Oxebridge Q017

Quality Management System Certification Audit - Remote Auditing Methods

Ver. 1.1

To verify the latest published edition of this standard, visit: www.oxebridge.com/standards

If you are interested in offering Oxebridge Q001 certification, contact Oxebridge today by writing to accreditation@oxebridge.com .

Oxebridge Quality Resources International LLC
Tampa FL USA | Lima PERU
www.oxebridge.com

Table of Contents

1.0 Purpose 2
2.0 References 2
3.0 Terms and Definitions 2
4.0 Overview 3
5.0 Requirements 4
5.1 General Requirements for Both Parties 4
5.2 General Requirements for the CB 4
5.3 Technical Requirements for the CB 4
5.3.1 General Technical Requirements 4
5.3.2 Conducting Verbal Interviews 5
5.3.3 Conducting Text-Based Interviews 6
5.3.4 Collecting Photographic or Prerecorded Video Evidence 6
5.3.5 Collecting Live Video Evidence 7
5.3.6 Collecting Electronic Records 8
5.3.7 Collecting Evidence via CMS Portals 8
6.0 Guidance 9
6.1 Overview 9
6.2 Options for Verbal Interviews (VOIP and Telephony) 9
6.3 Options for Text-Based Communications 9
6.4 Options for Photographic or Prerecorded Video Evidence 10
6.5 Options for Live Video Evidence 10
6.6 Options for Electronic Record Sharing / Email 10
6.7 Options for CMS Portals 11
6.8 Options for Electronic File Deletion 11
6.9 Notes on the Use of TOR 12
6.10 Notes on the Use of VPN 12
7.0 Best Practices 13
7.1 Overview 13
7.2 Best Practices for Verbal Interviews (VOIP and Telephony) 13
7.3 Best Practices for Text-Based Communications 13
7.4 Best Practices for Photographic or Prerecorded Video Evidence 14
7.5 Best Practices for Live Video Evidence 16
7.6 Best Practices for Electronic Record Sharing / Email 16
7.7 Best Practices for CMS Portals 17
7.8 Best Practices for Electronic File Deletion 17
7.9 Best Practices on the Use of TOR 17
7.10 Best Practices on the Use of VPN 17
8.0 Setting Up RAM Methods Prior to Audit 18

Revision History Table

Ver.	Effective Date	Nature of Changes
1.0	15 April 2020	Original release.
1.1	09 May 2020	• Sec: updated rules for streaming video evidence. • Moved details on physical security keys and data shredders to 5.3.1, removed details from other sections. • Section 5.3.7: added portal audit trail requirements. • Sections 5.3.4 and 5.3.5: Added requirements that photo and video provide sufficient coverage. • Section new section 7 on Best Practices. • Sec. 6.9: added Brave Browser as TOR option

1.0 Purpose

This document defines requirements and guidance for conducting Q001 certification audits using Remote Auditing Methods, or RAM.

NOTE: This document is not intended to ensure compliance with every security or privacy law in the nation of every user who may utilize it. The parties are solely responsible to ensure compliance with local, national and international laws.

2.0 References

Oxebridge Q001 – Quality Management System Requirements

Oxebridge Q002 – Quality Management System Certification Audit Minimum Evidence Requirements

Oxebridge Q003 – Quality Management System Certification Audit Requirements

Oxebridge Q006 – Quality Management System Certification Body Accreditation Requirements

3.0 Terms and Definitions

Reference Q005. Other terms and abbreviations:

2FA – Two Factor Authorization

CMS – Content Management System (sometimes referred to as “portals”)

E2EE – End to End Encryption

EAR – Export Administration Regulations (US)

GDPR – General Data Protection Regulation (UK)

HIPAA – Health Information Portability and Accountability Act (US)

ITAR – International Traffic in Arms Regulation (US)

P2P – Peer to Peer

RAM – Remote Auditing Methods (for this document "RAM" does ***not*** refer to Remote Access Memory)

SMS – Short Messaging Service

TOR – The Onion Router (network)

VOIP – Voice Over Internet Protocol

Controlled Information: information in any form that is subject to the client organization's restrictions, typically per statute or regulation (i.e, EAR, ITAR, HIPAA, GDPR, etc.)

Control Requirements – the requirements applicable to the client organization related to controlled information release or use, typically per statute or regulation (i.e., EAR, ITAR, etc.)

