WEBINAR: DEMYSTIFYING ISO 27001

Tim Pinnell

30/06/2021

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.

BOSTON
LONDON
BANGALORE
SHANGHAI

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.

nqa.

NEVER STOP IMPROVING

CERTIFICATION AND TRAINING SERVICES

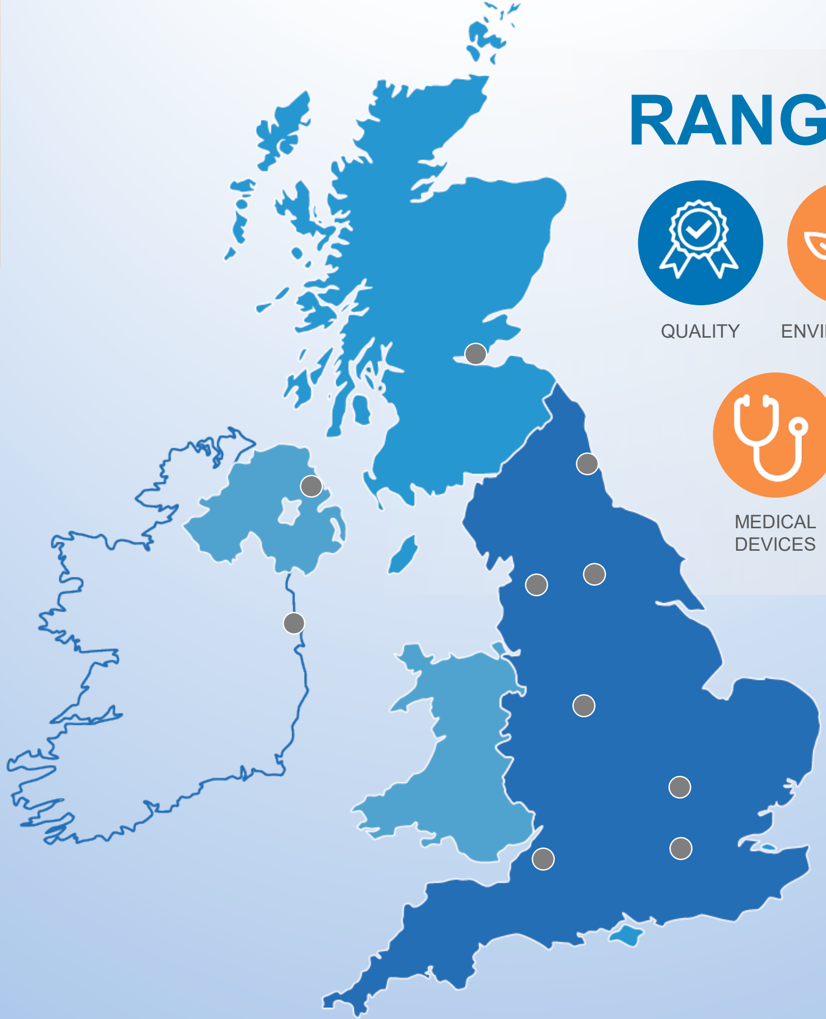
We specialise in management systems certification for:

- 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

nqa.

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

Tim Pinnell

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

NQA Information Security Assurance Manager

nqa.

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

- Clause comparison between ISO 9001 and ISO 27001
- Information security risk assessment
- Information security risk treatment
- Common pitfalls
- Outsourced security and managed service providers

