STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**ISMS Internal Auditing**
Effective Date:	**18 Dec 2019**
Reference Number:	**SOP-04-05**
Version Number:	**2.0**
Owner:	**ISMS Improvement Process Owner,**
Review Date:	**18 Dec 2021**

Table of Contents

1. Purpose

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

This document describes the procedure for conducting internal audits for information security compliance and effectiveness.

2. Scope

All audits created for the ISMS and TRE (Trustworthy Research Environment).

The management of non-conformances arising from any audit is out of scope of this procedure.

3. Responsibilities

The ISMS Improvement process owner is responsible for:
- Ensuring that the audit schedule is sufficient
- Assigning internal auditors to scheduled audits dependent on the auditors skills and experience
- Ensuring the audit scope is correct
- Monitoring the outcome of audits
- Managing the audit process
- Signing off on audit reports

Internal Auditors are responsible for:
- Ensuring their training is sufficient for conducting assigned audits
- Scheduling specific dates for the audit with the auditees
- Assigning auditees to the audit record
- Conducting the audit and writing up the audit
- Closing the audit once corrective actions are complete

Auditees are responsible for:
- Attending scheduled audits
- Responding to audit questions honestly

4. Procedure

4.1. Audit Schedule/Calendar

The ISMS Improvement process owner will schedule Internal Audits for each ISMS process in the Audit module of Q-Pulse and assign an appropriate lead auditor or team of auditors. The audit record should include the in-scope items for the process that is being audited. This will usually be a list of ISMS policy and procedure documents.
The audit schedule should cover all aspects of the ISMS at least once per year, although particular activities may be audited more or less frequently depending on their importance, business impact, technical difficulty or history of non-conformance.

The schedule should allow flexibility in the calendar for unscheduled audits in response to:
- Anticipated problem areas
- Actual problems, customer/user complaints or regulatory body requirements
- Requests from Management
- Unforeseen changes in circumstances or stakeholder requirements
- Recording the effectiveness of changes

4.2. Audit Preparation

The auditor will prepare for each audit as follows:
- The auditor will identify and select auditees to be included in the audit. The auditees will be representative of both the management and the users of the process or procedure.
- The auditor will confirm the date and time for the audit. It is expected that this will be within 1 month of the original scheduled date.
- The auditor will review the previous audit report covering the same process so that recently changed areas can be re-audited and any previously excluded areas can be focused on.
- The auditor will familiarise themselves with the policies and procedures in scope of the audit in order to prepare a suitable set of audit questions.
- The auditor will use the audit questions to prepare an audit checklist in Q-Pulse to guide the direction of the audit.
- The auditor should provide the auditees with a copy of the proposed checklist questions so that they may prepare the necessary evidence and allow the most effective use of the audit session.

4.3. Performing the Audit

During the audit, the auditor will:
- Make use of open questions to collect objective information concerning the subject being audited, the auditor will not lead the auditee into answering a question
- Not respond to rumour and hearsay
- Avoid confrontational situations and arguments; the purpose of the audit is to assess compliance and not to find fault with individuals
- Make notes to aid the writing of the audit report on the Audit Checklist
- Collect documentary evidence of conformity or nonconformity, e.g. Purchase order numbers, serial numbers and dates
- Not audit their own work. e.g. The ISM cannot audit the ISMS for compliance
- Keep the auditee informed on the progress of the audit and any findings.

4.4. Completing the Audit

As soon as practical after the audit the auditor will update Q-Pulse with the results of the audit checklist. The audit checklist will also:
- Record the good points as well as the bad
- Make constructive suggestions where possible (recorded as an observation)
- Record only factual evidence (not hearsay); including dates, document numbers or other forms of evidence identification such as purchase order numbers

The audit record card in Q-Pulse will then be completed and will:
- Clearly identify the areas where corrective actions are required
- Include the names of the auditor, auditees and the date of the audit

For each of the non-compliances a non-conformance record should be added to Q-Pulse. All non-conformances must be closed before the overall audit record can be closed. Closing the audit is the responsibility of the lead auditor.

