STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**ISMS Measurement and Monitoring**
Effective Date:	**01 Aug 2019**
Reference Number:	**SOP-04-04**
Version Number:	**2.8**
Owner:	**ISMS Improvement Process Owner,**
Review Date:	**01 Aug 2021**

Table of Contents

1. Purpose

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

This document provides the procedure for monitoring and measuring the information security management system in order to provide data for:

- Evaluating the effectiveness of the implemented controls or groups of controls
- Evaluating the effectiveness of the implemented ISMS
- Verifying the extent to which identified security requirements have been met
- Facilitating performance improvement of information security in terms of the organisation's overall business risks
- Management review to facilitate ISMS-related decision making and justify needed improvements of the implemented ISMS.

It provides the measurement topics that will be used for establishing the effectiveness of existing information security controls. Records of measurement will be recorded in Q-Pulse as a Routine Monitoring and Measurement record in the Audit module.

2. Scope

This document covers all monitoring and measurement of the ISMS that falls outside the scope of Internal Audit (SOP-04-05), Information Security Objectives (ISMS-02-12).

However, similarities between these various measures are unavoidable, therefore a 'best efforts' approach will be followed to prevent overlap between Routine Measurement and Monitoring and the different assessment activities.

3. Responsibilities

The ISMS Improvement Process Owner is responsible for:

- Ensuring that routine measurements are planned into Q-Pulse
- Ensuring that competent owners are assigned to routine measurements
- Ensuring that routine measurements are performed

The Information Security Steering Group (ISSG) is responsible for:

- Reviewing the results of routine measurement at the management review
- Actioning improvements based on the outcome of routine measurement

The Routine Measurement Owner is responsible for:

- Performing the measurement in a timely manner
- Recording the results of the measurement on Q-Pulse
- Generating corrective actions when trigger points are met
- Assigning appropriate action owners to corrective actions
- Closing routine measurement actions once complete
- Assessing the suitability of the measures to reflect the key issues affecting their processes and selecting new measures when appropriate

4. Procedure

4.1. RMM Audit Scheduling

Routine measurements shall be reported in a routine monitoring and measurement (RMM) record in the audits section of Q-Pulse. The ISMS Improvement Process Owner will prepare and schedule the RMM audit records prior to their proposed start date. RMM audits will be scheduled at a maximum frequency of monthly and a minimum frequency of bi-monthly depending upon the criticality and current threats affecting each process area.
Each RMM audit record will have the following information:

a) Number
The RMM audit records will be numbered with the prefix as follows:

Process	Number Prefix
ISMS Event and Incident Management	RMM-EVENT-MGMT-xx
ISMS Communication	RMM-COMMS-xx
ISMS Document Management	RMM-DOC-MGMT-xx
ISMS Improvement	RMM-IMPRV-xx
ISMS Management	RMM-MGMT-xx
ISMS Risk Management	RMM-RISK-MGMT-xx
Staff Induction, Update and Exit	RMM-STAFF-MGMT-xx
Staff Training and Competency	RMM-STAFF-TRG-xx
TRE Asset and Supplier Management	RMM-ASSET-MGMT-xx
TRE Data Management	RMM-DATA-MGMT-xx
TRE Information Governance	RMM-IG-xx
TRE Infrastructure and Security Management	RMM-INF-MGMT-xx
TRE Operations	RMM-OPS-xx
TRE Physical Security	RMM-PHYS-SEC-xx
TRE Project and User Account Management	RMM-PRJCT-MGMT-xx
TRE User Setup and End-Point Security	RMM-USER-SETUP-xx

b) Scope
The corresponding ISMS Process will be included here. However, the actual scope of the RMM measurements as detailed within the appendix in section 6.1 will be held in the RMM audit checklist.

c) Lead auditor
The lead auditor for the RMM audit will be identified. This person, also known as the routine measurement owner, will usually be the owner of the process in the scope of the RMM.

d) RMM Audit Status

- When first created the RMM audit record will have the status of ‘Scheduled’.
- Once the date is confirmed by the ISMS Improvement Process Owner the status will be changed to ‘Scheduled Confirmed’.
- The lead auditor will be prompted by email when the schedule is confirmed for the audit record and also within 3 days of the audit start due date.

- When the actual start date and end date for the RMM audit has been added to the record it will move to the status ‘Performed’.
- A completed RMM audit where the closed date has been added will have the status of ‘Closed’.

e) RMM Audit Checklist

The RMM audit checklist will contain the details of the measurements that are required and also propose the mechanism by which the measures can be prepared.

The measures are summarized in the Appendix in section 6.1. The measures may relate to monitoring the effectiveness of a control, establishing the presence of new threats or for generating data in response to a stakeholder’s requirements.

