



Your journey to ISO 27001 – Internal Audit and Certification

November 3, 2022

About IT Governance

The cyber risk and privacy management solutions provider



20 years of
experience, 200
employees



More than 12,000
clients across 5
continents



IT governance, risk,
and compliance
solutions



Comprehensive ISO
27001 product and
service portfolio

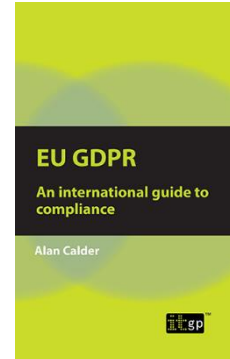
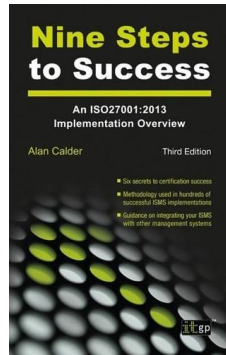


Introduction: Alan Calder

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).



01

Internal audits and preparing for a certification audit

02

The steps to conduct an internal audit

03

Common audit pitfalls and how to avoid them

04

The certification audit process.

05

Choosing a certification body and why it is important to make the right decision



Contents



Protect • Comply • Thrive

Types of Audit

ISO/IEC 27001

First party (internal):

The organization audits itself

Second party (supplier):

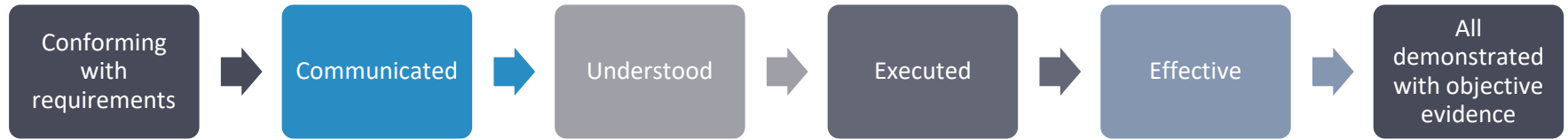
Clients audit their suppliers

Third party (certification):

Legal, regulatory, or registration audit

Why audit an ISMS?

Proactive assurance that the Management System and it's processes are:



Why audit an ISMS?

Objectives:



Why audit an ISMS?

ISO 27001:2013 Clause 9.2:

The organization shall conduct internal audits at planned intervals to provide information on whether the ISMS:

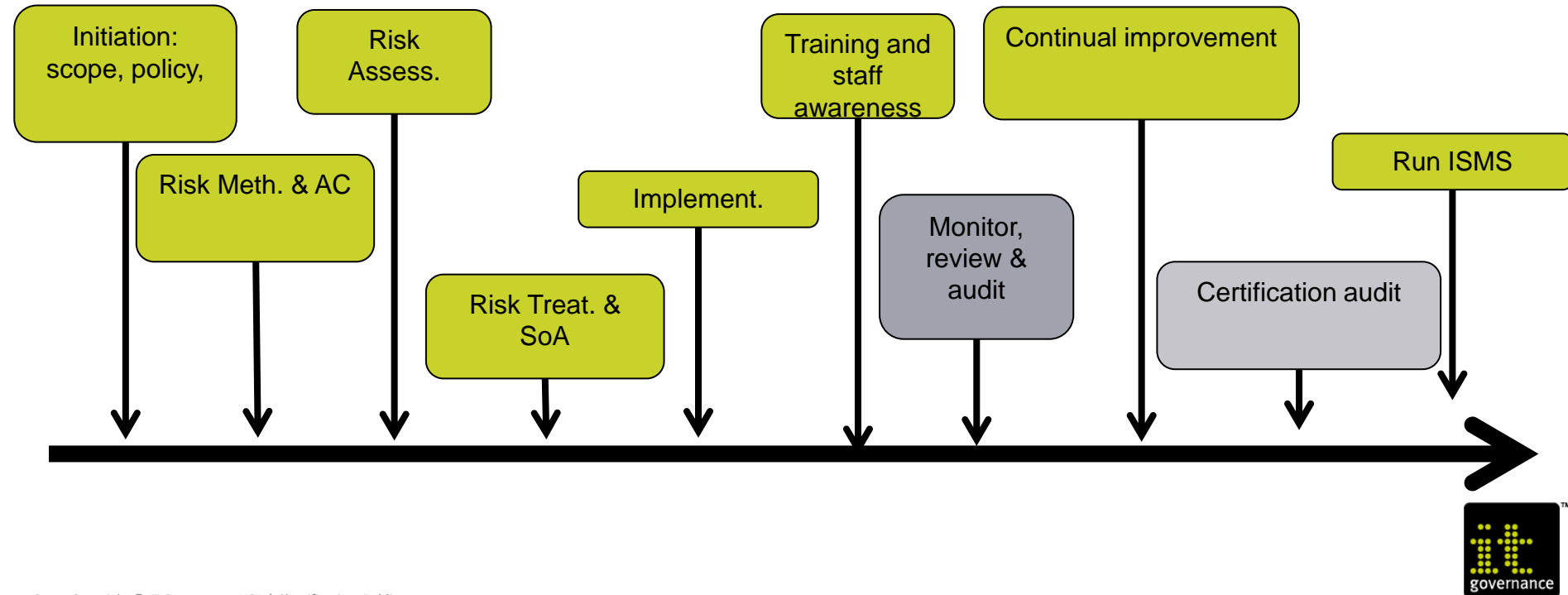
- conforms to
 - 1) the organization's own requirements for its ISMS
 - 2) the requirements of ISO 27001
- is effectively implemented and maintained

Audit:

- Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

ISMS Project

Roadmap



The role of ISMS audits

Does the ISMS conform to ISO 27001?

Does it conform to the specified information security requirements?

- Those set by interested parties?
- Information security risk acceptance criteria?
- Risk treatment decision?

Is it effective and maintained?

Does the ISMS perform as expected?

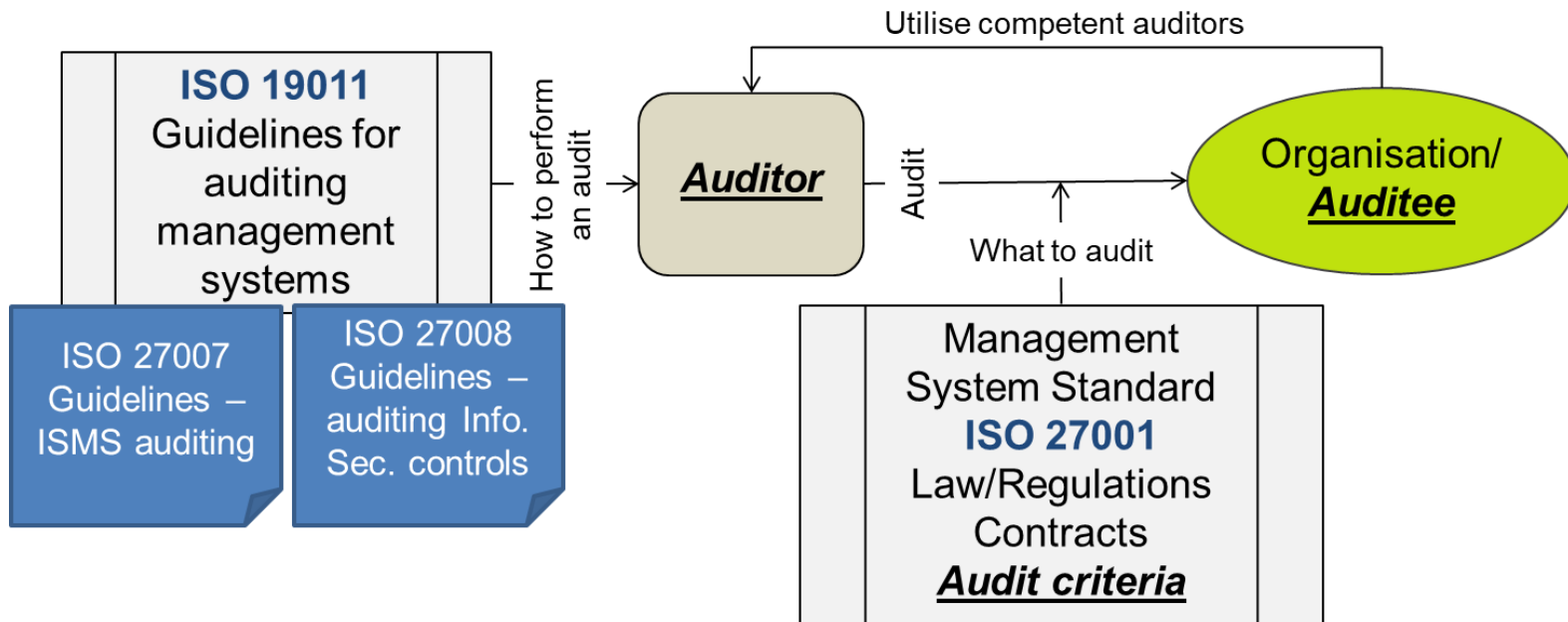
ISO 27001 Clause 9.2 extract

The organization shall:

- **plan ... implement and maintain an audit programme(s)**, ... take into consideration the importance of the processes concerned and the results of previous audits;
- Define the audit criteria and scope for each audit;
- Select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
- Ensure that the results of the audits are reported to relevant management; and
- Retain documented evidence of the audit programme(s) and the audit results.

Relevant standards

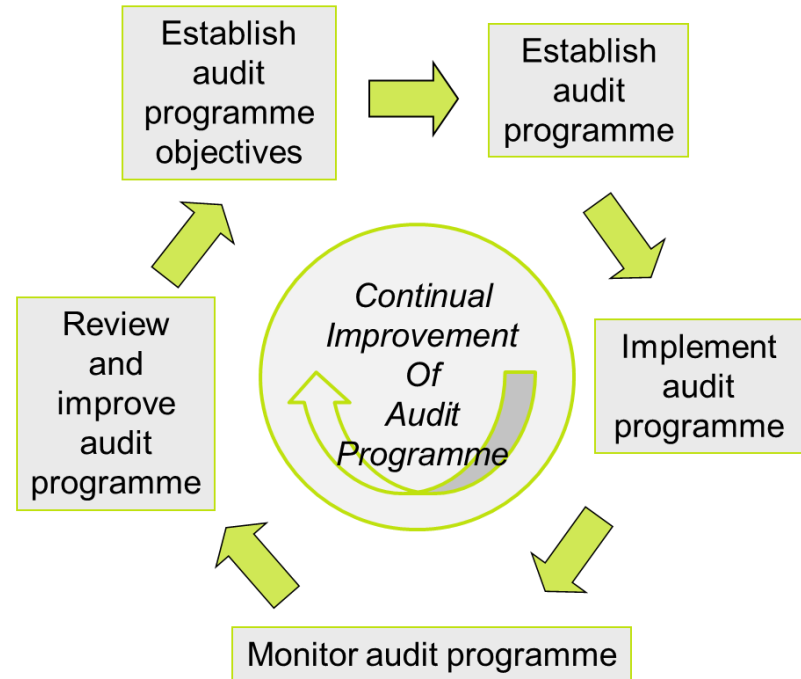
Guidelines for auditing



Audit programme

Approaches

- Must address entire system. Could scope separate audits:
 - Clause-by-clause/control-by-control
 - Geography/department/team
 - Process(es)
 - Mix of the above



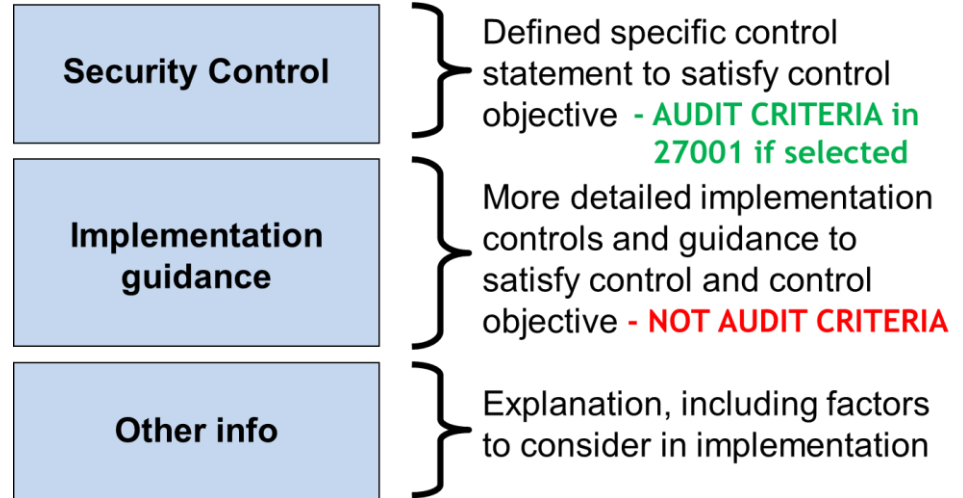
ISMS requirements

Audit

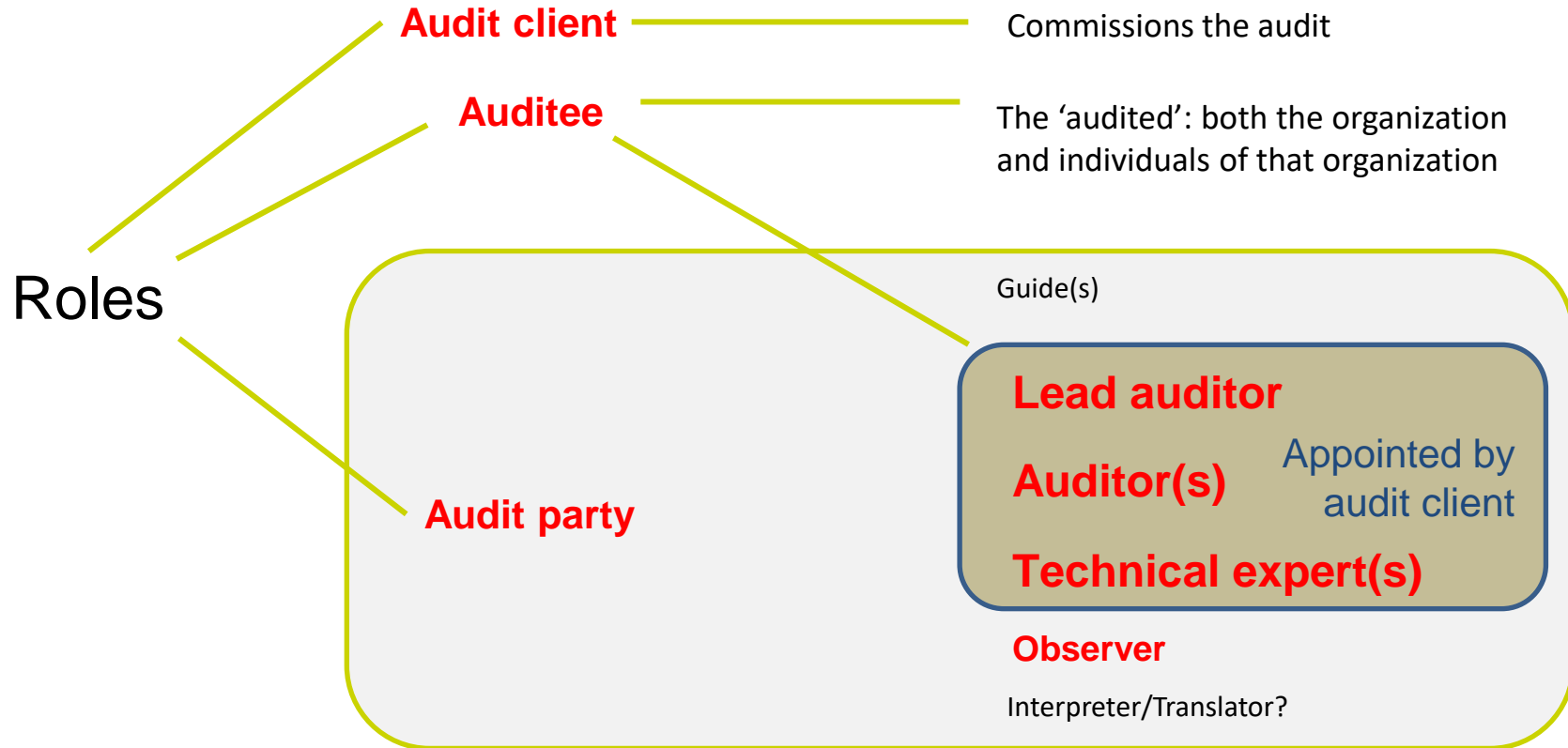
- Audit criteria
 - ISO 27001:2013
 - Normative reference ISO 27000
 - Contextual requirements
 - Organization's ISMS

Guidance:

- Other ISMS standards, especially ISO 27002:

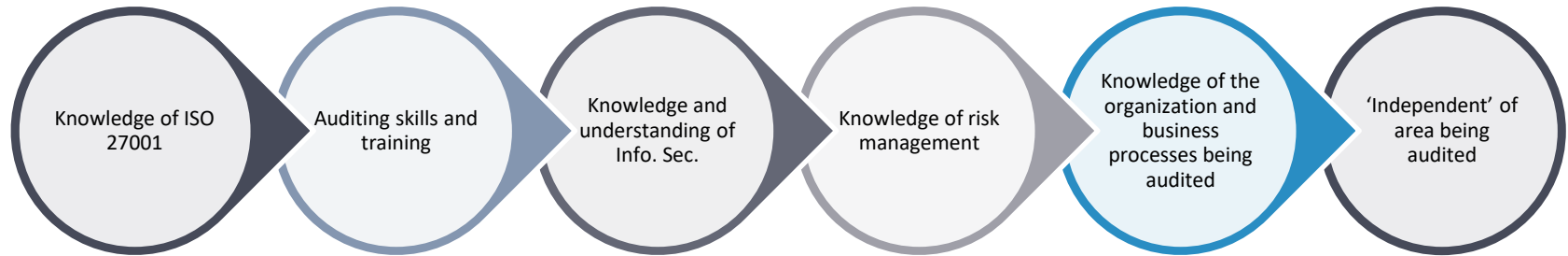


People's role in audits




ISMS auditor

Competencies and traits



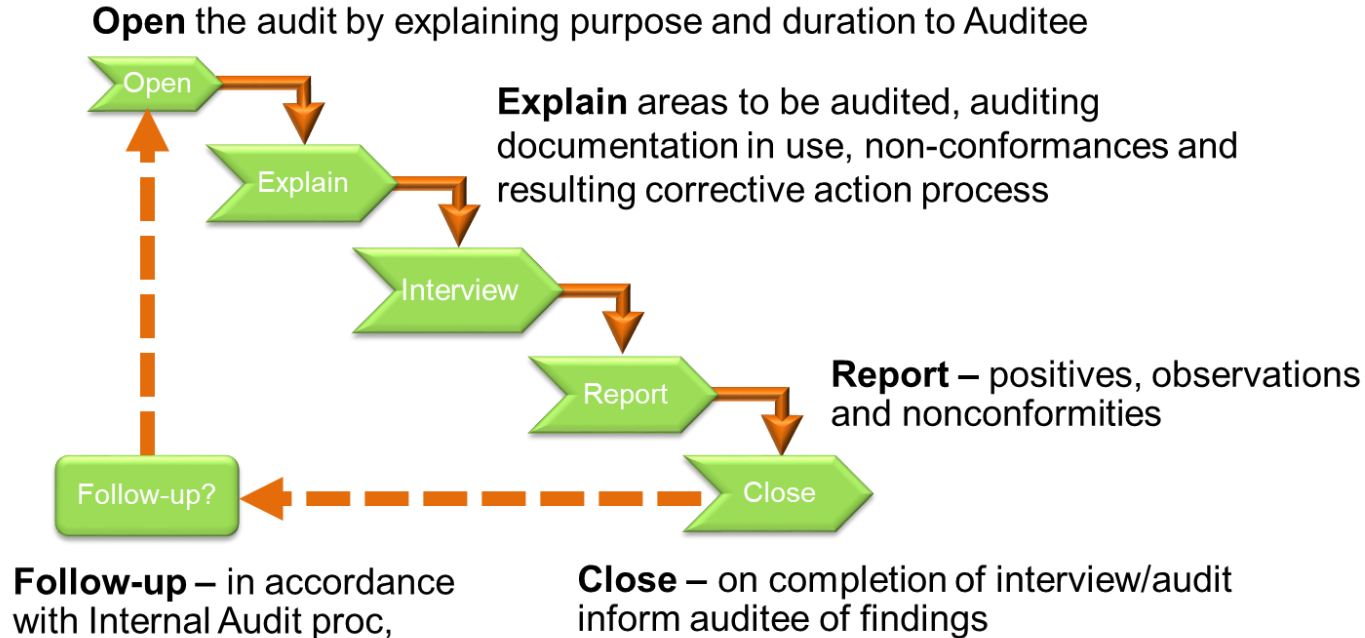
The four phases of audit

- Preparation (40%)
- Performance (30%)
- Reporting (10%)
- Follow-up (20%)  Follow-up/next audit

Planning an internal audit

- Audit assignment
 - Inform auditee
 - Inform auditor
- Provide auditor with necessary information:
 - Scope
 - Procedures and related documentation
 - Nonconformities raised previously, recent developments, planned changes, changes to key staff
 - Objective (conformance (ISMS, specific contract), improvement, efficiency, investigation, etc.)

Audit experience



Documenting nonconformities

Requirement <i>What is required</i>	Quote from <ul style="list-style-type: none">- law, regulations- contract,- audit client(/auditee?) management system, or- ISO management system standard
	Identify source of requirement
	Identify relevant clause of ISO management system standard
Finding <i>What was found</i>	Statement of how the requirement is not met
	Refer to evidence of not meeting the requirement, e.g. relevant documented information, observations, audit client statements (Or statement that no evidence was available during the audit to show the requirement was met)
‘So what?’ <i>Why it matters</i>	Statement of possible consequences or risks in terms of achievement of management system policy and objectives

Improvement

ISO 27001:2013 Clause 10

■ 10.1 Nonconformity and corrective action

- React to nonconformity:
 - Control and correct it
 - Evaluate need to eliminate cause and act as necessary
- Retain documented evidence of:
 - Nonconformities and actions taken
 - Effectiveness of any corrective action taken

■ 10.2 Continual improvement

- The organization shall continually improve the suitability, adequacy, and effectiveness of the ISMS

- **Nonconformity**: non-fulfilment of a requirement
- **Correction**: action to eliminate a detected nonconformity
- **Corrective action**: action to eliminate the cause of a nonconformity and to prevent recurrence

Continual improvement

MS standards: improvement focuses on three main areas

- Suitability – the extent to which the MS ‘fits’ and is right for the organization’s purpose, its operations, culture, and business systems
- Adequacy – the extent to which the MS is sufficient in meeting the applicable requirements
- Effectiveness – the extent to which planned activities are realized and planned results achieved

ISMS continual improvement

- Evolves – in light of developing technology, threats, new assets and vulnerabilities
- Improves efficiency of ISMS and controls in meeting security objectives
- Improves effectiveness of ISMS and controls in meeting security objectives

The benefits of internal audits

1
Informs conformity ahead of others discovering it

2
Ensures security stance is as intended, identifying areas requiring attention prior to a security event

3
Demonstrates and informs management commitment

4
Assists understanding and awareness of staff

5
Informs continual improvement

ISO 27001 Certification Audit

- The ISO 27001 certification audit takes place once an organisation applies for certification.
- Normally once it has implemented an information security management system (ISMS) addressing the requirements of ISO 27001.
- Regular certification audits to maintain certification.
- Although the process can seem intimidating, the right preparation can ensure the process runs smoothly – increasing the chances of a successful outcome.