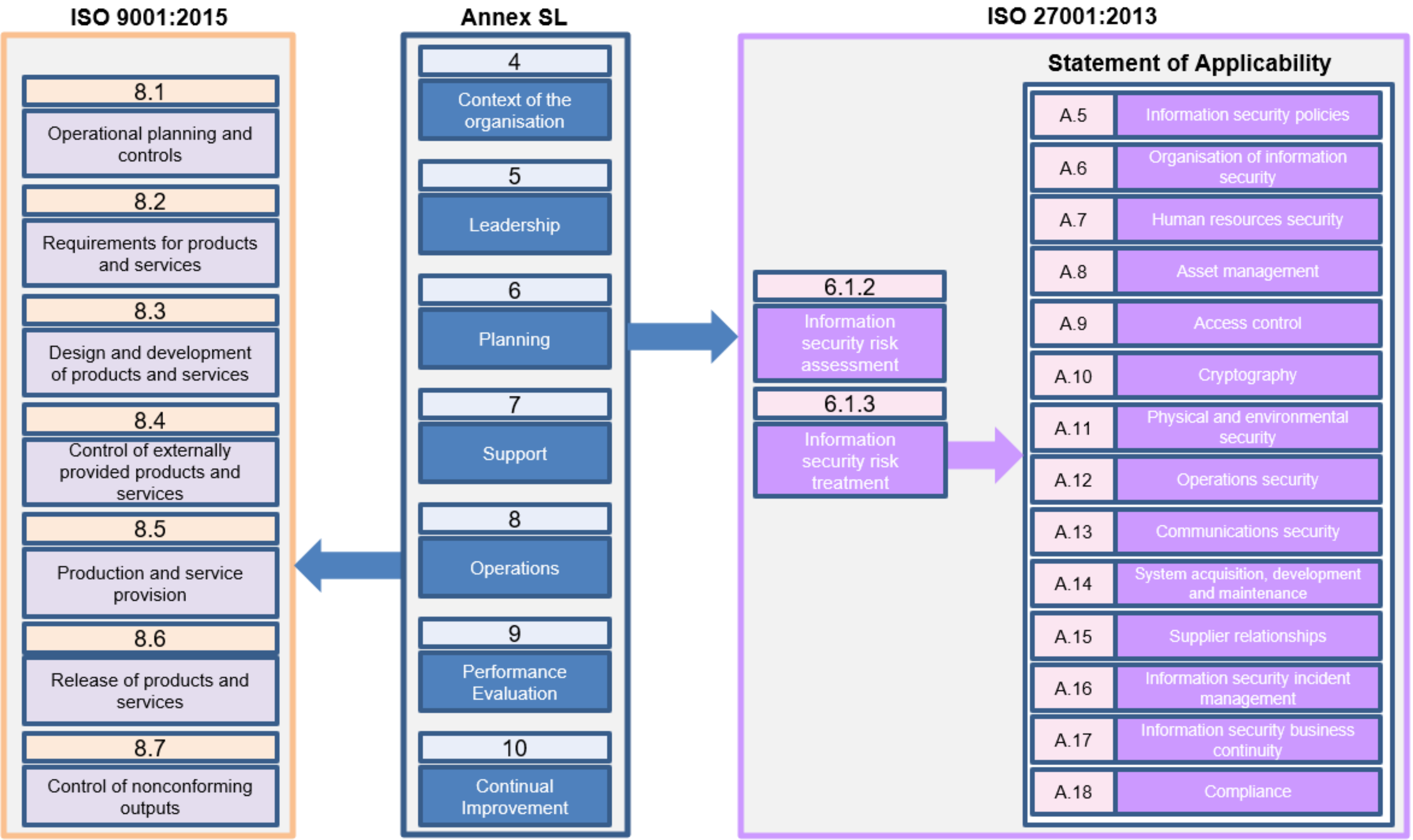
NQA ANNEX SL COMPARISON TOOL

	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**							
6.1	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	9001		Eliminating hazards and reducing OH&S risks		27001			
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 traceabaility					Service design and transition		

NEVER STOP IMPROVING

CLAUSE COMPARISON BETWEEN ISO 9001 and ISO 27001



ISO 9001:2015

8.1	Operational planning and controls
8.2	Requirements for products and services
8.3	Design and development of products and services
8.4	Control of externally provided products and services
8.5	Production and service provision
8.6	Release of products and services
8.7	Control of nonconforming outputs

Annex SL

4	Context of the organisation
5	Leadership
6	Planning
7	Support
8	Operations
9	Performance Evaluation
10	Continual Improvement

ISO 27001:2013

6.1.2	Information security risk assessment
6.1.3	Information security risk treatment

Statement of Applicability

A.5	Information security policies
A.6	Organisation of information security
A.7	Human resources security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communications security
A.14	System acquisition, development and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security business continuity
A.18	Compliance

CLAUSE 4

	ISO 9001	ISO 27001
4	**Context of the organisation**	
4.1	Understanding the organisation and its context	Understanding the organisation and its context
4.2	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of interested parties
4.3	Determining the scope of the quality management system	Determining the scope of the information security management system
4.4	Quality management system **and its processes**	Information security management system

CLAUSE 5

	ISO 9001	ISO 27001
5	**Leadership**	
5.1	Leadership and commitment	Leadership and commitment
5.1.1	General	
5.1.2	Customer Focus	
5.2	Policy	Policy
5.2.1	Establishing the quality policy	
5.2.2	Communicating the quality policy	
5.3	Organisational roles, responsibilities and authorities	Organisational roles, responsibilities and authorities

CLAUSE 6

	ISO 9001	ISO 27001
6	**Planning**	
6.1	Actions to address risks and opportunities	Actions to address risks and opportunities
6.1.1		General
6.1.2		**Information security risk assessment**
6.1.3		**Information security risk treatment**
6.2	Quality objectives and planning to achieve them	Information security objectives and planning to achieve them
6.3	Planning of changes	

NEVER STOP IMPROVING

CLAUSE 7

	ISO 9001	ISO 27001
7	**Support**	
7.1	Resources	Resources: '*The organisation shall determine and provide the resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS*'
7.1.1	General	
7.1.2	People	
7.1.3	Infrastructure	
7.1.4	Environment for the operation of processes	
7.1.5	Monitoring and measuring resources	
7.1.6	Organisational knowledge	

CLAUSE 7

	ISO 9001	ISO 27001
7	**Support**	
7.2	Competence	Competence
7.3	Awareness	Awareness
7.4	Communication	Communication
7.5	Documented information	Documented information