4.2. Completing the RMM Audit

Each routine measurement shall be recorded on Q-Pulse on the appropriate RMM audit record card.

The outcome of any routine measurement shall be:
1) Easy to understand;
2) Completed in a timely manner;
3) Objective, comparable and reproducible.
4) Will cover a period of 2 complete months prior to the audit date for bi-monthly audits or 1 complete month prior to the audit date for monthly audits.

Where values have fallen outside of agreed tolerances a security event or weakness shall be raised.

For records that require a standard form instead of a checklist, the completed form shall be attached to the record card.

Once the RMM audit record is complete and any required corrective actions have been completed the RMM audit record may be closed by the owner.

4.2.1. Review of ISMS-02-03 Index of Relevant Policy

Each RMM audit will include a review by the process owner of the relevant statutory, regulatory and contractual requirements for their process included in ISMS-02-03 Index of Relevant Policy. This review will identify any changes, including the addition of any new requirements and these will be sent to the document owner for inclusion in an updated version of the document.

4.3. RMM Audit Reporting

Summary data produced from routine monitoring and measurement shall be presented to the ISSG during management reviews and shall be used as an indicator of the performance of the system and controls.

4.4. Maintaining the Measures

The topics covered under routine measurement shall change in response to changing threats, regulatory requirements, effect of system improvements and stakeholder requirements.

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-04-05	ISMS\SOP\ISMS Improvement - SOP	ISMS Internal Auditing
ISMS-02-12	ISMS\Policy & Guidance\ISMS Management - policy & guidance	Information Security Measures
ISMS-02-07	ISMS\Policy & Guidance\ISMS Management - policy & guidance	ISMS Roles and Responsibilities
SOP-03-02	ISMS\SOP\TRE Operations - SOP	TRE User Manual and Agreement

6. Appendices

6.1. RMM Reporting Measures

All measures will usually be prepared for the two months preceding the reporting month, although this may be impacted by changes to the reporting cycle which will be reported to the process owners as appropriate.

ISMS Process	What will be measured/monitored/reported
ISMS Event and Incident Management	- Number of events/incidents logged and resolved. If 0 logged, then encourage reporting of events/incidents
	- Number of overdue events/incidents (at least 1 stage overdue)
	- Time taken for initial assessment of events
ISMS Communication	- Number of ISMS related updates delivered at last CHI Research Group meeting within the current reporting period
	- Number of e-mails to communicate information about the ISMS sent to all of CHI
ISMS Document Management	- Number of new documents
	- Number of revised documents
	- Number of documents pending review/approval
	- Number of document acknowledgements requested
	- Number of document acknowledgements overdue. Escalate if > 10% are overdue.
ISMS Improvement	- Number of audits conducted (Internal Audit, External Audit and Routine Monitoring and Measurement).
	- Number of Change Requests raised and implemented
ISMS Management	- Number of ISSG team members attending ISMS Board / Management Meetings. If <4, review and take action to increase attendance
	- The collection of processes remain appropriate and relevant for the ISMS: to be reviewed as part of the RMMs for this process
ISMS Risk Management	- Number of new risks added
	- Number of very high and high risks added
	- Number of items of evidence for Risk Treatment added and number of risks with treatment changes (number increased and decreased overall risk level)
Staff Induction, Update and Exit	- Number of new starters and number with corresponding checklist documents completed within 1 month attached to their Q-Pulse person record. Escalate if <50% are completed.

