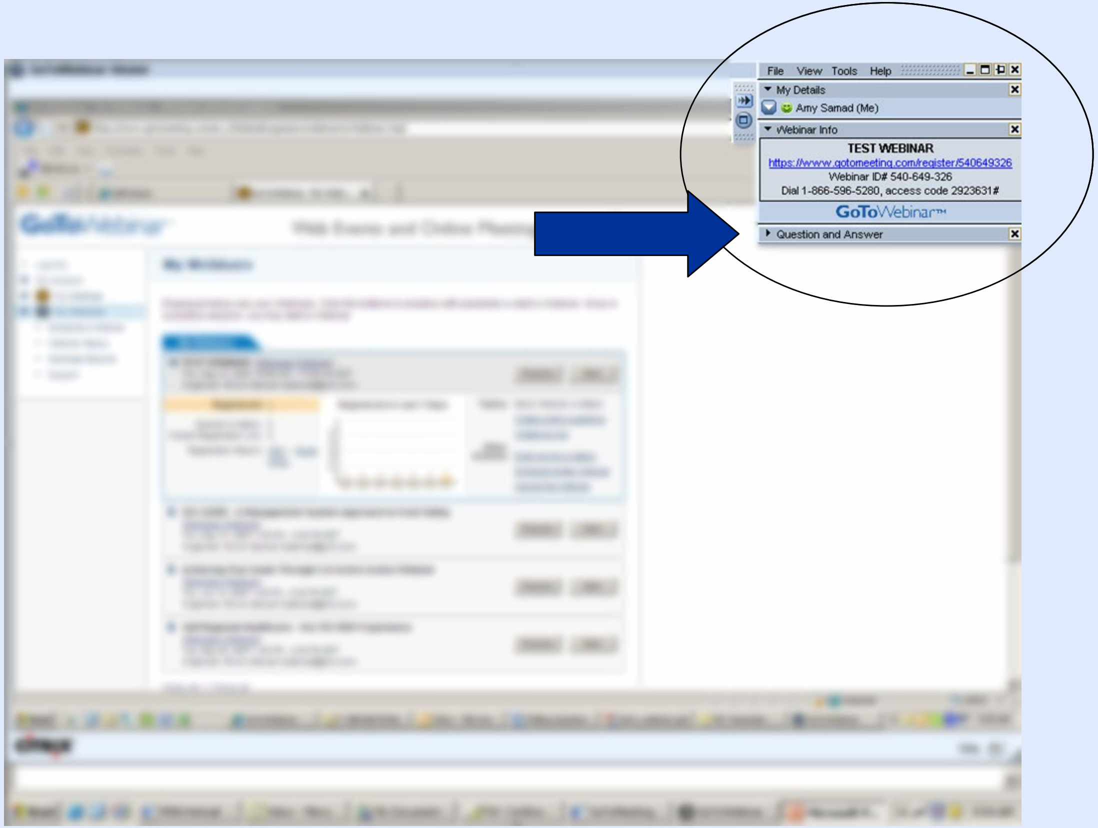
PJR – Your Partner for Quality Certification

PERRY JOHNSON
REGISTRARS, INC.

Your journey to ISO 27001: Project initiation, securing management support, and gap analysis

it governance

Alan Calder
Founder, Executive Chairman
IT Governance Ltd.

