SGS Knowledge Solutions

ENABLING SUSTAINABLE GROWTH BY ENHANCING
KNOWLEDGE, SKILLS AND PROCESSES

ISO/IEC 27001 and information security webinar

External webinar | Marcus Allen and Ray Woodford

12 May 2022

Agenda

- Introduction
- Cyber security threats and breaches
- What is ISO/IEC 27001:2013?
- The key benefits of information security certification
- Client case study – Burges Salmon
- ISO/IEC 27001 free survey offer from Thamer James
- Why use SGS as your certification body?

Presenters' information

Marcus Allen – main presenter, Thamer James

Marcus has twenty years' experience in ISO/IEC 27001, formerly BS7799 systems. He has worked with SGS on client assessments from the early 2000s onwards.

Marcus has helped hundreds of companies gain ISO standards and has worked with numerous software companies, especially smaller to medium sized enterprises and understands the need for a practical approach.

Marcus holds a Lead auditor qualification in ISO27001 and is an Associate member of the British Computer Society

Ray Woodford – Q&A presenter, SGS UK Ltd

Ray has over 40 years' experience in the information technology sector with extensive experience of implementing Information Security Management Systems, and Ray is also an associate member of the Business Continuity Institute.

Ray is a qualified lead auditor for ISO/IEC 27001, ISO 22301 and ISO 9001. Ray has 14 years' experience of auditing ISO/IEC 27001 Management systems and has been with SGS for eight years.

Ray is currently the UK Product Manager for ISO/IEC 27001, ISO 22301 and ISO 20000.

ISO/IEC 27001 – an introduction

Cyber security threats and breaches

Organization	Data protection breach	Date	Fine
Facebook & Linkedin	The breach affected 530 million Facebook users from 106 countries. The personal data exposed included Facebook ID numbers, names, phone numbers, dates of birth and location. The screen scraping attack happened because of an allowed vulnerability in Facebook. The use of screen-scraping to capture personal details was also used to breach the personal and professional data of 92% of LinkedIn users in April and July 2021	2021	TBC
Colonial Pipeline	Colonial Pipeline was effectively shut down by a ransomware attack that affected around 50 million customers. The hacking group, DarkSide, carried out the attack by encrypting data and stealing around 100 gigabytes of data. The company paid the $4.4 million ransom in bitcoin currency	2021	Ransom $4.4 million

Cyber security threats and breaches

Organization	Data protection breach	Date	Fine
EasyJet	Personal information of 9 million customers and credit card details of around 2,200 ‘accessed’ in cyber attack	2020	TBC
British Airways	Users of British Airways’ website were diverted to a fraudulent site. Through this false site, details of about 500,000 customers were harvested by the attackers	2018-2019	£183m
Marriott	The hotel group announced that hackers accessed the records of up to 383 million guests. The records included passport numbers and credit card information	2018	£99m
Carphone Warehouse	The attacker had installed malicious software on 5,390 tills in branches of Currys PC World and Dixons Travel. The rogue software went undetected for nine months, and personal information of 5.6 million people (full names, postcodes, email addresses and details of failed credit checks) was accessed	2018	£500,000

What is ISO/IEC 27001:2013?

- An Information Security Management System (ISMS) is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes
- Objectives:
  - Examine risk to company information security and implement controls (policies, procedures, treatments) to manage the risks
  - Manage threats to information assets
  - Establish, maintain and continually improve an effective ISMS
- The structure of the standard is the same as that of ISO 9001, ISO 14001 and ISO 45001 – known as 'Annex SL'
- ISO/IEC 27001 certification is suitable for any size of organization within any sector

Why should your business implement ISO/IEC 27001:2013?

- Demonstrates your organization keeps confidential information secure
- Increases customer and stakeholder confidence in how your organization manages risks
- Helps win new business by meeting tender requirements and enhancing the organization’s credibility
- Differentiates your organization against competitors
- Safeguards your valuable data and intellectual property

Why are software companies seeking ISO/IEC 27001 certification?