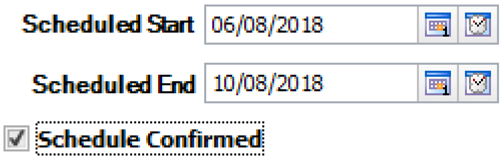
ISMS Process	What will be measured/monitored/reported
	- Number of leavers and number with corresponding checklist documents completed within 2 weeks and attached to their Q-Pulse person record. Escalate if <50% are completed.
Staff Training and Competency	- Number of people that need to complete data protection training. If not complete within 30 days of due date, send reminder email.
	- Number of TRE users that need to complete training. If not complete within 30 days of due date, send reminder email.
	- Number of current TRE users and the number that have completed their full induction (i.e. competency record on Q-Pulse is complete at all stages). If not complete within 30 days of due date, send reminder email.
TRE Asset and Supplier Management	- Number of new/removed TRE assets with summary of details.
	- Number of TRE asset warranties due to expire within the next 3 months with summary details of assets impacted
	- Check the 'Notes' section for each software asset record to make sure the total number of TRE users with access to that software does not exceed the limit of concurrent users as defined within the license
TRE Data Management	- Check that TRE Dataset asset register (Q-Pulse) corresponds with the data import section of the TRE Infrastructure Record? Is there a completed Data Checker form for this data transfer?
	- Number of imported datasets and the number that have a checksum recorded in the TRE infrastructure record
	- Check that TRE Dataset asset register (Q-Pulse) corresponds with the data export section of the TRE Infrastructure Record? Is there a completed Data Checker form for this data transfer?
	- Check data deletion records against project end dates
TRE Information Governance	- Number of TRE users' desks contravening clear desk policy
	- Number of TRE confidentiality issues detected at printers/photocopies/scanners
	- Number of other confidentiality issues detected at printers/photocopies/scanners
TRE Infrastructure and Security Management	- Are the security event logs being regularly monitored? Check that there have been two logins to the SIEM appliance from a system administrator or the ISM within the last working week.
	- Are virtual machines being provisioned with adequate security controls? Check that a PCI-DSS SCAP report is stored for the last virtual machine created.
	- Are data restore tests being regularly performed? Is there a data restore test within the last month?
	- Are virtual machine isolation tests being performed? Is there an isolation test report stored for the last virtual machine created?
	- Are keys being managed correctly? Are the keys for the last virtual machine created stored on the encrypted USB device in the safe?
TRE Operations	- Evidence of continuity of information security and project segregation testing.

ISMS Process	What will be measured/monitored/reported
	- Were all TRE data imports and exports completed within the expected time-scales (currently 2 weeks from receipt of request)
	- The TRE Infrastructure Record contains entries that reflect the TRE Project as defined by FORM-002 and FORM-008 if applicable.
	- The TRE Infrastructure Record contains completed 'Approval' entries for all completed work.
TRE Physical Security	- Number of visitors that failed to fill in a badge number in the VH Visitors’ book.
	- Number of visitors that failed to record their exit time in the VH Visitors’ book.
	- Number of signing-in sheets that are remaining in the Visitors’ book.
TRE Project and User Account Management	- Number of live TRE projects and status of pending projects.
	- Check that JIRA TRE project records match the TRE Infrastructure Record.
	- Check that each TRE Project record has the required paperwork attached for all projects created since the last reporting date.
	- Check each TRE Project record has an end date and that this date matches the TRE Infrastructure Record.
	- Identify any TRE Projects that have an end-date occurring within the next period of monitoring, and inform the TRE System Administrator via email if they need to review the project end date (as specified in the TRE Infrastructure Record) and to set themselves a reminder to carry out the project deletion on that date.
	- Number of 'active' TRE Projects and number with a FORM-002 that lists users requiring TRE user accounts.
TRE User Setup and End-Point Security	- Number of events/incidents related to TRE user end-point security.

6.2. Q-Pulse Usage Guideline

6.2.1. Confirming the RMM Audit Schedule

The RMM audit schedule can be confirmed by clicking the ‘Schedule Confirmed’ tick box on the RMM audit record.



Scheduled Start: 06/08/2018

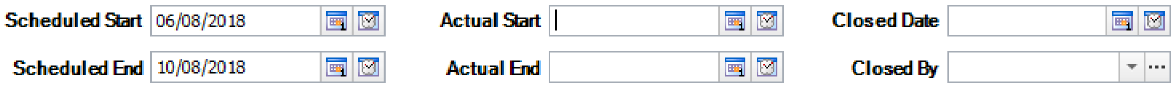
Scheduled End: 10/08/2018

☑ Schedule Confirmed

This will send a reminder to the lead auditor that the audit has been scheduled.

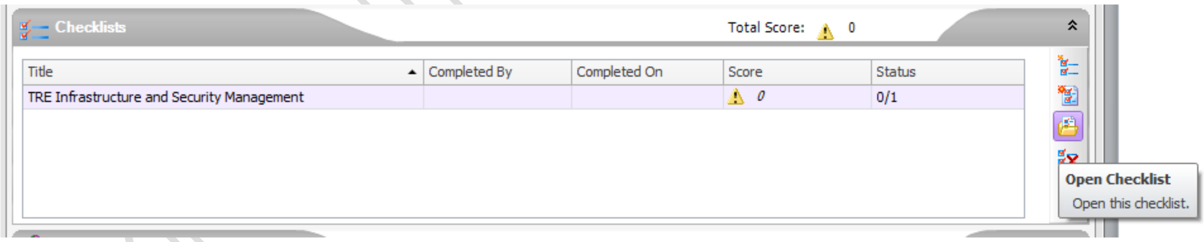
6.2.2. Completing the RMM Audit

When the RMM audit is performed the actual start and actual end dates should be updated and the record saved. This will change the RMM audit status to Performed and the measurement checklists can then completed