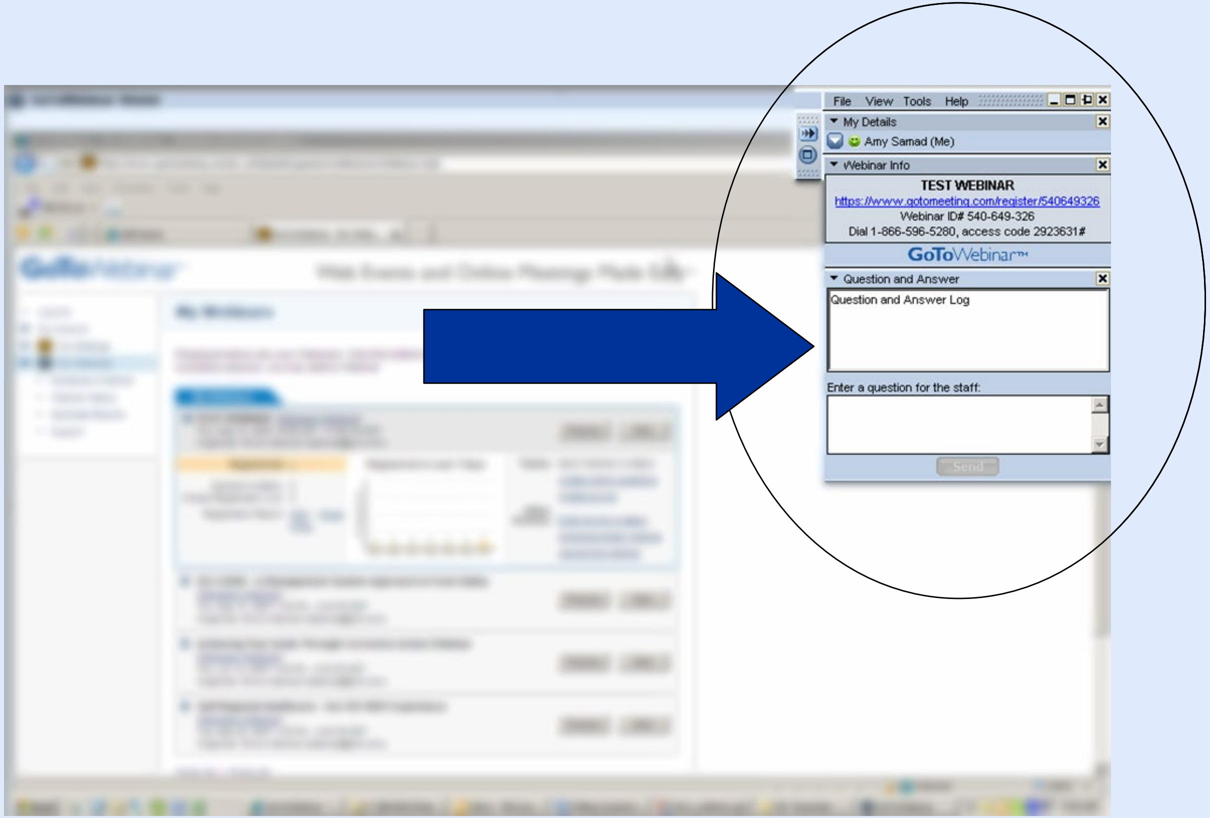


TEST WEBINAR

https://www.gotomeeting.com/register/540649326

Webinar ID# 540-649-326

Dial 1-866-596-5280, access code 2923631#



Amy Samad (Me)

TEST WEBINAR

https://www.gotomeeting.com/register/540649326

Webinar ID# 540-649-326

Dial 1-866-596-5280, access code 2923631#

Alan Calder

Founder & Executive Chairman, IT Governance Ltd.

Your journey to ISO 27001: Project initiation, securing management support, and gap analysis

August 10, 2022

About IT Governance

The cyber risk and privacy management solutions provider

20 years of experience, 200 employees

Comprehensive ISO 27001 product and service portfolio

More than 30,000 training course delegates

Over 1,300 ISO 27001 projects

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

Offices in Cambridge (UK), New York (USA) and Dublin (EU)

Working with IT Governance

Extensive experience

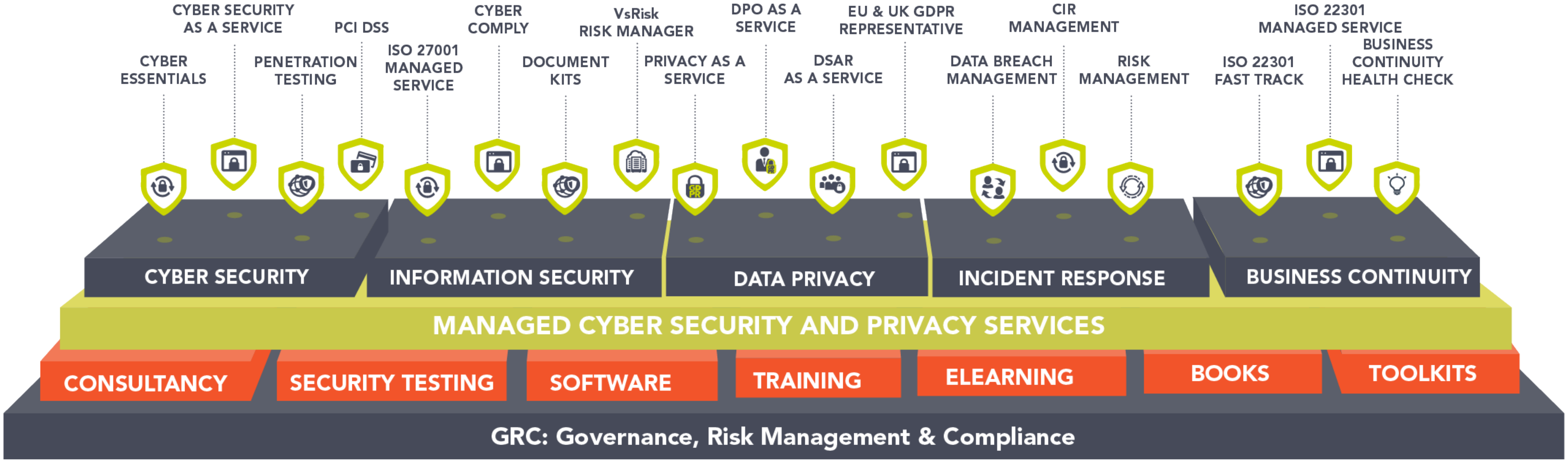
- Comprehensive coverage of the cyber security, privacy, business continuity and compliance domains

