



National Security Inspectorate

Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY

E: nsi@nsi.org.uk | W: nsi.org.uk

Security.Improved

Remote Audit Guidance

for NSI Systems approved companies

As an alternative to more traditional on site auditor visits, where circumstances permit NSI will offer a "remote audit" option. It is not suitable for all audits, however it is now supported by reliable communications tools making it, in most cases, a straightforward and effective process.

Under certain circumstances, approved companies may be offered a "remote audit" in place of a physical "on-site" audit. To be eligible for remote audits companies must:

- Have held NSI approval for the scheme being audited for a minimum of two years.
- Have the technical capability to participate in an effective remote audit.
- Have the relevant persons available to participate in the remote audit.
- Be able to share data and information in a format that facilitates an effective and efficient audit.
- Not have had any significant changes within the company that may affect the required audit duration, audit programme or scope of approval since the last audit.
- Have demonstrated a consistent track record of satisfactory performance of their quality management system and adherence to all applicable requirements of their scope of approval.

Please note audits involving technical site inspections are not suitable for remote audit and will require an on-site audit within the audit programme designed for each approved company.

This guidance explains the preparation you need to do before the audit, methods of remote communication that can be considered, the format of the audit itself, and the evidence NSI will expect to see during the audit.

1 Preparation

In order to complete the audit in an effective and efficient way it would be helpful if you could obtain and prepare some key documents prior to the start of the audit (see Appendix A).

If necessary, you can email documents and data to the NSI auditor a few days in advance of the audit. This will give the auditor time to review the documents. When deciding on the format of evidence to be emailed, sending several smaller files in PDF or Microsoft Word etc. is preferable. Alternatively, you may want to place relevant documentation in a specific remote audit folder the auditor can access and navigate during the audit.

Zip files are held up as a potential security risk by our email handling systems, and links to third party file transfer sites (e.g. Wetransfer.com) are also not permitted through our system.

Document no.	NSF 502	Document issue no.	2	Document issue date	May 2020
Document owner	Head of Field Operations (Systems)			Last review date	May 2020
Document classification	PUBLIC (RESTRICTED)			Page 1 of 6	

If you redact any confidential information from customer records (e.g. names, addresses, telephone numbers and confidential commercial details) for GDPR purposes, there must be a unique customer identifier available (e.g. site/contract number) in order to maintain the validity of the audit trail.

2 Remote Communication

There are a number of communication platforms that can be used to conduct the audit. NSI's default platform is "Skype for Business". It does not require you to have Skype for Business installed on your device, merely to have internet access, and a device with a microphone and speakers. If using a device without speakers or microphone, a mobile phone can be used in conjunction with screen sharing.

If you wish to use a platform other than "Skype for Business", such as "Microsoft Teams", please contact your auditor to arrange.

If Skype for Business is used, your auditor will send you a meeting invitation through Microsoft Outlook, which will appear in your inbox as an email. Upon opening the email you have the option to Accept, Reject or Decline the meeting request. Accepting this should add the audit appointment into your calendar complete with a link to access an online meeting.

To access the meeting at the agreed time single click the "Join Skype Meeting" hyperlink. You will be directed to the cloud based Skype application that will facilitate your access. It will enable you to share your desktop and enable voice communication with the auditor.

Note: Please test your microphone and speaker set up in advance of the audit.

The remote audit process is heavily reliant upon good levels of connectivity. If, for whatever reason, this is poor, or you have difficulty sharing your desktop control for the auditor to navigate your system, or if adding documents and media proves time consuming, then required documentation should be emailed to the auditor in advance of the meeting.

You may experience issues with connectivity that may delay the displaying of information on your or the auditor's desktop. Stopping and restarting the displaying of a desktop can often resolve these issues.

In extreme circumstances, it may require leaving and re-joining the meeting. Similarly, the opening and viewing of attachments may freeze or take an excessive time. Downloading these rather than opening may assist progress of the audit.

If the technical difficulties frustrate the audit process, the auditor may utilise email and telephone to continue the audit, however, if the audit is frustrated too much, the auditor may determine the audit should be rescheduled.

Your auditor will contact you in advance of the audit to test connectivity and capability and confirm the remote audit can take place.

Document no.	NSF 502	Document issue no.	2	Document issue date	May 2020
Document owner	Head of Field Operations (Systems)			Last review date	May 2020
Document classification	PUBLIC (RESTRICTED)			Page 2 of 6	

3 Audit

3.1 Opening meeting

The auditor will conduct the opening meeting. This will confirm the intended aspects to be covered and will ensure you are able to:

- Share your desktop within the meeting so evidence can be displayed and reviewed.
- Add documents and media to the meeting for the auditor to review.
- Grant control of your desktop to the auditor so they may navigate your PC.
- Confirm email addresses should samples be required to be sent for examination.

3.2 Audit Evidence

Evidence can be provided at the time of audit or in advance. Should evidence be provided in advance the auditor will be able to review this without requiring your full time attendance.