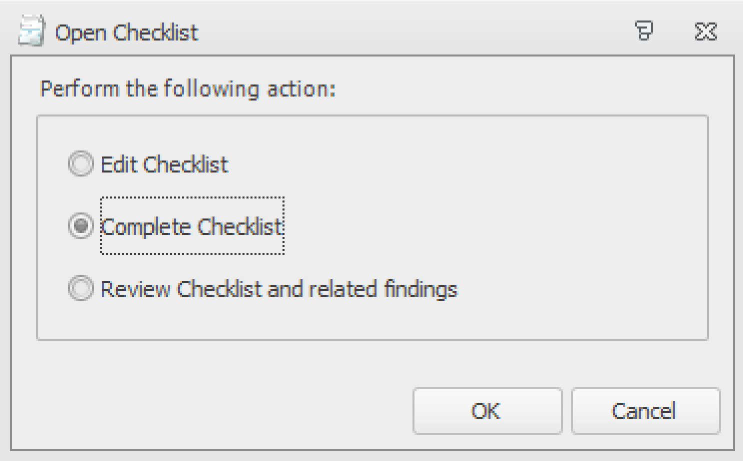
Scheduled Start	06/08/2018	Actual Start		Closed Date	
Scheduled End	10/08/2018	Actual End		Closed By	

To start adding the measurement results (completing the checklist), expand the checklist tab and click on the Open Checklist icon



Title	Completed By	Completed On	Score	Status
TRE Infrastructure and Security Management			⚠ 0	0/1

Select the ‘Complete Checklist’ option and click on OK



Open Checklist

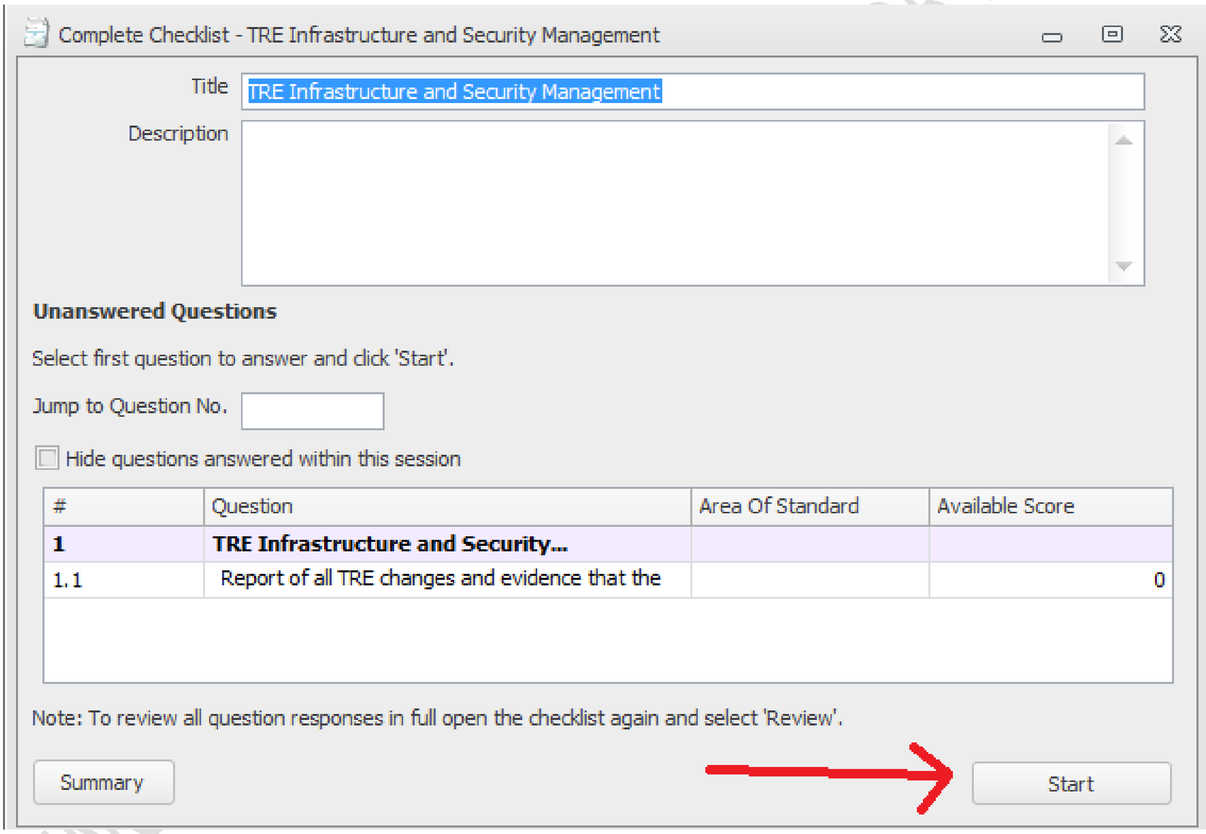
Perform the following action:

○ Edit Checklist

● Complete Checklist

○ Review Checklist and related findings

When the checklist is presented click on ‘Start’ to be presented with the checklist items



Complete Checklist - TRE Infrastructure and Security Management

Title: TRE Infrastructure and Security Management

Description:

Unanswered Questions

Select first question to answer and click 'Start'.