- The widest product and service portfolio in the industry, uniquely placed to help its clients successfully tackle today’s complex range of cybersecurity, risk management and compliance issues

- Over 15 years of practical, hands-on implementation experience, with a proven track-record of delivering a wide range of effective cybersecurity solutions for clients of all sizes across many different sectors.

Working with IT Governance

The world's one-stop-shop for governance, risk management and compliance solutions

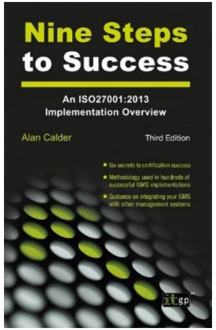


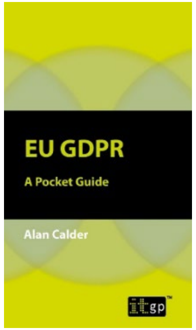
Introduction: Alan Calder

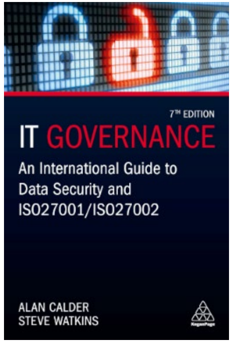
Founder and executive chairman of IT Governance

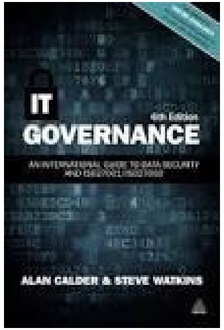
- Founder and executive chairman of IT Governance, the single source for everything to do with IT governance, cyber risk management and IT compliance.

- 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



Content

01 The growing importance of implementing an ISO 27001-compliant ISMS;

02 The Nine-Step ISO 27001 Implementation Project

03 Project mandate, project initiation

04 The gap analysis

05 Practical steps and solutions to conduct a gap analysis

Protect • Comply • Thrive

The growing importance of implementing an ISO 27001-compliant ISMS

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

ISO/IEC 27001

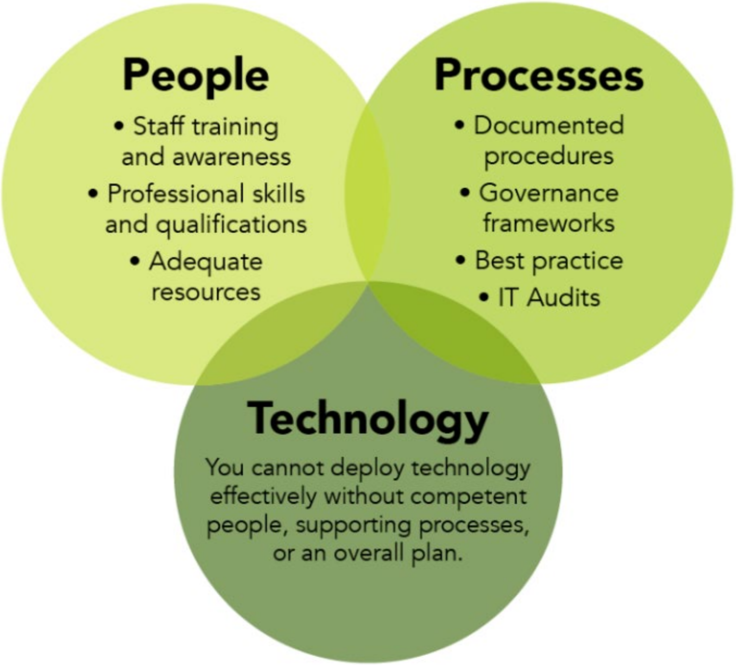
- ISO 27001 is the international standard that sets out the specification for an information security management system (ISMS).
- An ISMS is a best-practice approach to addressing information security.
- 20% growth rate globally.
- Internationally-accepted accredited certification.
- Aligns with internal and external drivers.
- Manages the confidentiality, integrity and availability of information (C, I, A).