4.0 Overview

This document provides both requirements and guidance for conducting audits using RAM. Where requirements are listed (in section 5.0 below), these are mandatory for any accredited Q001 certification body; failure to comply may lead to de-accreditation. For the guidance suggestions (in sections 6.0 and 7.0 below), these are suggestions for best practice and not mandatory.

It is understood that the Practical Audit portion is the step most likely where RAM will be utilized or required; the preliminary audit steps (Incident Investigation, Customer Feedback Review, etc.) are unlikely to require the use of RAM since these involve the client organization submitting information over traditional email. If the client wishes to impose additional security restrictions on the sending of that information, it may do so, and negotiate this with the CB.

RAM may be necessitated by any condition established by the client organization or the CB. This may include:

- Physical access limitations of the client organization's facilities due to emergency, weather event, disaster, pandemic, or any other legitimate reason.
- Remote organization locations in regions out of the normal service region of the accredited CB.
- The bulk of the work done by the client organization consists of intellectual property development or some other "soft" service which is well suited for RAM auditing, and where performing an on-site audit provides little value.

Where this document refers to "controlled" information, this shall mean information subject to regulatory, statutory or other controls, such as ITAR, EAR, HIPAA, GDPR, etc.

It is understood that RAM shall be used for two primary functions:

- **Conducting Interviews:** verbal testimony is a key form of evidence for any conformity assessment audit. The use of RAM facilities the exchange of verbal information, but must not expose the parties to leakage of confidential information, trade secrets or other controlled information in the process.
- **Evidence Gathering:** client organizations must submit evidence to prove their conformity to Q001, in accordance with the minimum evidence requirements established in Q002. This includes the submission of documents and records. RAM must ensure that such information is not accessed by an unauthorized party or in an unauthorized manner, as that could expose the parties to legal risks and potential crimes.

5.0 Requirements

5.1 General Requirements for Both Parties

The decision to utilize RAM shall be negotiated between the client organization and the CB during the initial audit contract development and audit planning, per Q003. Both parties – the organization and the CB – shall agree to the use of RAM. If either party disagrees, then RAM shall not be used, and a physical audit performed during the Practical Audit stage.

While this document attempts to be comprehensive, it is understood that methods and technology advance rapidly. Both parties shall not take any actions to circumvent the controls defined herein, or take any actions which would violate the intent to protect controlled information, whether or not specific rules are defined in this document.

5.2 General Requirements for the CB

Use of RAM by the CB shall only be used if all other accreditation requirements of Q006 are simultaneously met, including those for confidentiality and impartiality.

RAM may ***not*** be utilized during the Practical Audit when the client organization has opted for a Deep Dive audit.

The use of RAM shall ***not*** be a justification for the reduction of audit time as prescribed in Q007. The full required audit time ***must*** be completed whether or not RAM is used.

5.3 Technical Requirements for the CB

5.3.1 General Technical Requirements

The CB shall have the technical expertise to install, implement, maintain and update necessary technology related to the use of RAM. This shall include:

a) obtaining and maintaining suitable software licenses, registration keys, privacy keys, passwords, authorized user accounts, etc., as applicable to the RAM;

b) prohibiting the use of non-licenses (pirate) software related to RAM;

c) obtaining and maintaining suitable hardware necessary for the use of RAM, including computers, servers, internet access devices, hubs, firewalls, etc.;

d) obtaining and maintaining suitable methods and tools to prevent the unintended or unauthorized release of intellectual property, confidential information, trade secrets or other controlled information transmitted between the parties when using RAM;

e) utilizing appropriate staff with the necessary training, skills and education to utilize RAM;

f) ensuring staff have the applicable nationality, security clearance and other requirements applicable to the use of RAM to ensure compliance with the particular client organization's requirements;

g) ensure that whichever RAM techniques are used, the information passes through servers in countries that are not prohibited by the client organization's requirements or regulatory/statutory requirements;

h) ensure that where cell phone or other mobile devices are used which rely on cellular connectivity, that the cell service provider does not have services or applications which may override the other security measures mentioned herein.

i) ensure that any devices used are up to date and current on latest virus definitions and firewall rules, and that such protections are active;

j) ensure that controls extend to personal devices used, and not merely those owned and managed by the CB itself; if this is not possible, then the CB shall provide auditors or other staff with the necessary equipment conduct RAM-based audits in compliance with this document;

k) ensure that personal assistant devices (i.e, Google Assistant, Siri, Cortana, Bixby) are turned off and not capable of "listening" during RAM-based conversations;

l) prohibit the use of CB-owned or managed applications, portals or databases which may retain controlled information in a manner that violates the other requirements herein;

m) where physical security keys are used, these shall comply with FIDO U2F Open authentication standard at least;

n) Where digital data deletion programs ("data shredders") are used, these shall provide for permanent deletion using three-pass US Dept. of Defense 5220.22-M compliant algorithms when the data is stored on hard drives only, or NIST 800-88 compliant algorithms for either hard drives or solid state drives.