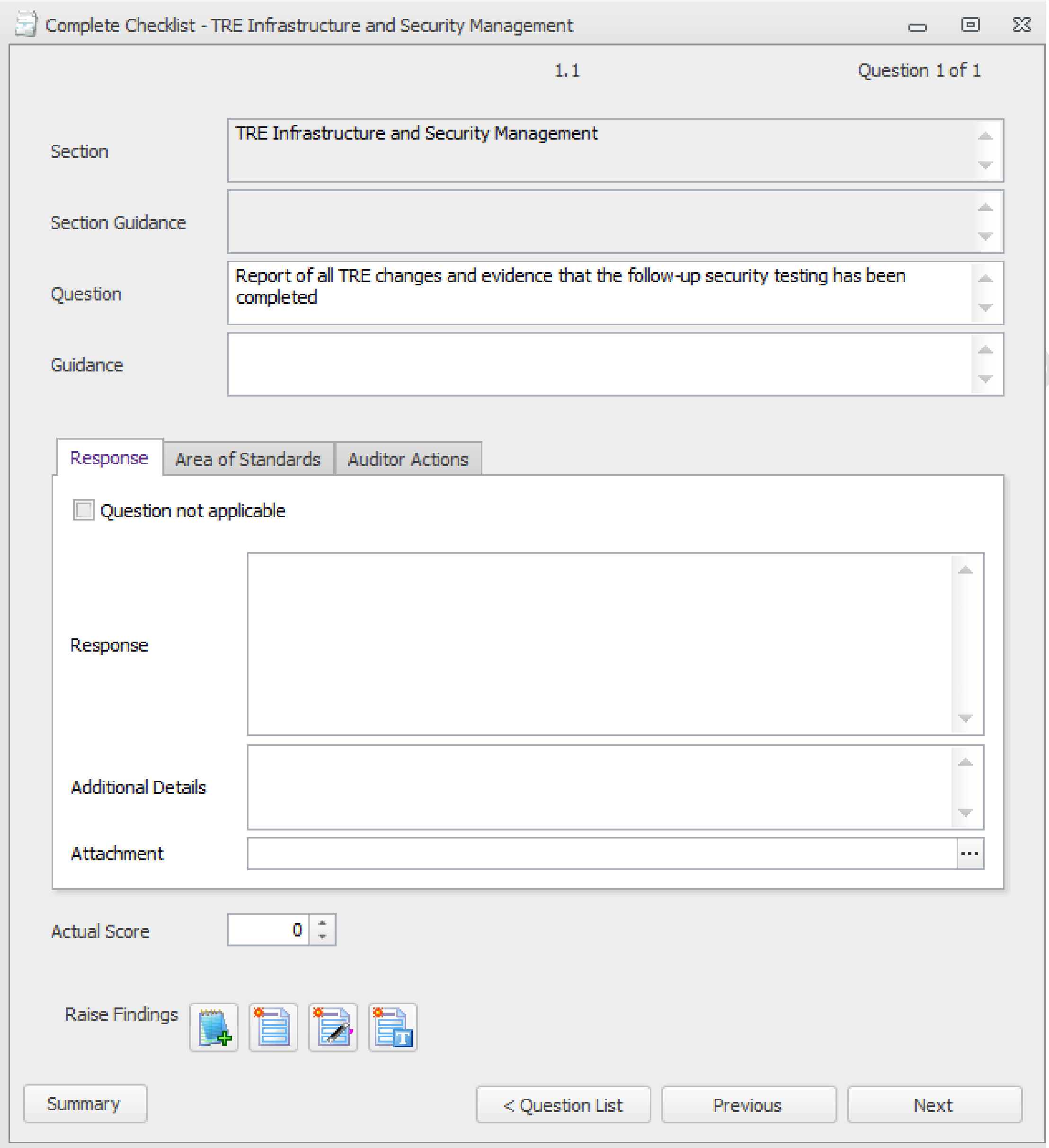
Jump to Question No.

□ Hide questions answered within this session

#	Question	Area Of Standard	Available Score
1	**TRE Infrastructure and Security...**		
1.1	Report of all TRE changes and evidence that the		0

Note: To review all question responses in full open the checklist again and select 'Review'.

