POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Supplier Management**
Effective Date:	**27 Sep 2019**
Reference Number:	**ISMS-03-06**
Version Number:	**3.0**
Owner:	**Information Security Manager,**
Review Date:	**27 Sep 2021**

Table of Contents

1. Purpose

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain. Organisations should regularly monitor, review and audit supplier service delivery to ensure that the information security terms and conditions of the agreements are being adhered to.

This policy defines the approach to assessing and selecting suppliers of services to the TRE and the regular review of existing suppliers. The TRE requires the security of its information to be maintained in order to ensure the overall service is a reliable resource for users and other stakeholders, and to meet its statutory and regulatory obligations.

2. Scope

The term “supplier” refers to any service provider, contractor, consultants or university (specifically The University of Manchester) that are not employees of the Centre for Health Informatics.

All contractors and supplier personnel who have the potential to impact the confidentiality, integrity and/or availability of TRE data by any interaction with the TRE infrastructure and environmental management systems at Vaughan House and the TRE data stored there are in the scope of this policy. This includes all services provided by the University that directly affect TRE infrastructure assets.

Categories of TRE assets and services that can be supplied to the organisation are shown in Table 1

The provision of datasets and data processing services (e.g. data anonymisation) is out of scope because the selection of data owner/controller/processor is the responsibility of the research project.

3. Responsibilities

The ISM is responsible for:

- Considering any potential risks associated with using each supplier and ensuring these are managed within the Information Security Risk Register

The TRE Operations Manager is responsible for:

- Using the results from supplier assessments to determine their suitability to become an approved TRE supplier

TRE Staff are responsible for:

- Maintaining an up to date Q-Pulse supplier record for each TRE supplier including the relationship to Q-Pulse TRE asset records
- Completing assessments for new and existing suppliers
- Maintaining an up to date record of all service plans, contracts, warranties and supplier agreements within the Q-Pulse records associated with the TRE assets provided by or supported by that supplier

4. Policy

4.1. Approved Suppliers

The term 'Supplier' means an organisation within, or external to the University that provides a TRE asset. Most assets procured for the TRE are either infrastructure components or services; both of which usually require service contracts and warranties to meet business continuity objectives.

A record is maintained for each TRE Supplier, along with the TRE assets provided by those suppliers. The suitability of a TRE supplier is determined by conducting an assessment of that supplier; both prior to initial procurement, and annually for existing suppliers.

4.2. Setting up new Suppliers

The TRE Operations team has full responsibility for the selection of all TRE suppliers; commissioned for both routine maintenance of existing assets and the procurement and delivery of new assets. An exception to this rule is where a particular service can only be supplied to the Centre for Health Informatics (CHI) by the University of Manchester's IT Services, HR or Estates departments. This is because all University departments must adopt the core services provided by the University. In this case a supplier assessment should still be conducted. However, as most University departments do not have the resource or internal procedures to respond to assessments of their suitability, a 'best-efforts' approach must be taken, which means it will not be possible to complete all sections of the supplier assessment form. In all cases, a written agreement or some form of correspondence should exist between CHI and the corresponding University department, and where possible, access to their documented procedures.

Another exception to CHI conducting its own supplier assessment is when the University's central finance department selects and appoints an external supplier from their list of 'approved suppliers'. The most common reason for this approach is cost (see section 4.2). In such cases, CHI expects the finance department to have conducted an assessment of that supplier and for the results to be made available. Furthermore, for the procurement of items critical to TRE security, members of CHI's ISSG will be consulted during the selection of supplier, realisation of product requirements and specification, and during contract negotiations.

In all cases, it is the responsibility of the TRE Operations team to ensure all necessary documentation is suitable and stored so that it easily accessible and auditable.

4.3. Cost of Supply

CHI is entitled to select suppliers and approve its own purchase orders below a certain low-band cost threshold (all purchase orders are overseen by University central finance who will notify us if the threshold is exceeded).

For purchase orders where the cost is above this low-band threshold, the University central finance department may require justification for the selection of the supplier, in which case we can provide the results of our assessment of that TRE Supplier.

For purchase orders that are above an upper-band cost threshold, the University central finance department may choose to conduct its own supplier selection process, e.g. a tender exercise, which will involve some due diligence.

4.4. Criticality of a TRE Supplier

It is necessary to adopt a risk-based approach when determining the scrutiny of assessment for a supplier of TRE assets and services. The TRE/ISMS risk register places emphasis on the confidentiality of data. Most services provided to the TRE only have the potential to impact the availability of TRE data, while some have the potential to impact the integrity; both of which are therefore deemed to be 'non-critical' services (meaning unlikely to impact TRE data confidentiality). Services supplied to the TRE that directly handle TRE Data, or have the potential to impact its confidentiality are deemed to be 'critical' and therefore the corresponding Supplier is classified as critical within the ISMS.

Services provided to the TRE are recorded within the ISMS Asset Register (the Q-Pulse Asset module), where an asset record can be marked as critical within the properties section. A supplier of a critical asset is categorised as a Critical Supplier by selecting 'Yes' within the corresponding Q-Pulse supplier record.

