UCD IT Services
Seirbhísí TF

IT Security Review Process (Web Version)

Published: April 2020

Updated: January 2021

Contents

1. Background

UCD is a large, diverse institution with 120,000 active IT accounts and up to 70,000 unique devices connecting to the network on any given week. The University relies on a large and complex IT environment to support its core operations.

The University has seen significant increases in cybercrime over the past decade. Never more so than at the present time has cybersecurity been so important in terms of protecting the University's reputation, the availability of IT systems, and the confidentiality and integrity of staff and student personal data.

In order to mitigate against these risks, security reviews need to be undertaken on the critical IT solutions and systems of our IT architecture. The purpose of these security reviews is to identify and document unmitigated risks that may exist on new or existing university information systems or information technology (IT) solutions and provide recommendations to mitigate these risks.

The purpose of this document is to define the IT Security Review Process to clarify when a review is needed, how it is undertaken and who needs to be involved.

2. IT Security Review Process

- 2.1 When to carry out an IT Security Review

An IT Security Review should be undertaken on all critical IT solutions and systems including systems located on-premise or hosted externally (e.g. cloud solutions) that process confidential or personally identifiable University information such as financial records, assessment details, student, staff or alumni records, in any of the following instances:

- When a new IT system or solution is being deployed. In this scenario the security review should be included within the scope of the deployment project.
- When an existing IT system or solution is being upgraded or replaced or there is a significant change to the system architecture or platform. In this scenario the security review should be included within the scope of the upgrade project.
- For existing enterprise systems or solutions that do not have a planned upgrade, a security review should be undertaken on a regular basis, ideally every 5 years. This should also include cloud solutions. In this scenario, the security review may be treated as a project in its own right.

The IT Security team within IT Services can also offer advice and should be included in the conversation early on in the process.

Note

- Security reviews will typically be undertaken by an external security consultancy company. Where a security review is undertaken as part of a new implementation or upgrade project, the cost of the review will need to be budgeted for within the project costs.
- When purchasing a new cloud service or replacing an existing on premise system with a cloud service, IT Services Cloud Security Assessment Questionnaire should be completed by the Project Manager/Supplier of the cloud service as part of the discovery and initiation phase of the project. The completed evaluation document will help determine the scope of the security review.
- For a scheduled review of an existing system, the IT system owner is responsible for ensuring that a stand alone project is included in the list of IT projects and that a project manager and budget, which is typically €25k has been allocated to the project.
- The IT Services Project Management Framework (www.ucd.ie/itservices/itpmo) includes a reference to the IT Security Review as a reminder to project managers.

- 2.2 Key steps when carrying out an IT Security Review

	Step	Responsible
1	Liaise with the IT Security team during the Initiation & Discovery phase of the project to determine the scope of the review. For cloud service reviews, the Cloud Security Checklist must be completed by the Project Manager/Supplier of the cloud services prior to commencing the review. The completed document will help inform the scope of the security review. The completed document should be sent to the IT Security Team for review.	IT Project Manager
2	Create a Request for Quotation (RFQ) document which will be sent to an external IT Security Partner in order to provide a quotation for the review. *This may require a two-phase approach where Phase 1 focuses on the security of the architecture/Platform of the proposed solution and Phase 2 which will test the security of the solution, including any dependencies where the security of the services is shared between the supplier and the University such as data integration points, network access controls, account security, peripheral devices, University processes and procedure, etc.* *Assuming a satisfactory recommendation out of Phase 1, UCD will proceed to implement the new solution, which will then allow for the Phase 2 security review and penetration test of the deployed solution.* See appendix A below for "Security Review RFQ - Document Template" **Important considerations before sending an "RFQ".** ● Will the cloud service provider allow an external penetration test of the service under review? This should be clarified with the provider before sending out the "RFQ" as it will have a bearing on the cost. If the cloud provider is unwilling for UCD to undertake an independent penetration test, the supplier should be asked to provide a copy of the results of the most recent test including the date of the test, its finding and name of the company who carried out the test. A copy of these findings should be provided to UCD's security partners as part of the review. ● If UCD has permission for a penetration test, it will need to be clarified if the test can be conducted in a live or test environment and if the test can be undertaken inside or outside of normal working hours? Any tests outside normal working hours may incur additional charges. This should be clarified in the "RFQ", so that the IT Partner can provide an accurate quote up front.	IT Project Manager Review draft version with IT Security team and members of IT Services who may be involved in the delivery of the service, such as Servers and Storage (Authentication), Networks team (VPN, network access, ports, etc), etc

