Enhanced 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 into a contract with the supplier or using their product.

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

When to use the Enhanced assessment process

You should use the Enhanced 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 value of the contract with the supplier will exceed £10,000.*
- Engaging a new supplier who will handle, or have access to, University data **AND** where the value of the contract with the supplier will 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 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 do **not** need to use this process for the following proposals:

- Contracts with a value of less than £10,000. Use the **Standard 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 at the tender stage of a procurement or 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 an Enhanced assessment

The University uses the Scottish Government Cyber Security Procurement Support Tool for Enhanced assessments.

Step 1: Register to use the Scottish Cyber Security Procurement Support Tool

1. Go to the Scottish Government Cyber Assessment Service webpage.
2. Click on **Complete a Risk Profile Assessment (RPA)**.
3. Select **Register for an account**.
4. Select **Buyer** as the type of organisation, and select **UNIVERSITY OF ABERDEEN** from the picklist.
5. Complete the registration form with your name and contact details, and accept the terms of use.

The member of University staff who registers and completes the RPA does not have to be the budget holder. Any member of staff engaging a supplier can use the Service.

6. Activate your account when you receive the confirmation email from the Cyber Security Procurement Support Tool (CSPST). Follow the steps to authenticate your account.

Once registered, you use the Service to generate a bespoke questionnaire for the supplier to complete. This is known as a Risk Profile Assessment (RPA). The RPA is based on the minimum security requirements the University would expect the supplier to be able to meet for the software or service you wish to procure.

Step 2: Complete a Risk Profile Assessment

1. From the CSPST homepage, click on **Complete a Risk Profile Assessment (RPA)**.
2. Work through the RPA, answering the questions on each screen to create a risk profile.

   You will need to provide outline information about the proposal, the data processing involved, integration with the University's IT network and the impact in the event something goes wrong.

There is explanatory guidance alongside many of the questions in the RPA. If you want further help to answer the questions, contact the IT Service Desk and ask for help with the Enhanced Supplier Cyber and Data Assessment process.

3. At the end of the initial set of questions, you will be asked to confirm your answers by ticking a check box. Click **Get Risk Profile**.
4. The system will generate a draft Risk Profile Assessment Report as a pdf document. Download it and save it to your shared drive.
5. Digital & Information Services (DDIS) now need to review the draft Report before it is completed. 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 draft Risk Profile Assessment Report to the request.
6. DDIS will recommend whether to add additional questions, or to ask the supplier to provide certification or supporting evidence.
7. The system will generate a final Risk Profile Assessment Report as a pdf document.
8. The Report will have a Risk Assessment Reference, an 8-character reference for use in the next step.

Step 3: Ask the supplier to complete the Supplier Assurance Questionnaire

Send the link to the Cyber Security Procurement Support Tool, to the supplier with the 8-character Risk Assessment Reference.

The link and Reference can be included in the tender documentation you require the supplier to complete or as part of your request for further details about their product or service.

Ask the supplier to register to use the Scottish Government Cyber Security Procurement Support Tool and complete the Supplier Assurance Questionnaire (SAQ) using the Risk Assessment Reference provided.

Answering the SAQ 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 complete it.

Step 4: Forward the completed questionnaire to DDIS for assessment

1. The supplier will return the completed SAQ to you with the other tender documentation.

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 5: 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 sufficient 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 Enhanced Supplier Cyber and Data Assessment process