Table 1 lists services/assets provided to the TRE and the corresponding level of criticality:

Asset Type	Criticality (to TRE Data Confidentiality)
Software and licenses	Non-Critical
Electrical power (to server room)	Non-Critical
Temperature control (within server room)	Non-Critical
Server hosting (external to server room)	Non-Critical (as TRE data cannot be made available from an externally hosted service)
Data Backup services (external to server room)	Critical
Network connectivity	Non-Critical
Network vulnerability scanning	Non-Critical
Penetration Testing	Critical
Security Auditing/Standards Certification	Critical
Site security	Non-Critical
Personnel (Recruitment)	Critical
Personnel (Training)	Non-Critical

Table 1

To summarise: the TRE Asset is first classified as a 'Critical Asset' and recorded as such within the Asset Module (See SOP-05-01 Bringing Assets into the TRE for more details). Then, the Supplier Record corresponding to the supplier of that critical asset is flagged as a 'Critical Supplier'.

Q-Pulse doesn't readily allow Asset records to be linked to Supplier records. The only way to achieve a persistent relationship is to link asset purchase/warranty/maintenance events with a Supplier. In practice, this has the advantage that the supplier of asset support/maintenance isn't always the same organisation that the asset was purchased from. It also ensures that each TRE asset must have some record of where it was purchased from and its ongoing warranty/service contract status. SOP-05-01 provides details of how to record these details within the asset record, and link it to the supplier.

4.5. Supplier Assessment Process

In addition to the consideration for information security, the assessment will be commensurate with the criticality and complexity of the product or service to be provided and the maturity and reputation of the supplier and product within the IT industry.

The workflow for approving a TRE supplier is:

Potential Suppliers identified => **Supplier Questionnaire completed (Sections A or B of FORM-010)** => **Completed questionnaire reviewed (Q-Pulse audit record created)** => **Issues identified during review are resolved => Supplier approved/rejected for provision of TRE services/assets**

The Supplier Assessment form (document FORM-010) is split into two main parts: Part A is for new Suppliers (e.g. tender exercise, or setting them as first-time suppliers) and Part B is for existing Suppliers (renewal of their 'approved supplier' status).

In some cases, a supplier may publish information that helps potential customers with their selection, in which case some or all of the assessment questionnaire can be completed by the TRE Operations team.

4.5.1. New Suppliers

Part A Section 1 of FORM-010 must be completed by all new suppliers, and Section 2 by Critical Suppliers. A new Supplier record should be created in the Q-Pulse Supplier's module and a copy of the completed form must be attached to a new Supplier Assessment audit record in Q-Pulse (see Appendix).

4.5.2. Suppliers with ongoing Service Provision

Part B of FORM-010 must be completed every 12 months by all suppliers. A copy of the completed form must be attached to a new the Supplier audit record in Q-Pulse.

4.5.3. One-off Suppliers

For suppliers that provide a one-off product e.g. a software vendor, it may not be appropriate to set up and ongoing supplier management relationship. In such cases, management of the software should be passed on to the TRE Systems Administrator. The TRE Systems Administrator will be responsible for ensuring that the licensing requirements are complied with and that the service is assessed at regular periods to ensure that it does not fall out of support. They will also ensure that information security risks are assessed to ensure that any risks associated with the product which become apparent during use of the product are highlighted to decision makers in the organisation so that they can be mitigated or removed.

4.6. Supplier Assessment Review

After Part A or B has been completed for an individual supplier, it is necessary for the supplier review to be completed by the TRE Operations team. This review is completed as part of an audit record in Q-Pulse and will contain a checklist that forms the basis of the review process and the additional rationale for supplier selection. Some of the checklist questions map directly to the responses on FORM-010, while others are derived from the response expected from several questions.

Where key criteria are not initially met, the supplier can be given the opportunity to provide a resolution within an agreed time limit. Details must be recorded in the audit response, or if necessary raising a security event in Q-Pulse.

In scenarios where the University is allocating the provision of a service to a 3rd party organisation, and where the University has conducted its own assessment of that supplier, it is acceptable for the TRE service to use the findings of the University's own supplier assessment.

4.6.1. Checklist Questions

The list of questions or checks that will be used for the assessment review are:

- QMS certified to a recognised standard
- ISMS certified to a recognised standard
- Staff vetting and training
- Product road map
- Commitment to continuous improvement
- Quality and project planning
- Documentation of user/supplier responsibilities
- Document revision notification
- Business Continuity plan
- Information Security Continuity plan
- Disaster Recovery plan

The final outcome of the assessment review will be included in the Q-Pulse audit record.

4.7. Communication with Suppliers during assessment

Suppliers of critical assets/services must agree to permit and facilitate audits of any relevant aspects of their information security management system by the TRE Operations team and to address any findings of such audits in order to preserve the security of information to the TRE's standards and requirements.

The transmission of information between the TRE and a supplier must be encrypted to a level commensurate with the security classification of the information.

TRE information may not be copied by any supplier other than as far as is necessary for providing an agreed service to the TRE.

Suppliers of critical assets/services must have a security incident reporting process in place to a standard and design acceptable to the TRE to ensure that any incidents involving TRE information are immediately reported to the TRE Operations team. Suppliers must agree to undertake any remedial action required by the TRE Operations team and ensure that this is implemented in an auditable way.

