Your Journey to ISO 27001:
Updates, transition strategy, and implementation

7 September 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 6 continents

More than 1,000 penetration tests delivered

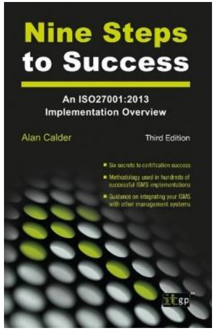
itgp
it governance
Vigilant software
GRC international group plc
GDPR.co.uk
GRC eLearning
DQM GRC
GRCLaw

Introduction: Alan Calder

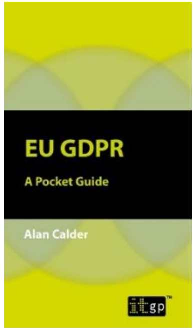
Founder and executive chairman of IT Governance

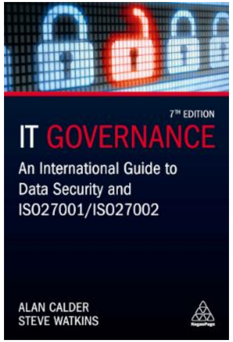
- Founder and executive chairman of IT Governance, the single source for everything to do with IT governance, cyber risk management, and IT compliance.

- Author of *IT Governance: An International Guide to Data Security and ISO27001/ISO27002* (Open University textbook).



Nine Steps to Success
An ISO27001:2013 Implementation Overview
Alan Calder
Third Edition
Six secrets to certification success
Methodology used in hundreds of successful ISMS implementations
Guidance on integrating your ISMS with other management systems
itgp





7TH EDITION
IT GOVERNANCE
An International Guide to Data Security and ISO27001/ISO27002
ALAN CALDER
STEVE WATKINS

IT GOVERNANCE
6th Edition
AN INTERNATIONAL GUIDE TO DATA SECURITY AND ISO27001/ISO27002
ALAN CALDER & STEVE WATKINS

01 ISO/IEC 27001:2022 and a transition strategy

02 The baseline security criteria to implement an ISO 27001-compliant ISMS

03 The five steps in an ISO 27001 information security risk assessment

04 How to secure organization-wide commitment

05 Practical steps and solutions to implement ISO 27001

Contents

Protect • Comply • Thrive

ISO/IEC 27001:2022 and a transition strategy

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Nine steps to implementing ISO 27001

Nine Steps to Success: An ISO 27001:2013 Implementation Overview

STEP 4

Management framework

- Defining the scope of your ISMS – the parts of your organization you'll be protecting.
- Create the scope for your ISMS implementation project.

STEP 5

Baseline security controls

- An organization's security baseline is the minimum level of activity required to conduct business securely.
- You should define your security baseline using the information collected during your ISO 27001 risk assessment.