CLAUSE 8

	ISO 9001	ISO 27001
8	**Operation**	
8.1	Operational planning and control	Operational planning and control
8.2	Requirements for products and services	Information security risk assessment: ‘*The organisation shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur*’
8.3	Design and development of products and services	Information security risk treatment: ‘*The organisation shall implement the risk treatment plan*’
8.4	Control of externally provided processes, products and services	
8.5	Production and service provision	
8.6	Release of products and services	
8.7	Control of nonconforming outputs	

CLAUSE 9

	ISO 9001	ISO 27001
9	**Performance evaluation**	
9.1	Monitoring, measurement, analysis and evaluation	Monitoring, measurement, analysis and evaluation
9.1.1	General	
9.1.2	**Customer satisfaction**	
9.1.3	Analysis and evaluation	
9.2	Internal audit	Internal audit
9.3	Management review	Management review

CLAUSE 10

	ISO 9001	ISO 27001
10	**Improvement**	
10.1	General	Nonconformity and corrective action
10.2	Nonconformity and corrective action	Continual improvement
10.3	Continual improvement	

6.1.2 INFORMATION SECURITY RISK ASSESSMENT

6.1.2 INFORMATION SECURITY RISK ASSESSMENT

Part 1: Define
Criteria for accepting risks
Criteria for when risk assessments should be performed
Criteria for ensuring repeatability and consistency
Part 2: Identify
Identify risks to the Confidentiality, Integrity and Availability (CIA) of information
Identify the risk owners
Part 3: Guess
Assess the impact
Assess the likelihood
Determine the level of risk
Part 4: Prioritise
Compare the levels of risk against the risk criteria
Prioritise risks for treatment

6.1.2 INFORMATION SECURITY RISK ASSESSMENT

Define criteria for:

Accepting Risks

ACCEPT

- Risk score is less than 6 or Moderate

TREAT

- Risk score is greater than 6 or High or above
- Revenue loss >20%
- Public damage to reputation
- Harm to employees

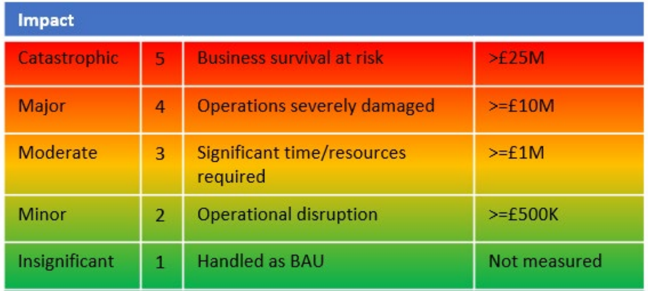
TERMINATE

- Risk score is Extreme

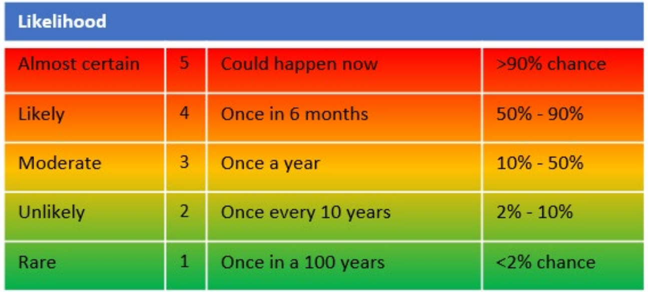
Performing Assessments

- Before an infrastructure change
- A change in regulation or law
- Following a security breach
- Following an IT failure
- Before a major software change
- Following a global incident
- Following a vulnerability assessment
- Every year
- The acquisition of a business
- Engaging a new supplier

Risk Assessments



Impact			
Catastrophic	5	Business survival at risk	>£25M
Major	4	Operations severely damaged	>=£10M
Moderate	3	Significant time/resources required	>=£1M
Minor	2	Operational disruption	>=£500K
Insignificant	1	Handled as BAU	Not measured



Likelihood			
Almost certain	5	Could happen now	>90% chance
Likely	4	Once in 6 months	50% - 90%
Moderate	3	Once a year	10% - 50%
Unlikely	2	Once every 10 years	2% - 10%
Rare	1	Once in a 100 years	<2% chance

6.1.2 INFORMATION SECURITY RISK ASSESSMENT

Identify the information security risks:

Ref	Information Asset	Risk		Owner
		CIA	Description	
1	Customer data	C	Personal data breach by phishing resulting in ICO fine and reputational damage	Sales Director
2	Customer data	A	Customer data removed by exiting employee resulting in loss of business to competitors	Sales Director
3	Sales data	A	Unable to process sales due to hardware failure resulting in short term revenue drop	Sales Director
4	Product designs	A	Network failure halting manufacturing process resulting in lost orders	Production Director
5	Website	A	Failure of any type at hosting provider prevents customer orders being received resulting in loss of sales	Sales Director
6	Database	I	Index corruption mixes customer records resulting in poor customer service	Sales Director
7	Laptops	A	Theft or loss leading to replacement cost	HR Director

NEVER STOP IMPROVING

6.1.2 INFORMATION SECURITY RISK ASSESSMENT

Analyse the risks (guess)