For each checklist item a dialog will be presented where the appropriate response (e.g. a measurement result, attachment or comment) can be added.



1.1 Question 1 of 1

Section: TRE Infrastructure and Security Management

Section Guidance:

Question: Report of all TRE changes and evidence that the follow-up security testing has been completed

Guidance:

□ Question not applicable

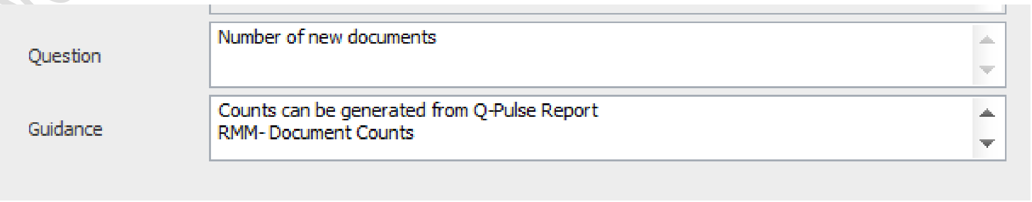
Response:

Additional Details:

Attachment:

Actual Score: 0

Where applicable further guidance will be presented in the 'Guidance' section. This will include details of how the information for the measure can be collected.

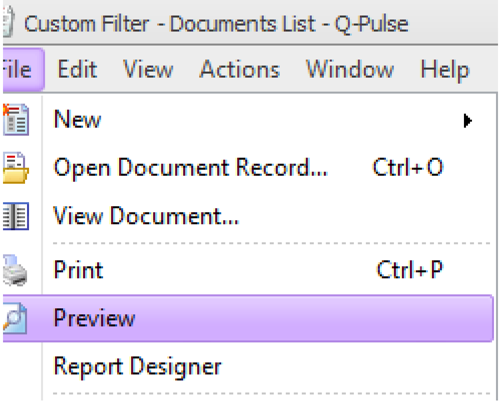


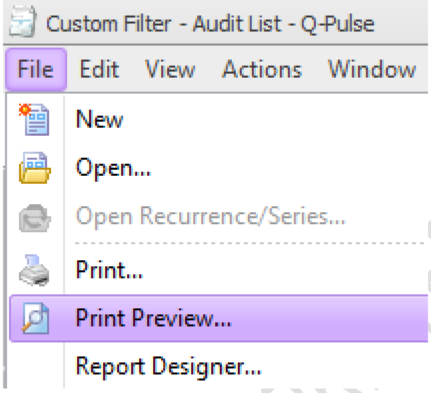
Question: Number of new documents

Guidance: Counts can be generated from Q-Pulse Report
RMM- Document Counts

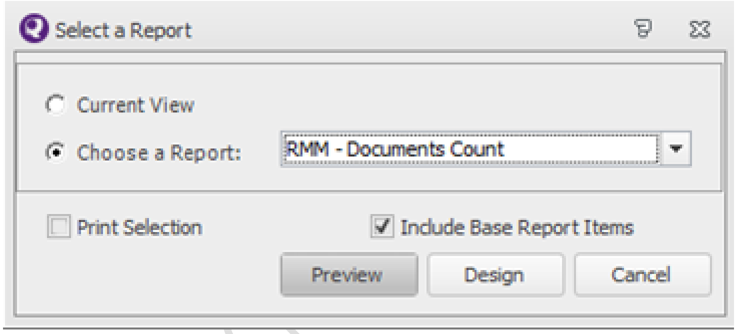
Where a Q-Pulse report is available to provide the information for a measure this can be accessed as follows:

Select the correct list from the Q-Pulse Launchpad. From the list view select File -> Preview (or File -> Print Preview, depending on the menu option presented)





Ensure the ‘Choose a Report’ option is selected and then select the appropriate report for the measure from the dropdown and click on ‘Preview’ to view the report.