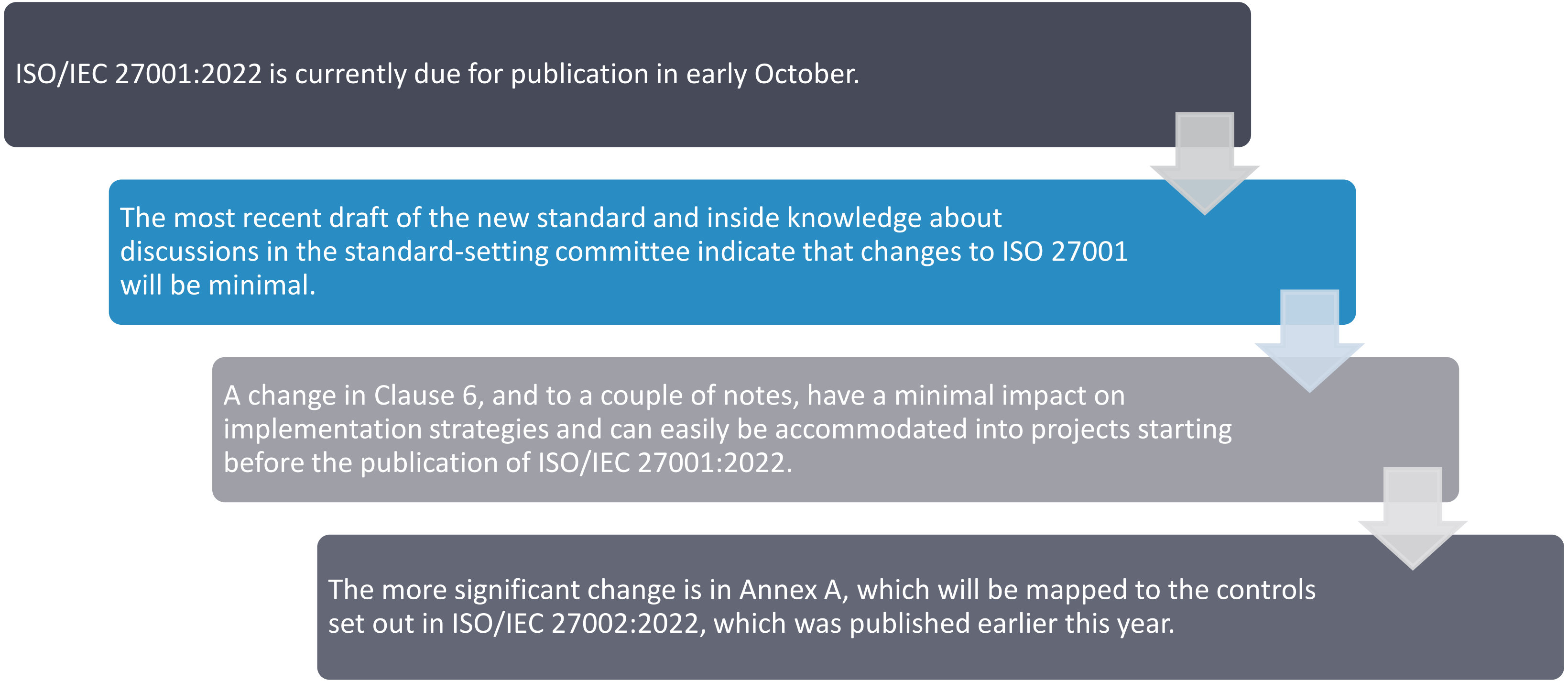
STEP 6

Risk management

- Treat the risk by applying information security controls laid out in ISO 27001.
- Terminate the risk by avoiding it entirely.
- Share the risk.
- Accept the risk (if it doesn't pose a significant threat).

ISO/IEC 27001:2022

How different is the new standard?



ISO/IEC 27001:2022 is currently due for publication in early October.

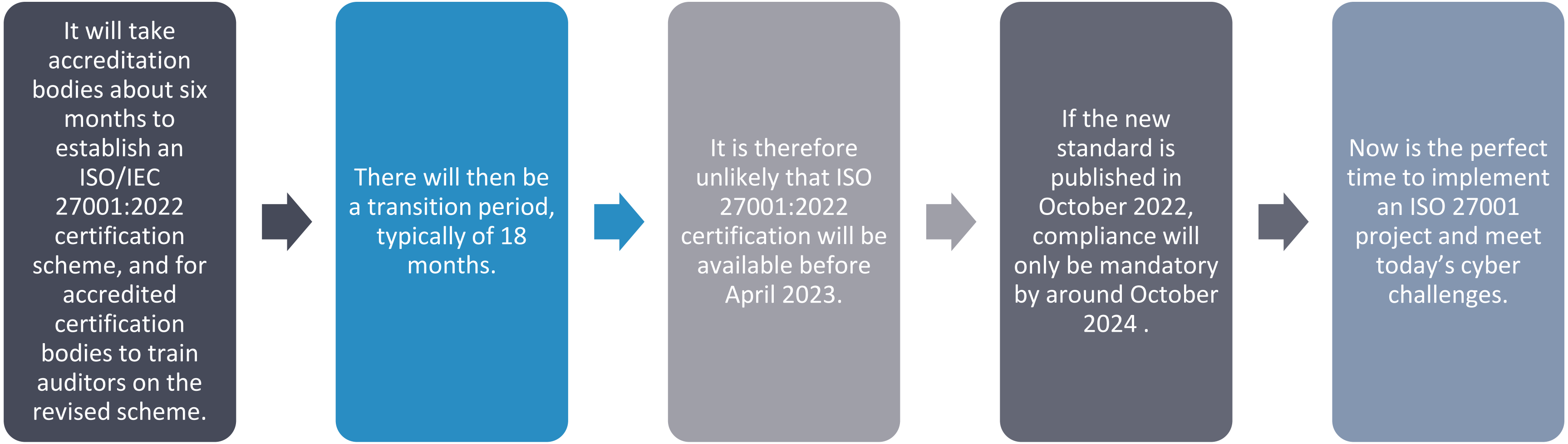
The most recent draft of the new standard and inside knowledge about discussions in the standard-setting committee indicate that changes to ISO 27001 will be minimal.