Ref	Description	Impact	Likelihood	Risk level
1	Personal data breach by phishing resulting in ICO fine and reputational damage	4	4	Very High
2	Customer data stolen by exiting employee resulting in loss of business to competitors	3	2	Moderate
3	Unable to process sales due to hardware failure resulting in short term revenue drop	3	3	High
4	Network failure halting manufacturing process resulting in lost orders	4	4	Very High
5	Failure of any type at hosting provider prevents customer orders being received resulting in loss of sales	3	3	High
6	Index corruption prevents retrieval of customer records resulting in poor customer service	2	1	Low
7	Theft or loss leading to replacement cost	1	3	Low

Impact			
Catastrophic	5	Business survival at risk	>£25M
Major	4	Operations severely damaged	>=£10M
Moderate	3	Significant time/resources required	>=£1M
Minor	2	Operational disruption	>=£500K
Insignificant	1	Handled as BAU	Not measured

Impact		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood		1	2	3	4	5
Almost certain	5	High	High	Very High	Extreme	Extreme
Likely	4	Moderate	High	High	Very High	Extreme
Moderate	3	Low	Moderate	High	High	Very High
Unlikely	2	Low	Low	Moderate	High	High
Rare	1	Low	Low	Low	Moderate	High

Likelihood			
Almost certain	5	Could happen now	>90% chance
Likely	4	Once in 6 months	50% - 90%
Moderate	3	Once a year	10% - 50%
Unlikely	2	Once every 10 years	2% - 10%
Rare	1	Once in a 100 years	<2% chance

6.1.2 INFORMATION SECURITY RISK ASSESSMENT

Evaluate the risks:

Ref	Description	Impact	Likelihood	Risk level	Priority
1	Personal data breach by phishing resulting in ICO fine and reputational damage	4	4	Very High	1
2	Customer data stolen by exiting employee resulting in loss of business to competitors	3	2	Moderate	5
3	Unable to process sales due to hardware failure resulting in short term revenue drop	3	3	High	4
4	Network failure halting manufacturing process resulting in lost orders	4	4	Very High	2
5	Failure of any type at hosting provider prevents customer orders being received resulting in loss of sales	3	3	High	3
6	Index corruption prevents retrieval of customer records resulting in poor customer service	2	1	Low	6
7	Theft or loss leading to replacement cost	1	3	Low	6

NEVER STOP IMPROVING

6.1.3 INFORMATION SECURITY RISK TREATMENT

6.1.3 INFORMATION SECURITY RISK TREATMENT

Evaluate the risks:

Define and apply an information security risk treatment process:
Select risk treatment options
Determine the controls necessary for the risk treatment options
Compare the selected controls with those in Annex A
Produce a Statement of Applicability
Create a risk treatment plan
Obtain risk owner approval for the plan
Calculate the residual risk and obtain risk owner approval for the residual risk

6.1.3 INFORMATION SECURITY RISK TREATMENT

Select risk treatment options:

Ref	Description	Impact	Likelihood	Risk level	Priority	Treatment
1	Personal data breach by phishing resulting in ICO fine and reputational damage	4	4	Very High	1	Treat
2	Customer data stolen by exiting employee resulting in loss of business to competitors	3	2	Moderate	5	Accept
3	Unable to process sales due to hardware failure resulting in short term revenue drop	3	3	High	4	Treat
4	Network failure halting manufacturing process resulting in lost orders	4	4	Very High	2	Treat
5	Failure of any type at hosting provider prevents customer orders being received resulting in loss of sales	3	3	High	3	Treat
6	Index corruption prevents retrieval of customer records resulting in poor customer service	2	1	Low	6	Accept
7	Theft or loss leading to replacement cost	1	3	Low	6	Accept

Accept

- Risk score is less than 6 or Moderate

Treat

- Risk score is greater than 6 or High or above
- Revenue loss >20%
- Public damage to reputation
- Harm to employees

Terminate

- Risk score is Extreme

6.1.3 INFORMATION SECURITY RISK TREATMENT

Determine necessary controls:

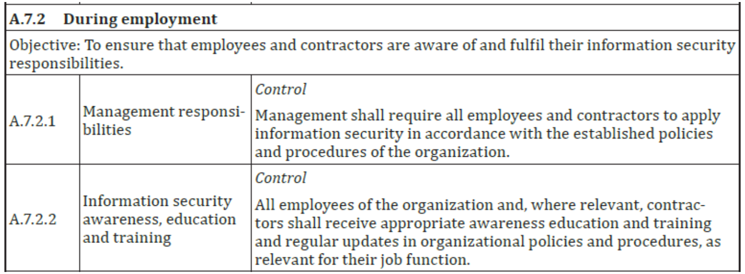
Ref	Description	Impact	Likelihood	Risk level	Priority	Treatment
1	Personal data breach by phishing resulting in ICO fine and reputational damage	4	4	Very High	1	Treat