5. Cross-referenced ISMS Documents

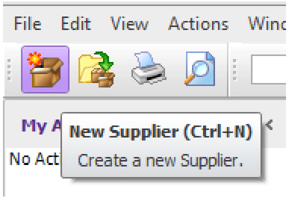
Number	Type	Title

6. Appendices

6.1. Use of Q-Pulse to Manage Supplier Records

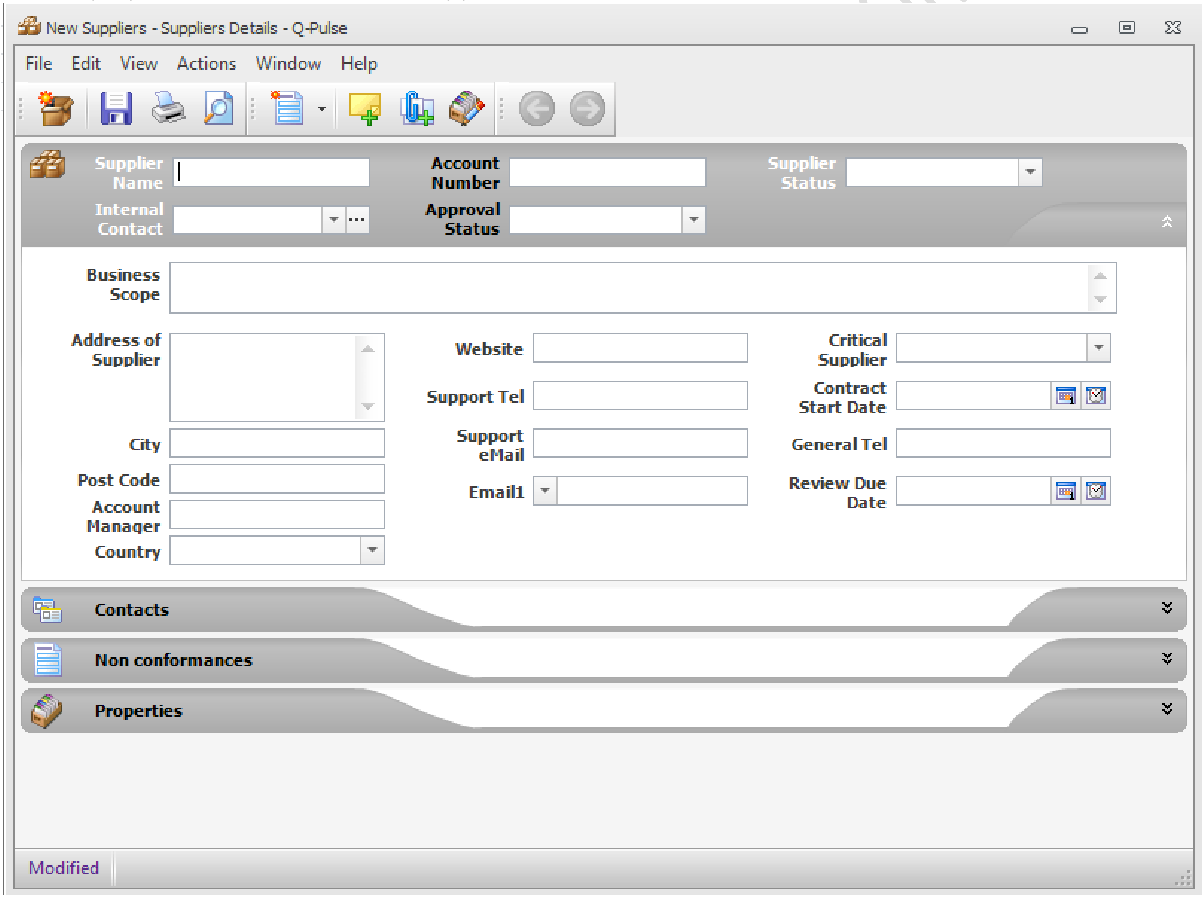
6.1.1. Create a New Supplier Record

From the Supplier module click on the New Supplier icon to add a new supplier



New Supplier (Ctrl+N)
Create a new Supplier.

This displays the screen where the supplier details can be added.



The key fields are:

Supplier Name – The name of the supplier

Account Number – The number of the account with the supplier (their reference)

Supplier Status – To indicate whether the supplier is currently suppling services or not

Account Manager – Name of the primary contact from the supplier

Approval Status – Status of the audit of the supplier

Address of Supplier – Contact address of the supplier

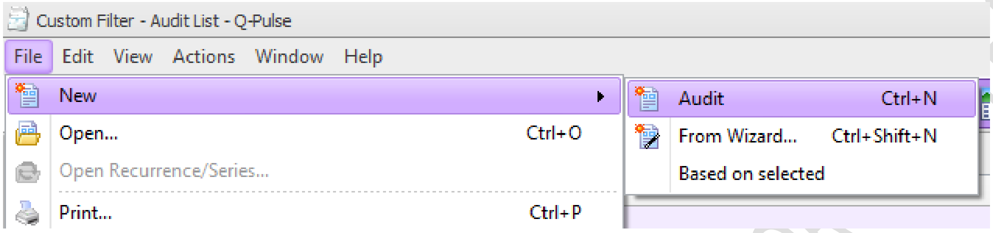
Critical Supplier – Is this the supplier of a critical TRE asset?