	• What environment can the security reviewed, Test, Dev or Production? • What notice period must be given to the supplier prior to the test commencing. • What is the extent of the review, penetration test, vulnerability assessment, network review, process review, etc. • Will the review include a security review of integration components between UCD systems and the new services? If so, will the API's be available for the review? • Will the review include a review of the business processes and procedures such as user account management, access security controls, authorisation procedures? If so, this documentation must be available for the review? • Does the security of the service depend on any University security controls, processes or policies? If so, these dependencies will need to be included in the security review of the service. • Is a non-disclosure agreement required between UCD, the Supplier of the systems and\or the security Partner in order to share information and findings between all parties?	
3	On the basis that the cost is under €25k, a three quotes approach can be taken rather than a full tender. *The IT Security team can advise on supplier contact details.*	IT Project Manager
4	Arrange a review of the RFQ responses with key project members. The review should include a member from the IT Security team and members of other IT Services teams who will be involved in the delivery of the service e.g. Servers and Storage for SSO / MFA, Networks for integration with existing services, EAG for API development, etc. Choose the most appropriate security firm to carry out the review. There is a template Security Service Scoresheet available in the project's directory.	IT Project Manager
5	Execution of the Security Review. Project Technical Lead to provide external security consultants with • Application and architecture details. • Provide access to system, typically accounts with different levels of permissions • Architecture documentation, including integrations with existing systems. • Service level descriptor of the new service. • Intrusion prevent and detection tools and procedures to detect, prevent and respond to security incidents. • Completed cloud security review (if available)	IT Project Manager

	● Any other details relevant for the security assessment. ● Ensure that UCD staff and external suppliers are available to answer any questions that arise during the review. This may involve answering security questionnaires, conference calls or emails between parties, etc. The external security team may require meeting or calls with UCD's technical support and development staff including EAG developer, Infohub support team, UCD Networks, UCD Email delivery team and external suppliers such as HEAnet (SSO security), Version 1, etc. ● Arrange dates and times to carry out the review. Security testing times may be required to be outside of business hours depending on the supplier's requirements. ● Assist with any technical security requirements between the supplier and the security company.	
6	Arrange a review of the draft security report with UCD IT Security team, the system owner, IT consultancy partner and the Business owner. If IT Services is both the system and business owner of the system under review, then include a senior member of staff from the department who is responsible for the data that the system processes. e.g Finance, HR, Registry, Alumni, etc.	IT Project Manager
7	Send the draft report to the system supplier and organize a review meeting between all parties including the IT security partner, business owners, technical personnel from the suppliers company, UCD IT Security team and business or data owners from UCD.	IT Project Manager
8	Agree the final version of the report and what actions are required to be completed prior to and after go-live. The IT Project manager is responsible for ensuring that the findings and actions from the review are notified to the Project Steering Group, Business Project Manager, IT Security Team and Data Owner.	IT Project Manager
9	Liaise with the system supplier on the reports security recommendations and incorporate all actions from the security report into the project plan.	IT Project Manager
10	A. *Reviews of new or upgrades to existing services* Follow-up with suppliers on implementation of high-risk actions pre go-live. <Go to step 11>.	IT Project Manager.

