Security and Privacy Assessment Process and Checklist

Enterprise Information Security

Contents

1. Introduction

The security assessment and privacy assessment are a collaborative process that identifies security and privacy issues and evaluates the level of risks that could be affected by a cyberattack, data breach or other related security incidents. A risk is defined by the level of financial loss, disruption, or damage to the reputation of the university from some sort of failure or misuse of information and systems.

The requirement of the security assessment should be initiated by the Enterprise Architecture Services Team after initial analysis and capturing business requirements for any new technology or services. The business case and solution design document or detailed design document should be completed prior to requesting a security assessment via Service Central.

The security assessment must be completed prior to the privacy assessment, which will allow the Privacy Officer to make an informed decision about the identified risks and if the risk is acceptable or not based on ACU's risk appetite.

Step 1 – Security Assessment

The security assessment process is to ensure appropriate protection and safeguard for the university information and systems; therefore, the risk analysis will be performed based on the following documents.

- **Business case or Proposal for Business change** – key document to support the service or product or project to justify the benefits to the university.
- **ACU ICT Security Assessment Template V3** – This should be completed by the vendor.
- **HECVAT** – HECVAT is a questionnaire framework for the third-party vendor's assessment tool that appropriately assesses security and privacy needs unique to higher education to measure vendor risk. This could be included if the vendor is willing to share the completed HECVAT or agree to complete the HECVAT **instead of** the ACU ICT Security Assessment Template V3.
- **Solution Architect Document (SAD)** – Blueprint for the solution with all aspects and concerns from the target solution and transition from as-is to to-be state. This should include the stakeholder information and ACU point of contact for the vendor and the vendor's website.
- **Detailed Design Document** for Project Planning and Development (high and low level) for all automated and enhancement projects. This should include the stakeholder information and ACU point of contact for the vendor and the vendor's website.

The security assessment request should be submitted via Service Central. Ensure that all documents relevant to the requested security assessment are attached to the request. The Enterprise Information Security Team cannot perform an accurate security assessment if the necessary documents are not submitted with the request. If the documents are NOT fully completed, this will cause delays to the assessment process.

Step 2 – Privacy Assessment

The privacy assessment that is conducted by the Privacy Coordinator requires the following documents.

- **ACU Vendor Checklist for Privacy Impact Assessment (PIA)(Ver 5)** – This must be completed by the vendor.
- **DOC2 32550 Privacy Impact Assessment Template V6** – This must be completed by the ACU stakeholder.
- **Security Assessment Report** – This is completed by the Enterprise Information Security team in Step 1 above.

Ensure that all documents relevant to the requested privacy assessment are FULLY completed before submitting the request via Service Central.

For further information about Cybersecurity, please contact the Enterprise Information Security Team: IT.SecurityAssessments@acu.edu.au or security assessment request via Service Central. For Privacy, contact privacy@acu.edu.au or Service Central / Privacy Advice.

2. Documents to be submitted

The following documentation must be provided as part of the security assessment and privacy assessment process to ensure an efficient and timely outcome.

Document	Attached
Business case or Proposal for Business change	□
Solution Architect Document (SAD)	□
Detailed Design Document (for all projects)	□
ACU ICT Security Assessment Template V3	□
HECVAT (if vendor has completed)	□
ACU Vendor Checklist for Privacy Impact Assessment (PIA)(Ver 6)	□
DOC20 32550 Privacy Impact Assessment Template V5	□

Vendor Liaison Checklist

All the documents that are required assist the Enterprise Information Security team and the Privacy team to assess risks effectively to strengthen ACU's security posture. Therefore, ensure all documents relevant to the security and privacy assessments are fully completed by the vendor and stakeholders before submitting the request via Service Central. Submitting documents with partial responses may result in a delay in the security and privacy assessment process which may lead to a postponement of projects.

The following contents outline some tips on liaising with vendors:

- All documents are fully completed and verified for inconsistent or misleading responses as it will slow down the assessment process.
  e.g., check vendor's responses, they might state data storage is AWS Sydney in one document and then state data storage is AWS UK in another document.

- The responses are not populated with links that refer to other external documents/sources.
  e.g., a link to a whitepaper or a website for ACU to research and source information for the questions.

- Answers provided by vendors are deemed to be binding. Therefore, ensure that the right person/team completes the ACU's key assessment documents, not the sales team.
  e.g., Document templates such as ACU ICT Security Assessment Template V3 or HECVAT are completed by Security or Risk Management Team, Vendor Checklist for Privacy Impact Assessment (PIA) and DOC20 32550 Privacy Impact Assessment Template V5 are completed by the Data Protection Officer (DPO).

3. Security & Privacy Assessment Process

The following process will be used to complete the security assessment and privacy assessment.