Maintenance End Date – Date of the end of the service contract
Review Due Date – When the next audit review is due for the supplier
eMail1 – General or account manager email for the supplier

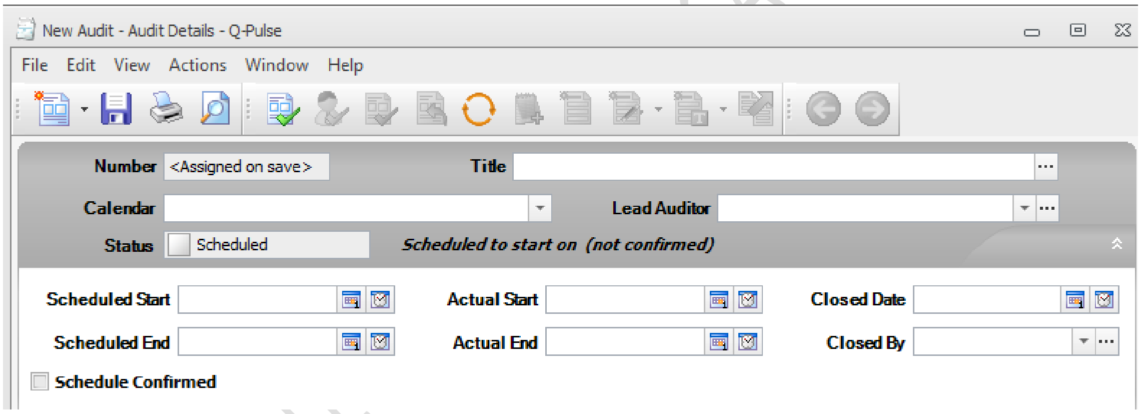
6.2. Use of Q-Pulse to Manage Supplier Audits

6.2.1. Create a New Supplier Audit Record

Use the File -> New –> Audit to create a new audit record.



Complete the necessary audit details

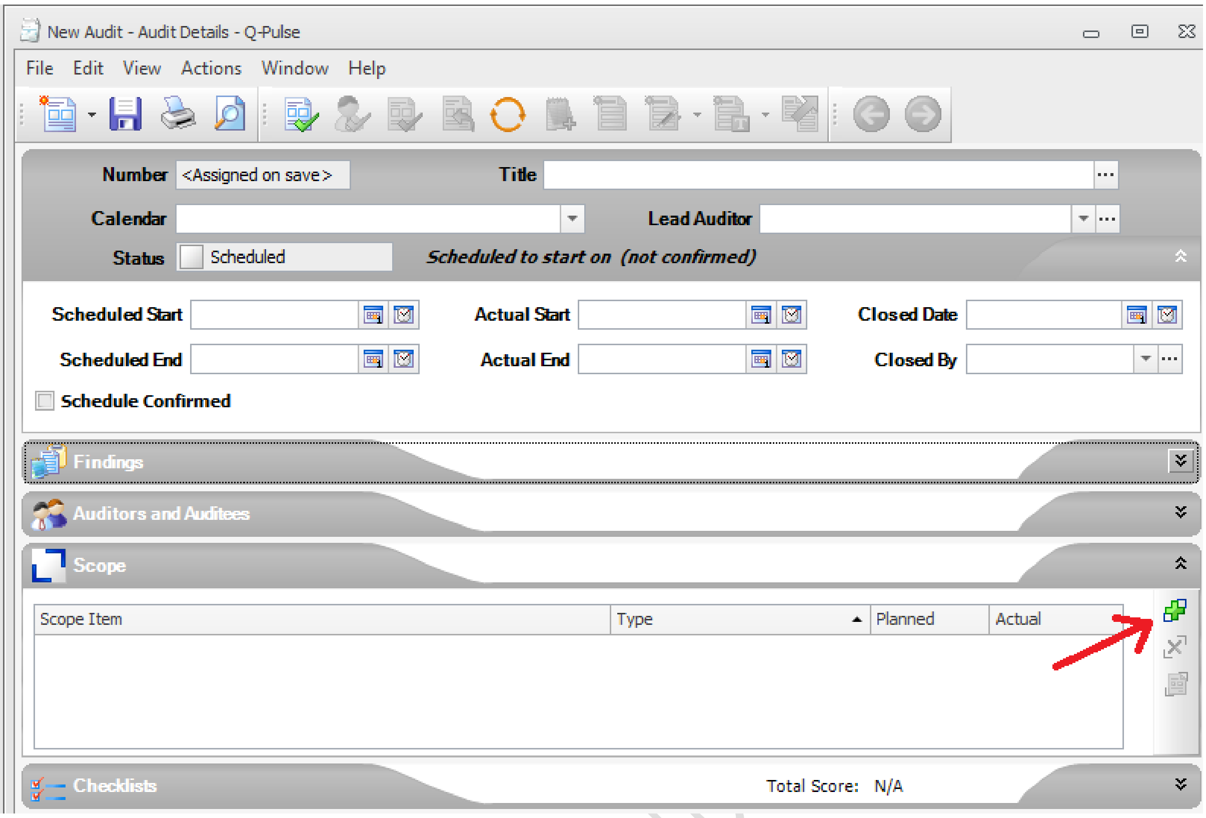


Number <Assigned on save>
Title
Calendar
Lead Auditor
Status Scheduled

Title – Enter the title of the audit ‘Supplier *first/annual* audit – *Supplier name’*
Calendar – ‘Supplier audit’
Lead Auditor – Name of the person completing the supplier audit.
Scheduled Start/End - Enter the audit start and end dates as appropriate

The audit number (SUP-xxx) will be assigned when the record is saved.

Expand the ‘Scope’ section and click on the ‘+’ symbol to add the supplier to the audit scope.