The benefits of implementing ISO 27001

- Achieve and maintain **multiple legal** compliance requirements.
- Simplify RFQ responses and reduce third-party information security **audits.**
- Meet client/customer **contractual requirements.**
- Obtain an **independent endorsement of** your security posture.
- **Demonstrate cyber** security commitment - board/ stakeholders / clients / regulators.
- Reduce cyber risk by improving security **culture, structure** and **process – with cyber insurance benefits.**
- Protect and enhance **reputation** and **competitive advantage – win new business, keep existing!**

Three pillars of information security

ISO 27001 provides comprehensive cover of all aspect of information security.



People
• Staff training and awareness
• Professional skills and qualifications
• Adequate resources
Processes
• Documented procedures
• Governance frameworks
• Best practice
• IT Audits
Technology
You cannot deploy technology effectively without competent people, supporting processes, or an overall plan.

The Nine-Step ISO 27001 implementation project

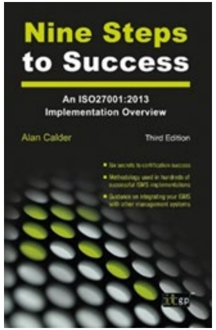
governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Nine Steps to Success

Robust, established implementation process.



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

1. Project mandate

2. Project initiation

3. ISMS initiation

4. Management framework

5. Baseline security criteria

6. Risk management

7. Implementation

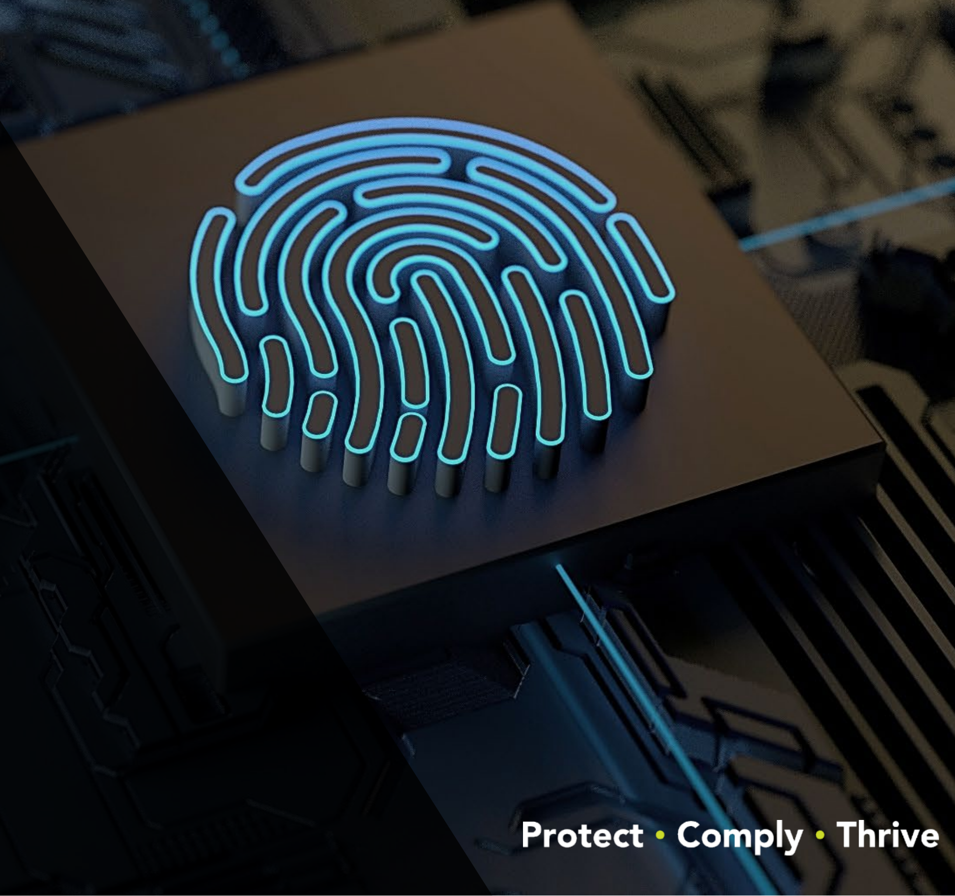
8. Measure, monitor and review

9. Certification

Project mandate, project initiation

it governance

Our Expertise,
Your Peace of Mind



Secure board commitment

The Board and Senior Management

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

An ISMS can give the board improved visibility over its security regime.

Effective cyber security is an ongoing process. Armed with the right information, the board can manage cyber risk and stay ahead of cyber criminals.