1. Introduce phishing training for all staff
2. Add phishing training to new starter induction programme
3. Add phish reporting capability to Outlook
4. Implement automated phishing detection tool
5. Ensure anti-virus provider can detect malware associated with phishing
6. Implement automated security event alerting and log analysis tool
7. Review account permissions
8. Implement remote mobile device management

6.1.3 INFORMATION SECURITY RISK TREATMENT

Compare the selected controls with those in Annex A:

1. **Introduce phishing training for all staff**
2. **Add phishing training to new starter induction programme**
3. Add phish reporting capability to Outlook
4. Implement automated phishing detection tool
5. Ensure anti-virus provider can detect malware associated with phishing
6. Implement automated security event alerting and log analysis tool
7. Review account permissions
8. Implement remote mobile device management
9. *Security controls for the other risks*
10. *Security controls for the other risks*
11. *Security controls for the other risks*

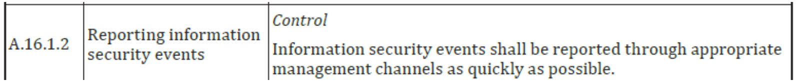


A.7.2	**During employment**	
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management responsibilities	*Control* Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
A.7.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

6.1.3 INFORMATION SECURITY RISK TREATMENT

Compare the selected controls with those in Annex A:

1. Introduce phishing training for all staff
2. Add phishing training to new starter induction programme
3. **Add phish reporting capability to Outlook**
4. Implement automated phishing detection tool
5. Ensure anti-virus provider can detect malware associated with phishing
6. Implement automated security event alerting and log analysis tool
7. Review account permissions
8. Implement remote mobile device management
9. *Security controls for the other risks*
10. *Security controls for the other risks*
11. *Security controls for the other risks*

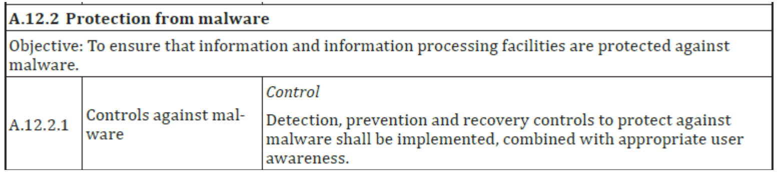


A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.

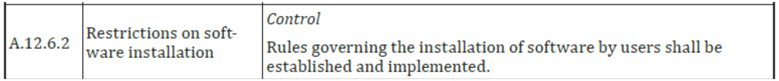
6.1.3 INFORMATION SECURITY RISK TREATMENT

Compare the selected controls with those in Annex A:

1. Introduce phishing training for all staff
2. Add phishing training to new starter induction programme
3. Add phish reporting capability to Outlook
4. **Implement automated phishing detection tool**
5. Ensure anti-virus provider can detect malware associated with phishing
6. Implement automated security event alerting and log analysis tool
7. Review account permissions
8. Implement remote mobile device management
9. *Security controls for the other risks*
10. *Security controls for the other risks*
11. *Security controls for the other risks*



A.12.2 Protection from malware		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1	Controls against malware	*Control* Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

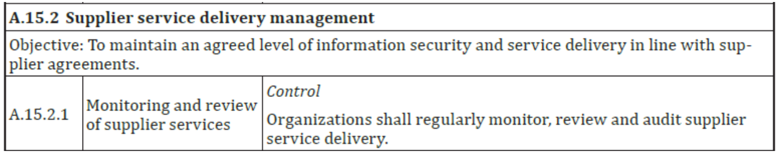


A.12.6.2	Restrictions on software installation	*Control* Rules governing the installation of software by users shall be established and implemented.

6.1.3 INFORMATION SECURITY RISK TREATMENT

Compare the selected controls with those in Annex A:

1. Introduce phishing training for all staff
2. Add phishing training to new starter induction programme
3. Add phish reporting capability to Outlook
4. Implement automated phishing detection tool
5. **Ensure anti-virus provider can detect malware associated with phishing**
6. Implement automated security event alerting and log analysis tool
7. Review account permissions
8. Implement remote mobile device management
9. *Security controls for the other risks*
10. *Security controls for the other risks*
11. *Security controls for the other risks*

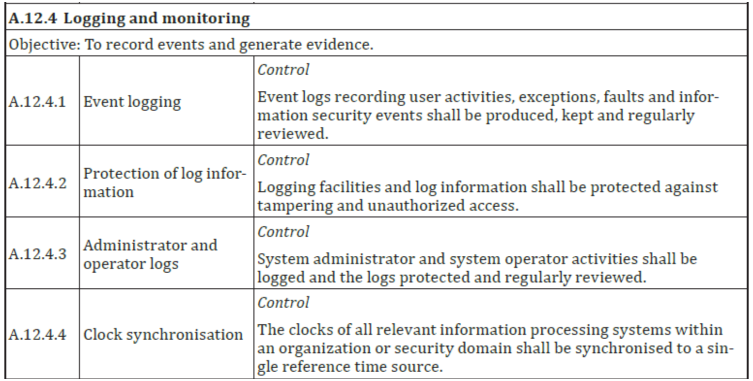


A.15.2 Supplier service delivery management		
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.		
A.15.2.1	Monitoring and review of supplier services	*Control* Organizations shall regularly monitor, review and audit supplier service delivery.

