



WEBINAR: ISO 22301:2019 – DEMYSTIFYING BUSINESS CONTINUITY

Tim Pinnell
NQA's Information Security Assurance Manager
24th September 2021



— 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.



AMERICA'S NO.1

Certification body in
Aerospace sector

GLOBAL NO.1

Certification body in
telecommunications and
Automotive sector

TOP 3 IN THE UK

ISO 9001, ISO 14001,
ISO 45001, ISO 27001

GLOBAL NO.3

Certification body in
Aerospace sector

CHINA'S NO.1

Certification body in
Automotive sector

UK'S NO.2

Certification body in
Aerospace sector



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



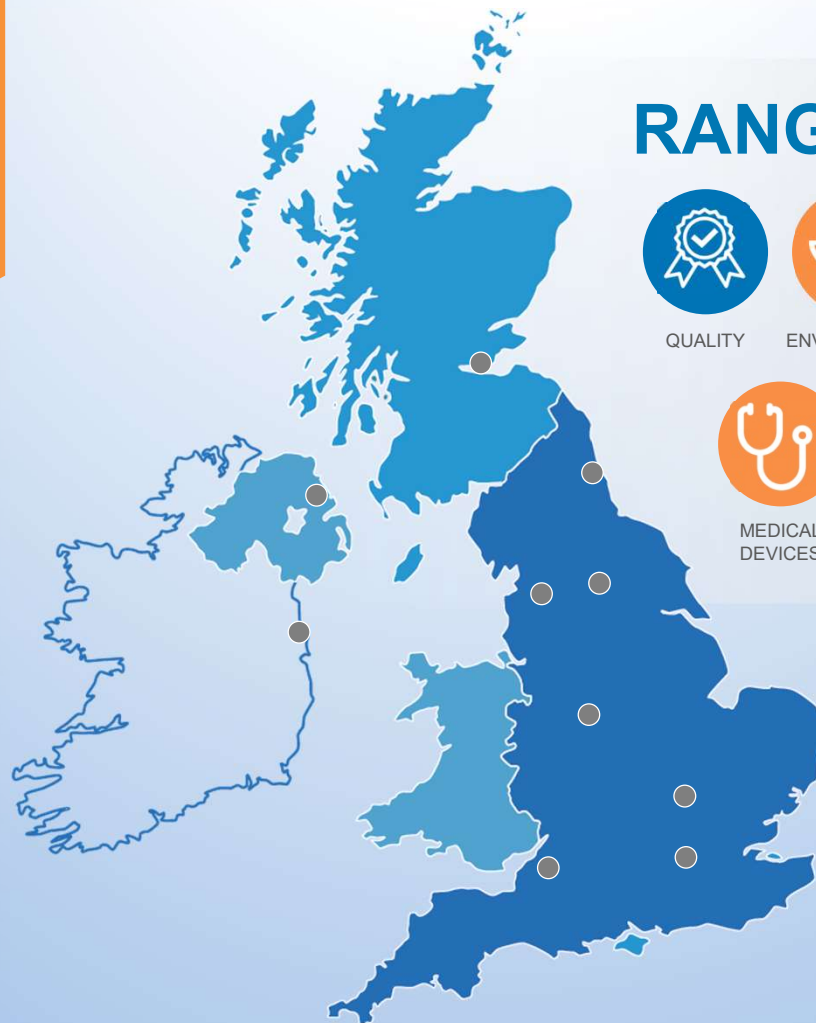
e-Learning /
Live Webinars



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
- **Advanced** Training

 CQI |  IRCA
APPROVED TRAINING PARTNER





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



Tim Pinnell

BSc, MSc, PCIP, CIPP/E,
CISMP, Information Security

NQA Information Security Assurance Manager



Tim has worked in telecommunications cyber and information security for over twenty years. From the early World Wide Web days to today's globally connected information services, Tim brings a wealth of experience in security, compliance and governance. Throughout his career he has played a leading role in adopting, consulting and implementing information security compliance standards, including ISO 27001, PCIDSS and Cyber Essentials, helping organizations understand the risks facing their businesses and the controls needed to mitigate them.

“ The rigour of a certified management system has sped up the process and ensured that we have been able to deliver what our clients need: an uninterrupted service. ”

E.L.F.S.

AGENDA FOR WEBINAR

- A brief introduction to ISO 22301
 - The impacts and benefits of a business continuity management system
 - How ISO 22301 integrates into your existing certification / management system
 - The key steps in implementing a BCMS
-



NEVER STOP IMPROVING

WHY BUSINESS CONTINUITY?



CHARACTERISTICS OF OPERATIONAL RESILIENCE



5%



25%



25%



28%



- Top level commitment
- Preparedness
- Flexibility
- Awareness
- Opacity
- Just culture
- Risk-based culture

MANAGEMENT SYSTEMS

- ISO 22301 Business Continuity Management
- ISO 27001 Information Security Management
- ISO 27701 Privacy Information Management
- ISO 27017 Information Security for Cloud Service Providers
- ISO 14001 Environmental Management
- ISO 45001 Occupational Health and Safety
- ISO 20000 IT Service Management





NEVER STOP IMPROVING

ISO 22301:2019 BENEFITS





NEVER STOP IMPROVING

BENEFITS

- Leadership commitment to resilience
- Reputational
- Protection and recovery
- Financial





NEVER STOP IMPROVING

ISO 22301:2019 INTRODUCTION



ISO 22301:2019 INTRODUCTION

What is ISO 22301?

- The international standard for Business Continuity Management

Requirements:

- Plan
- Establish, Implement, Operate & Maintain
- Monitor & Review
- Continually Improve

A BCMS includes the following components:

- Policy
 - People
 - Processes
 - Documented Information
-

INTEGRATION WITH OTHER STANDARDS

- ISO 22301 follows the same high level management structure for all ISO management system standards.
- Context; Leadership; Planning and Support – there is little difference between ISO 22301 and other standards such as ISO 9001 and ISO 14001.
- Operation – you will still need to plan, implement and control the processes needed to meet requirements. They are simply different process from what you will have implemented for other standards.
- Performance Evaluation and Continual Improvement – there is little difference between ISO 22301 and other standards such as ISO 9001 and ISO 14001.



[illegible]

8	OPERATION							
8.1	Operational planning and control	Operational planning and control	Operational planning and control	Operational planning and control	Operational planning and control	Operational planning and control	Operational planning and control	Operational planning and control
8.1.1			General					
8.1.2			Eliminating hazards and reducing OH&S risks					
8.1.3			Management of change					
8.1.4			Procurement					
8.2	Requirements for products and services	Emergency preparedness and response	Emergency preparedness and response	Design	Information security risk assessment	Service portfolio	Business impact analysis and risk assessment	Management of change
8.2.1	Customer communication					Service delivery	General	
8.2.2	Determining the requirements for products and services					Plan the services	Business impact analysis	
8.2.3	Review of the requirements for products and services					Control of parties involved in the service lifecycle	Risk assessment	
8.2.4	Changes to requirements for products and services					Service catalogue management		
8.2.5						Asset management		
8.2.6						Configuration management		
8.3	Design and development of products and services			Procurement	Information security risk treatment	Relationship and agreement	Business continuity strategies and solutions	Outsourcing
8.3.1	General					General	General	
8.3.2	Design and development planning					Business relationship management	Identification of strategies and solutions	
8.3.3	Design and development inputs					Service level management	Selection of strategies and solutions	
8.3.4	Design and development controls					Supplier management	Resource requirements	
8.3.5	Design and development outputs						Implementation of solutions	
8.3.6	Design and development changes							
8.4	Control of externally provided processes, products and services					Supply and demand	Business continuity plans and procedures	
8.4.1	General					Budgeting and accounting for services	General	
8.4.2	Type and extent of control					Demand management	Response structure	
8.4.3	Information for external providers					Capacity management	Warning and communication	
8.4.4							Business continuity plans	
8.4.5							Recovery	
8.5	Production and service provision					Service design, build and transition	Exercise programme	
8.5.1	Control of production and service provision					Change management		
8.5.2	Identification and traceability					Service design and transition		
8.5.3	Property belonging to customers or external providers					Release and deployment management		



NEVER STOP IMPROVING

ISO 22301:2019 IMPLEMENTATION



OPERATION

- Plan, implement and control the processes needed to meet requirements of the standard
- Criteria for operating the processes
- Control the processes
- Document the processes
- Control changes to the processes



BIA AND RISK ASSESSMENT

Business Impact Analysis:

- Identify an organisations key prioritised activities and the impact a disruption can have on those activities over a period of time.
- Identify a time frame when failure to resume those activities would become unacceptable to an organisation (Maximum Tolerable Period of Disruption – MTPD)
- Set a time frame and level for the resumption of disruptive activities (Recovery Time Objective - RTO)
- Identify internal and external activities and resources that support its key activities.

Risk Assessment:

- Identify the risk of disruption to an organisations key activities and determine which risks require treatment. Risk can be internal and external.
-

STRATEGIES AND SOLUTIONS

Based on results of its BIA and risk assessments, an organisation shall identify, implement and maintain business continuity strategies and solutions to:

- Meet the requirement to continue and recover prioritised activities.
 - Protect the organisations priorities activities and reduce the likelihood of disruption.
 - Limit the impact and period of disruption to an organisations products and services.
 - Take into consideration the cost and benefits; and the amount and type of risk it is willing to take.
 - Identify and provide adequate resources for the recovery and continuation of prioritised activities; resources typically include: People, Information and ICT, infrastructure, equipment and consumables, finance, logistics and transport, partners and suppliers.
-

BUSINESS CONTINUITY PROCEDURES

- Should be specific regarding the immediate actions to be taken during a disruptive incident.
- Focus on; and minimise the impact of incident.
- Assign roles and responsibilities.
- Response structure that identifies a team(s) responsible for responding to disruption.
- Warning and communications.



BUSINESS CONTINUITY PLANS

- Documented business continuity plans providing guidance and information to teams responding to a disruption are to be established and maintained.
 - The plans should contain details of the actions required to continue or recover operations within the predetermined timeframe; at an agreed level and subsequent return to normal operations.
 - A document process detailing the actions required to return to normal operations should be established.
-

EXERCISE PROGRAMME

- An exercise programme to test the validity of an organisations business continuity, strategy and solutions is to be implemented.
- Exercises should be based upon appropriate scenarios, conducted at planned intervals and when significant changes occur.
- Records of exercises are to be maintained and any lessons identified/opportunities for improvement fed back into the plan as part of the PDCA Cycle.



EVALUATION OF DOCUMENTATION AND CAPABILITIES

- **Organisations shall evaluate its business continuity documentation and capabilities at planned intervals, to ensure its continued suitability, adequacy and effectiveness.**
 - BIA & risk assessments
 - BC Strategies, solutions, plans & procedures
 - **Evaluation**
 - Review, analysis, exercises, tests, post incident reports and performance evaluation
 - **Suppliers and partners**
 - **Compliance with legal and regulatory requirements.**
-

PLANNING A BUSINESS CONTINUITY MANAGEMENT SYSTEM

Tasks	Output
Planning	Business Continuity Objectives
Business Continuity Risk Assessment	Documented risk assessment
Business Impact Analysis	Documented BIA iaw the standard
Strategies and Solutions	Strategies that meet the requirements identified in the BIA and RA to recover the prioritized activities
Business Continuity Plans	Documented BC plans and procedures
Exercise Programme	Calenderised programme Sufficient coverage of prioritized activities
Evaluation of BC documentation and Capabilities	Internal audit programme Management review Post-incident reviews Supplier reviews Monitoring of changes to applicable legislation

MANDATORY DOCUMENTS

Clause	Document
4.2.2	Applicable legal requirements, regulations or laws, and any other identified requirements
4.3.1	The scope of the BCMS
4.3.2	Exclusions from the scope of the BCMS
5.2.2	The Business Continuity Policy
6.2.1	Business Continuity objectives
7.2	Evidence of personnel competence
7.5.1	Documentation required by the standard (this list) and anything else considered necessary for the effectiveness of the BCMS
8.1	Information necessary to have confidence that the operational planning and control processes are being carried out as planned
8.4.1	Business continuity plans and procedures
8.4.2.4	Documented procedures for each response team
8.4.3.1	Warning and communication procedures
8.4.4.1	Business continuity plans
8.4.5	Recovery and restoration processes
8.5	Post-exercise reports
9.1	Results of monitoring, measurement, analysis and evaluation of the performance of the BCMS
9.2.2	Evidence of the implementation of the audit programme and the audit results
9.3.3.2	Results of the management reviews
10.1.3	The nature of non-conformities and what was done about them, and the results of the corrective action



NEVER STOP IMPROVING

Q&A





NEVER STOP IMPROVING

THANK YOU

Warwick House | Houghton Hall Park | Houghton Regis | Dunstable | LU5 5ZX | United Kingdom

0800 052 2424 | info@nqa.com | www.nqa.com