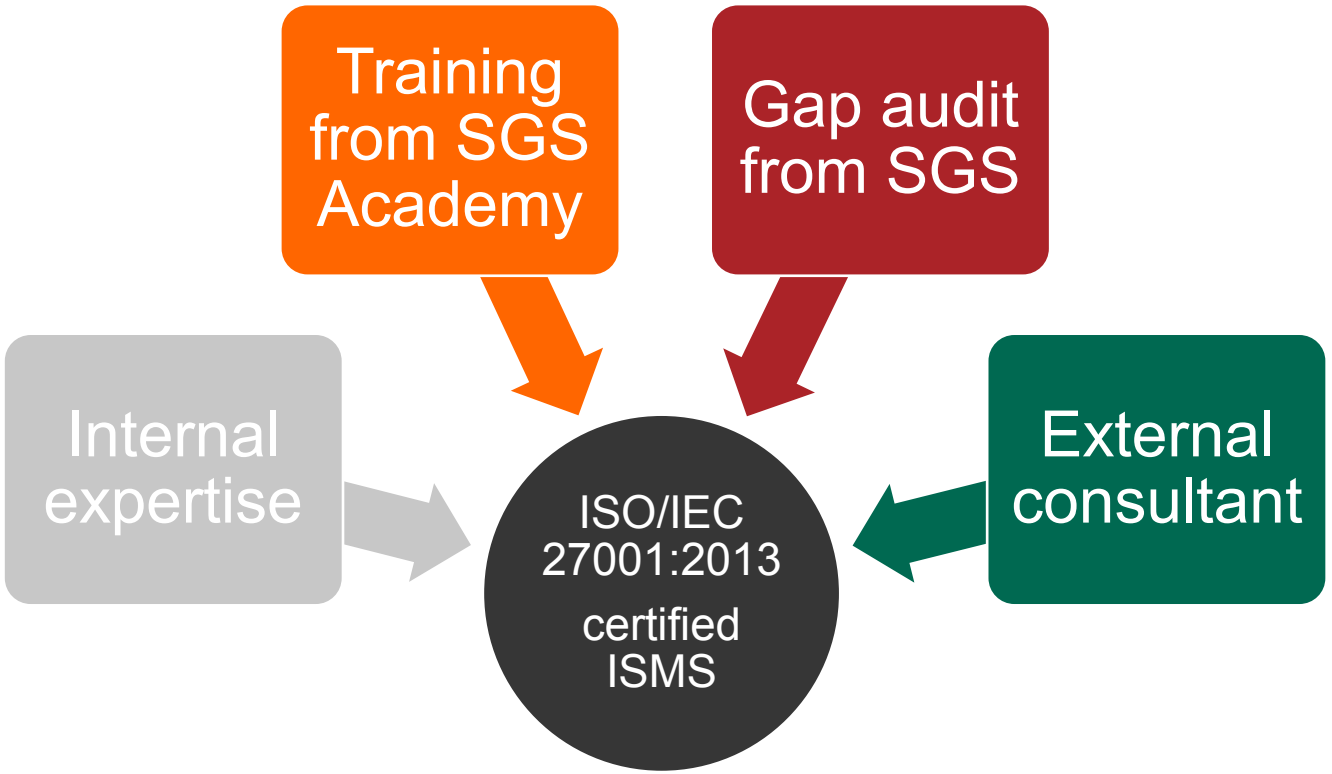
- Extreme competition with new start-ups
- Creating a positive differentiator is key
- As the businesses grow customer contracts are requiring some sort of verification of compliance with information security frameworks
    - ISO/IEC 27001 is widely seen as that mark

Why should your business implement ISO/IEC 27001:2013?