5.3.2 Conducting Verbal Interviews

When using RAM to conduct verbal interviews with client organization representatives, the CB:

a) ***Shall*** confirm with the client organization if any verbal information will include intellectual property, confidential information, trade secrets or other controlled information that would necessitate special RAM considerations. If not, then traditional telephony methods (landline, cellular or VOIP) may be used to communicate this information. If RAM is determined necessary, then the requirements in sections 5.3.2.(b) through (d) shall be met.

Note: in very few cases would spoken information be sensitive enough to disallow traditional telephony.

b) ***Shall*** utilize a secure Voice Over IP (VOIP) service that allows for End-To-End Encryption (E2EE), and that prohibits the access of the call by anyone other than the caller and receiver. This must prevent interception or access to the call by the VOIP provider itself, as well as any servers the call routs through.

c) ***Shall not*** utilize any image or file sharing features within the call without first ensuring compliance with the other applicable requirements for collecting evidence via RAM within this document.

d) ***Shall not*** allow any nonauthorized third parties or individuals not relevant to the audit to overhear or participate in the call.

5.3.3 Conducting Text-Based Interviews

When using RAM to conduct text-based interviews ("chat") with client organization representatives, the CB:

a) ***Shall*** confirm with the client organization if any text-provided information will include intellectual property, confidential information, trade secrets or other controlled information that would necessitate special RAM considerations. If not, then traditional text methods (SMS, commercial instant messaging app, etc.) may be used to communicate this information. If RAM is determined necessary, then the requirements in section 5.3.3(b) through (f) shall be met.

b) ***Shall*** utilize a secure messaging service that allows for End-To-End Encryption (E2EE), and that prohibits the access of the content of the message by anyone other than the sender and receiver. This must prevent interception or access to the message by the messaging service provider itself, as well as any servers the message routs through.

c) ***Shall*** utilize a service that also provides for auto-deletion of messages ("disappearing messages"). Such auto-deletion must not only be on the devices involved, but also the text message service provider servers.

d) ***Shall not*** utilize any image or file sharing features within the call without first ensuring compliance with the other applicable requirements for collecting evidence via RAM within this document.

e) ***Shall not*** capture any images of the messages ("screenshot" or "screen capture".)

f) ***Shall not*** allow any nonauthorized third parties or individuals not relevant to the audit to see the information within the messages.

5.3.4 Collecting Photographic or Prerecorded Video Evidence

When using RAM to collect photographic or prerecorded video evidence from the client organization, the CB:

a) ***Shall*** include photographic evidence of sufficient coverage to provide the necessary evidence.

b) ***Shall*** utilize secure image or file sharing technology that provides E2EE protection that prohibits viewing of the image by anyone other than the CB and client organization. This must prevent interception or access to the image or video by any service providers, as well as any servers the image or video routs through.

c) ***Shall*** delete the image or video files using three-pass US Dept. of Defense 5220.22-M compliant data sanitizing ("shredding") software when the data is stored on hard drives only, or NIST 800-88 compliant data sanitizing method for either hard drives or solid state drives. Alternatively, the files may be shared using a messaging service that also provides for auto-deletion of messages ("disappearing messages"). Such auto-deletion must not only be on the devices involved, but also the messaging service provider servers.

d) ***Shall not*** attach or embed the image, nor any captured image from the video ("screenshot") in any Q001 report or document.

e) ***Shall not*** allow any nonauthorized third parties or individuals not relevant to the audit to see the image or video.