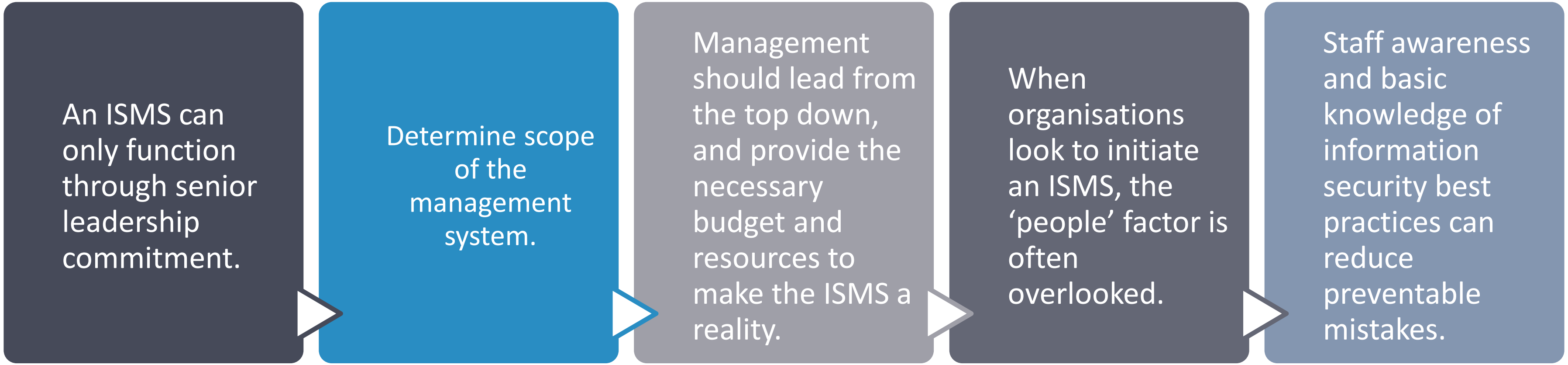
Regular communication between management and the board on cyber security is critical to protect company interests and ensure accountability.

When the board determines risk appetite, information security professionals can deliver an ISMS that enables business success.

Executives that fail at cyber security often find their careers impacted.

Project mandate: securing organisation-wide commitment

People are critical to success



An ISMS can only function through senior leadership commitment.

Determine scope of the management system.

Management should lead from the top down, and provide the necessary budget and resources to make the ISMS a reality.

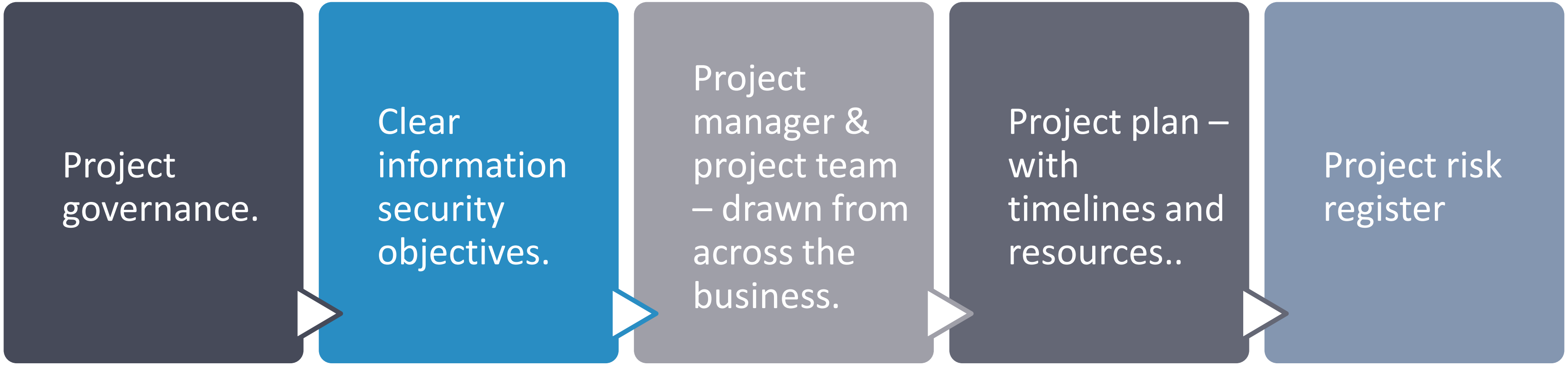
When organisations look to initiate an ISMS, the ‘people’ factor is often overlooked.

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

Document a Project Mandate that describes high level objectives, resources and timelines.

Project initiation

The PID provides detailed structure for the ISMS project.



Project governance.

Clear information security objectives.

Project manager & project team – drawn from across the business.

