nqa.

WEBINAR: BACK TO BASICS – ISO 27001

Barri-Jon Graham - Risk Evolves

4th November 2022

OUR PURPOSE IS TO HELP CUSTOMERS DELIVER PRODUCTS THE WORLD CAN TRUST

NQA is a **world leading certification body** with global operations.

NQA specialises in certification in **high technology** and engineering sectors.

LONDON
BOSTON
SHANGHAI
BANGALORE

AMERICA'S NO.1
Certification body in **Aerospace** sector

TOP 3 IN THE UK
ISO 9001, ISO 14001, ISO 45001, ISO 27001

CHINA'S NO.1
Certification body in **Automotive** sector

GLOBAL NO.1
Certification body in **telecommunications** and **Automotive** sector

GLOBAL NO.3
Certification body in **Aerospace** sector

UK'S NO.2
Certification body in **Aerospace** sector

nqa.

NEVER STOP IMPROVING

CERTIFICATION AND TRAINING SERVICES

We specialize in management systems certification for:

QUALITY

AEROSPACE (QUALITY)

AUTOMOTIVE (QUALITY)

ENVIRONMENT

ENERGY

HEALTH AND SAFETY

INFORMATION RESILIENCE

FOOD SAFETY

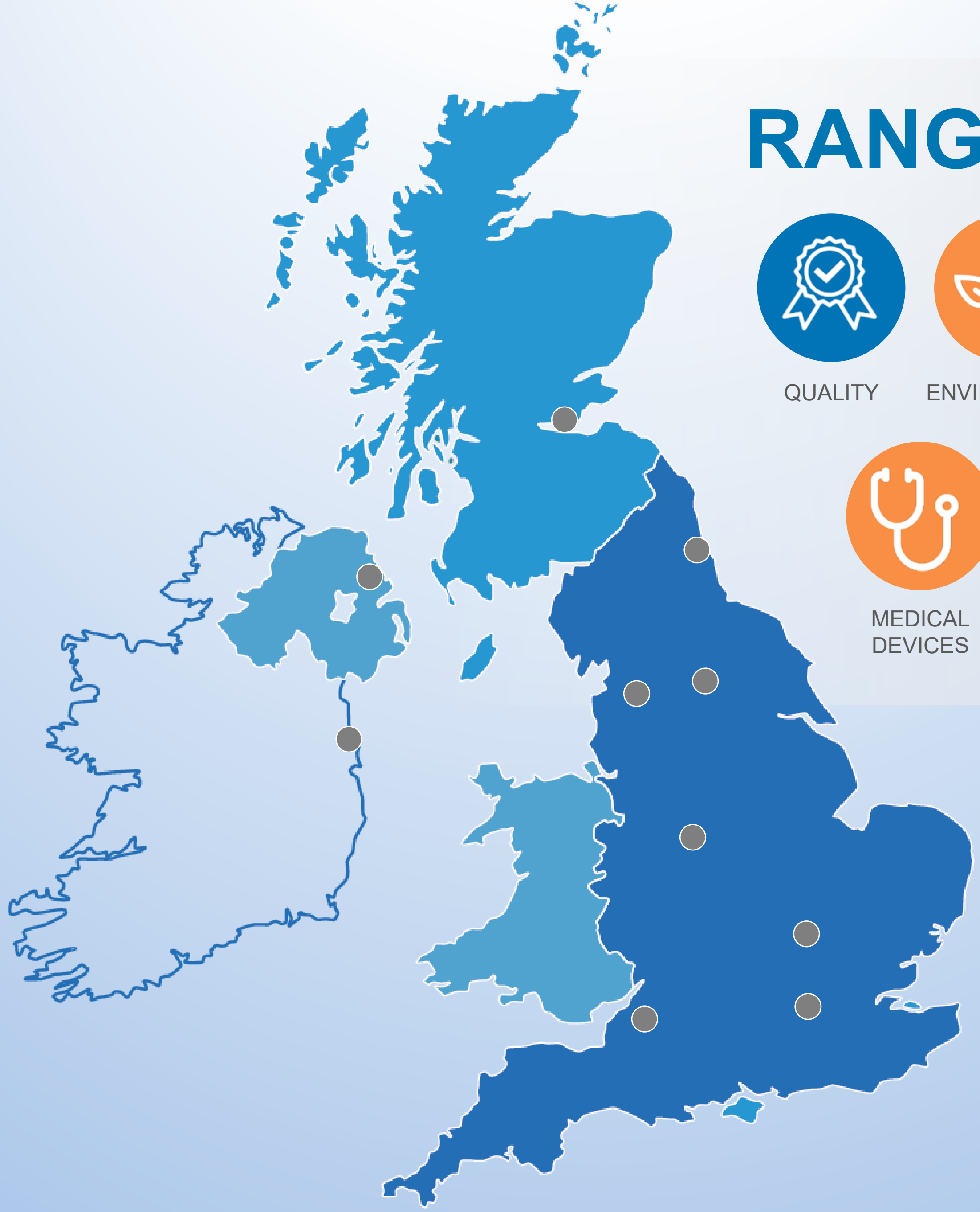
RISK MANAGEMENT

MEDICAL DEVICES

NATIONWIDE TRAINING SERVICES

ACCREDITED COURSES

- Virtual Learning
- e-Learning / Live Webinars
- In-house Training
- Public Training Nationwide Locations



RANGE OF COURSES

- QUALITY
- ENVIRONMENT
- ENERGY
- HEALTH AND SAFETY
- INFORMATION SECURITY
- MEDICAL DEVICES
- BUSINESS CONTINUITY
- AEROSPACE
- INTEGRATED MANAGEMENT

- **e-Learning** Introduction
- **1 day** Introduction Courses
- **2 day** Implementation Courses
- **2 day** Internal Auditor – NQA or IRCA
- **5 day** Lead Auditor – NQA or IRCA

CQI | IRCA APPROVED TRAINING PARTNER

nqa.

NEVER STOP IMPROVING

KEY INFO

- 45 minute webinar
- Questions in the chat box
- Q&A at the end
- Recording of webinar circulated shortly

YOUR PRESENTER

- 23 years experience of Security, Threat Intelligence and Protection of people and assets.
- Worked in a range of roles including public and private sector protection including Critical National Infrastructure.