A change in Clause 6, and to a couple of notes, have a minimal impact on implementation strategies and can easily be accommodated into projects starting before the publication of ISO/IEC 27001:2022.

The more significant change is in Annex A, which will be mapped to the controls set out in ISO/IEC 27002:2022, which was published earlier this year.

ISO/IEC 27001:2022

What is the likely transition timetable?



It will take accreditation bodies about six months to establish an ISO/IEC 27001:2022 certification scheme, and for accredited certification bodies to train auditors on the revised scheme.

There will then be a transition period, typically of 18 months.

It is therefore unlikely that ISO 27001:2022 certification will be available before April 2023.

If the new standard is published in October 2022, compliance will only be mandatory by around October 2024 .

Now is the perfect time to implement an ISO 27001 project and meet today’s cyber challenges.

ISO/IEC 27001:2022

What might a transition strategy look like?

- Organizations can go ahead, today, and implement a management system that can be certified to ISO/IEC 27001:2013, and can do so in the knowledge that the transition to ISO/IEC 27001:2022 will only require minimal effort.
- The management system documentation will need to be updated to reflect the Clause 6 changes.
- As a minimum, your Statement of Applicability will have to be amended to map your 2013 controls the 2022 controls – and that mapping is already set out in ISO/IEC 27002:2022.
- At any time before transition, you can implement controls from ISO 27002:2022 – as long as you map them to your existing ISO 27001:2013 Annex A.

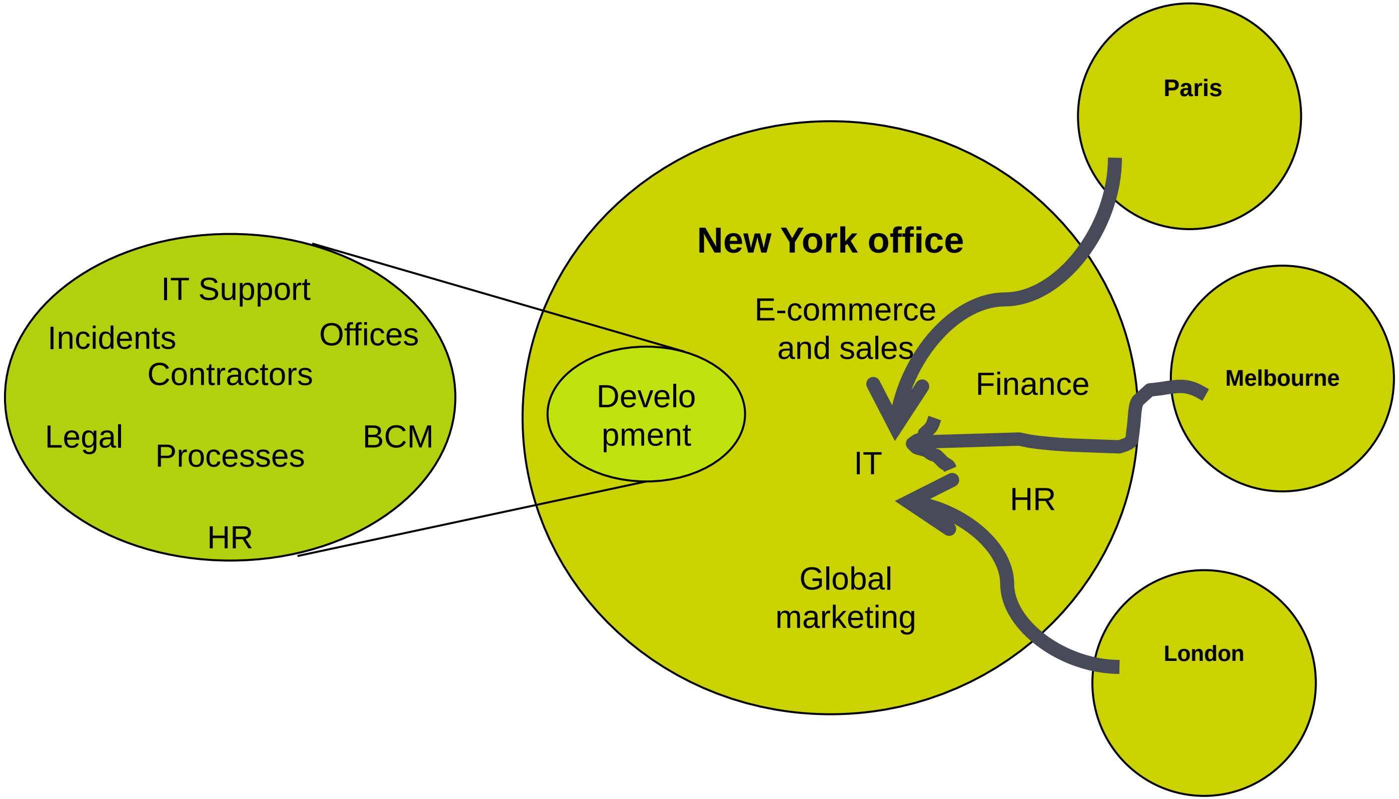
The baseline security criteria to implement an ISO 27001-compliant ISMS

it governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Clause 4: Scope

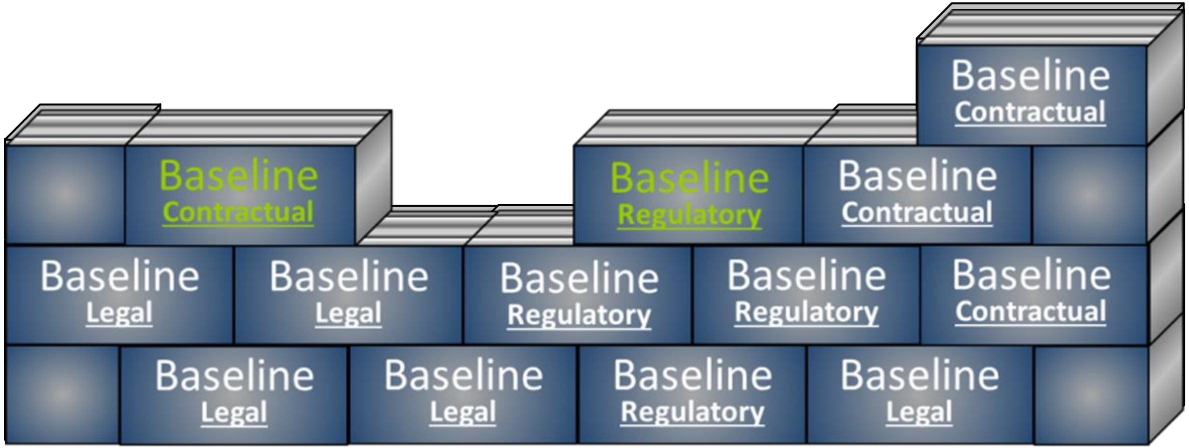


Clause 4: Interested parties and issues: Baseline Security Criteria

Most already exist – question extent of 'repeatable and dependable' and measurement