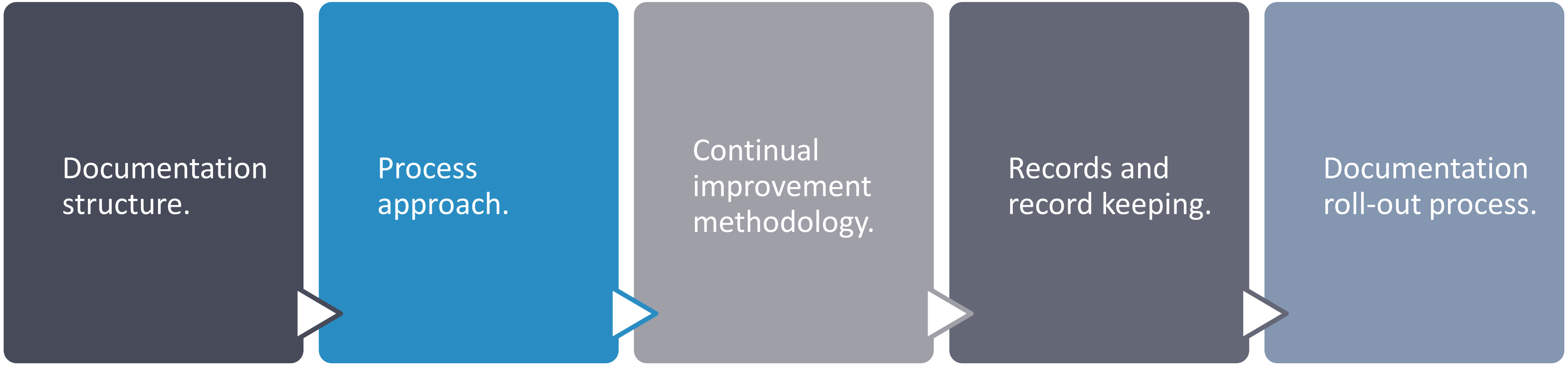
Project plan – with timelines and resources..

Project risk register

Expanded project mandate or a Project Initiation Document (PID).

ISMS initiation

Project framework



Documentation structure.

Process approach.

Continual improvement methodology.

Records and record keeping.

Documentation roll-out process.

Establish the working approach to project implementation.

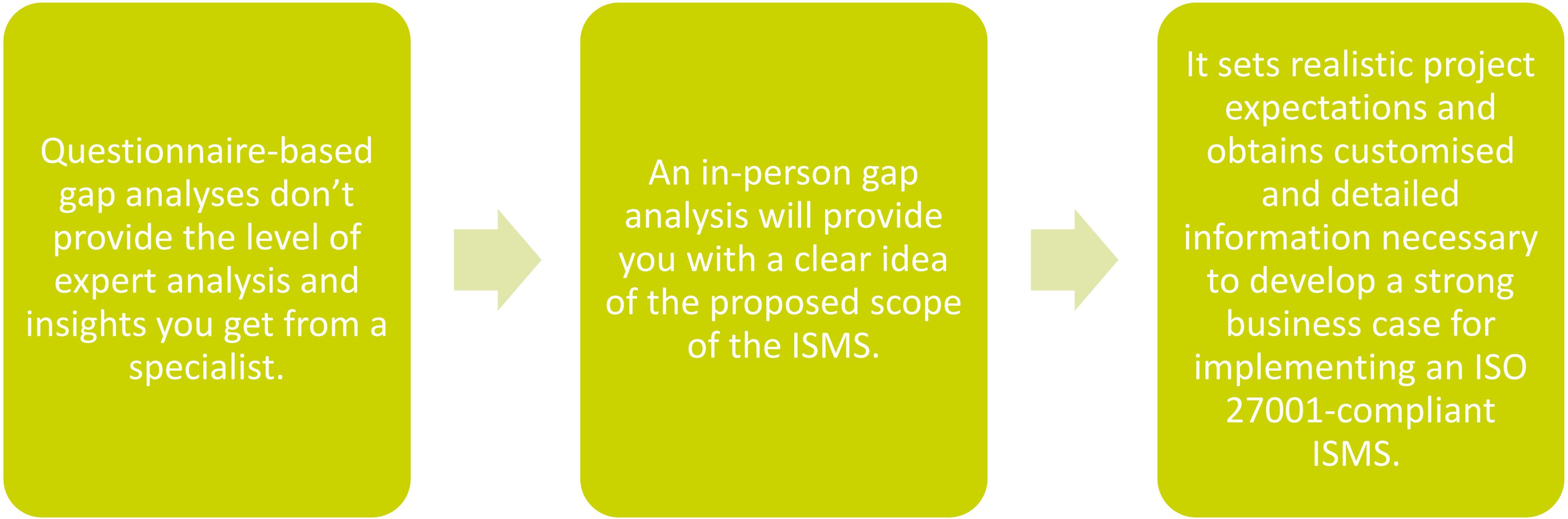
The ISO 27001 gap analysis

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Gap analysis

Questionnaire vs. in-person gap analysis



Questionnaire-based gap analyses don’t provide the level of expert analysis and insights you get from a specialist.