5.3.5 Collecting Live Video Evidence

When using RAM to collect live ("streaming") video evidence, including videoconferencing streams, and including those that may allow for screensharing, document exchanges and file transfers, from the client organization, the CB:

a) ***Shall*** include videographic evidence of sufficient coverage to provide the necessary evidence.

b) ***Shall*** utilize secure videoconferencing technology that provides E2EE protection that prohibits viewing of the stream by anyone other than the CB and client organization. This must prevent interception or access to the stream by any service providers, as well as any servers the stream routs through.

c) ***Shall*** only allow invited participants in the stream, with a predetermined access code, password, or other control mechanism, to prevent access by unauthorized persons or the public.

d) ***Shall*** provide for all information exchanged during the stream, including any documents or data exchanged, to be deleted from the service provider's servers once the stream is ended.

e) ***Shall not*** capture any image ("screenshot") from the stream at all.

f) ***Shall not*** retain any files or documents transferred during the stream and, if required, securely delete such files using three-pass US Dept. of Defense 5220.22-M compliant data sanitizing ("shredding") software when the data is stored on hard drives only, or NIST 800-88 compliant data sanitizing method for either hard drives or solid state drives.

g) ***Shall not*** attach or embed the image, nor any captured image from the video ("screenshot") in any Q001 report or document.

5.3.6 Collecting Electronic Records

When using RAM to collect electronic records, including documents, as evidence from the client organization, the CB:

a) ***Shall*** utilize secure email services or secure file sharing technology that provide E2EE protection that prohibits accessing the files by anyone other than the CB and client organization. This must prevent interception or access to the information by any service providers, as well as any servers the information routs through.

b) ***Shall***, when using email providers for the transfer or electronic records, utilize two-factor authorization or physical keys when accessing the email account, to ensure the actual users are accessing the accounts.

c) ***Shall*** delete the file using three-pass US Dept. of Defense 5220.22-M compliant data sanitizing ("shredding") software when the data is stored on hard drives only, or NIST 800-88 compliant data sanitizing method for either hard drives or solid state drives.

5.3.7 Collecting Evidence via CMS Portals

When using a content management system (CMS) portal developed by the client organization for which it has been granted temporary access, the CB:

a) ***Shall*** ensure it follows all client instructions on access and use of the portal

b) ***Shall not*** capture any image ("screenshot") from the portal at all.

When using a CMS that it has developed for client evidence gathering, the CB:

c) ***Shall*** ensure the portal requires password authenticated logins of all users, preferably with two-factor authorization.

d) ***Shall*** ensure the client organization may only view information related to itself and its account, and not that of any other CB client.

e) ***Shall*** ensure the portal provides full audit trail of logins, file view and access, and IP address of users.

f) ***Shall*** ensure the information residing on the portal is encrypted to those not logged in.

g) ***Shall*** ensure that client passwords and access credentials are deleted within 24 hours of the last required session.

h) ***Shall*** ensure the portal itself is hosted by a server or company capable of meeting the other security requirements named herein.

i) ***Shall*** ensure that information or files deleted from the portal are permanently deleted in a manner that prohibits them from being revived.

6.0 Guidance

6.1 Overview

The following section provides guidance on how to comply with the requirements set forth in section 5.0 above. This guidance is recommended, but not mandatory.

References to any third-party providers does not mean the provider is endorsed by Oxebridge. Furthermore, features and applications change over time, and may fall out of compliance after publication of this document. Users have the sole responsibility to ensure providers and applications meet the requirements of this document.

6.2 Options for Verbal Interviews (VOIP and Telephony)

Typically, traditional telephony (cell phone calls, landline calls, VOIP calls) will be sufficient for verbal exchanges, since it is difficult to pass controlled information via verbal communications.

Where such information may be passed, or where the client organization is otherwise concerned over the leak of confidential information, the CB may wish to utilize a secure VOIP solution.

Typically, standard services such as Skype do not offer sufficient end-to-end encryption of calls; some services, such as Google Duo or Hangouts, may listen in to calls in order to mine data for later advertising.

Options:

- Cellcrypt (https://www.cellcrypt.com/)
- Signal (https://signal.org/)

6.3 Options for Text-Based Communications

While not useful for long audit conversations, SMS and instant messaging platforms may occasionally be used to transmit information in brief snippets. These are often used simultaneously with voice calls, as client organizations may send information via text or instant message to the CB representative on the voice call.

Text messaging services are notorious for poor security and mining of the text information for advertising purposes. Skype, WhatsApp, Viber and traditional cell phone texting via SMS may not be sufficient for such use cases, even when using a “private message” feature. Care must be taken when selecting and using such services to ensure the messages are secure, and can be deleted securely with no chance of recovery. Some applications now offer secure auto-deletion of messages after the message has been viewed.