	Process Team	Task
1	**Enterprise Architecture Services** Evaluate the business objective and identify security/privacy assessment requirements.	Create the Business case or Proposal for Business Change and Solution Architect Document (SAD) or detailed design document (for automated projects) that provides detail about the product/service/project. **Note***: If it is an automated project, a Detailed Design Document for project planning demonstrating high and/or low-level design is required in addition to the business case.*
2	**Enterprise Architecture Service** Gather information for the security assessment and privacy assessment by liaising with the stakeholder and/or vendors of the product/service or project development team.	Actions to be taken: • Contact the vendor for HECVAT **or** forward the ACU ICT Security Assessment template V3 to the vendor to complete. • Forward the Vendor Checklist Privacy Impact Assessment (PIA) to the vendor to complete. • Forward the DOC20 32550 Privacy Impact Assessment Template V5 to the ACU Stakeholder to complete.
3	**Enterprise Architecture Service** Submit the security assessment request to Enterprise Information Security via Service Central under the category - “Security Assessment”.	The request must include the following documents: • Business case • Solution Architect Document (SAD) • Detailed Design Document for all new automated projects. • HECVAT or ACU ICT Security Assessment Template V3 • ACU Vendor Checklist for Privacy Impact Assessment (PIA) Ver 6 • DOC2 32550 Privacy Impact Assessment Template V5
4	**Enterprise Information Security**	Conduct the security assessment: • Identification - conduct initial information analysis • Assessment – Identify security controls and define risks • Define mitigation strategies and recommendations to reduce the likelihood of identified risks.
5	**Enterprise Information Security**	Forward the Security Assessment Report to Enterprise Architecture Services as per the Service Central request, and to the Privacy Coordinator.
6	**Privacy Coordinator**	Conduct Privacy Assessment based on completed Security Assessment Report and privacy documents.
7	**Privacy Coordinator**	Request approval from the Privacy Officer to proceed (based on the sensitive information and data residency information).

Appendix A - Security Assessment Checklist

The following checklist will assist what information is required for the security assessment and privacy assessment. It outlines key steps to take before requesting a security assessment and privacy assessment to the Enterprise Information Security team (EIS).

	Checklist	EIS
1	Is the security assessment for a new product, service, or project? Product □ Service □ Project □	
2	If it is a new product, is it currently in use? Yes □ No □ Please provide information.	
3	If the security assessment is for a new product or service, please provide the ACU stakeholder contact information.	
4	If the security assessment is for a new product or service, did the Enterprise Architecture Services Team evaluate the business objective? Yes □ No □ N/A □ Is the case Business case or Proposal for Business chang**e** attached? Yes □ No □ Is the Solution Architect Document (SAD) attached? Yes □ No □ N/A □	
5	If the security assessment is for a project, is it a new project or enhancement? New Project □ Enhancement □ What stage of the project is it currently at? Is the Detailed Design Document attached? Yes □ No □ Is the IT engagement questionnaire completed? https://acu.service-now.com/service_central?id=service&sys_id=e6b6fde3dbcc6340cc45e3334a96193b Yes □ No □	
6	Is ACU ICT Security Assessment Template V3 completed by the vendor and attached?	

	Checklist	EIS
	Yes □ No □	
7	Has the vendor completed HECVAT? Yes □ No □ If yes, HECVAT is attached? Yes □ No □	
8	Is the ACU Vendor Checklist for Privacy Impact Assessment (PIA) Ver 6 FULLY completed by the vendor and attached? Yes □ No □	
9	Is the DOC20 32550 Privacy Impact Assessment (PIA) Template V5 completed by the ACU stakeholder and attached? Yes □ No □	

Appendix B - References to Documents

- **HECVAT – HIGHER EDUCATION COMMUNITY VENDOR ASSESSMENT TOOLKIT**

HECVAT provides an easy-to-read A-F rating system that assists the Enterprise Information Security Team to quickly analyse and make a better-informed decision about vendor security.

The **HECVAT**, or Higher Education Community Vendor Assessment Tool, is a questionnaire framework designed to help institutions of higher education measure their vendor risk. HECVAT was developed by EDUCAUSE's **Higher Education Information Security Council (HEISC),** a team devoted to security, data governance, and compliance in higher education. Note that the latest version of the template needs to be used.

The following HECVAT tools can be used:

- **HECVAT, Full 3.03:** A 265-question framework for vendor assessment or
- **HECVAT, Lite 3.03:** A lightweight questionnaire used to expedite the vendor onboarding process.

- **ACU ICT SECURITY ASSESSMENT TEMPLATE V3**

  ACU ICT Security Assessment v3 (name of application).xlsx

- **DOC20 32550 PRIVACY IMPACT ASSESSMENT TEMPLATE V5**

  DOC20 32550 Privacy Impact Assessment Template V5 (2).docx

- **VENDOR CHECKLIST FOR PRIVACY IMPACT ASSESSMENT (PIA)**

  ACU Vendor Checklist for Privacy (PIA) (Vers 6) (INSERT VENDOR NAME HERE).xlsx