An in-person gap analysis will provide you with a clear idea of the proposed scope of the ISMS.

It sets realistic project expectations and obtains customised and detailed information necessary to develop a strong business case for implementing an ISO 27001-compliant ISMS.

Conducting an ISO 27001 gap analysis

Top 5 benefits

1) Gain a high-level overview of what needs to be done to achieve ISO 27001 certification

- An ISO 27001 gap analysis enables you to gain a true picture of your information security posture by assessing and comparing your organisation’s existing information security arrangements against the Standard’s requirements.

2) Scope your ISMS parameters across all business functions

- Conducting an ISO 27001 gap analysis gives you a clear insight into the extent of the implementation project, enabling you to accurately determine what to include in the scope of your ISMS.

3) Secure top management commitment

- The gap analysis can help estimate the resources and budgetary needs of the ISO 27001 project.
- By translating cyber risks into business terms, you can ensure your organisation’s leadership makes well-informed decisions by clearly demonstrating how the ISMS will help the company avoid risks or reduce costs.

4) Understand what you need to do next

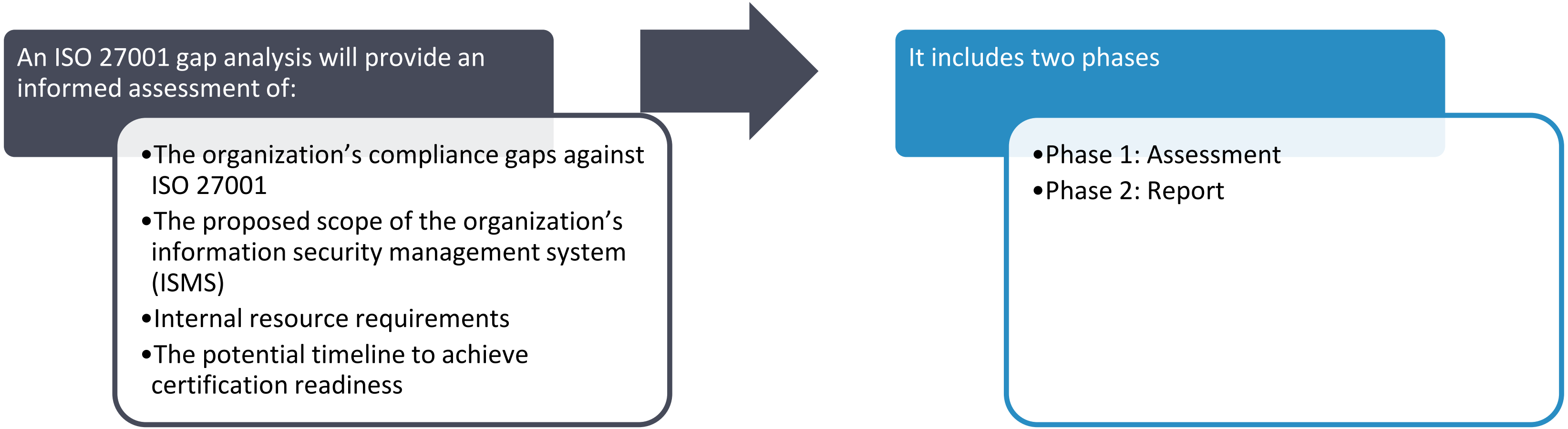
- After completing the ISO 27001 gap analysis, you’ll receive an outline action plan as well as an indication of the level of internal management effort required to implement the ISMS.
- This valuable insight enables you to confidently plan a strategic roadmap for the next steps of your implementation project.

5) Accredited certification and how to get there

- The ISO 27001 gap analysis process provide you with the potential timeline to achieve certification readiness
- The post-audit report indicates what further measures are required to achieve certification to the Standard.

ISO 27001 gap analysis

- An ISO 27001 gap analysis provides a high-level overview of what needs to be done to achieve certification and enables you to assess and compare your organisation's existing information security arrangements against the requirements of ISO 27001.
- It is the ideal solution for organisations that need to measure their current state of compliance against the Standard and enables you to scope your ISMS parameters across all business functions.