Options:

- Cellcrypt (https://www.cellcrypt.com/)
- Signal (https://signal.org/)

6.4 Options for Photographic or Prerecorded Video Evidence

During audits it may be necessary for the client organization to send an image or graphic as evidence, or send a prerecorded video. This information must also be protected as it may contain confidential or controlled information.

Often the same messaging applications as reference in 6.3 above may be used for this, so that guidance would apply.

Options:

- Cellcrypt (https://www.cellcrypt.com/)
- Signal (https://signal.org/)

When gathering photographic or videographic evidence, the following practices may be used:

A. Request a comprehensive floor plan of the facilities included in the management system scope.
B. Plan the intended photographic for videographic evidence by annotating the floor plan with positions where such images are to be taken, and at what angle. Number each annotated position for reference.
C. Request the auditee then submit the photos and/or videos with files that reference the annotated position numbers.

6.5 Options for Live Video Evidence

Streaming video and web conferencing is on the rise, prompted by the recent coronavirus pandemic. Unfortunately, main service providers and applications in this area typically do not comply with national or international privacy and security regulations. Skype, Zoom, Cisco Webex, GoToMeeting and others typically expose the users to risks of loss of data or breaches.

Any conferencing platform must ensure the conference “rooms” or sessions are access controlled (perhaps through a password, event ID or entry key), to prevent unauthorized users from attending or “bombing” the session. The communications must be end-to-end encrypted, so that even if the information travels in countries not covered by applicable regulations, no one but the intended recipients can view the information.

Options:

- Signal (https://signal.org/)

6.6 Options for Electronic Record Sharing / Email

Email remains a critical way to share data. CBs should resist using email to gather audit evidence, as the email messages and attachments are typically viewable at any stage along the message’s transit from sender to recipient. True end-to-end encryption of email is uncommon, despite claims by a given provider. Emails received on cellular devices are then further at risk of data loss.

Use of email should ensure the messages are fully encrypted throughout transit, that no server records remain of the messages after they are sent, and that deletion of the email ensures it is unrecoverable. Providers should offer two-factor authorization for each login, to ensure the person intended to receive the email is actually accessing the account.

Options:

- Proton Mail (https://protonmail.com/)
- Mail2Tor (https://mail2tor.com/)
- Posteo (https://posteo.de/en)

6.7 Options for CMS Portals

The use of Content Management System portals such as Sharepoint or Dropbox has grown in popularity. Typically these are used internal to the organization, but present risks when allowing outside access, such as a CB auditor or other third-party. Care must be used when selecting such portals.

Where the client organization grants access to the CB auditors to their portal, the responsibility for security and privacy thus resides primarily with the client organization. The CB need only follow the instructions for use by the client organization, while ensuring they do not breach any other requirements herein.

In some cases, the CB may elect to establish their own such portal for use by client organizations. This is discouraged by Oxebridge. Web-based applications such as OneDrive, Google Drive, Dropbox, Bluejeans, Box.com, MS Teams, Google Hangouts and others typically do not secure the files sufficiently to allow compliance with key regulations such as ITAR; some may offer add-on services to ensure this, but these must be carefully researched.

However, the following options may allow a CB to set up a client portal and still remain compliant with the necessary regulations.

Options:

- RegDOX (https://www.regdox.com/)
- Microsoft Azure Government (https://azure.microsoft.com/en-us/global-infrastructure/government/)
- Microsoft Office 365 US Government for Defense (https://www.microsoft.com/en-us/microsoft-365/government/compare-office-365-government-plans)
- Box for Government (https://www.box.com/industries/government)
- Google GSuite with Virtru (https://www.virtru.com/)

6.8 Options for Electronic File Deletion

Occasionally a CB may receive a file in evidence that it must delete after the information has been reviewed. Deletion of a file in a typical Windows or Apple operating system does not make the file unrecoverable, but merely makes it temporarily invisible to the user. To securely delete a file, the file’s position on the device’s memory drive or location must be rewritten with “junk data” (typically 1s and 0s) to make it unrecoverable.

In the past, hard drives could be rewritten easily with such junk data using a DOD 5220.22-M compliant “data shredder” application. The advent of solid state drives makes this more difficult, but the standard NIST 800-88 includes provisions for this. If the CB's system only comprises hard drives, then the DOD method is sufficient; if solid state drives or memory on a chip is used, then the NIST method should be used instead.