The auditor will agree relevant timings with you for periodic updates, to review findings and for any additional information to be requested.

3.3 Closing meeting

Once the audit has been completed the auditor will conduct a closing meeting to brief you on the audit findings and take you through any Improvement Reports that have been raised. These will be available through the NSI Website as usual and will require a response within 21 days of the audit.

The auditor will grant you control of their laptop at which point you should sign for the audit using your mouse. If you are unable to sign the audit report in this way then an email will be sent detailing the audit findings, and you should reply with your acceptance of the audit findings.

4 Audit topics

Appendix A details the sample audit topics and some of the typical audit evidence the auditor will need to review during the audit. It is appreciated that, due to the current situation, it may not be possible for some of the information to be available.

Document no.	NSF 502	Document issue no.	2	Document issue date	May 2020
Document owner	Head of Field Operations (Systems)			Last review date	May 2020
Document classification	PUBLIC (RESTRICTED)			Page 3 of 6	

APPENDIX A

TOPIC	EVIDENCE
Quality Management System	<ul style="list-style-type: none"> The Quality Management System documentation including the quality policy and quality objectives.
Risk & Opportunities	<ul style="list-style-type: none"> The company assessment of quality risks and opportunities.
Management Review	<ul style="list-style-type: none"> Evidence of management system review.
Internal Audit of the quality management system	<ul style="list-style-type: none"> The current internal audit schedule. A sample of internal audit reports together with their investigations, root cause analysis and corrective actions (where applicable).
Engineer/product audits	<ul style="list-style-type: none"> The current product audit schedule. A sample of product audit reports together with their investigations, root cause analysis and corrective actions (where applicable).
Competency and training	<ul style="list-style-type: none"> A sample of current records of employee competencies and training.
Customer Satisfaction and complaints	<ul style="list-style-type: none"> Records of the measurement of customer satisfaction. Records of any customer complaints together with records of their investigation, corrective action and resolution.
Monitoring and measuring resources	<ul style="list-style-type: none"> Records of calibration for the equipment used by the company (i.e. Digital multi-meters, insulation testers and sound pressure level meters as applicable).
Security Screening (where applicable)	<ul style="list-style-type: none"> Where you have recently employed new staff in relevant employment, the complete records of security screening to BS 7858:2019 code of practice.

Document no.	NSF 502	Document issue no.	2	Document issue date	May 2020
Document owner	Head of Field Operations (Systems)			Last review date	May 2020
Document classification	PUBLIC (RESTRICTED)			Page 4 of 6	

Use of logos and certification marks	<ul style="list-style-type: none"> Examples of the use of NSI, UKAS and, where applicable, BAFE logos on company documentation and web/media sites.
System design, installation and commissioning processes	<p>Where possible, records of the enquiry, design, installation and commissioning processes of two recently installed systems (I&HS, CCTV, Access Control & FD&A as applicable).</p> <p>Records to be provided include:</p> <ul style="list-style-type: none"> ➤ Risk assessment/site location survey notes. ➤ System Design Proposal (SDP)/quotation. ➤ Customer acceptance/order placement. ➤ As Fitted Specification (if changed from SDP above). ➤ Commissioning certificate/checklist. ➤ Record of operational checks. ➤ Handover certificate/customer acceptance. ➤ NSI Certificate of Compliance/BAFE certificate of compliance.
Preventive Maintenance	<ul style="list-style-type: none"> Previous 6 months preventive maintenance monthly achievement statistics. The scheduling records for three customers who have had a contracted routine maintenance carried out in the last 6 months prior to the audit. The preventive maintenance records for the three customers above.
Corrective Maintenance	<ul style="list-style-type: none"> Previous 6 months corrective maintenance response time statistics for 4-hour response for intruder and hold up alarm systems and/or 8-hour response for fire systems. Records of the corrective maintenance process (time of call, time of response, dockets) for three recent 'call outs' where an engineer response to site has been required.

Document no.	NSF 502	Document issue no.	2	Document issue date	May 2020
Document owner	Head of Field Operations (Systems)			Last review date	May 2020
Document classification	PUBLIC (RESTRICTED)			Page 5 of 6	

False Alarm Management	<ul style="list-style-type: none"> • Intruder False Alarm Management statistics (also known as "P" figures as per BS 8473) for the past six months. • The number of remotely monitored systems that have lost response and are currently awaiting reinstatement (where applicable). • Details of a customer that has lost police response and include: <ul style="list-style-type: none"> ➤ time and date of the three false alarms; ➤ confirmation of how these were reset (either remotely or in attendance); ➤ the engineer report for attendance; ➤ the police withdrawal letter date; ➤ the date from which time the response level drops; and ➤ evidence of you informing the ARC of the change in police response level for the customer. • If no systems are "off response" then examples of any false alarm activation and the company actions would suffice.
------------------------	---

Document no.	NSF 502	Document issue no.	2	Document issue date	May 2020
Document owner	Head of Field Operations (Systems)			Last review date	May 2020
Document classification	PUBLIC (RESTRICTED)			Page 6 of 6	