New Audit - Audit Details - Q-Pulse

Number: <Assigned on save>

Title:

Calendar:

Lead Auditor:

Status: Scheduled

Scheduled to start on (not confirmed)

Scheduled Start:

Scheduled End:

Actual Start:

Actual End:

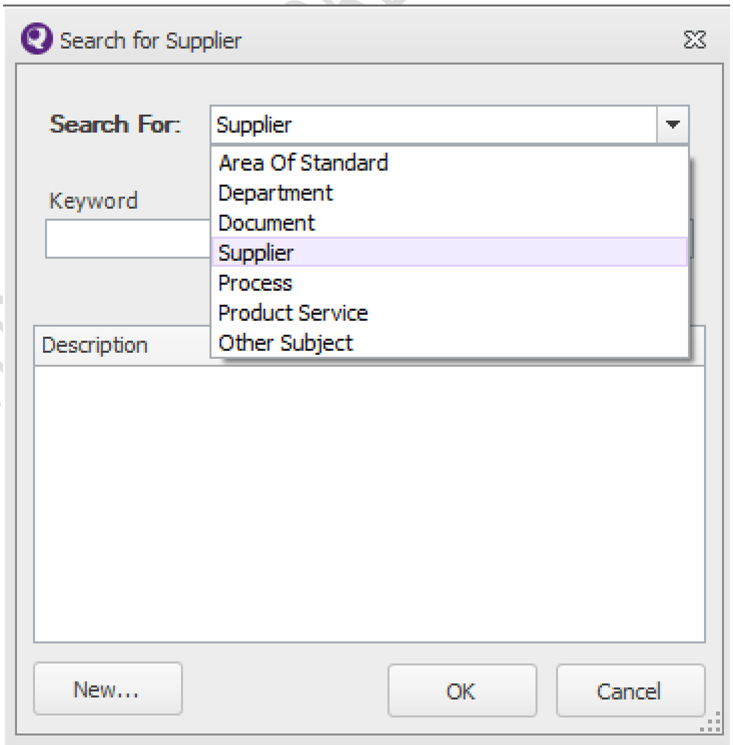
Closed Date:

Closed By:

□ Schedule Confirmed

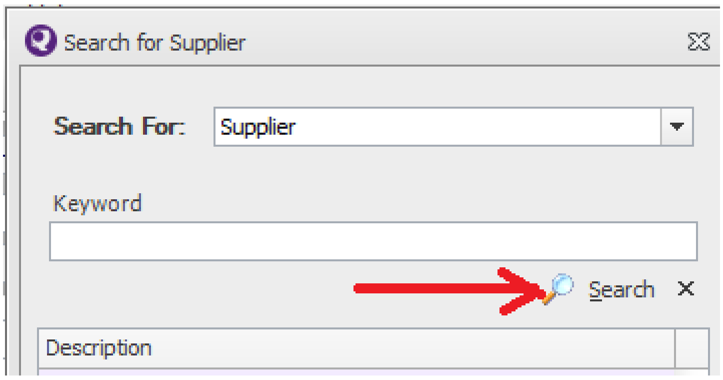
Scope Item	Type	Planned	Actual

Select ‘Supplier’ from the ‘Search For:’ dropdown list.


Search for Supplier

Search For: Supplier

Click on the ‘Search’ button



Search for Supplier

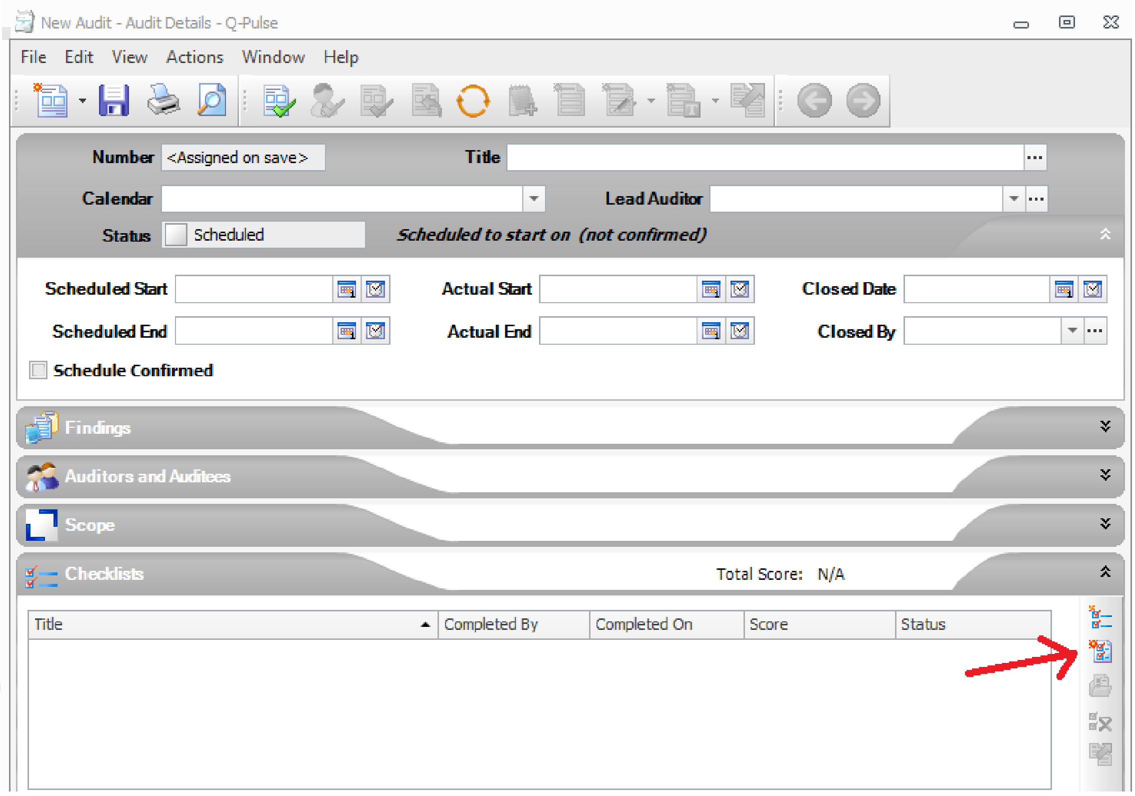
Search For: Supplier

Keyword

This will return a list of the suppliers stored in the Supplier module. Select the appropriate supplier name and click 'OK' to add the supplier to the audit scope.

