WEBINAR: HOW TO PREPARE FOR AN ISO MANAGEMENT SYSTEM AUDIT

Tim Pinnell & Helen Barge

28/01/2022

nqa.
NEVER STOP IMPROVING

KEY INFO

- 45 minute webinar
- Questions in the chat box
- Q&A at the end
- Slides and recording circulated following webinar

YOUR PRESENTERS

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.

riskevolves

Helen Barge
Founder and MD of Risk Evolves Ltd

Helen is the friendly face of risk management and compliance. Her award-winning consultancy, Risk Evolves, helps growing businesses realise the benefits of compliance with Cyber Essentials, IASME Governance, ISO9001(Quality), ISO14001 (Environmental), ISO27001 (Information Security) and ISO45001 (Health & Safety).

Helen's a great believer that consultants should 'practice what they preach'. Not only is Risk Evolves certified to ISO9001, it was also the first business NQA certified to both ISO27001 and ISO27701 (the Data Privacy extension).

As well as supporting clients with compliance and risk management projects, Helen is a popular speaker and trainer. She also represents the needs of growing British businesses on several committees, including the FSB and the West Midlands Cyber Resilience Centre.

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.

nqa.

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 specialise in management systems certification for:

QUALITY

AEROSPACE (QUALITY)

AUTOMOTIVE (QUALITY)

ENVIRONMENT

ENERGY

HEALTH AND SAFETY

INFORMATION RESILIENCE

FOOD SAFETY

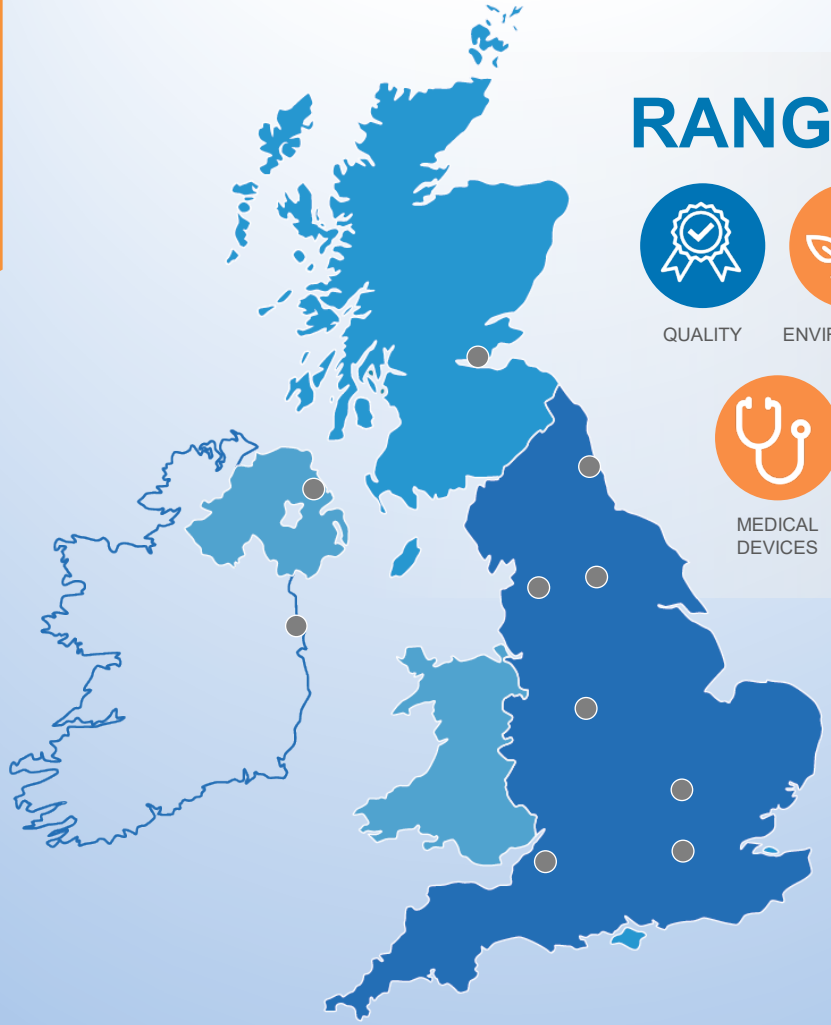
RISK MANAGEMENT

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.