Benefits of ISO 27001 certification



Win new business and retain your existing customers



Avoid financial penalties and losses



Protect and enhance your reputation



Comply with business, legal, contractual and regulatory requirements



Improve structure and focus



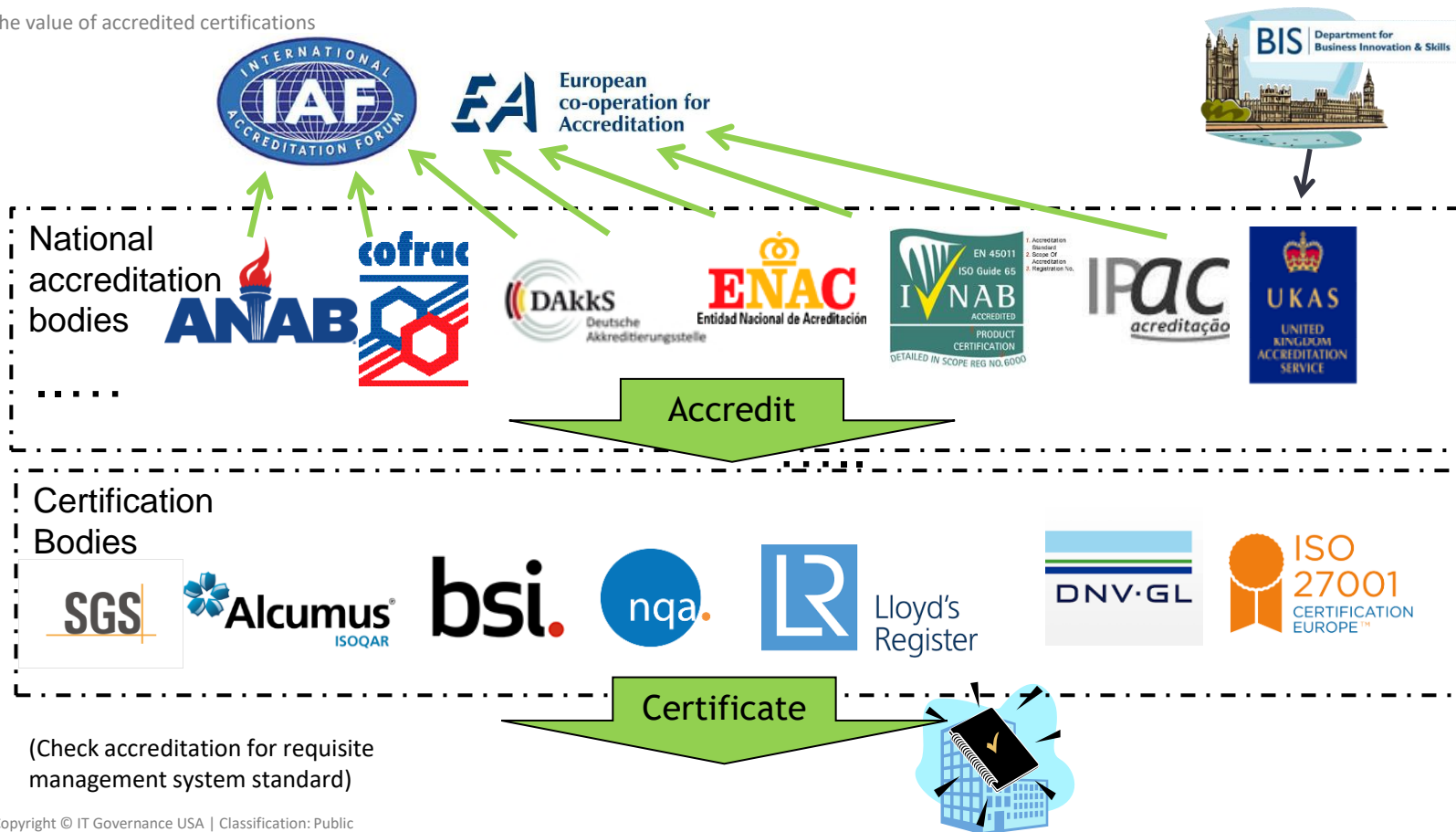
Reduce the need for supplier/regulatory audits



Obtain an independent opinion about your security management

Choosing a certification body

The value of accredited certifications



How do you choose your certification body?

