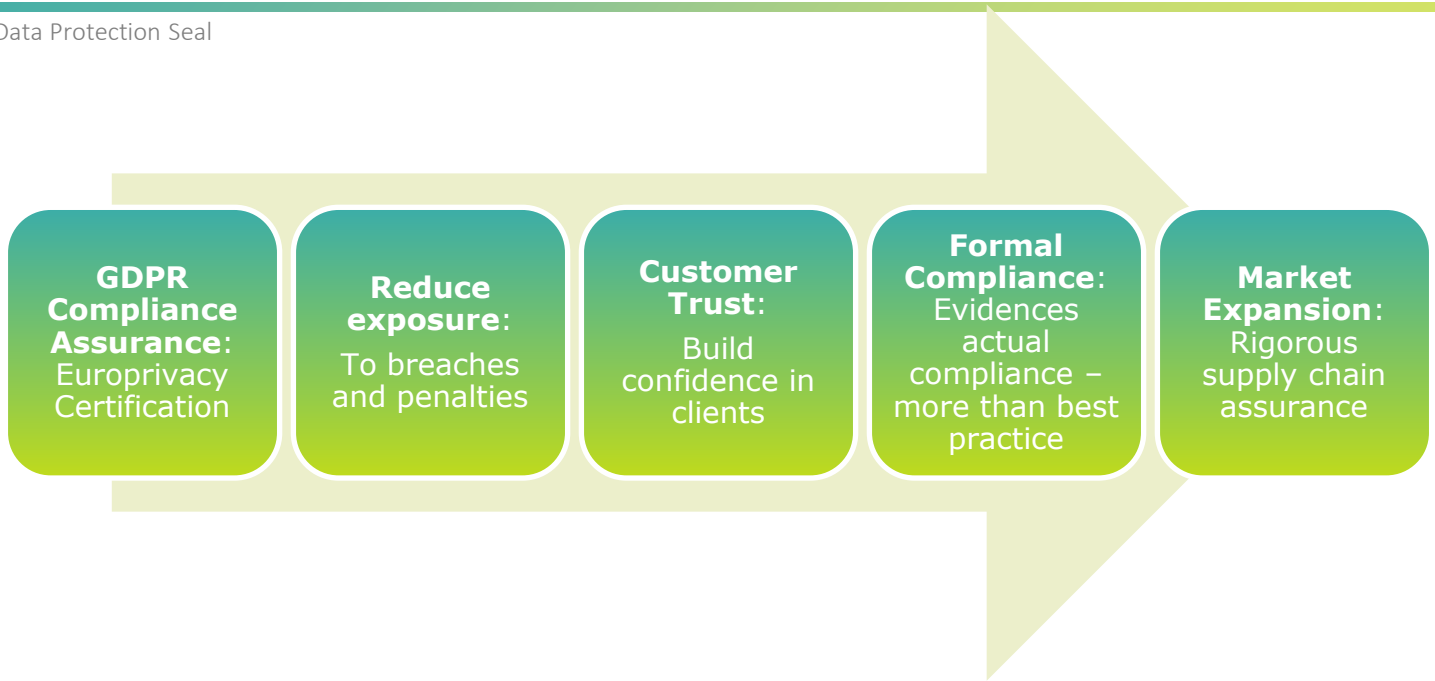
The European Data Protection Seal

- Europrivacy enables both data controllers and data processors (with DPOs) to formally certify that their data processing activities comply with the GDPR and other relevant data protection laws.
- Europrivacy certification is recognised in all 27 EU member states and will be taken into account by the data protection authorities in the case of litigation.
- To achieve certification, organisations must meet, among others, the Europrivacy GDPR core criteria, which are maintained by the ECCP and its Europrivacy International Board of Experts.
- The core criteria allow organisations to assess their compliance with regard to:
  - Lawfulness of data processing;
  - Special data processing;
  - Data subjects' rights;
  - Data controllers' responsibilities;
  - Data processors;
  - Security of processing and data protection by design;
  - Management of data breaches;
  - DPIAs (data protection impact assessments);
  - DPOs (data protection officers); and
  - Transfers of personal data to third countries or international organisations.

EuroPrivacy recognises an accredited ISO 27001 certificate as demonstrating compliance with the GDPR requirements in respect of security of processing.