6.2.1.1. Adding the Checklist

To add the audit checklist expand the checklist section and click on 'Add Checklist from Template'.



New Audit - Audit Details - Q-Pulse

Number: <Assigned on save>

Title:

Calendar:

Lead Auditor:

Status: Scheduled

Scheduled to start on (not confirmed)

Scheduled Start:

Actual Start:

Closed Date:

Scheduled End:

Actual End:

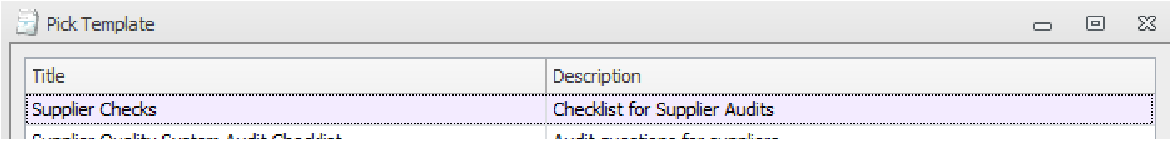
Closed By:

□ Schedule Confirmed

Total Score: N/A

Title	Completed By	Completed On	Score	Status

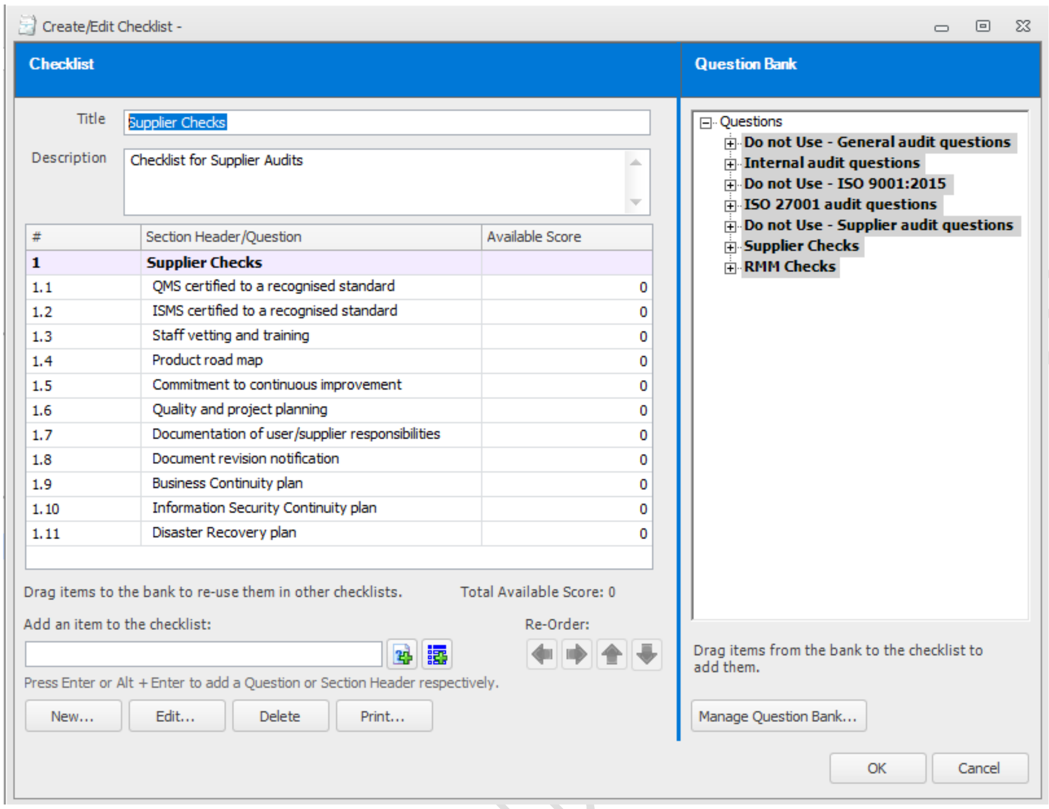
Select the Supplier Checks template and click on 'OK'



Pick Template

Title	Description
Supplier Checks	Checklist for Supplier Audits
Supplier Quality System Audit Checklist	Audit questions for suppliers

This will display the checklist. Click on ‘OK’ and save the audit record.



Title: Supplier Checks

Description: Checklist for Supplier Audits

#	Section Header/Question	Available Score
1	**Supplier Checks**	
1.1	QMS certified to a recognised standard	0
1.2	ISMS certified to a recognised standard	0
1.3	Staff vetting and training	0
1.4	Product road map	0
1.5	Commitment to continuous improvement	0
1.6	Quality and project planning	0
1.7	Documentation of user/supplier responsibilities	0
1.8	Document revision notification	0
1.9	Business Continuity plan	0
1.10	Information Security Continuity plan	0
1.11	Disaster Recovery plan	0

Drag items to the bank to re-use them in other checklists. Total Available Score: 0

Add an item to the checklist:

Press Enter or Alt + Enter to add a Question or Section Header respectively.