6.1.3 INFORMATION SECURITY RISK TREATMENT

Compare the selected controls with those in Annex A:

1. Introduce phishing training for all staff
2. Add phishing training to new starter induction programme
3. Add phish reporting capability to Outlook
4. Implement automated phishing detection tool
5. Ensure anti-virus provider can detect malware associated with phishing
6. **Implement automated security event alerting and log analysis tool**
7. Review account permissions
8. Implement remote mobile device management
9. *Security controls for the other risks*
10. *Security controls for the other risks*
11. *Security controls for the other risks*

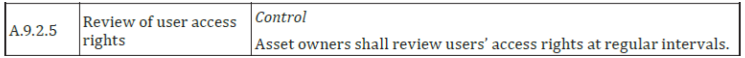


A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1	Event logging	*Control* Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
A.12.4.2	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.12.4.3	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
A.12.4.4	Clock synchronisation	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.

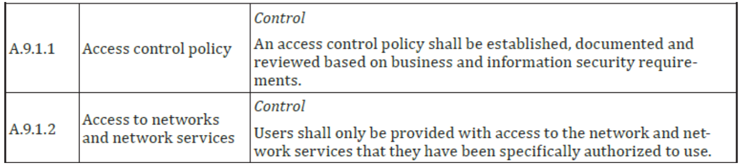
6.1.3 INFORMATION SECURITY RISK TREATMENT

Compare the selected controls with those in Annex A:

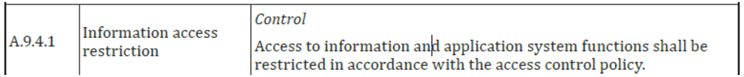
1. Introduce phishing training for all staff
2. Add phishing training to new starter induction programme
3. Add phish reporting capability to Outlook
4. Implement automated phishing detection tool
5. Ensure anti-virus provider can detect malware associated with phishing
6. Implement automated security event alerting and log analysis tool
7. **Review account permissions**
8. Implement remote mobile device management
9. *Security controls for the other risks*
10. *Security controls for the other risks*
11. *Security controls for the other risks*



A.9.2.5	Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.



A.9.1.1	Access control policy	*Control* An access control policy shall be established, documented and reviewed based on business and information security requirements.
A.9.1.2	Access to networks and network services	*Control* Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

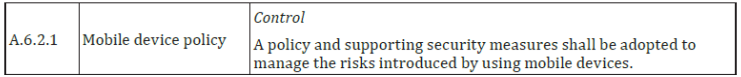


A.9.4.1	Information access restriction	*Control* Access to information and application system functions shall be restricted in accordance with the access control policy.

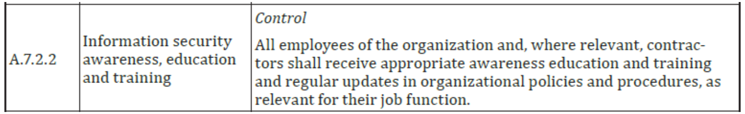
6.1.3 INFORMATION SECURITY RISK TREATMENT

Compare the selected controls with those in Annex A:

1. Introduce phishing training for all staff
2. Add phishing training to new starter induction programme
3. Add phish reporting capability to Outlook
4. Implement automated phishing detection tool
5. Ensure anti-virus provider can detect malware associated with phishing
6. Implement automated security event alerting and log analysis tool
7. Review account permissions
8. **Implement remote mobile device management**
9. *Security controls for the other risks*
10. *Security controls for the other risks*
11. *Security controls for the other risks*



A.6.2.1	Mobile device policy	*Control* A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.



A.7.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

6.1.3 INFORMATION SECURITY RISK TREATMENT

Produce a Statement of Applicability:

The Statement of Applicability should list *every* Annex A control

Annex A Control (*examples*)		**Justification for inclusion**	**Control implemented?**	**Justification for exclusion**
A.5.1.1	Policies for information security	General security requirement	Yes	N/A
A.6.2.1	Mobile device policy	Risk treatment for risk 1	Yes	N/A
A.7.2.2	Information security awareness, education and training	Risk treatment for risks 1, 6 & 12 Required for ISMS	Yes	N/A
A.12.2.1	Controls against malware	Risk treatment for risks 1 & 2	Partial – see risk treatment plan	N/A
A.14.2.1	Secure development policy	N/A	N/A	We do not do any software development
A.16.1.3	Reporting information security weaknesses	Risk treatment for risk 1 General security requirement	Yes	N/A
A.18.1.4	Privacy and protection of PII	DPA 2018 and GDPR compliance	Yes	N/A

6.1.3 INFORMATION SECURITY RISK TREATMENT

Formulate a risk treatment plan:

Risk treatments		Start	Finish	Resources / activities	Cost	Owner
1	Introduce phishing training for all staff	16/06/21	30/09/21	• Third party training provider • Media licenses	• £1.5k • £250 pa	HR Director
2	Add phish reporting capability to Outlook	01/07/21	30/09/21	• Identify tool • Test and implement	Est. £2.3k pa	IT Director
3	Implement automated phishing detection tool	01/07/21	02/08/21	• Engage MSP to establish capability • Test and implement	TBD	IT Director
4	Ensure AV provider can detect malware associated with phishing	01/05/21	15/05/21	Contact provider	Time only	IT Director
5	Implement automated security event alerting and log analysis tool	01/04/21	30/10/21	• Product evaluation • Test, tune and implement	£50k	IT Director
6	Review account permissions	01/06/21	Completed		Time only	CSO
7	Implement remote mobile device management	05/01/22	01/06/22	• Select product • Replace old iPhones • Test and implement	• £5k • £8k • Time	IT Director

6.1.3 INFORMATION SECURITY RISK TREATMENT

Obtain risk owners' approval of plan and acceptance of the residual risk:

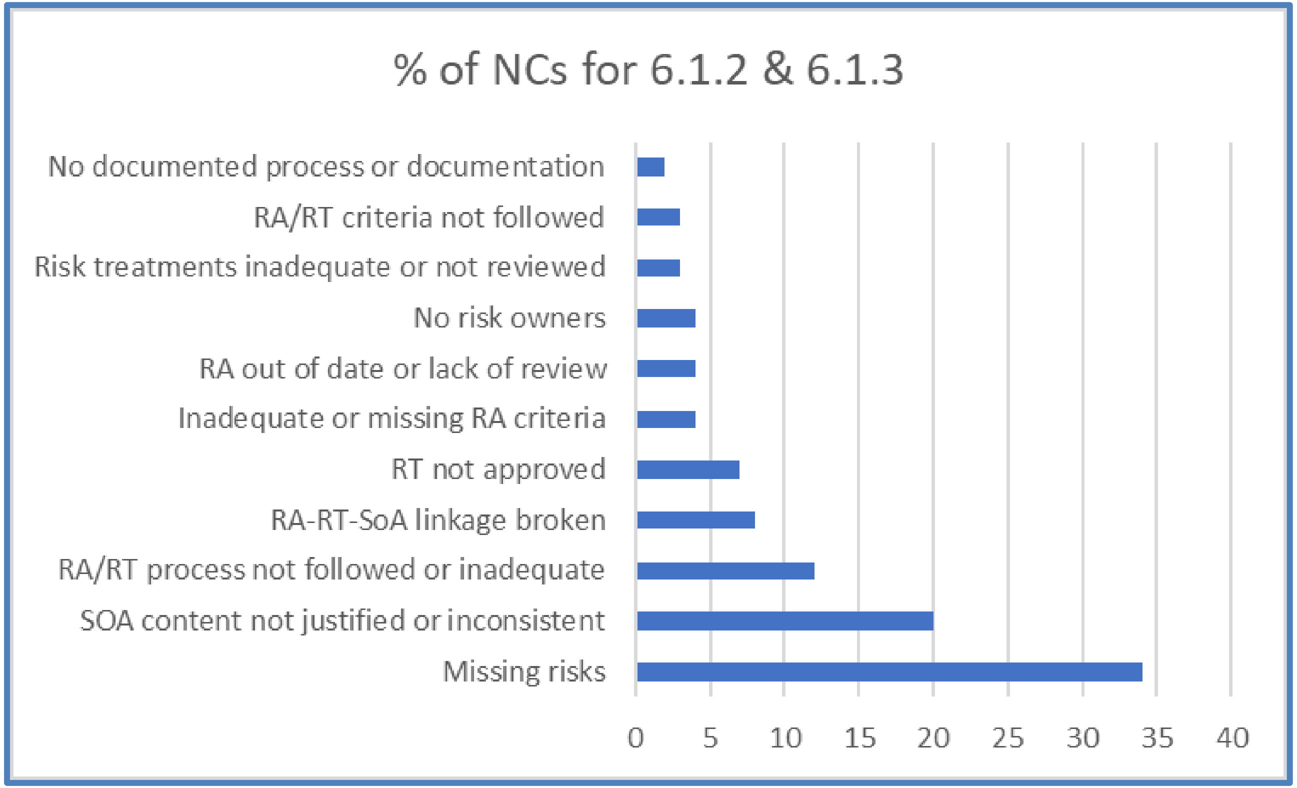
	Description	Pre-treatment risk scores			Priority	Treatment	Residual risk		
		Impact	Likelihood	Risk level			Impact	Likelihood	Risk level
1	Personal data breach by phishing resulting in ICO fine and reputational damage	4	4	Very High	1	Treat	4	2	High
2	Customer data stolen by exiting employee resulting in loss of business to competitors	3	2	Moderate	5	Accept			
3	Unable to process sales due to hardware failure resulting in short term revenue drop	3	3	High	4	Treat	3	1	Low
4	Network failure halting manufacturing process resulting in lost orders	4	4	Very High	2	Treat	3	2	Moderate
5	Failure of any type at hosting provider prevents customer orders being received resulting in loss of sales	3	3	High	3	Treat	3	2	Moderate
6	Index corruption prevents retrieval of customer records resulting in poor customer service	2	1	Low	6	Accept			
7	Theft or loss leading to replacement cost	1	3	Low	6	Accept			

NEVER STOP IMPROVING

COMMON PITFALLS – CAUSES OF NON-CONFORMITIES

NEVER STOP IMPROVING

COMMON CAUSE OF MINOR NCs IN 6.1.2 AND 6.1.3



6.1.1 ACTIONS TO ADDRESS ISMS RISKS AND OPPORTUNITIES

6.1.1 -> Risks to the ISMS
6.1.2 -> Risks to information

Part 1
Identify risks and opportunities to the ISMS:
• Ensure the ISMS can achieve its intended outcomes
• Prevent or reduce undesired effects
• Achieve continual improvement
Part 2
Plan actions to address the risk and opportunities
Plan how to integrate and implement the actions into the ISMS processes
Evaluate the effectiveness of the actions

Example risks:

- Poor leadership
- Insufficient funding to operate the ISMS
- Poorly documented information
- Lack of competence
- Inadequate management oversight

Example opportunities:

- Market differentiation
- Reduced cost of security failure

NEVER STOP IMPROVING

6.2 INFORMATION SECURITY OBJECTIVES

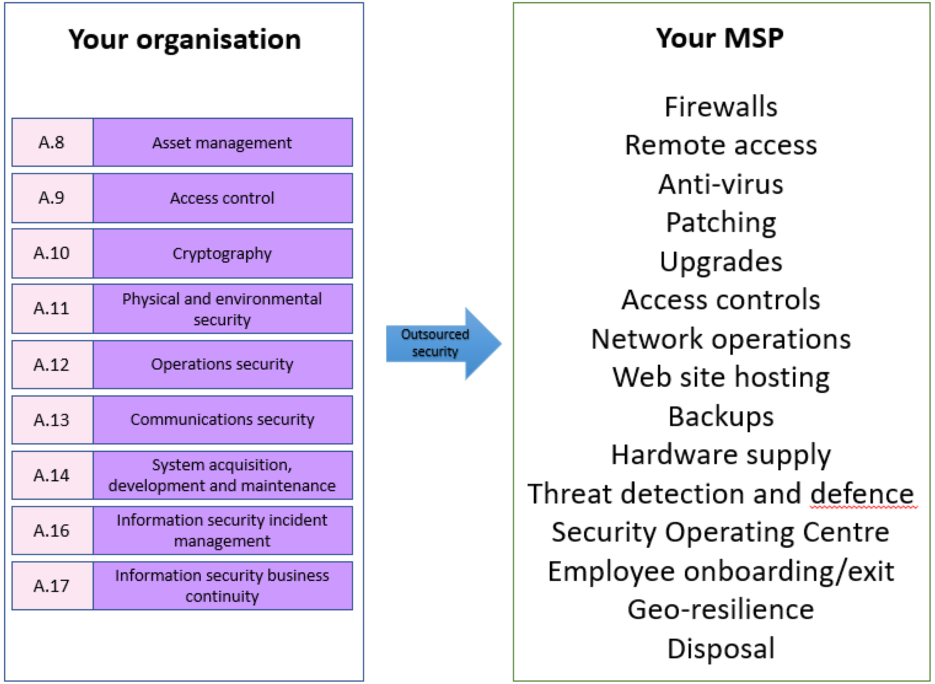
1. Must be derived from the Security Policy
2. Must take into account the risk assessment and treatment
3. Must be communicated
4. Must have plans to achieve them in place

Typical causes of non-conformities:

- A complete lack of objectives (major non-conformity)
- They are business objectives, not information security objectives
- The objectives are not consistent with the Information Security Policy
- The objectives do not take into account the information security risks
- There is a lack of resources assigned to achieve the objectives or no ownership has been assigned
- There are no plans to achieve the objectives
- There are no targets or performance metrics to monitor progress towards achievement
- Performance monitoring is not taking place, such as with Key Performance Indicators or within the Management Review

OUTSOURCED SECURITY AND MANAGED SERVICE PROVIDERS

Hold them to account



Your organisation

A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communications security
A.14	System acquisition, development and maintenance
A.16	Information security incident management
A.17	Information security business continuity

Your MSP

Firewalls
Remote access
Anti-virus
Patching
Upgrades
Access controls
Network operations
Web site hosting
Backups
Hardware supply
Threat detection and defence
Security Operating Centre
Employee onboarding/exit
Geo-resilience
Disposal

What is necessary for Clause 9.1?

The organisation shall determine what needs to be monitored and measured, including information security processes and controls

- What reporting do you receive?
- How well are the security controls performing?
- How much are they telling you?
- How many near misses?
- Are they responding to the latest threats and vulnerabilities?
- What are they contracted to provide?

> *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.**

WHAT WE COVERED

- Clause comparison between ISO 9001 and ISO 27001
- Information security risk assessment
- Information security risk treatment
- Common pitfalls
- Outsourced security and managed service providers

nqa.
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