Select a Report

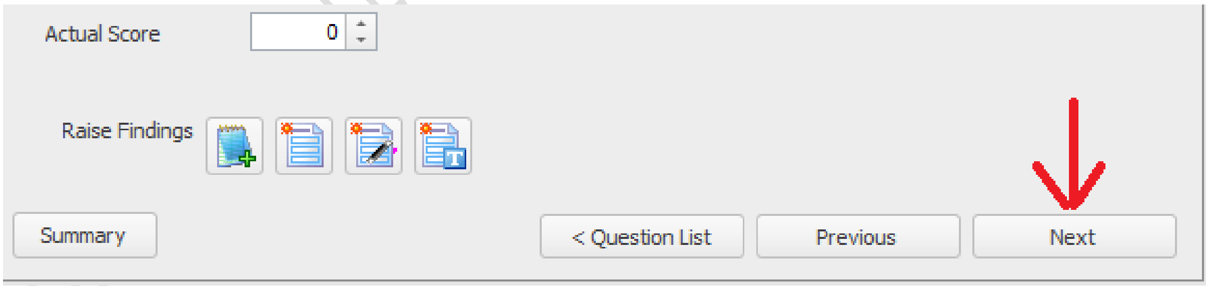
○ Current View

● Choose a Report: RMM - Documents Count

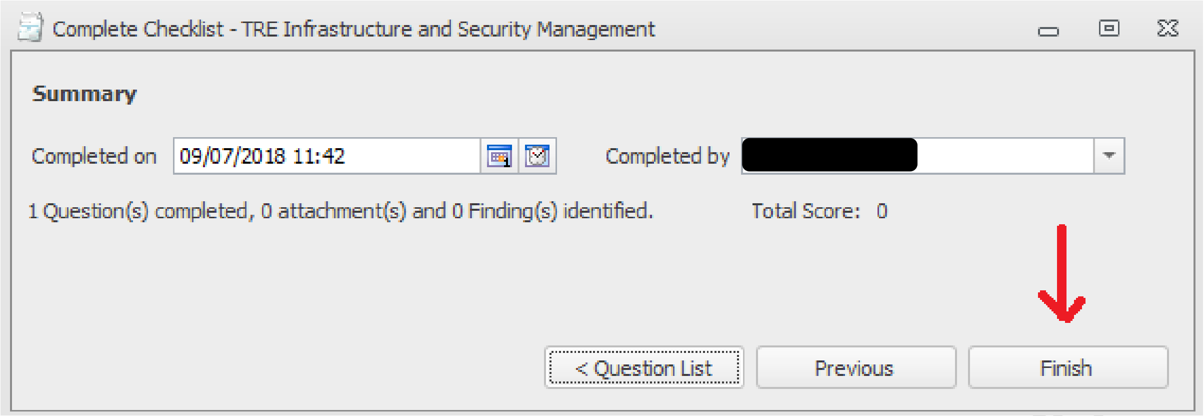
□ Print Selection

☑ Include Base Report Items

Once the response has been entered subsequent questions can be accessed using the ‘Next’ button.


Actual Score 0

After the final checklist item has been presented a ‘Finish’ option will be provided.



Complete Checklist - TRE Infrastructure and Security Management

Summary

Completed on 09/07/2018 11:42

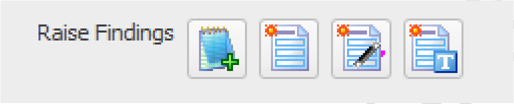
Completed by [redacted]