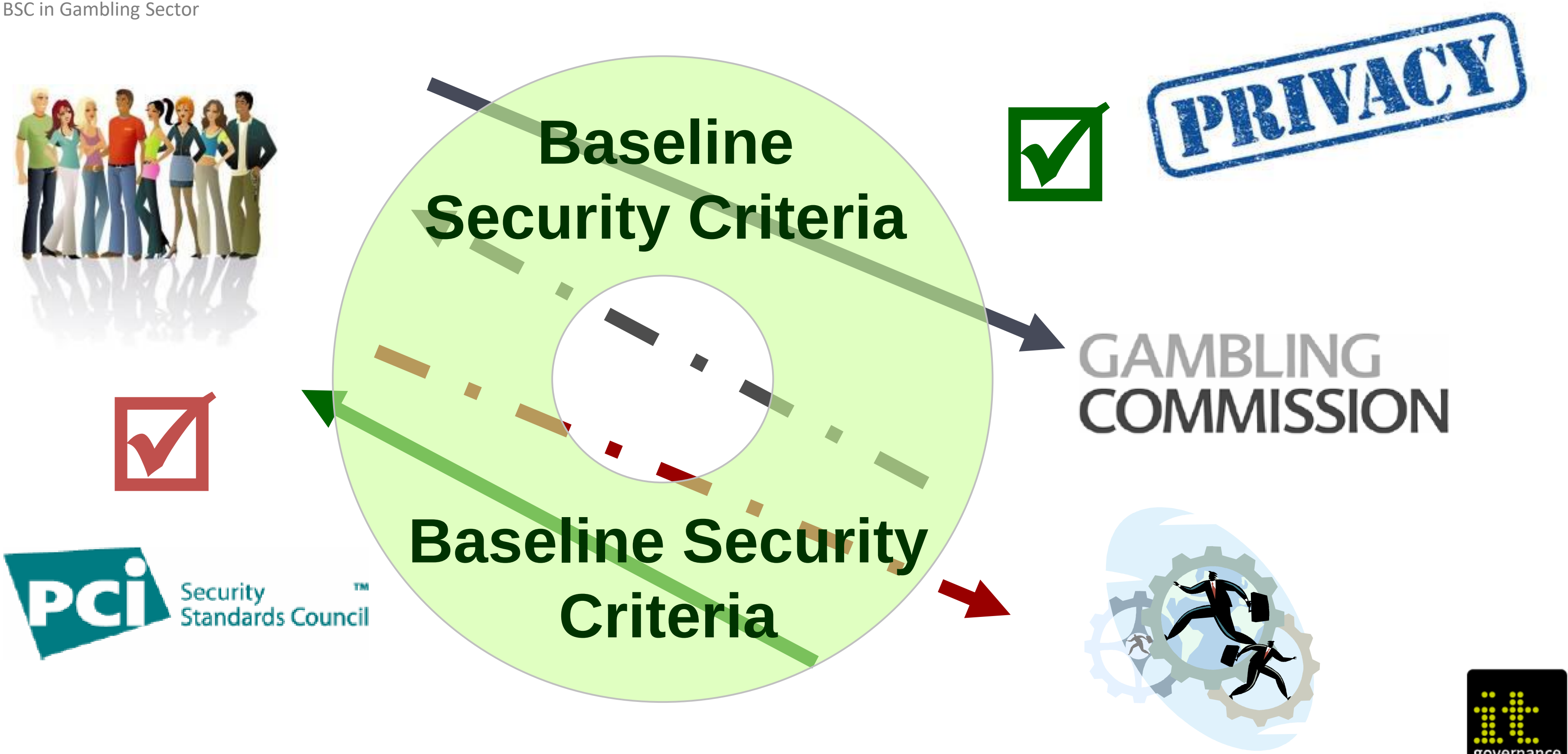
Main drivers for legal and regulatory compliance:

- National security
- Corporate governance
- IP protection
- E-commerce
- ID theft & data protection
- Industry-specific reqs.



Clause 4: Interested parties and issues

BSC in Gambling Sector


Baseline Security Criteria
PRIVACY
GAMBLING COMMISSION
PCI Security Standards Council ™
Baseline Security Criteria

The five steps in an ISO 27001 information security risk assessment

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

5 steps to an effective ISO 27001 risk assessment

An ISO 27001 risk assessment helps organizations identify, analyze, and evaluate weaknesses in their information security processes.

1. Establish a risk management framework

- A formal risk assessment methodology needs to address several issues:
  - Your organization’s core security requirements
  - Risk scale
  - Risk appetite
  - Methodology: scenario- or asset-based risk assessment

2. Identify risks – a ‘risk‘ pre-supposes a combination of likelihood and impact.

- Identifying the risks that can affect:
  - Confidentiality
  - Integrity
  - Availability

3. Analyse risks - what threats are likely to exploit which vulnerabilities?

- Identify the threats and vulnerabilities that apply to each asset.
  - For example, if the threat is ‘theft of mobile device’, the vulnerability might be ‘a lack of formal policy for mobile devices’.

4. Evaluate risks

- Use a risk assessment matrix to help you identify which risks need to be treated and prioritize them.

5. Select risk treatment options

- There are several ways you can treat a risk:
  - Avoid the risk by eliminating it entirely
  - Modify the risk by applying security controls
  - Share the risk with a third party (through insurance or by outsourcing it)
  - Retain the risk (if the risk falls within established risk acceptance criteria)

Risk assessment – scenarios

What you need to consider

Event

- Disclosure
- Interruption
- Modification
- Theft
- Destruction
- Ineffective design
- Ineffective execution
- Rules and regulations
- Inappropriate use

Asset/resource

- People and organization
- Process
- Infrastructure (facilities)
- IT infrastructure
- Information
- Applications

Time

- Duration
- Timing of occurrence (critical/non-critical)
- Timing needed to detect

Actor

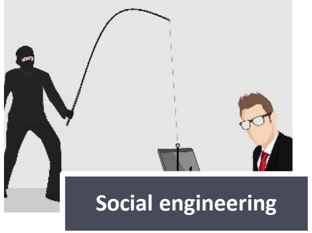
- Internal (staff/ contractor)
- External (competitor/ outsider/ business partner/ regulator/ market)

Threat type

- Malicious
- Accidental/error
- Failure
- Natural
- External requirement

Risks.

Top ten risks to consider in your ISO 27001 risk assessments



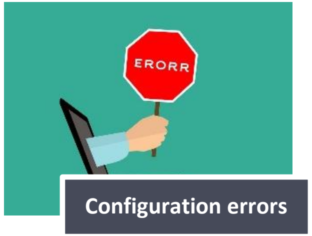
Social engineering

Unauthorized network access

Information disclosure

Equipment malfunction

Loss of power



Configuration errors

Hardware theft

Destruction of records

Natural disasters

Terrorist attacks

How to secure organization-wide commitment

governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Securing organization-wide commitment

The board and senior management

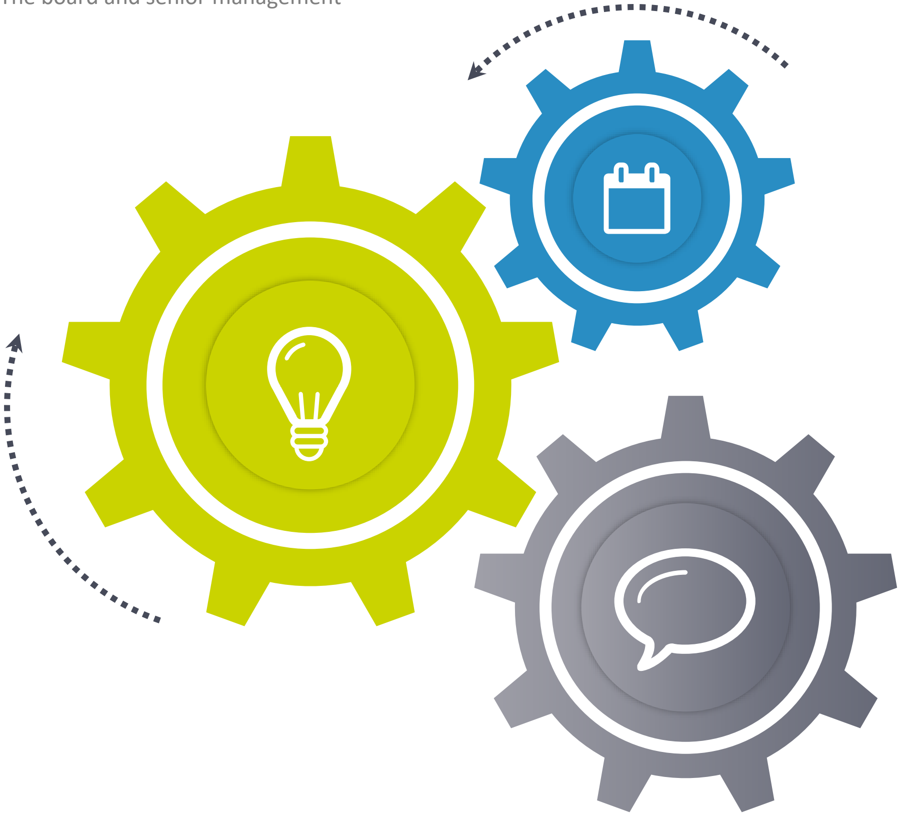
Only 44% of global boards are involved in setting the overall security strategy.