Questions
- **Do not Use - General audit questions**
- **Internal audit questions**
- **Do not Use - ISO 9001:2015**
- **ISO 27001 audit questions**
- **Do not Use - Supplier audit questions**
- **Supplier Checks**
- **RMM Checks**

Drag items from the bank to the checklist to add them.

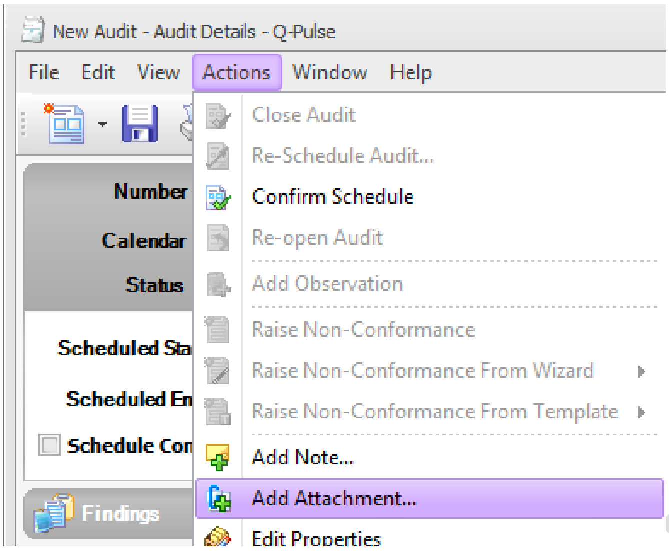
The supplier review checklist contains the following items:

- QMS certified to a recognised standard
- ISMS certified to a recognised standard
- Staff vetting and training
- Product road map
- Commitment to continuous improvement
- Quality and project planning
- Documentation of user/supplier responsibilities
- Document revision notification
- Business Continuity plan
- Information Security Continuity plan
- Disaster Recovery plan

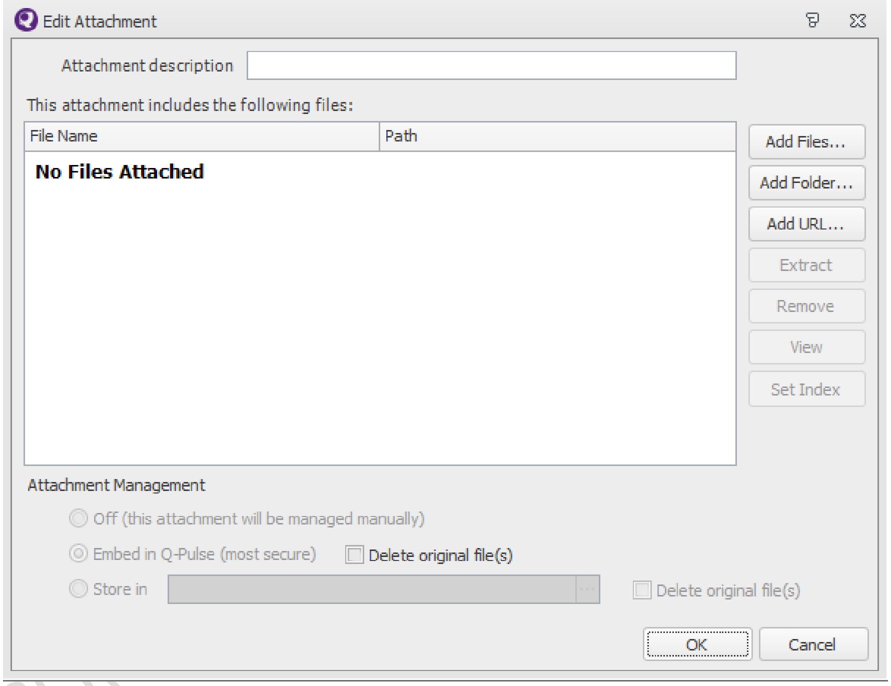
6.2.2. Starting the Audit

To start the audit, enter a date into the Actual Start field and save the record. The audit status will change to ‘Performed’ and the audit can be performed.

Attach the copy of FORM-010 to the audit record using Actions-> Add Attachment.



This displays the ‘Edit Attachment’ dialog.



No Files Attached

○ Off (this attachment will be managed manually)

○ Embed in Q-Pulse (most secure) □ Delete original file(s)

○ Store in □ Delete original file(s)

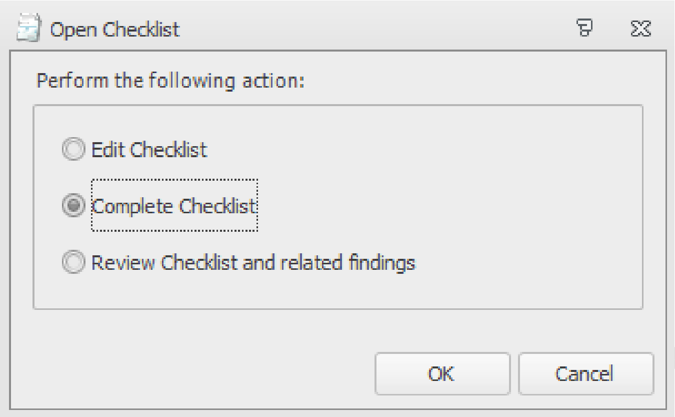
Click on the ‘Add Files’ button to display windows explorer where the file to be attached can be located and selected.