1 Question(s) completed, 0 attachment(s) and 0 Finding(s) identified.

Total Score: 0

6.2.3. Raising Observations, Security Events or Non-Compliances

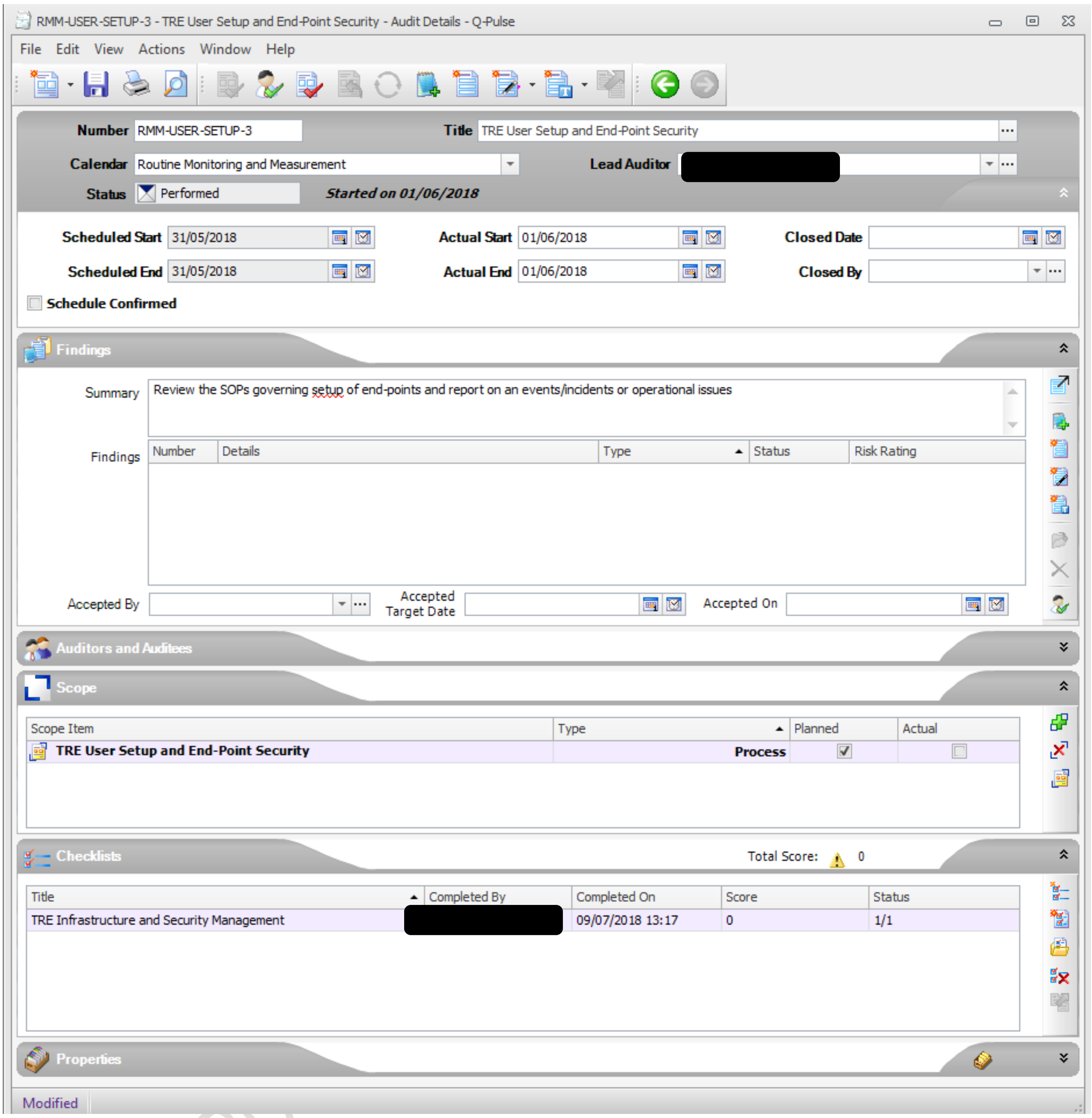
If any security events, observations, or non-compliances are discovered during the RMM audit these may be raised during the checklist completion using the ‘Raise Findings’ buttons.



6.2.4. Closing the RMM Audit Record

The RMM audit record can be closed provided all associated actions have been closed.

The record is closed by adding the ‘Closed Date’ and ‘Closed By’ to the RMM audit record and saving the updated record.


RMM-USER-SETUP-3 - TRE User Setup and End-Point Security - Audit Details - Q-Pulse

Number	RMM-USER-SETUP-3	Title	TRE User Setup and End-Point Security
Calendar	Routine Monitoring and Measurement	Lead Auditor	[redacted]
Status	Performed	*Started on 01/06/2018*	

Scheduled Start	31/05/2018	Actual Start	01/06/2018	Closed Date	
Scheduled End	31/05/2018	Actual End	01/06/2018	Closed By	

□ Schedule Confirmed

Findings

Summary: Review the SOPs governing setup of end-points and report on an events/incidents or operational issues

Findings:

Number	Details	Type	Status	Risk Rating

Accepted By: Accepted Target Date: Accepted On:

Auditors and Auditees

Scope

Scope Item	Type	Planned	Actual
TRE User Setup and End-Point Security	**Process**	☑	□

Checklists Total Score: ⚠ 0

Title	Completed By	Completed On	Score	Status
TRE Infrastructure and Security Management	[redacted]	09/07/2018 13:17	0	1/1

Properties

Modified

- **Number:** The RMM Record ID.
- **Title:** The name of the corresponding ISMS Process.
- **Calendar:** The Q-Pulse Audit Module Calendar being used (always Routine Monitoring and Measurement for RMM events).
- **Lead Auditor:** The person conducting the RMM event.
- **Actual End/Closed Date:** The action of specifying the end date and closing the record indicates that the RMM Event has been completed
- **Findings/Summary:** It is advisable to describe the objectives of the RMM here.
- **Findings/Findings:** This is where any observations, security events or non-compliances raised during the completion of the audit checklist are placed.
- **Auditors and auditees:** A list of anyone involved in conducting the RMM event (usually only the person specified in the ‘Lead Auditor’ field).
- **Scope:** The corresponding ISMS Process will be included here.
- **Checklists:** This is where the results of the RMM are placed including any attached supporting documents

- **Properties:** Additional information (not usually required).

6.2.5. Editing the RMM Audit Checklist

Where checklists no longer represent the critical measures for the process it may be necessary to update them. This activity should be completed with the assistance of the Q-Pulse Administrator.