- Confirms you are meeting legal, contractual and regulatory requirements
- Manages and minimizes risk exposure – avoids financial penalties from data breaches
- Promotes a harmonized organization culture

The various routes to prepare for ISO/IEC 27001:2013

- There are four main routes organizations use to aid implementation of an ISMS:



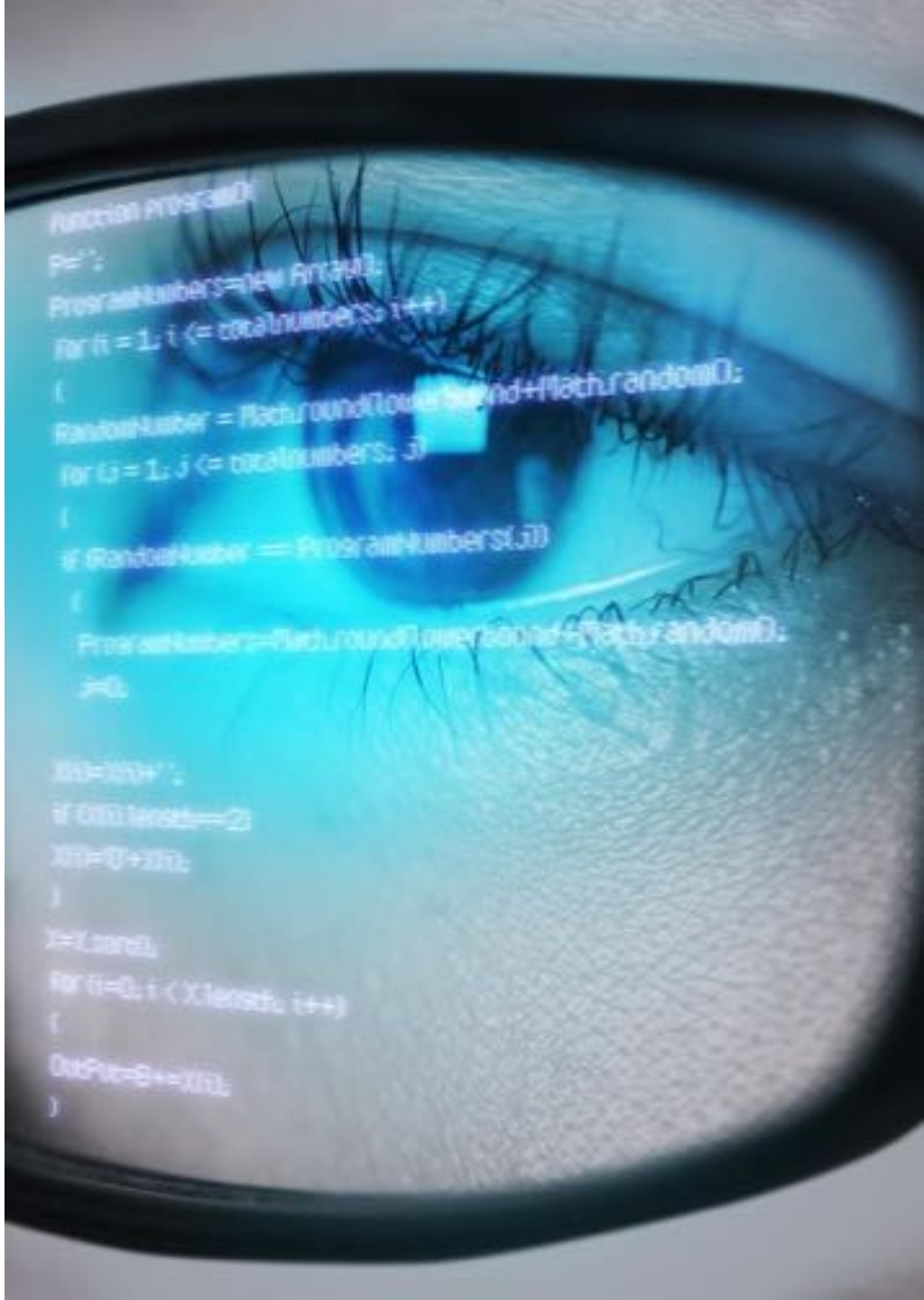
ISO/IEC 27001:2013 – Avoid the pitfalls of implementation