- Certified Cyber Professional by National Cyber Security Centre.
- Operated as Chief Information Security Officer for number of clients in the UK

OBJECTIVES

(HOPEFULLY) YOU WILL UNDERSTAND

- The fundamentals of ISO 27001 requirements.
- Common Pitfalls.
- Why ISO 27001 can help.
- An idea of some of the changes on the horizon.

The importance of ISO27K

The status of data in the modern society is almost unrecognisable from even 10 years ago. This makes data both incredibly sensitive and necessarily highly regulated and scrutinised.

More importantly, every single organisation has it in some capacity.

Threat actors know this and want our data as it leads to financial gain or reputational enhancement whilst conversely causing significant financial and reputational damage to their victims.

That is also not to mention inadvertent data loss…

- Data is one of the most valuable resources within an organization.
- Data breach is expensive!
- No longer simply in the domain of IT Department; universal responsibilities are the norm.
- We want to be a success whilst being savvy. ISO helps with this outcome.

ISO 27001

What is it?!

There is a common misconception about what ISO27001 actually is. To some it is “cyber security stuff”.

That is really not true.

It is a way of working which helps you/your organisation identify and control risks associated with your information assets.

Note that this does not include cast iron guarantees that breaches become impossible; merely that a mechanism has been established to identify and reduce the associated risks.

- ISO 27001 is the International Standard describing the best practices for an ISMS
- Based on controls and measures to achieve an understanding of information security.
- Requires formulation of procedures and practices including:
  - Risk Management
  - Monitoring and Analysis of your management system
  - Identifying and generating improvements
- It is NOT: Breach Insurance/Guaranteed security of your IT assets.