For the procedure for handling non-conformances see SOP-02-03

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-02-03	ISMS\SOP\ISMS Management - SOP	Managing Security Events and Weaknesses
SOP-04-04	ISMS\SOP\ISMS Improvement - SOP	ISMS Measurement and Monitoring
ISMS-04-01	ISMS\Policy & Guidance\ISMS Improvement - policy & guidance	ISMS Management Review

6. Appendices

6.1. Guideline for Completing Internal Audit Records in Q-Pulse

6.1.1. Confirming Audit Schedule

Once the audit date has been confirmed the status of the audit can be moved from 'Scheduled' to 'Schedule Confirmed' by ticking the 'Schedule Confirmed' tick-box and saving the audit record. Completing this action will send an email to the Lead Auditor assigned to the audit.

6.1.2. Adding an Auditor or Auditee

The auditors and auditees assigned to the audit record can be found on the 'Auditors and Auditees tab.

New auditors or auditees can be added by clicking on the 'Add auditor' or 'Add Auditee' buttons. This will display the 'Search for Person' form where the person can be searched for and selected.

6.1.3. Checking Scope Items

The audit scope items can be checked on the audit record card within the 'Scope' tab. This will list the processes and procedures to be included in the audit.

6.1.4. Managing Checklists

6.1.4.1. Adding a Checklist

To add a checklist, open the 'Checklists' tab on the audit record

Click on the [icon] button to add a new checklist. This will display the 'Create/Edit Checklist' form.

Add a title and description for the checklist.

Checklist items can be added from the Question Bank by dragging them to the checklist. However, it is expected that most questions will be added by typing them in and adding them to the checklist.

The can be added via the 'Add item to checklist' box.

Items can be added as questions or section headers . Section headers are used to organise and structure the audit and may typically be the name of a scope item e.g. Document Control (SOP-02-01).

If an item is added incorrectly it can be edited or deleted using the buttons available on the 'Create/Edit Checklist' form. The button will display the 'New/Edit Question' form where the question text can be modified as necessary.

Once all of the checklist questions have been added the checklist can be saved by clicking on the 'OK' button and the checklist will be presented on the 'Checklist' tab in the audit record.