Options:

- Killdisk (https://www.killdisk.com/)
- White Canyon (https://www.whitecanyon.com/)

6.9 Notes on the Use of TOR

Privacy advocates frequently speak of TOR, or The Onion Router network. Websites and messaging services served through TOR typically require special software, and are highly secure.

TOR is, however, primarily used for privacy purposes. It is expected that the CB and client organizations are not hiding their identities from each other, to this document does not specifically advocate for the use of TOR-based solutions. However, if privacy is a concern, then most of the options and resources named here can be used simultaneously with a TOR service, or through the TOR browser.

Options

- TOR Browser (https://www.torproject.org/)
- Brave Browser - use "Private Window with TOR" option (https://www.brave.com)

6.10 Notes on the Use of VPN

"Virtual Private Networks" (or VPNs) are commonly used to protect some information on data exchanges from being viewed by telecom carriers, websites or other third parties. Typically, the use of the solutions herein that provide end-to-end encryption obviate the need for VPNs, but the use of a VPN on top of the other solutions may increase security slightly. VPNs may also allow users in one country to access systems in another country which may have instituted blocks against the user's home country.

Options

- Private Internet Access VPN (https://www.privateinternetaccess.com/)

7.0 Best Practices

7.1 Overview

The following section provides best practices when collecting evidence of each type. These are highly recommended, but not mandatory requirements.

7.2 Best Practices for Verbal Interviews (VOIP and Telephony)

When conducting verbal interviews, the following practices should be observed:

A. Ensure the connection is clear, and all parties can hear each other.

B. Utilize translators when language issues are present. Ensure the translator is approved by both the auditing body and the auditee, so that their translations can be trusted. Using certified third-party, independent translators is recommended; if so, the parties should share the cost of such translators.

C. Speak clearly, and slowly. Ensure the other party understands the comment or question.

D. Allow the other party to ask questions if they do not understand something.

E. Do not interrupt; listen intently.

F. Manage time by not allowing conversations to go off-track, get distracted, or roam into different topics.

G. Take notes, but be sure any notes do not include confidential or restricted information.

H. Destroy all notes after the audit is completed.

7.3 Best Practices for Text-Based Communications

When utilizing text-based communications, the following practices should be observed:

A. Ensure appropriate security options are enabled in the messaging applications before beginning (end to end encryption, etc.)

B. Be conscious of message length limits, and do not send long messages that exceed these limits. The other party may not receive the entire message, and the sender may not get any alert telling them of this fact.

C. Type clearly and correct any errors before sending.

D. Avoid using internet jargon, shorthand or abbreviations (“LOL,” “AFAIK,” etc.) as they may not be understood by the other party.

E. Avoid using emojis (emoticons) (“ 😉 ”)as they may not be understood by the other party, or may not be received at all.

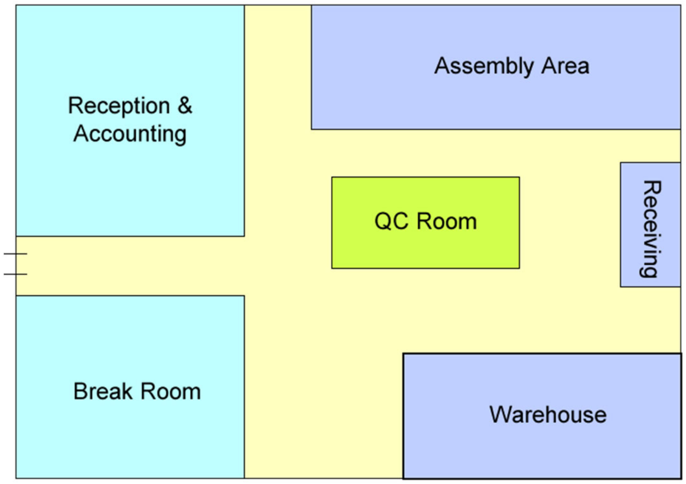
F. If text messaging begins to become to lengthy or confusing, convert to an alternate form of communication such as voice or email.