An ISO 27001 gap analysis will provide an informed assessment of:

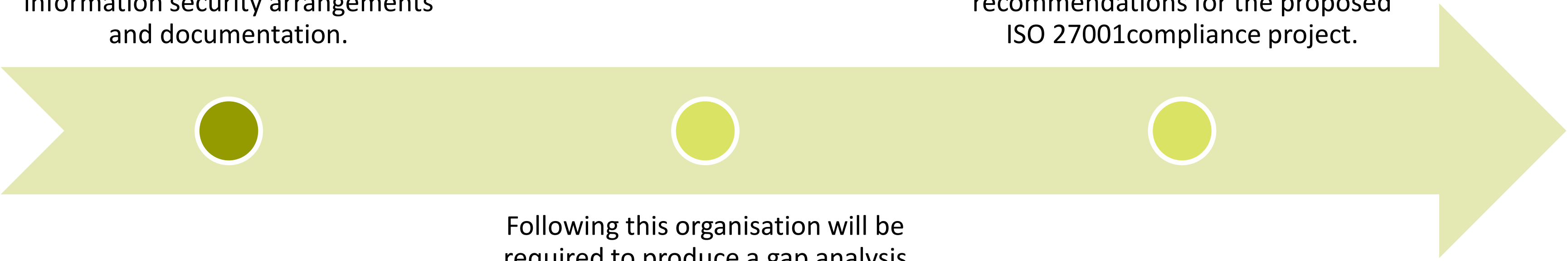
- The organization's compliance gaps against ISO 27001
- The proposed scope of the organization's information security management system (ISMS)
- Internal resource requirements
- The potential timeline to achieve certification readiness

It includes two phases

- Phase 1: Assessment
- Phase 2: Report

ISO 27001 gap analysis

Phase 1: Assessment



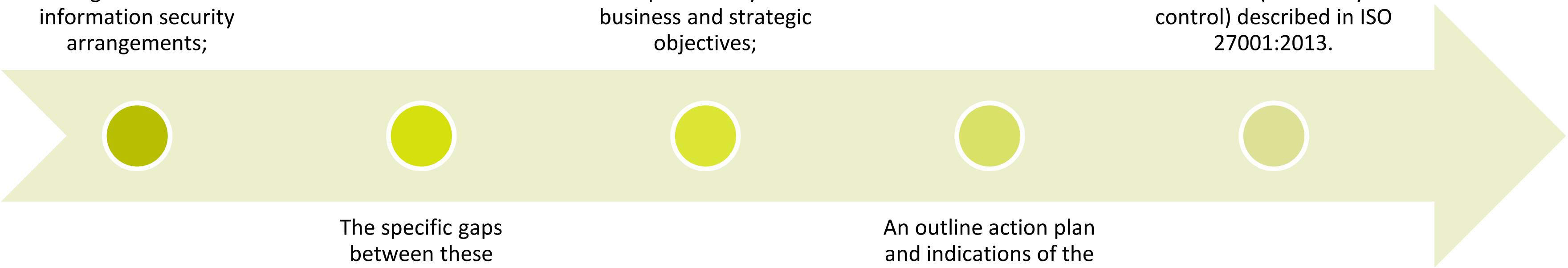
An ISO 27001 specialist needs to interview key managers and perform an analysis of your existing information security arrangements and documentation.

Following this organisation will be required to produce a gap analysis and write a report collating the findings of these investigations.

The report will detail areas of compliance and areas requiring improvement and provide further recommendations for the proposed ISO 27001compliance project.

ISO 27001 gap analysis

Phase 2: Report



The overall state and maturity of the organization’s information security arrangements;

The specific gaps between these arrangements and the requirements of ISO 27001;

Options for the scope of an ISMS, and how they help to meet your business and strategic objectives;

An outline action plan and indications of the level of internal management effort required to implement an ISO 27001 ISMS;

A compliance status report (red/amber/green) against the management system clauses (clause-by-clause), as well as the information security controls (control-by-control) described in ISO 27001:2013.

How can IT Governance help?

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

How IT Governance can help

Our solutions

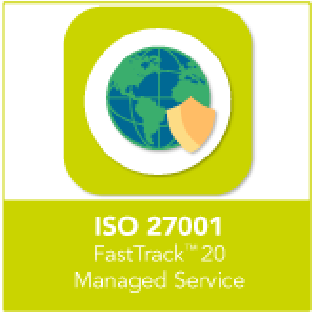
Chartered Institute of Information Security
IBITGQ ACCREDITED
CIS LI
ISO 17024:2012 certificated
Certified ISO 27001 ISMS Lead Implementer Training Course

Learn the skills needed 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



Outsource the management and maintenance of your ISMS, as well as benefit from the reliable advice and practical experience of an ISMS specialist.

Find out more

A complete set of easy-to-use, customizable and fully ISO 27001-compliant documentation templates, which will save you time and money

Find out more

Next time: Risk Assessment

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Thank you

Get in touch

How you can find us

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

PERRY JOHNSON
REGISTRARS, INC.

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

Questions

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive