Standard Supplier Cyber and Data Assessment

Supplier assessments help the University to prevent cyber-attacks and data breaches by assessing whether external suppliers could pose a security risk to the University network, IT systems or University data.

It is University policy that staff engaging a new cyber supplier or service carry out an assessment before entering a contract with the supplier or using their product. This should happen regardless of whether there is an associated cost.

There are two levels of assessment. This guidance note describes the Standard process.

When to use the Standard assessment process

You should use the Standard process for any of the following proposals:

- Engaging a new supplier who will have a connection to, or access to, the University IT system or network **AND** where the total value of the contract with the supplier will **not** exceed £10,000.*
- Engaging a new supplier who will handle, or have access to, University data **AND** where the total value of the contract with the supplier will **not** exceed £10,000.*
- Giving an existing supplier a different connection to the University IT system or network or greater access to University data AND where the value of the contract will **not** exceed £10,000.*

⚠ *These contract values are exclusive of VAT. Systems or services which fall into scope but are supplied free of charge to the University should also be subject to this assessment process.

You should **not** use this process for the following proposals:

- Contracts with a value over £10,000. Use the **Enhanced assessment process** instead.
- Research projects involving external research partners. Use the checks in the Research Award Management System to assess cyber security and data protection risks instead.

The process works most effectively when seeking quotations from potential suppliers. This allows you to assess the supplier's security measures alongside the features of their product or service. If you wait until you have identified a preferred supplier and the assessment finds unacceptable cyber security or data protection risks, you may have to re-start the procurement process from the beginning.

How to carry out a Standard assessment

The University uses a questionnaire that the supplier is required to complete for the Standard assessment.

Step 1: Describe the service or software you wish to use

1. Download the Standard Supplier Cyber and Data Questionnaire.
2. Complete Part 1 of the questionnaire. Give brief details of the service or software you wish the supplier to provide and the University data the supplier will have to store or process.
3. Save the part-completed questionnaire in your shared drive with your other procurement documentation.

The member of University staff who completes Part 1 of the Questionnaire does not have to be the budget holder. It can be filled in by any member of staff administering the procurement.

Step 2: Send the part-completed questionnaire to potential suppliers

The questionnaire can be sent as part of your request for infomation from the supplier about their product or service.

Completing Part 2 of the questionnaire should not be onerous for a supplier, but it may involve input from several staff. You may wish to allow the supplier up to ten working days to return it.

Step 3: Forward the completed questionnaire to DDIS for assessment

1. The supplier should return the completed questionnaire to you. They may also provide some supporting evidence or documents as attachments.
2. Digital & Information Services (DDIS) now need to assess the information provided by the supplier in the completed questionnaire. Please log a request for this with the IT Service Desk by emailing servicedesk@abdn.ac.uk or visiting myit.abdn.ac.uk. Attach the questionnaire to the request and include the keyword **SCDA** in the subject.

DDIS will then assess the information provided by the supplier. There are several possible outcomes:

- All security and governance measures appear acceptable. You will be advised that there are no cyber security or data protection issues with the proposal.
- DDIS require additional information to complete the assessment. You will be asked to liaise with the supplier to obtain further information.
- The proposal does not meet the University’s minimum cyber security or data protection requirements. You will be advised that engaging the supplier would breach University policy.

Step 4: Liaise with the supplier to conclude the proposal

Feedback from DDIS will determine what you need to do at this stage.

The proposal can go ahead once there are enough security measures in place to protect the University network, IT systems or University data. This may involve finalising a contract in which the supplier is bound to maintain those security measures for the term of the arrangement with the University.

Liaison with the supplier at this stage can involve several rounds of interaction. You should allow four weeks for this stage before you need the service or software to be in operation.

For any questions about this process, contact the IT Service Desk and ask for help with the Standard Supplier Cyber and Data Assessment process.