7.4 Best Practices for Photographic or Prerecorded Video Evidence

When gathering photographic or videographic evidence, the following practices may be used:

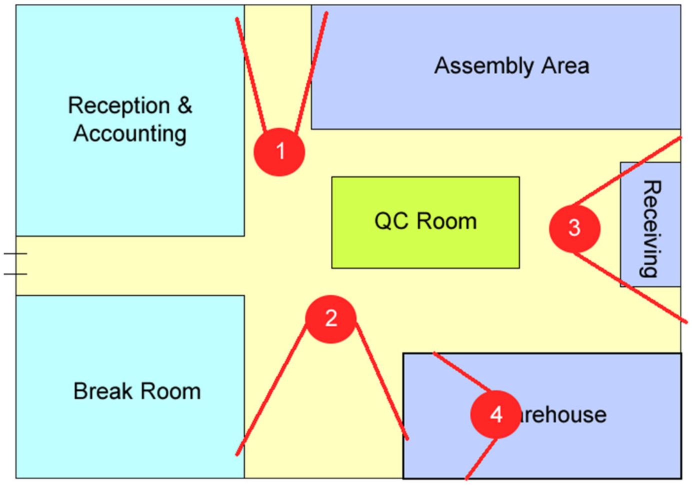
A. Request the auditee send a comprehensive floor plan of the facilities included in the management system scope. This should be sent well in advance of the audit, during audit planning. Request the auditee take photos or videos of the highest resolution possible, to allow enlarging or zooming afterward.

EXAMPLE:



B. Plan the intended photographic for videographic evidence by annotating the floor plan with positions where such images are to be taken, and at what angle. Number each annotated position for reference.

EXAMPLE:

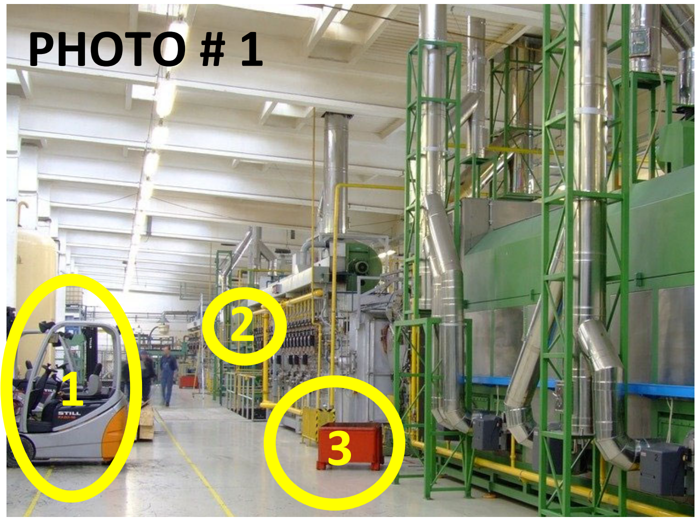


C. Request the auditee then submit the photos and/or videos with files that reference the annotated position numbers.

EXAMPLE:

D. The auditor may then review the photo or video and annotate areas with findings or observations which require additional questions. For photos, this may be done by annotating the image with reference points, and then providing questions or statements of findings related to each reference points in follow-up emails or the official audit report. For video, timestamps may be used in lieu of annotated reference points.

EXAMPLE:



Dear client:

Please provide the following information for each highlighted reference mark:

1: Provide evidence the forklift has current maintenance records.

2: Provide evidence the gauges are current on calibration, if they are calibrated.

3: What is this red box? Please provide some information on this.

E. In all cases, the floor plans and images may be marked up by hand or through computer annotations, provided the information is clear.

F. When specific photos or videos are not sufficient, the auditor may ask for better or additional images to be provided.

G. In all cases, ensure any exchange of photos, videos or reports abides with all other requirements for ensuring security and confidentiality of the information.

7.5 Best Practices for Live Video Evidence

When utilizing live video, the following practices should be observed:

A. Ensure the video platform or applications have all appropriate security options enabled (encryption, passwords, etc.) before beginning.

B. Test video and audio between all participants to ensure everyone can see and hear the others.

C. Use audio only for conversations that do not require video, to save bandwidth. Toggle cameras on when needed.

D. Obtain a floor plan ahead of time (see 7.4 above) and reference this when directing the auditee to position and manipulate the live camera.

E. Follow all conversation guidance defined in 7.2 for video conversations as well.

F. When a video image is unclear, request a photo be taken to review later; ensure the photo is taken and submitted in a manner compliant with other requirements.

G. During breaks, turn off webcams and mute microphones. If another party has forgotten to do this, alert them so that no private conversations or images are intruded upon.

H. Only use file sharing features in the video stream platform if doing so will remain compliant with all other security and confidentiality requirements.