Leveraging Europrivacy Certification

The European Data Protection Seal

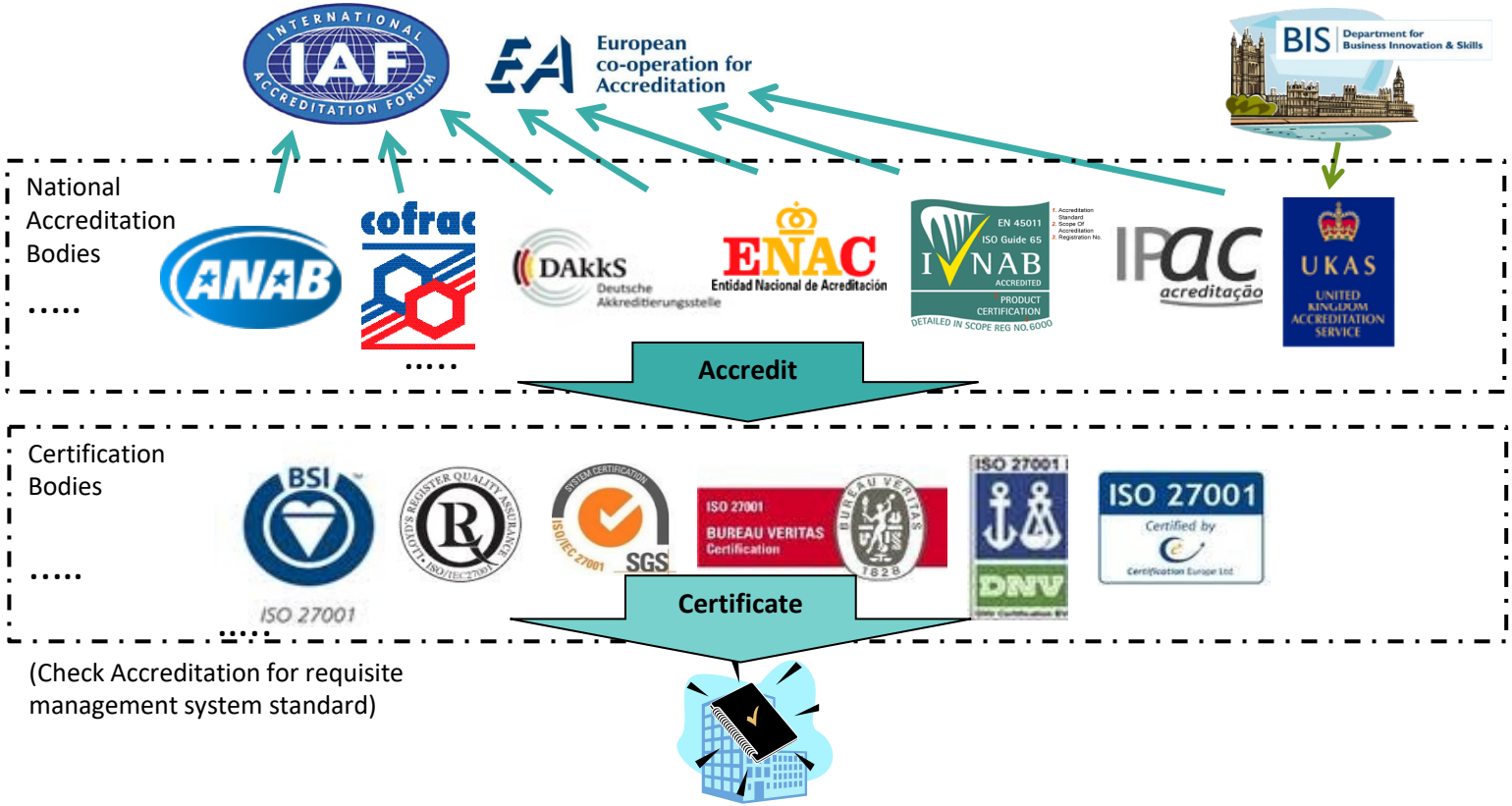


EuroPrivacy certification is an add-on to an ISO 27001 ISMS. It deals very specifically with GDPR requirements. It is being extended to include specific requirements of other legislation.

How CyberComply can help you integrate ISO 27701 in your ISO 27001 ISMS.

ISO 27001/27701/EuroPrivacy Certification

ISO 27001 certification overview



CyberComply for ISO 27701, ISO 27001 and Europrivacy certification

CyberComply is a modular platform that provides organisations with the following benefits:

Automated risk assessment and ISO 27001 document generation

Simplify risk assessment and document production (e.g. the Statement of Applicability and risk treatment plan) with CyberComply's automation capabilities.

Cost-effective management system maintenance and GDPR integration

Using CyberComply reduces ongoing maintenance costs and seamlessly integrates with the GDPR's requirements.

Mapping of the ISO 27001 Annex A controls to multiple frameworks

Easily comply with multiple regulations and industry standards by leveraging CyberComply's mappings of ISO 27001 Annex A controls.

Streamlined incident tracking and collaboration

Manage incidents from start to finish within CyberComply's unified platform designed for cyber security and data privacy.

Stakeholder notifications and comprehensive incident logging

Keep stakeholders informed with incident notifications and maintain an audit trail through a complete incident log.

Intuitive real-time dashboard for incident management

Access an interactive dashboard that provides a real-time overview of incidents and tasks, tailored to your preferences.

CYBER COMPLY

Find out more

Our ISO 27001/27701/EuroPrivacy solutions

EuroPrivacy solutions

- As certified partners of the European Centre for Certification and Privacy, we bring a wealth of expertise in data protection.
- We provide a comprehensive suite of services with our sister companies IT Governance Europe and GRCI Law, specialising in GDPR-compliant processes, ISO/IEC standards, Cyber Essentials, PCI DSS, and more.
- Our expert consultants are committed to helping clients all over the world obtain Europrivacy certification, achieving this with the help of our specialised GDPR tools.

How IT Governance can help

Our ISO 27701 solutions

Train with ISO 27001 experts and learn how to extend an ISO 27001 ISMS to deliver an ISO 27701 PIMS (privacy information management system).

Find out more

Train with ISO 27001 experts and learn how to extend an ISO 27001-compliant audit programme and conduct an ISO 27701 PIMS audit.

Find out more

Get the true picture of your ISO 27001 compliance gaps, and receive expert advice on how to scope your project and establish your project resource requirements.

Find out more

Extend your ISMS (information security management system (ISMS) to cover data protection and privacy with our FastTrack™ service.

Find out more

Get in touch

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

Like us on Facebook
/ITGovernanceLtd

Follow us on Twitter
/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

Like us on Facebook
/itgovernanceeu

Follow us on Twitter
/ITGovernanceEU

United States

Visit our website
www.itgovernanceusa.com

Email us
servicecentre@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


Thank you


Questions