PREPARING YOUR BUSINESS FOR
THE FUTURE
www.riskevolves.com

Requirements

ISO 27001 utilises the Annex SL model which is consistent across a number of ISO standards.

The Key difference in ISO27001 is that Annex A comes in to play. The risk you identify when completing Clause 6: Planning functions are able to be controlled using a pre-baked number of risk controls which are listed for you!

In the 2013 iteration of the standard there were 114 controls though this has now been reduced.

- Clauses 0 – 3 guidance for core concepts
- Clauses 4 – 10 specify the requirements needed to demonstrate conformity
- Annex A – Where the Risk Controls are found!
  - These are not mandatory
  - Required to be considered as a minimum
  - Can be augmented by controls not specifically listed within your ISMS

First Steps

Before you speak with a CB you need to undertake a number of internal processes and establish a few things to make sure they are right for the organisation where the ISMS is going to exist.

Usually this commences with a GAP analysis to identify activities already in place and discover where something needs to be changed or initiated.

Commonly an organisation may already have a risk management policy or framework which is either partially or fully compliant with aspects of ISO 27001 for example. In these cases, starting from scratch wouldn't make sense.

- Define your scope: Everything or just Something?
- Perform a review of assets which are to be protected. Not just hardware!
- Complete Risk Assessment
  - Identify ownership
  - Consider Annex A controls to be used
  - Think about things you cannot control too
  - Risks can also = opportunities – map these!
- Document InfoSec Policies & Commence Operations for ISMS
- Audit, Analyse & Improve

Pitfalls

riskevolves

We see some of the common pitfalls for ISMS implementation here. These will naturally be ironed out by ensuring improvement measures are in place and effective.

Avoid them in the first instance! Plan each step of implementation and measure effectiveness. If you don't have buy in for organisational restructure for example or no clear lines of communication set by management then this is not going to work.

Consultants are a definite capability enhancer but they cannot be the only way you ensure compliance and success.

Failing to prepare is preparing to fail – practice and adjust.

- The Right Scope: Over ambitious? Too Modest?
- Who does what – How? When?
- Top Management buy in
- We have technical controls – we don't need an ISMS
- What happens if…
- Outsourcing the problem entirely?
- Third Parties – Cloud Services – IT MSP's

PREPARING YOUR BUSINESS FOR **THE FUTURE**
www.riskevolves.com

New ISO27001 Standard

ISO 27001: 2022 was published on 1st October 2022, following the release of ISO 27002:2021 which was published on 16th Feb 2022.

Due to a change in the Information Security climate in the past couple of years, the update to ISO 27002 and in turn ISO 27001 was required in order to meet the ever changing environment and risks business's face. The themes of the controls allow for controls to overlap into a number of areas ensuring risks are managed and treated accordingly with your Statement of Applicability.

- The 14 control groups and objectives no longer exist. They have been replaced with 4 control groups which are:
  - Organisational (Clause 5)
  - People (Clause 6)
  - Physical (Clause 7)
  - Technology (Clause 8)

- There are 93 controls instead of 114
  - 19 controls are consolidated
  - 11 new controls
  - There are no deleted controls.

THEME CLAUSES	
5. Organisational	7. Physical
6. People	8. Technology

PREPARING YOUR BUSINESS FOR
THE FUTURE
www.riskevolves.com

CONNECT WITH US

✉ info@riskevolves.com

☎ +44 (0) 1926 800710

in @riskevolves

@riskevolves

@riskevolves

▶ Risk Evolves

NEVER STOP IMPROVING

Q&A

nqa.

NEVER STOP IMPROVING

THANK YOU

Warwick House | Houghton Hall Park | Houghton Regis | Dunstable | LU5 5ZX | United Kingdom
0800 052 2424 | | www.nqa.com