What do we do?

- Risk Management
- Data Privacy
- Information Security
- Environmental, Social & Governance
- ISO Certifications
- Health & Safety

Resilience through effective Risk Management

www.riskevolves.com

PREPARING YOUR **BUSINESS** FOR
THE FUTURE

> *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

- The benefits of ISO management system certification
- Annex SL standards and PDCA
- The audit cycle
- Your auditor's audit expectations
- Preparing for the audit
- The audit
- Participating in the audit
- Post-audit and dispute resolution

nqa.
NEVER STOP IMPROVING

THE BENEFITS OF ISO MANAGEMENT SYSTEM CERTIFICATION

Who and what is ISO

- Global organisation
- Internationally agreed specifications
- Management Systems
- Designed to manage risk
- Oversee regular reviews
- Interlocks with national organisations

Why adopt and ISO Certificate

- To support good corporate governance, risk and compliance management
- To provide stakeholder confidence and assurance via independent external audit
- To ensure reliable delivery of products and services
- To demonstrate a commitment to continual improvement
- To meet a ‘pre-requisite’ for some clients & markets
- To gain entry into supply chains – and remain!
- To deliver cost reductions

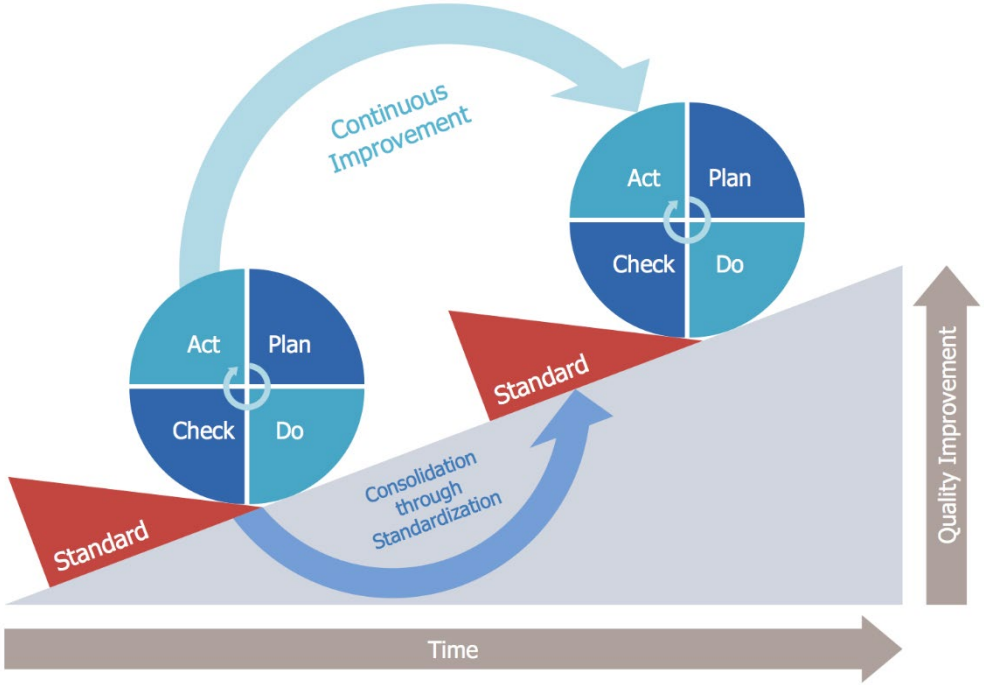
www.riskevolves.com

PREPARING YOUR BUSINESS FOR THE FUTURE

nqa.
NEVER STOP IMPROVING

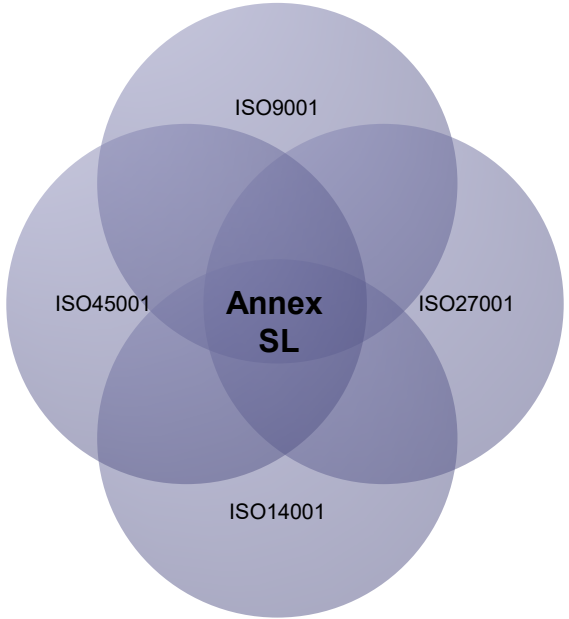
ANNEX SL STANDARDS AND PDCA

Principle – Continuous Improvement



Integration with other standards

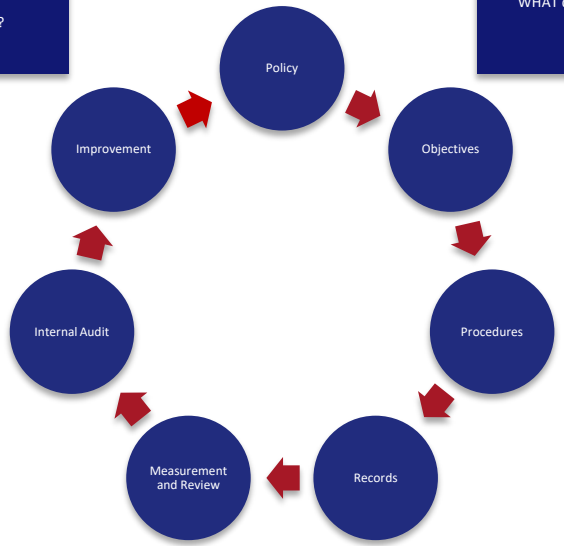
- ISO9001:2015, ISO14001:2015, ISO27001:2013 and ISO45001:2018 have all adopted Annex SL
- Provides common structure between standards and other schemes