Note: any format of file type can be attached e.g. a Word document (.docx) or a scanned image (.pdf). The file must be closed before it can be attached to Q-Pulse.

After the file has been selected click on ‘OK’ and save the audit record.

6.2.2.1. Completing the Audit Checklist

Expand the Checklist section and double click on the checklist. This will present the dialog providing an option to ‘Complete Checklist’. Select this option and click on ‘OK’



Perform the following action:

○ Edit Checklist

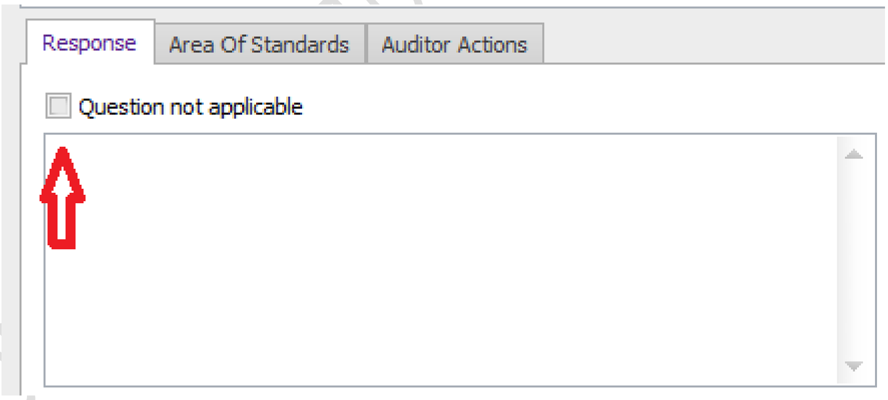
● Complete Checklist

○ Review Checklist and related findings

The checklist will be presented. Click on the Start button to be presented with each checklist question.

Complete the response for each question and use the Next button the progress through the questions until the checklist is complete.

If any question is not applicable for the particular audit, tick the ‘Question not applicable’ box to continue.

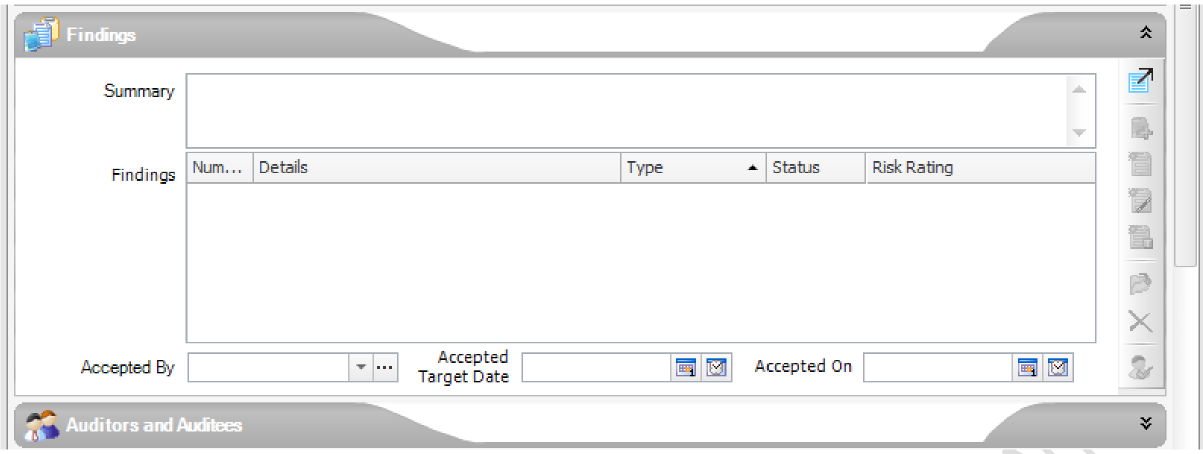


☐ Question not applicable

Save the audit record when the checklist is complete.

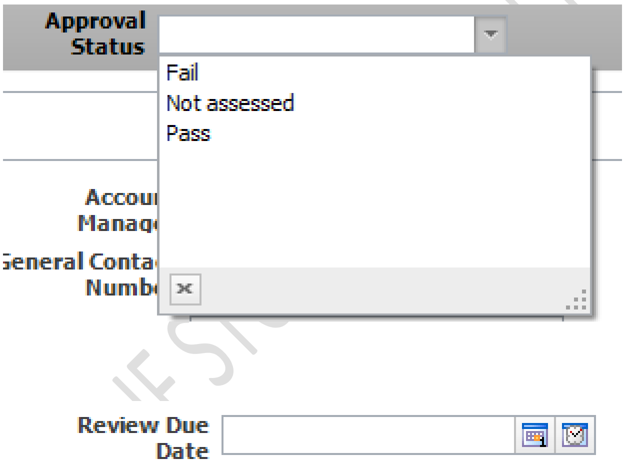
6.2.2.2. Audit Findings

The overall outcome of the audit can be recorded in the ‘Findings’ section of the audit record. This should summarise the outcome of the audit.



6.2.3. Updating the Supplier Record

When the audit is complete the supplier record should be updated to show the new approval status of the supplier and when the next review of the supplier is due.


Approval Status
Fail
Not assessed
Pass
Accou
Manag
General Conta
Numb
Review Due Date