6.1.4.2. Editing a Checklist

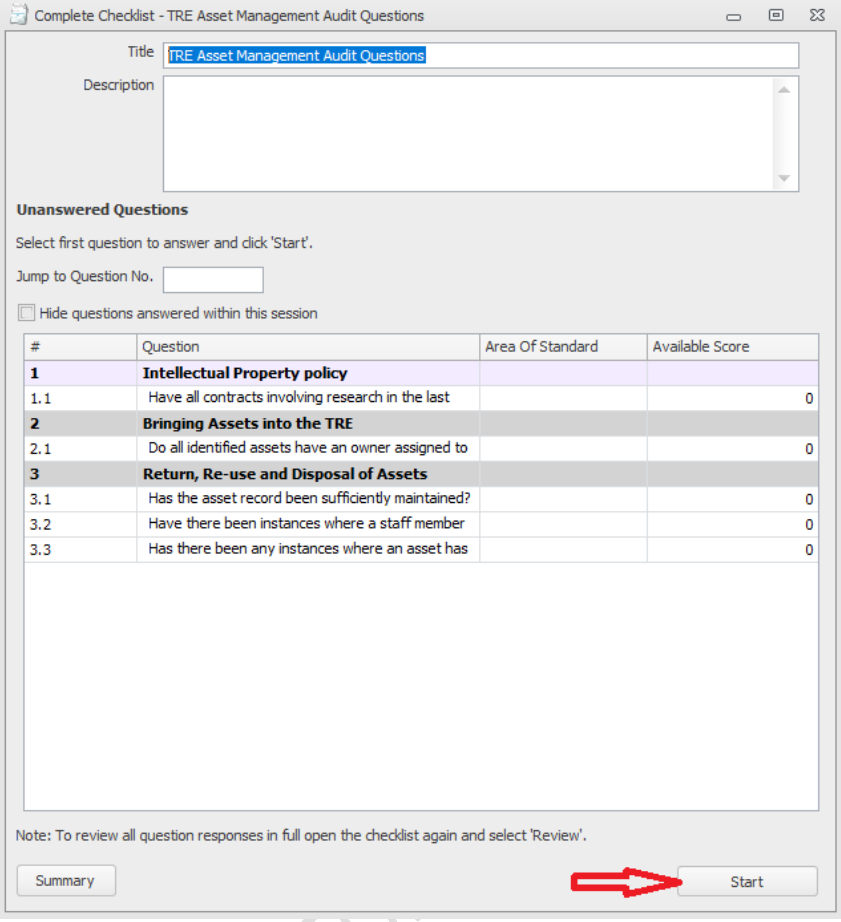It may be necessary to edit a checklist to add additional questions or update existing questions. This can be completed by selecting the checklist and clicking on the 'Open Checklist' [icon] button. This will display the 'Open Checklist' dialog where the 'Edit Checklist' option should be selected.
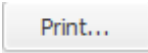
The checklist will be displayed and the question can be edited or new question added as previously described.
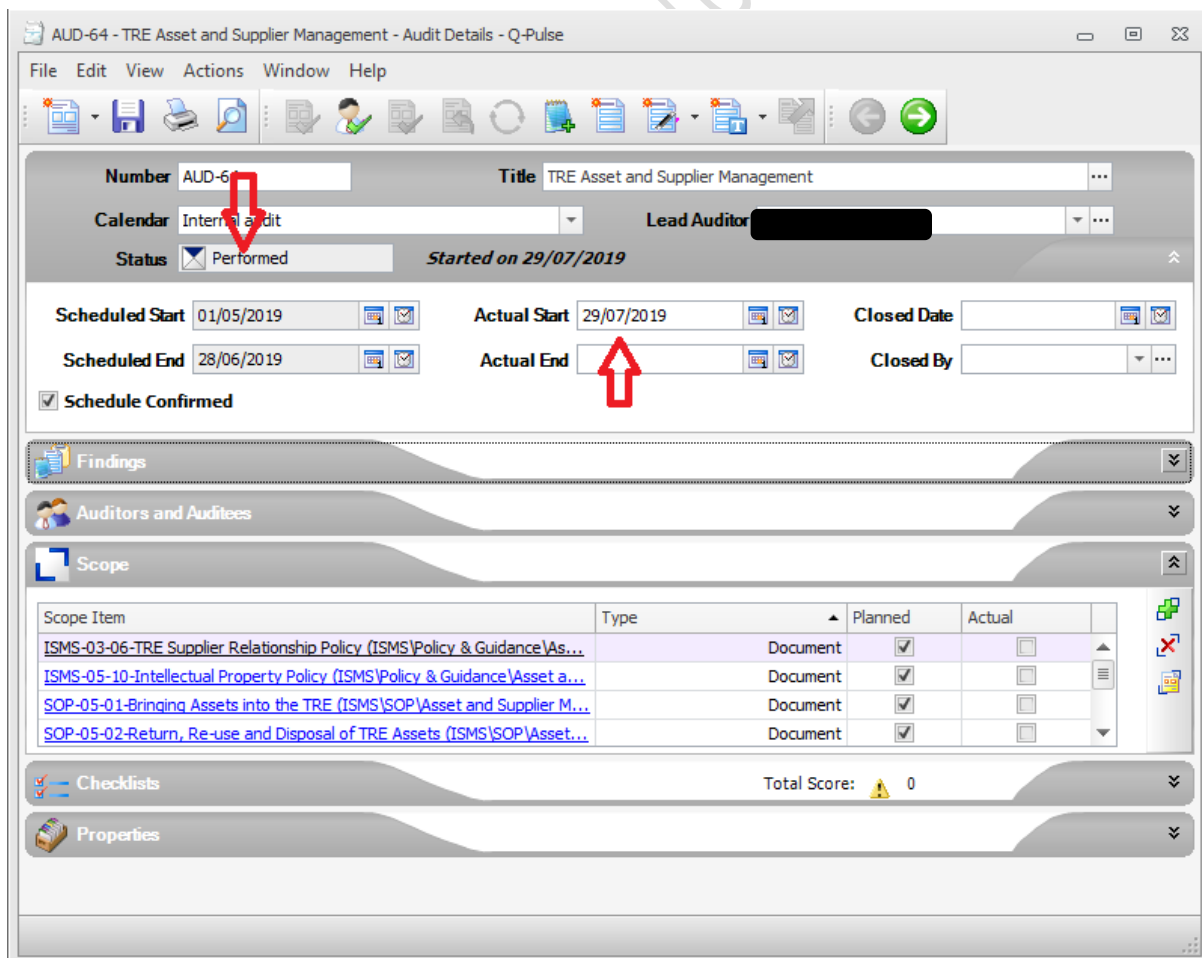
6.1.4.3. Printing the Checklist