- Any organisation that claims to be an accredited certification body should be able to show you a current copy of its schedule of accreditation with ISO/IEC 17021-1:2015, issued by a national accreditation body for the relevant scheme.
- Don't choose solely based on price – also consider the competence of auditors, relevance to your sector, spread of schemes, geographical presence and customer service.

Selecting a certification body

Factors to consider

Although your chosen certification body should not impact your success in achieving certification, keep in mind the following::

- Cultural fit
 - Pricing
 - Competence of auditors
 - Relevance to your sector
 - Spread of schemes
 - Geographical presence
 - Customer service
-
- Any organisation that claims to be an accredited certification body should be able to show you a current copy of its schedule of accreditation with ISO/IEC 17021-1:2015, issued by a national accreditation body for the relevant scheme.

Accredited vs. unaccredited certification

ACCREDITED

- Certification body assessed by relevant accreditation body
 - Competence
 - Impartiality
 - Performance capability
- Widely recognised
 - Many government contracts
 - Sector schemes
- Ongoing 'check and challenge' with recertification every three years

- Unknown/inconsistent performance, quality and competence monitoring
- Dubious requirements for those seeking certification:
 - Documentation audit only
 - Certificate per site
- Certificate valid >25 years
- Pricing based solely on turnover

UNACCREDITED

ISO 27001 certification checklist



ISMS indicators

Does the ISMS demonstrate that it is conforming to ISO/IEC 27001:2013?

- Effectiveness
- Internal audit
- Management review



Timing

Fit with other activities

- Frequency of surveillance audits
- Fit with other MSS certifications



Internal audit and management review

- Implemented?
- Effective?
- Will be maintained?



Conformity not perfection

ISMS “only” needs to conform, improvement follows...

How IT Governance USA can help

Our solutions



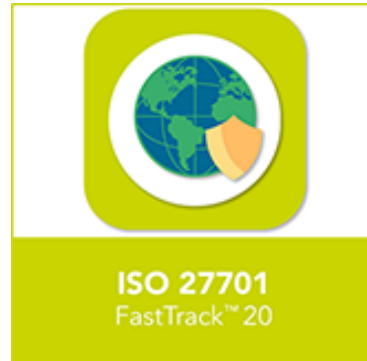
Learn how to extend an ISO 27001-compliant ISMS to cover privacy information management.

[Find out more](#)



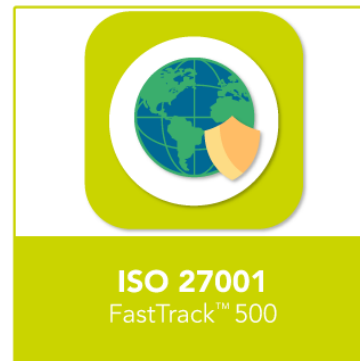
This tool lists all the requirements from ISO 27701:2019, against which you can assess your current state of compliance and prioritize work areas.

[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



A satellite view of Earth from space, showing the curvature of the planet and city lights at night. The image captures a wide expanse of the Earth's surface, with the dark blue of the oceans and the lighter blue of the atmosphere visible. Numerous bright yellow and orange lights from cities and towns are scattered across the landmasses, creating a glowing pattern against the dark background. The horizon line is clearly visible, separating the Earth from the blackness of space.

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](https://www.linkedin.com/company/it-governance)



Follow us on Twitter

[/ITGovernanceLtd](https://twitter.com/ITGovernanceLtd)



Like us on Facebook

[/ITGovernance](https://www.facebook.com/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](https://www.linkedin.com/company/it-governance-europe-ltd)



Follow us on Twitter

[/itgovernanceeu](https://twitter.com/itgovernanceeu)



Like us on Facebook

[/ITGovernanceEU](https://www.facebook.com/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](https://www.linkedin.com/company/it-governance-usa-inc)



Follow us on Twitter

[/ITGovernanceUSA](https://twitter.com/ITGovernanceUSA)



Like us on Facebook

[/ITG_USA](https://www.facebook.com/ITG_USA)