An ISMS can give senior management real visibility over its security regime.

Effective cybersecurity is an ongoing process. Senior management have an essential role to play in setting risk appetite and in providing leadership (which includes committing resources and personal example).

Securing organization-wide commitment

The board and senior management



Senior management's risk appetite enables security managers to identify which risks to avoid, modify, share, or retain (such as through cyber insurance), as well as reviewing specific risk response plans.

Regular communication between management and the board on cybersecurity is critical to protect company interests and ensure accountability.

The board must also ensure that the CISO is reporting to the appropriate levels within the organization.

Securing organization-wide commitment

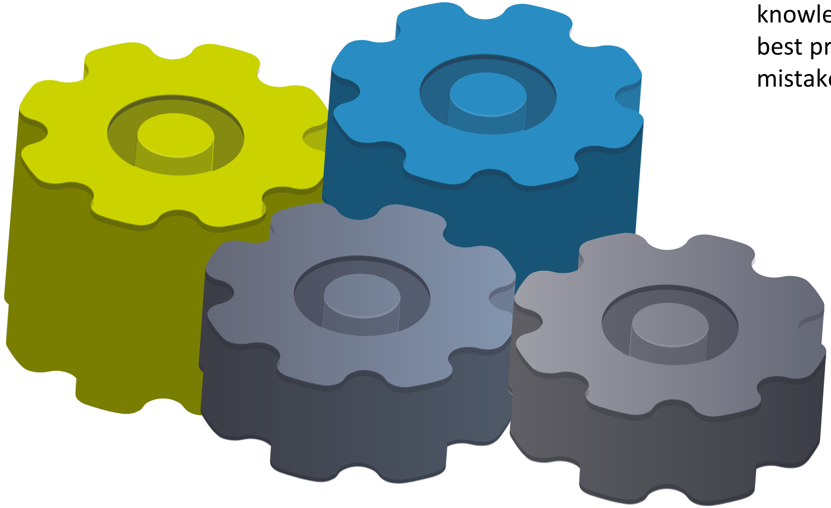
Employees

Why?

Everyone has a role to play in ensuring the CIA of information.

What?

Staff awareness can provide basic knowledge of information security best practices to reduce preventable mistakes.



Who?

Therefore, everyone has a role to play in the ISMS.

How?

Using engaging training, tools, and thought-provoking activities, organizations can make staff aware of the daily cyber risks they face, and suggest actions and procedures to minimize such risks.

Securing organization-wide commitment

Questions to ask your CISO

What are the top risks facing our organization?

Are we conducting regular information security risk assessments?

Are we testing our systems before a problem arises?

o we have an effective information security awareness program?

In the event of a data breach, what is our response plan?

Are we adequately insured?

When did we last test our recovery procedures?

Practical steps and solutions to implement ISO 27001

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

How IT Governance USA can help

Our solutions

Chartered Institute of Information Security
IBITGQ ACCREDITED
CIS LI
ISO 17024:2012 certificated
Certified ISO 27001 ISMS Lead Implementer Training Course

Learn the skills to lead an ISO 27001-compliant ISMS implementation project.

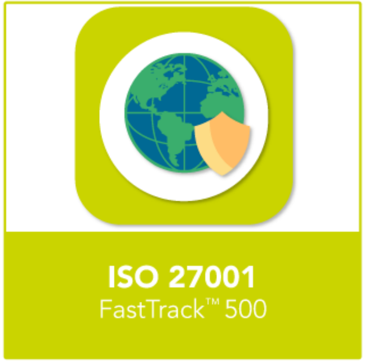
Find out more

A specialist, in-person review of your current information security posture against the requirements of ISO/IEC 27001:2013.

Find out more

The package includes all the consultancy support you need to help you implement an ISMS quickly and cost-effectively

Find out more



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

Find out more

Thank you

Join us for part 3!

Sign up for the next webinar

WEBINAR

Your journey to ISO 27001

Privacy integration

Alan Calder
Founder and Executive
Chairman, IT Governance

October, 6 2022, 11:00am (EST)

Book now

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

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

Questions

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive