OPERATIONAL RESILIENCE

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

- Definitions of Operational Resilience
- How to recognise operational resilience
- Management standards and operational resilience
- A brief introduction to ISO 22301
- The impact and benefits of a business continuity management system
- Implementing ISO 22031

Definitions of Operational Resilience

DEFINITIONS

- **First Definition**

Operational resilience is the ability to alter operations in the face of changing business conditions. It is the ability to quickly ramp up or slow down with quick and local process modification.

- **Second Definition**

The ability to adapt to risk that affects its core operational abilities. It is a property of effective risk management. It is a subset of enterprise resilience, the ability to manage operational risk.

CHARACTERISTICS OF OPERATIONAL RESILIENCE

5%

25%

25%

28%

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

MEASURING OPERATIONAL RESILIENCE

- Finding and assessing its vulnerabilities and its supply chain vulnerabilities
- Reducing the likelihood of disruption with planning, controls, flexibility and redundancies
- Detecting disruption in itself and supply chains
- Measuring its operational resilience.

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

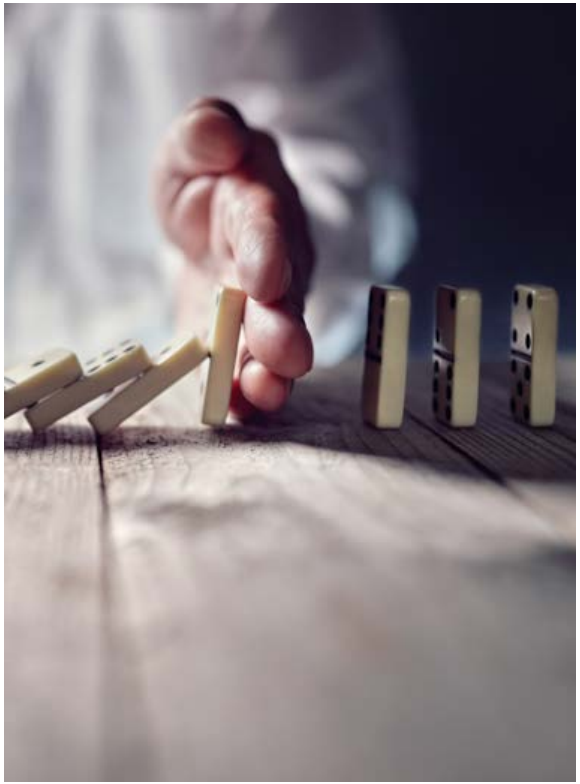
ISO 22301:2019 INTRODUCTION

- **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

ISO 22301:2019 – BENEFITS

BENEFITS

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



ISO 22301:2019 – INTEGRATION

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.

NQA ANNEX SL COMPARISON TOOL

	ISO 9001	ISO 14001	ISO 45001	ISO 50001	ISO 27001	ISO 20000-1	ISO 22301	ISO 55001
4	**CONTEXT OF THE ORGANISATION**							
4.1	Understanding the organization and its context	Understanding the organization and its context	Understanding the organization and its context	Understanding the organization and its context	Understanding the organization and its context	Understanding the organization and its context	Understanding the organization and its context	Understanding the organization and its context
4.2	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of workers and interested parties	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of stakeholders
4.2.1							General	
4.2.2							Legal and regulatory requirements	
4.3	Determining the scope of the quality management system	Determining the scope of the environmental management system	Determining the scope of the OH&S management system	Determining the scope of the energy management system	Determining the scope of the information security management system	Determining the scope of the service management system	Determining the scope of the business continuity management system	Determining the scope of the asset management system
4.3.1							General	
4.3.2							Scope of the business continuity management system	
4.4	Quality management system and its processes	Environmental management system	OH&S management system	Energy management system	Information security management system	Service management system	Business continuity management system	Asset management system
5	**LEADERSHIP**							
5.1	Leadership and commitment	Leadership and commitment	Leadership and commitment	Leadership and commitment	Leadership and commitment	Leadership and commitment	Leadership and commitment	Leadership and commitment
5.1.1	General							
5.1.2	Customer Focus							
5.2	Policy	Environmental policy	OH&S policy	Energy policy	Policy	Policy	Policy	Policy
5.2.1	Establishing the quality policy					Establishing the service management policy	Establishing the business continuity policy	
5.2.2	Communicating the quality policy					Communicating the service management policy	Communicating the business continuity policy	
5.3	Organisational roles, responsibilities and authorities	Organisational roles, responsibilities and authorities	Organisational roles, responsibilities and authorities	Organisational roles, responsibilities and authorities	Organisational roles, responsibilities and authorities	Organisational roles, responsibilities and authorities	Roles, responsibilities and authorities	Organisational roles, responsibilities and authorities
5.4			Consultation and participation of workers					
6	**PLANNING**							
	Actions to address risks and	Actions to address risks and	Actions to address risks and	Actions to address risks and	Actions to address risks and	Actions to address risks and	Actions to address risks and	Actions to address risks and

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		

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.

EVALUTION 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.**

nqa.
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