To print the checklist (e.g. to send to the auditees) select the [Print...] button from the 'Create/Edit Checklist' form. This will display the 'Select a Report' dialog. Select the 'Choose a Report' report option and the report ' Audit Checklist Details'. The 'Preview' button will display a copy of the checklist in a pdf format which can be downloaded and sent to the auditees.
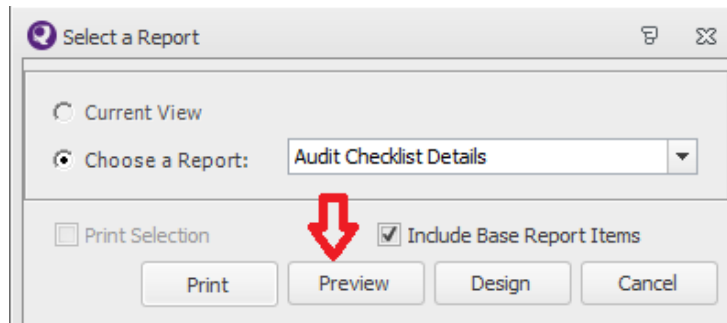
6.1.4.4. Completing the Checklist

In order to complete the checklist the audit status must be set to Performed by adding an actual start date to the audit record and saving the record.

Then open the checklist by selecting the checklist and clicking on the 'Open Checklist' button.
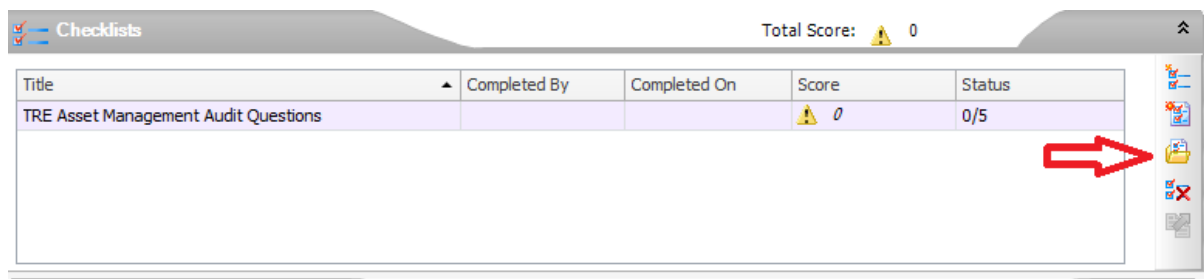
This will display the 'Open Checklist dialog. Select the 'Complete Checklist' option.
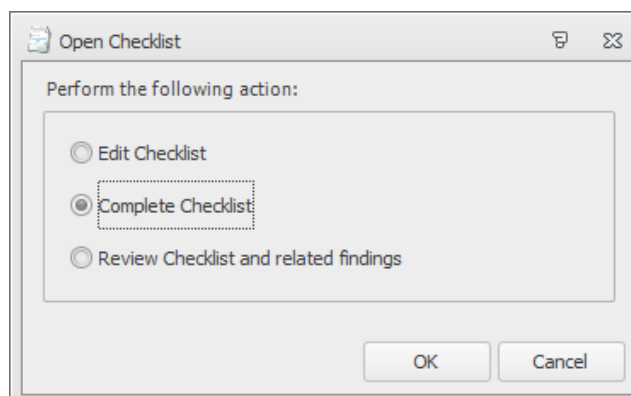
Click on the 'Start' button.

Add the response to the audit question and click on the 'Next' button to proceed to the following question.

After the final question the 'Complete Checklist form will be display. Add the completed date and click on the 'Finish' button to complete the audit checklist.

6.1.4.5. Raising Findings

During the audit any findings may be raised as an observation or a non-compliance using the buttons presented on the 'Complete Checklist' form.