	B. Scheduled stand alone reviews of existing systems Any critical or high risks discovered during the review of an existing system should be immediately sent to the relevant group responsible for the risk, this could be a third party support provider (Version1), IT Services support team e.g. UCD Networks or the system or software provider. The IT Project manager is responsible for ensuring the Business Owner, Data Owner and IT Security team are made aware of any critical or high risks discovered during the review and ensure that any issues are escalated with the team responsible. <Skip to step 12>	
11	Decision on Go Live - Go/No Go will depend on the outcome of the security review and if any critical or high issues can't be addressed before going live. The IT Project manager is responsible for ensuring that the Steering Group, Business Project Manager, IT Security Team and Data Owner are made aware of any critical or high risks before deciding if to go-live with these risks or postpone. Any decision to go-live is the responsibility of the Steering Group, Business Project Manager and Data Owner, who must accept any known critical or high risks.	IT Project Manager
12	Follow up on the implementation of remaining medium/low risk actions either post go-live or in the case of a schedule review, the fixes should be applied in line with the reviews recommended timelines, typically within 2 weeks for medium issues and 4 weeks for low issues. The IT Project manager is responsible for ensuring that the Steering Group, Business Project Manager, IT Security Team and Data Owner are kept updated on the progress of any outstanding risks. The Steering Group, System Owner, Business Owner and Data Owner are responsible for accepting all risks that cannot be addressed post go-live.	IT Project Manager *IT Security can provide the Project Manager with assistance following up on any outstanding risks.*

Appendix

1. Security Review RFQ - Email Template

Subject: Security review services for UCD - Request for Quotation

Dear <Name of IT Security Partner>

Please see attached a request for quotation, detailing security review services required by University College Dublin.
Please note that email responses are requested by <Date of Submission>. Please do not hesitate to contact me if you require any further details.

Regards,
<Project Manager>

2. Security Review RFQ - Document Template

1.Overview

UCD <*customer name, e.g. Registry, HR, IT Services*> is undertaking a project to <*enter brief description*>. Following a procurement process, the <*product/solution name*> solution from <*supplier name*> has emerged as the preferred solution. This is a comprehensive solution which will have <on-premise and cloud components>.

The purpose of this document is to outline a request for tender for services required by University College Dublin to conduct a security review of key components of the new system.

1.1 Services Required

The services required are a security assessment of <*System name*> to ensure that the system has implement appropriate technical control to detect, prevent, and respond to security threats. This should include the following:

- A vulnerability assessment and penetration test of <system name>.
- A review of the <system name> architecture design, backup procedures, disaster recovery policy and business continuity plan to ensure that the system meets the University expectations in terms of availability and data recovery.
- A review of <system name> intrusion detection and prevention technical controls and procedures to protect, detect and respond to security related incidents.
- A security review of the Integration between <system name> with UCD SSO authentication service.
- A security review of how University accounts and permissions will be managed, including the procedures for the creation and deletions of accounts, managing user permissions, etc.
- A review should highlight any security risks from University dependencies that are outside the direct control of the <System name> such as the use of BYOD to access the system.

Where necessary, UCD would expect the external security partner to be available to spend some time on-site at UCD to attend meetings and discuss findings with UCD staff.

The successful bidder will also be required to organise and manage communications with <supplier name>.

1.1 Alternate Services Require (IF two Phases are required)

Phase 1 – Architecture Review

- Review of the architecture of the <*product/solution name*> solution. The solution is <*give brief overview – is it on-premise, cloud based, maybe a hybrid of the two? SaaS, Iaas. etc. Does it include new hardware components*>
- This phase of the review will require a deep knowledge of XXX in order to assess its ability to operate securely within the UCD environment, as well as understanding the security issues that arise when connecting <*xxx*>

During this phase, UCD will provide the external security partner with documentation provided by <supplier name> in relation to its architecture and security. We will also provide a contact in <supplier name> who can be consulted as questions arise.

Phase 2 – Detailed Security Review & Penetration Test

- Penetration testing and vulnerability assessment of the <*system/solution name*> system and architecture.
- The review should highlight any security risks from University dependencies that are outside of the direct control of the system or service e.g
    - Risks from University's account access security controls and procedures e.g any risks introduced from UCD's Single Sign On, password policy, etc.
    - Risk from endpoint devices either University owned or BYOD.
    - Risk from University network security controls where the security of the system or components of the system relies on the University's network to provide security.
    - Risk due any changes to the application security settings that are not inline with the application vendors recommended security settings.
- Review of the security of any proposed integrations with UCD's other business systems.
- A review of proposed processes and procedures proposed for the support and management of <*system/solution name*>*. This should include a review of* user account management procedures (joiners, leavers & movers), application and access security controls, etc.
- Review of the systems intrusion prevention and detection technical tools and procedures which have been implemented to protect, detect and alert system owners to cyber security risks.
- Review of any custom development (API) required for the ployment of the service, such as account management, user permissions, data flows between existing University systems and databases, etc. if applicable).