- Significant focus on risk management across the enterprise aligned with ISO31000
- Allows for easier integration as elements can be shared



Policy, Objectives and procedures

Improvement :
How do we continue to improve ?

Policy :
WHAT does the organisation want to achieve ?



Internal Audit :
Are we doing what we said we would do and is it done consistently ?

Objectives :
HOW will the organisation achieve the policy ?

Measurement and Review
WHAT actions should we take based on what the data is telling us ?
Corrective Actions

Procedures :
Customer Related Processes
Purchasing
Risk Mgmt / Interested Parties
Internal Audit
Non Conforming Product
Control of Records etc....

Records :
WHAT data can be collect to evidence what we do?

www.riskevolves.com

PREPARING YOUR BUSINESS FOR THE FUTURE

nqa.
NEVER STOP IMPROVING

THE AUDIT CYCLE

INITIAL AUDIT

Stage 1

Is the client ready for Stage 2?

YES

Stage 2

Is the management system implemented and effective?

YES

STAGE 1

Stage 1

- Mandatory documentation check
- Areas of Concern
- Recommendation to proceed to Stage 2

Clauses

- Scope of the ISMS (clause 4.3)
- Information security policy and objectives (clauses 5.2 and 6.2)
- Risk assessment and risk treatment process (clause 6.1.2 & 6.1.3)
- Statement of Applicability (clause 6.1.3 d)
- Risk treatment plan (clauses 6.1.3 e and 6.2)
- Risk assessment report (clause 8.2)

Mandatory records

- Records of training, skills, experience and qualifications (clause 7.2)
- Monitoring and measurement results (clause 9.1)
- Internal audit program (clause 9.2)
- Results of internal audits (clause 9.2)
- Results of the management review (clause 9.3)
- Results of corrective actions (clause 10.1)
- Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

STAGE 2

ISO Clauses

4: Context of the organisation

5: Leadership

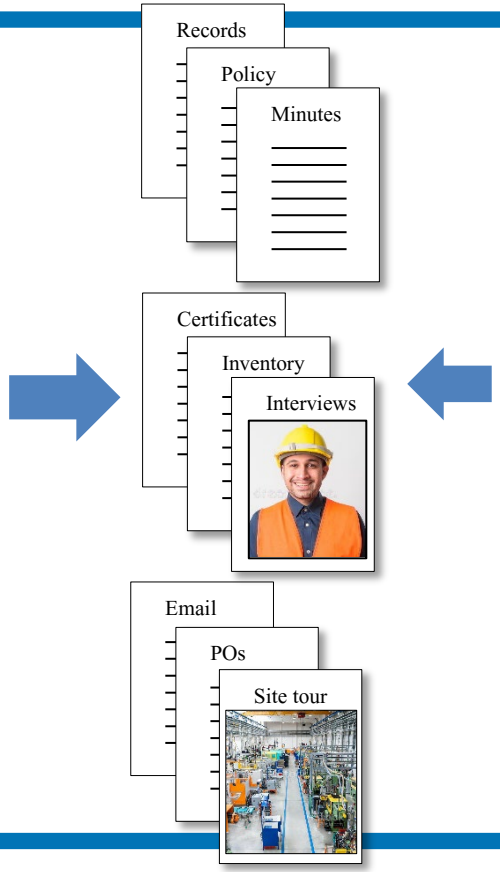
6: Planning

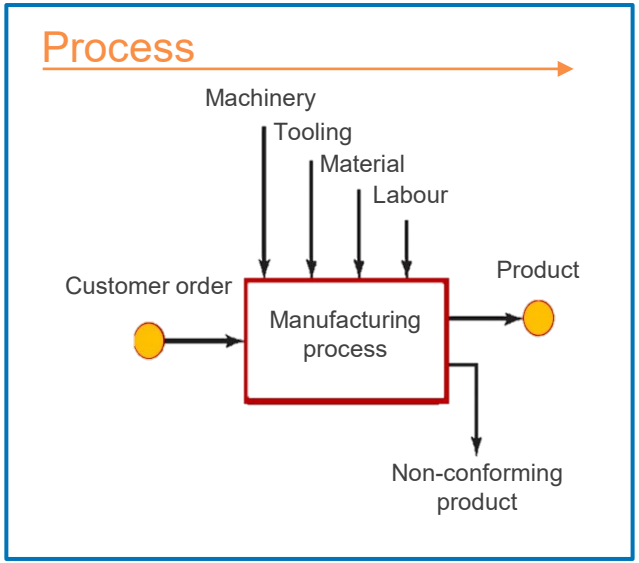
7: Support

8: Operation

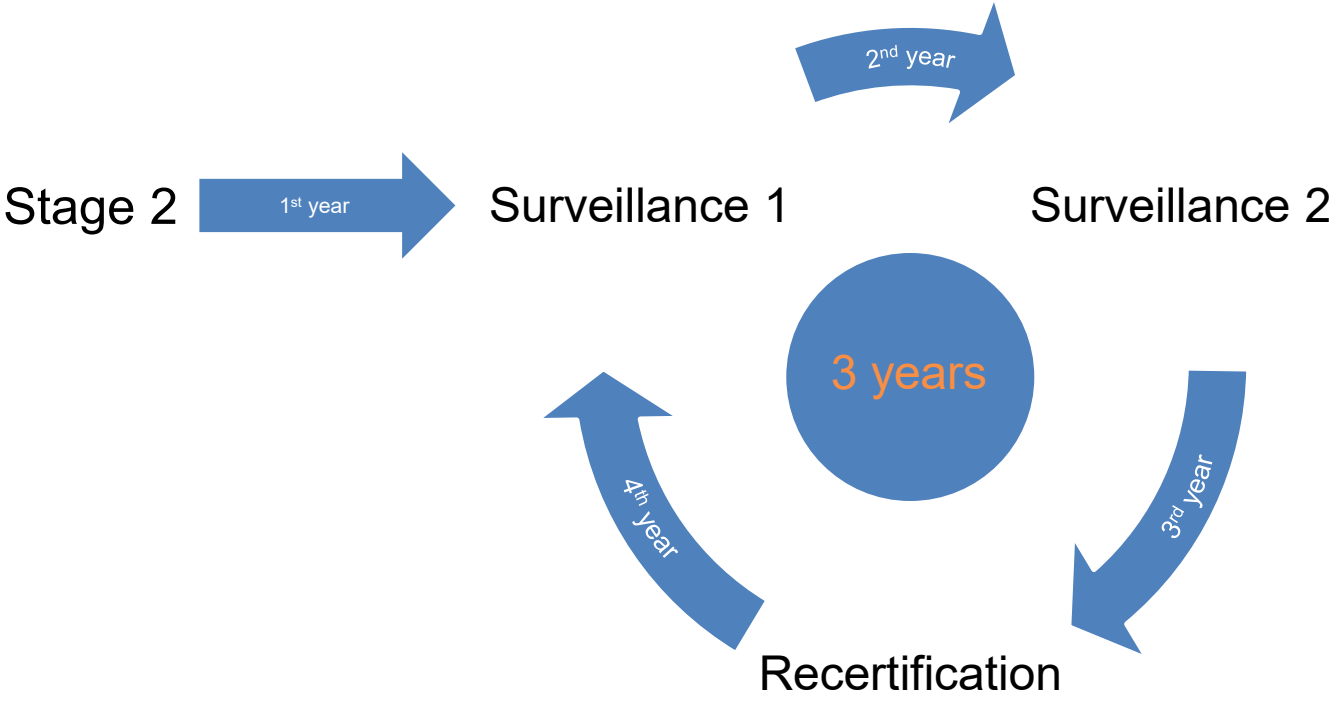
9: Performance evaluation

10: Improvement





SURVEILLANCE AND RECERTIFICATION



nqa.
NEVER STOP IMPROVING

YOUR AUDITOR AND THEIR AUDIT EXPECTATIONS

AUDITOR CHARACTERISTICS

ISO 17021

Requirements for bodies providing audit and certification of management systems

a) Ethical
b) Open-minded
c) Diplomatic
d) Observant
e) Perceptive
f) Versatile
g) Tenacious
h) Decisive
i) Self-reliant
j) Professional
k) Morally courageous
l) Organised

EVIDENCE

1. No mandatory requirement? Still need evidence!
2. The standard is your friend
3. Tell me then show me
4. Provide in-date evidence
5. Provide relevant evidence
6. Be explicit
7. Beware auditors' luck
8. But don't worry too much about simple Minor NCs
9. Interviews
10. Wandering eyes

Clause 4.3

When determining the scope the organisation **shall** *consider* the external and internal issues referred to in 4.1, the requirements referred to in 4.2 and interfaces and dependencies between activities performed by an organisation and those that are performed by other organisations. The scope **shall** be available as documented information

Clause 7.5.1

The organisation's management system **shall** include documented information required by this standard and documented information determined by the organisation as being necessary for the effectiveness of the management system

nqa.
NEVER STOP IMPROVING

PREPARING FOR THE AUDIT

What will the Auditor expect to see?

Intent

- Support from ‘Top Management’, ‘tone from the top
- Clear Policy & Objectives, cascaded through the organisation
- Interview top management

Implementation

- Evidence of the Integrated Quality Management System in operation
- Knowledgeable staff
- Record keeping

Effectiveness

- Improvement & corrective actions
- 12+ weeks data
- Management review
- Internal Audit

Preparing for your Audit

12 weeks before:

- Conduct an internal audit
- Review and validate that the scope is appropriate
- Review your previous audit report for findings, recommendations
- Check the date of your audit!

8 weeks before:

- Conduct a Management review
- Confirm Auditor availability and audit agenda with the certification body
- Arrange interviews with staff
- Check status of actions

4 weeks before

- Confirm Auditor and ask for any requirements (remote, onsite, access needs, dietary requirements)
- Communicate to organisation, remind people where documentation is
- Check documentation is accessible
- Check meeting notices, availability and room bookings

1 week before:

- Arrange visitor badge, parking space
- Provide directions to auditor
- Return agenda to auditor with names for interviews and confirmed timing
- Organise coffee, biscuits and lunch!

www.riskevolves.com

PREPARING YOUR BUSINESS FOR THE FUTURE

nqa.
NEVER STOP IMPROVING

THE AUDIT

THE AUDIT PLAN

Day 1		Day 2	
0900	Opening Meeting	0900	Opening meeting
0915	Review of previous findings	0915	Manufacturing processes
0945	Context of the organisation (4)		
1030	Leadership (5)	1030	Customer support
1115	Planning (6)		
1200	Lunch	1200	
1300	Support (7)	1300	Site tour
1400	Operations (8)	1400	Finance processes
1500	Performance evaluation (9) Continual Improvement (10)	1500	Report writing
1600	Report writing		
1700	Interim closing meeting	1700	Closing meeting

Stage 1 AoC

The organisation has not planned an internal audit programme that would provide information that the management system conforms to the requirements of the standard.

Stage 2 Finding

Documentation reviewed: Internal Audit Plan 22-23 v1.xlsx.

- Programmes internal audits against procedural requirements and system arrangements.
- Confirmed that the Audit Plan suitably ensures internal audit against the requirements of the ISO standard.
- Confirmed that the Audit Plan covers all sites including suitable risk-based sampling of operational sites.

NON-CONFORMITIES

1. Is the management system implemented and effective?
2. Auditors try to prove conformity; non-conformities are a side-effect

Stage 1

- Area of Concern

Stage 2, Surveillance, Recertification

- Opportunity for Improvement
- Minor NC
- Major NC

Minor: does not affect the capability of the management system to achieve the intended results

Major: affects the capability of the management system to achieve the intended results

MAJOR VS MINOR

Management Review (ISO 27001)

Top management **shall** review the management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The review **shall** include:

a) Status of actions from previous meetings
b) Changes in internal and external issues
c) Feedback on the performance including
    1) Nonconformities and corrective actions
    2) Monitoring and measurement results
    3) Audit results
    4) Fulfillment of objectives
d) Feedback from interested parties
e) Results of risk assessment and risk treatment plans
f) Opportunities for continual improvement

Major Non-Conformity

No management review has taken place, or the organisation cannot present any evidence to show that it has taken place.

Certification cannot be recommended or certification could be suspended / withdrawn

Minor Non-Conformity

The management review has taken place but mandatory item 'fulfilment of objectives' was not discussed, or there is no evidence to show that it was discussed.

Certification can be recommended unless there is a trend with sufficient volume that suggests the management system is not performing as expected

DISAGREEMENTS

- Non-conformities are an enabler of continuous improvement
- Clear communication in both directions
- Your organisation is unique
- Please don’t take offence, it’s not personal
- You should expect a consistent audit experience
- The auditor’s decision is final..
- But you can appeal

nqa.
NEVER STOP IMPROVING

PARTICIPATING IN THE AUDIT

Managing your Auditor

- Be Polite !
- Be honest and provide facts, explain the process you follow
- Be prepared to challenge
  - Tell the auditor if the question is not within your area of responsibility
  - Ask the auditor to re-phrase the question if you don't understand what they are asking
  - Pause the Audit if you can't resolve disagreements
- Remember:
  - They are only human and don't know your business as well as you do
  - They cannot provide consultation but …
  - It's an opportunity to pick their brains on what they see elsewhere

nqa.
NEVER STOP IMPROVING

POST-AUDIT

NEXT STEPS

- Closing meeting
- Minor NCs
  - 90 days to return CAP
  - Corrective actions inspected at next audit
- Major NCs
  - 10 days to return CAP
  - May require a special visit to confirm closure

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 | | www.nqa.com