Top challenges

- Scope of certification
- Obtaining top management buy-in and raising staff awareness
- Conducting information security risk assessments
- Creating and managing the ISMS documentation
- Understanding the requirements of the standard

Scope of certification

- What information is the organization looking to protect?
- Where is the information stored?
- If the scope is too big it can impact on time and costs
- If the scope is too small the company could be more vulnerable to risks that have not been considered



Top management buy-in and raising staff awareness

- Top management
  - Alignment with business strategy to meet the organization’s strategic objectives
  - Cultural change required and driven by buy-in from all senior managers
  - Defined roles and responsibilities
  - Communication plan
- Staff awareness
  - Involvement in project
  - Representatives from internal departments and/or teams
  - Information security awareness training

  Policies and procedures

Information security risk assessments

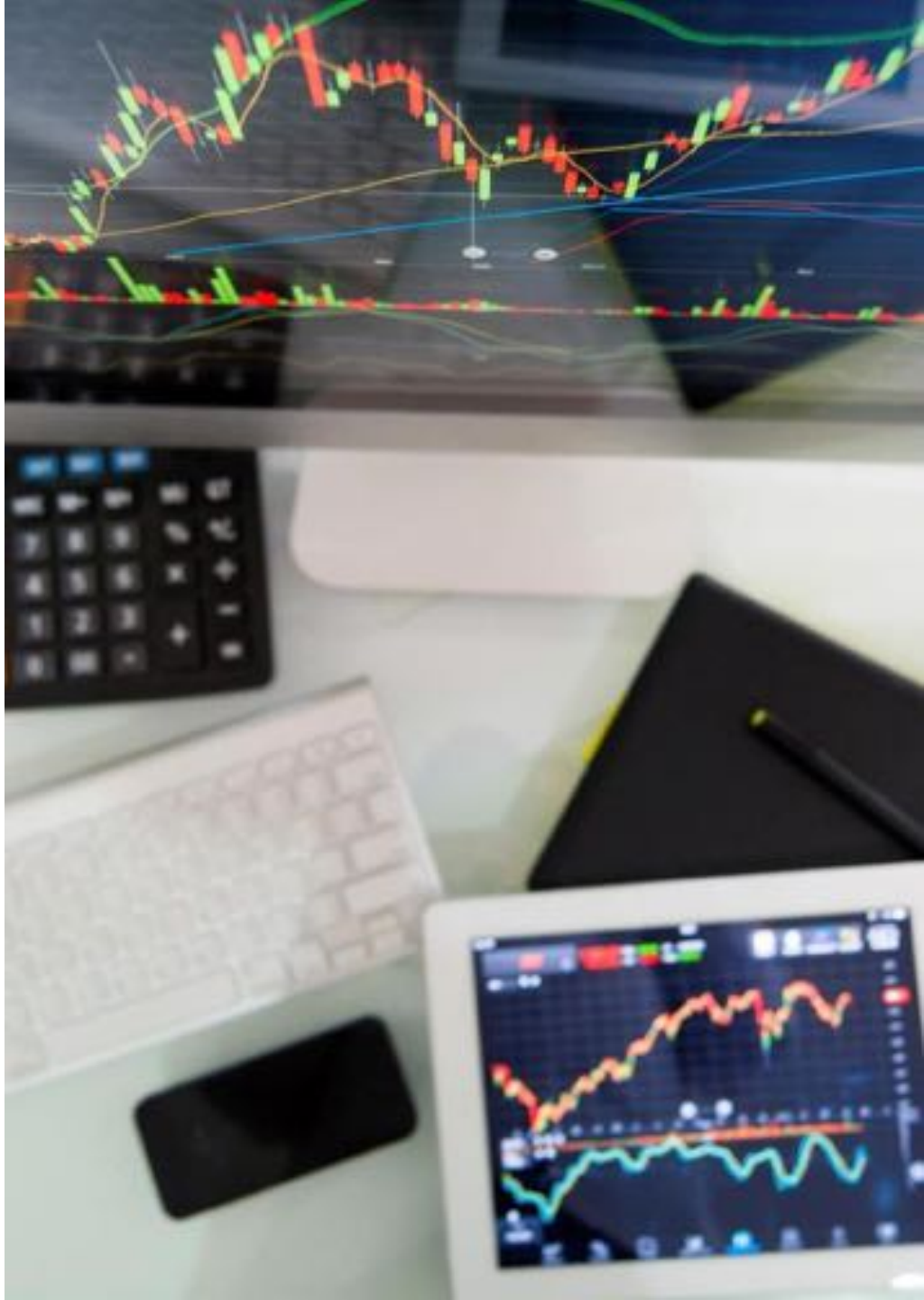
- Don’t implement controls without carrying out risk assessments
- Consider risks related to the loss of confidentiality, integrity and availability
- Don’t over-complicate your risk assessment method – keep it simple
- Risk treatment
- Ensure that the “Statement of Applicability” identifies the selected controls and explains any exclusions