Where necessary, UCD would expect the external security partner to be available to spend some time on-site at UCD to attend meetings and discuss findings with UCD staff.

The successful bidder will also be required to organise and manage communications with <supplier name>.

2.Deliverables & Timelines

In the case of both phases, the expected output of a review is a security report including all risks and vulnerabilities discovered during the review.

The report should include an **executive summary** which includes a list of all key findings and their perceived severity. The severity of each risk should be calculated using a combination of the business impact and the likelihood of the risk occurring, for example

		Likelihood of occurrence		
		Unlikely	Possible	Likely
Business Impact	Insignificant	Low (1)	Low (2)	Medium (3)
	Minor	Low (2)	Medium (3)	Medium (4)
	Moderate	Medium (3)	Medium (4)	High (5)
	Major	Medium (4)	High (5)	High (6)
	Critical	High (5)	High (6)	Critical (7)

The **main body of the report** should include a detailed explanation for each finding, including a technical description of the risk, the potential impact to the business should the risk not be resolved and recommendations on how to resolve or mitigate the risk.

Phase 1 Timelines

UCD requires the following timelines to be met.

Supplier Response	
Preferred Supplier Chosen	
Contract Signed and Work Started	
Draft Report Phase 1	
Review of findings by all parties	
Final Report Phase 1	

Phase 2 Timelines

Phase 2 timelines are subject to the timescale specified for implementation of the software. Indicative timelines are <*XXX*>

UCD may request additional assistance to subsequently review specific fixes implemented to address issues identified by this review and advise how effectively each risk has been mitigated. A daily rate is requested to address any additional assistance required.

3. UCD's Responsibilities

UCD will provide the following input to the project:

- Resources to assist with technical access and knowledge of UCD's systems

- Manage the notification to the Software Vendor in relation to scope and timing of review.
- Assist with determining the level of business impact associated with any risks identified.
- UCD to ensure all relevant release letters, non-disclosure and security test agreements are signed between the Security Review Partner, Software Vendor and UCD.
- Coordinate on follow up actions from the security review

4.Technical Overview

4.1 Infrastructure

<Provide an infrastructure overview>

Further details regarding University integration points and processes with the *<system/solution name>* will be provided on commencement of the project.

4.2 Database

<Provide a Database overview>

4.3 Interfaces

<enter the new system name> will interface with university systems including.

- *E.g. Identity Manager*
- *etc*

Also include any data extracts.

4.4 Application

<Provide a System/Application overview and associated modules within it>

4.5 Authentication & Access

<Provide details of the proposed authentication method, e.g. SSO, and how access will be managed and maintained – who can see what>

5.University College Dublin

University College Dublin is the largest University in Ireland with seven colleges and thirty-eight schools offering a comprehensive range of undergraduate and postgraduate programmes. The University is a research-intensive institution. Its student population is approximately 30,000, including more than 4,000 international students. The University is also a major employer with over 4,000 personnel. The main campus of the University is situated at Belfield, about 5 km to the south of the centre of Dublin. Further information on the University is available via the internet at www.ucd.ie

6.Supplier Response

Please email your responses, to include costs that are inclusive of VAT, to *<enter name and email address of the IT Services Project Manager>* (cc itadmin@ucd.ie) by *<enter deadline – date and time>*

Responses should include:

- The Company's approach to fulfilling the requirements outlined
- Confirmation of deliverables
- Confirmation of timelines (or if it is felt the above timelines cannot be met, tenderers should propose an alternative timeline)
- The number of days, rates per day and total cost
- Daily Rate for additional services requested as part of this review
- Out of hours rates (if applicable)
- Agreement that the findings from the review, including initial draft finding can be shared with the supplier of the system or cloud service under review.
- CVs of staff who will be involved in the engagement
- 2 references to comparable organisations where similar security services have been delivered.
- Responses should not exceed 5/6 pages in length, excluding staff CVs.