7.6 Best Practices for Electronic Record Sharing / Email

When utilizing emails to communicate, the following practices should be observed:

A. Ensure both parties are using the secure email method, and not just one party.

B. Ensure the email software or platform used has all necessary security options enabled.

C. Send test emails between the parties to ensure the software or email platform works for all involved.

D. Keep email communications brief, and on-topic.

7.7 Best Practices for CMS Portals

When utilizing CMS portals, the following practices should be observed:

A. Ensure participants are trained on the portal usage; this is often a significant undertaking, and this document is not replacement for CMS training provided by the portal provider or IT administrator.

B. Ensure participants have login credentials that are secure and current.

C. Ensure the portal administrator has set the proper access rights for each participant (read only, edit, etc.).

D. Ensure all security options are properly activated.

7.8 Best Practices for Electronic File Deletion

When utilizing file deletion software, the following practices should be observed:

A. Ensure the software has the appropriate file deletion algorithm (DoD vs NIST, etc.) selected before deletion.

B. Ensure the method selected is suitable for the type of media being used (hard drive, solid state drive, USB drive, etc.).

C. Ensure the number of passes is correctly selected.

7.9 Best Practices on the Use of TOR

When utilizing TOR, the following practices should be observed:

A. Ensure the TOR browser being used is up to date. Update the browser before beginning any audit activities.

B. Ensure Javascript and Flash are disabled.

C. If connection is poor, use the browser feature to establish a new TOR identity and/or new network, and reload the site.

7.10 Best Practices on the Use of VPN

When utilizing VPN, the following practices should be observed:

A. Update the VPN software before beginning any audit activities.

B. Ensure the VPN killswitch is activated, so that internet is disabled if the VPN is lost or crashes.

C. Ensure the best VPN server is selected based on the region of the user.

D. Ensure encryption options are set in the VPN software.

E. If available, ensure the MACE option is activated to block adware, tracking and malware.

F. Utilize UDP connection type whenever possible.

8.0 Setting Up RAM Methods Prior to Audit

The accreditation standards Q003 and Q006 define the steps required by a CB for establishing the audit scope and preparatory steps. This includes determining if RAM will be used, and preparing for it. Those standards do not provide guidance on ***how*** to prepare for RAM, however; therefore, guidance on this is provided here.

Once it has been established that RAM will be used, the CB should determine to what extent it will be used. Specifically, this means identifying which of the following forms of evidence will require RAM usage:

- Verbal Interviews (typically via phone or VOIP)
- Text-Based Interviews (typically via SMS text messaging or instant messaging app)
- Photographic or Prerecorded Video Evidence (typically via file sharing or messaging app)
- Live Video Evidence (typically via video streaming platform or web conferencing)
- Electronic Records (typically via email, but possibly via file sharing or messaging app)
- Evidence via CMS Portals (via corporate web portal or online document repositories)

Once that is determined, the CB should review its internal capabilities to ensure all the general requirements of section 5.0 are met. If not, then the CB should update systems or applications, obtain software and licenses, etc., to ensure it can meet the requirements before the audit begins. If it still cannot, the CB should alert the client that RAM may not be able to be used for the audit.

Obtaining the resources for RAM may be done as follows:

1. Select a data deletion app (see 6.8) and install it on any computer which will be used during the audit. Be sure to set its default protocol to either the DOD or NIST method, as deemed appropriate.
2. Select a secure VOIP solution (see 6.2) if it is expected that controlled information will be transmitted verbally during interviews. Install these applications on the devices needing them, along with any specific security settings. Instruct the client organization to do the same on their end.
3. Select a messaging app that can be used for instant messages or file transfers (see 6.3, 6.4 and 6.5.) Install this and ensure the necessary security options are set up before use (auto deletion of messages, two-factor sign-in authorization, etc.) Instruct the client organization to do the same on their end.
4. Select a secure email service to use for file transfers or other written communications which may include controlled information (see 6.6.) Install this and create email accounts for both the CB representative ***and*** the client. Write down the login credentials (username, password, etc.) and provide to those needing access. Explain that this will only be used when the client needs to send controlled information

to the CB, as the account may be deleted after the audit. It should not be used as the main email method for the client to contact the CB.

5. Select a secure platform for any web conferencing (see 6.7.) Create the necessary accounts, and then set up the applicable meeting sessions for the audit dates. Invite attendees as required. Ensure the meeting session requires controlled access via a password or meeting ID key.
6. Request a floor plan of all facilities within the scope of the management system, so planning of photographic and videographic evidence may be conducted.

The above assumes the CB has elected not to use a CMS portal, VPN or TOR.