Creating and managing the ISMS documentation

- Producing too much documentation
- Documentation too technical/high level
- Documentation does not cover all requirements
- Documentation update process not in place
- Documentation repository

Understanding the requirements of the standard

- External help from consultant to write the ISMS
- Familiarization with the standard with a consultant or training course
- ISMS management team
- ISO/IEC 27001 training
- Internal audit team



Case study – Burges Salmon

"SGS auditors were friendly and engaged with relevant people from the firm to discuss various documents, talk about their experiences with the compliance process and clarify any issues. We knew that they would challenge us but that, ultimately, it would help us get to where we wanted to be."

Free ISO/IEC 27001 survey

- Thamer James is offering a FREE of charge ISO/IEC 27001 survey to benchmark software companies to this international standard
- Thamer James will also advise on areas of strength and weakness
    - Get in contact to book your free survey

SGS ACADEMY

ENHANCING PEOPLE AND BUSINESSES

- A global leader in professional training, SGS Academy has unrivaled expertise in professional development training
- Our courses enable learners to gain the skills they need to stay up to date with industry regulations and to advance in their careers
- Through training we enable employees to continuously update their skills and increase their employability
- Businesses can rely on SGS Academy to help them to develop and retain talent and become more sustainable

SGS ACADEMY

ENHANCING PEOPLE AND BUSINESSES

- All training courses are being run either in person or virtually at the moment
  - Virtual training is simple to arrange and cost-efficient
  - Offers more flexibility
  - Ensures the safety and welfare of our learners and tutors
  - Maintains same quality delivery as classroom learning
  - Delegates can continue their personal development whilst working from home

Why use SGS?

- Globally SGS is the world's leading inspection, verification, testing and certification company
- In the UK SGS's certification business is divided in to four regions:
  - South East England
  - Wales and South West England
  - Northern England
  - Northern Ireland and Scotland
- Each region has their own dedicated team
- Think global – act local

Why choose certification from SGS?

- SGS is accredited by the United Kingdom Accreditation Service (UKAS) to provide certification in the UK
- SGS has been assessed against internationally recognized standards to demonstrate our competence, impartiality and performance capability
- We work with you in partnership to deliver certification and derive maximum benefits from it
- Our friendly and knowledgeable team provide a personal touch

Why choose certification from SGS?

- SGS auditors are consistently rated highly by our customers
- Results from our most recent customer satisfaction survey:
  - 85% of respondents were very satisfied with the knowledge of our auditors
  - 87% of respondents were also very satisfied with the auditor communication – confirming their auditor was clear, open-minded and informative
  - 90% of respondents were very satisfied with the timeline for delivery of the audit report
  - 93% of respondents felt very satisfied that the site visit was structured to suit their operations

Thank you!

Do you have any questions?

uk.nowisthetime@sgs.com

+44 (0) 1276 697 715

www.sgs.co.uk/certification