University of Toronto

Information Risk Management Questionnaire

For Information Services

# Introduction

When considering new or upgrades to information services for use at the University of Toronto, it is essential to understand the risk to the University that the new / upgraded service presents. This is done so that a decision may be made in full awareness of risk whether to proceed with the proposed service, modify it, or select another service entirely (and repeat the process of risk evaluation).

Risk to the University through the use of information services can occur for many reasons – threats to private or personally identifiable and other sensitive information, or vulnerabilities in the software, hardware, out-sourced or built-to-order components. This questionnaire’s purpose it to identify those sources of risk so that risk mitigation action may be taken.

Ideally, this questionnaire would be done as part of a product or vendor discovery process, such as in an RFP phase, prior to product or vendor selection and would remain with the project documentation, being updated throughout the project lifecycle to reflect risk management decisions. If the Information Security and Enterprise Architecture (ISEA) department of the Information Technology Services (ITS) portfolio is not coordinating the completion of the questionnaire with product suppliers and project managers, we request that copies of the completed questionnaire be returned to ISEA to be held in confidence for future reference.

The final product of the questionnaire and interviews with suppliers are the Privacy Impact Assessment and the Threat / Risk Assessment document (IRMA) that articulates the potential risks represented by the proposed solution, in the context of existing University of Toronto risk mitigation services, infrastructure and practices.

# Document Control Information

## Project and Sponsor, University of Toronto

|  |  |
| --- | --- |
| Date |  |
| Project Title |  |
| Sponsor |  |
| Department |  |
| Departmental Data Custodian |  |
| Project Lead |  |
| Lead’s Contact Details |  |
| PIA/TRA lead |  |
| PIA/TRA contact details |  |

## Vendor / Supplier Name:

|  |  |
| --- | --- |
| Vendor / Supplier name |  |
| Contact Name |  |
| Contact Details |  |

Contents

1. Introduction 1

2. Document Control Information 2

3. Product Summary and Asset Enumeration 4

4. Information Collection 6

5 Privacy Impact Assessment Questionnaire 10

6 Security Documentation 13

7 Threat / Risk Assessment Questionnaire Introduction 16

8 TRA for Applications or Systems (Internal or External) 17

9 TRA for Networked Hardware / Appliances 33

10 TRA for Professional Services provided to the University 42

11 TRA for Development Services provided to the University 46

12 Additional Notes and Comments 51

Appendix NIST CyberSecurity Framework Controls 52

# Product Summary and Asset Enumeration

|  |
| --- |
| Product Summary Please provide a description of the product or service (solution), its purpose, how it functions, service scope and the benefits it is expected to provide to the sponsoring unit, and to the University as a whole. The purpose should outline whether the solution being introduced addresses a new issue or opportunity, replaces an existing service that is at end of life, reduces risk, or a combination of the above. |
|  |
| Lifecycle Please provide a description of the anticipated lifecycle of major upgrades for this solution, or if no upgrades are expected, the longevity of this solution. |
|  |
| Partners and Sub-contractors Where aspect(s) of the solution are not directly provided by the contracted vendor or the service, please detail the relationship with the external vendor / supplier: What is provided, and under what terms of service? |
|  |

|  |
| --- |
| Flow Diagram Please provide a data flow diagram/s, including protocols of all data in transit, and mechanisms of storage. The diagram should indicate the flow of information from creation / collection to final destruction. Please include non-electronic data flows as well as electronic. |
| **ID.AM-3 [[1]](#footnote-1)** |

# Information Collection

ID.GV-4

|  |  |  |
| --- | --- | --- |
| Identify the kinds of information involved in the project | | |
| * + 1. The University does not share user attributes of exceptional sensitivity (plain-text passwords, or a users’ Social Insurance Number or any attribute that could lead to user impersonation or identity theft) by default. Please indicate if the proposed solution requires access to such attributes. | | |
| **Information Type or Data field Collected** | **Purpose of Collection** | **How is this information collected** |
|  |  |  |
|  |  |  |
|  |  |  |
| * + 1. List any information collected about individuals in their personal capacity. | | |
| **Information Type or Data field Collected**  Example: First name, last name, email, IP address  (Add rows as needed.) | **Purpose of Collection**  Example: Account registration/creation, functionality of system, security log | **How is this information collected** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| * + 1. List any information collected about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| * + 1. Please indicate all information collected or created by the solution that does not directly support the functionality required by the University.   *Hint: Does the solution collect more information by default than is necessary? Does the solution create analytics based on use or content? Does the system record an individual’s usage of the technology?* |  |
| * + 1. Information provided by Administrators and Operators   What system-level information does the solution require to connect with / provide service to the University?  *Hint: This information may include service or system-level identification, authentication, authorization data; configuration, protocol, or other data required to achieve a successful connection.* |  |
| * + 1. Service Generated Information   What user-facing information is created or captured by the solution?  *Hint: Includes information that is collected / created by or input into the solution that is visible to end-users.* |  |
| * + 1. System Generated Information   What information is created by the solution as part of its operation?  *Hint: Includes information that is not visible to end-users, but which is visible to system administrators such as metadata associated with user and administrative activities, temporary system / log / backup files, traffic data, access or transaction logs etc.)* |  |

|  |  |
| --- | --- |
| Does the solution provider intend to share University-provided information with external partners or third parties? This question includes PII as well as business data.[[2]](#footnote-2) | **Yes/No if Yes:** |
| **If Yes:** |  |
| * + 1. What is the information and purpose of this sharing System Generated Information |  |
| **Information** | **Purpose of sharing** |
|  |  |
|  |  |
| * + 1. Has the University agreed to this sharing? |  |
| * + 1. Who will the information be shared with? |  |
| * + 1. How will the information be shared? |  |
| * + 1. What safeguards exist to ensure that the sharing will be limited to the stated purposes? |  |
| * + 1. What safeguards exist to ensure that the data will be protected at the same level as in the immediate vendor / supplier’s possession? |  |

|  |  |
| --- | --- |
| For all created or generated data (including meta and derivative data – such as usage or preference data) detail the contractual terms in place to | |
| * + 1. Establish and enforce the University’s ownership of all collected and created data at all times and in all contexts. |  |
| * + 1. Establish that data sharing agreements with the solution provider and the solution provider’s partners (if any) do not out-live any part of the University’s contractual relationship with the solution provider. |  |
| * + 1. Ensure the data is not re-shared by the solution provider’s third-party partners (if any). |  |
| * + 1. Establish an end-of-life for data, including data disposal requirements, between the University of Toronto and the solution provider / between the solution provider and any third-party service partners. |  |

# Privacy Impact Assessment Questionnaire

A guided discussion on the use of user-associated or personally identifiable information (PII)[[3]](#footnote-3)

|  |  |
| --- | --- |
| Is any Personally Identifiable Information collected? | **YES/NO** |
| **YES – continue** | NO. Please skip the remainder of this section and go to the [Security Documentation](#_Security_Documentation) section. |
| Notification and Collection – please provide details for the following:[[4]](#footnote-4) |  |

|  |  |
| --- | --- |
| * + 1. How are individuals notified about the collection of their information? Please be specific, by providing timing and method, or explaining exemption from notice of collection. |  |
| * + 1. How is personal information collected directly from the individual? Explain the form of collection (for example, orally, hardcopy form, online portal, etc.) |  |
| * + 1. Is personal information collected indirectly from another source, or covertly? Why? |  |
| * + 1. How, and how often are collection controls reviewed to ensure effectiveness? |  |
| * + 1. Is collection of all the personal information (specified in 4.1) necessary? Why or why not? |  |

|  |  |
| --- | --- |
| If an externally hosted service, please provide details for the following: |  |

|  |  |
| --- | --- |
| * + 1. Solution provider’s privacy policy – please provide a link and a copy of the policy. |  |
| * + 1. The person or role responsible for acting as a Privacy Officer; i.e. responsible for the maintenance and execution of the privacy policy. |  |
| * + 1. Notification procedures for privacy policy updates. |  |
| * + 1. Processes for individuals to query / challenge / modify stored personal data. |  |
| * + 1. User opt-out provisions / process – in whole or part, and data management options in the event of an opt-out. |  |
| * + 1. Notification and opt-out provisions / processes in the event of new uses of PII by either the solution provider or the solution provider’s third-party partners (if applicable)?   *If so the solution provider must supply details of the notification process* |  |
| * + 1. Can users opt-out of the solution’s or service partner’s (individually or in whole, if applicable) products at any time? |  |
| * + - 1. If so the solution provider must supply details of the opt-out process. |  |

|  |  |
| --- | --- |
| Lifecycle of Private Information – please provide details for the following: |  |

|  |  |
| --- | --- |
| * + 1. Information retention duration / policy. |  |
| * + 1. Information disposal practices / policy. |  |
| * + 1. Please describe the process by which the University can reliably confirm the destruction of personal (PII) data under the following conditions: |  |
| * + - 1. Once the information has reached its agreed end-of-life. |  |
| * + - 1. At the termination of data sharing agreements between the University and the solution provider, and between the solution provider and third-party partners (if any). |  |
| * + - 1. Under any change in solution ownership status (such as sale or bankruptcy) unless re-negotiated with the University, as per points 4.2 through 4.2.2.5 above. |  |
| * + - 1. In the event of user opt-out from the solution, in whole or in part. |  |

# Security Documentation

## Software As A Service (SaaS)

## SAAS providers

If an external vendor is providing the solution in its entirety, please provide the following:

|  |  |  |
| --- | --- | --- |
| **Documentation Type** | **Submitted to the University as part of this process (Yes, No, N/A)** | **Document Source or URL** |
| Security Policy \* |  |  |
| End User License Agreement |  |  |
| Audits (SOC 2 or equivalent)\* |  |  |
| Results of practical network-intrusion testing / application scanning (i.e. PEN testing). \* |  |  |

\* Non-disclosure is available. If you are unable to provide the documents, please provide Letters of Attestation.

## Partners to SaaS providers

If the external vendor partners work with third-parties to provide the solution to the University, please submit details of the following on behalf of the third parties: (PR.AT-3[[5]](#footnote-5))

|  |  |  |
| --- | --- | --- |
| **Documentation Type** | **Submitted to the University as part of this process (Yes, No, N/A)** | **Document Source or URL** |
| Security Policy \* |  |  |
| End User License Agreement |  |  |
| Audits (SOC 2 or equivalent) \* |  |  |
| Results of practical network-intrusion testing / application scanning (i.e. PEN testing). \* |  |  |

\* Non-disclosure is available. If you are unable to provide the documents, please provide Letters of Attestation.

## Infrastructure As A Service (IaaS)

If a cloud service provider is being used to provide only a hosting infrastructure for the solution or application, please submit the following documentation for the (cloud) hosting service.

|  |  |  |
| --- | --- | --- |
| **Documentation Type** | **Submitted to the University as part of this process (Yes, No, N/A)** | **Document Source or URL** |
| SOC1 or SOC2 audit or equivalent \* |  |  |

\* Non-disclosure is available. If you are unable to provide the documents, please provide Letters of Attestation.

## Internal University Applications or Solution Providers

(ID.GV-1)

If the application or solution is provided / developed / managed by any unit within the University, regardless of the where the application / solution is (SAAS, IAAS, or internally hosted), please provide details about standards, guidelines and/or procedures followed.

|  |  |  |
| --- | --- | --- |
| Documentation Name and Type  (Wiki, Blog, Document repository etc.)  *Examples: Security guidelines in Document repository / Backup procedures in Wiki / Architectural models or diagrams* | Location | Maintainer / Owner | **Document Source or URL** |
|  |  |  |
|  |  |  |
|  |  |  |

## Other legislation

(ID.GV-3)

|  |  |
| --- | --- |
| * + 1. If handling credit card data, is the solution Payment Application Data Security Standard (PCI-DSS) compliant? Please provide details. |  |
| * + 1. Does the solution comply with the Accessibility for Ontarians with Disabilities Act (AODA) accessibility requirements? If not, what accessibility standard is followed? Please provide compliance certification. |  |
| * + 1. Is the solution obliged to comply with functional requirements that may be present in jurisdictions other than Ontario, Canada? Please provide details. |  |

# Threat / Risk Assessment Questionnaire Introduction

Note: **Please complete the section that is relevant to this project.** Do not complete sections that are not relevant.

Note: Not all sub-sections may be relevant to the solution under consideration. If not relevant, please indicate as ‘**Not Applicable’**. If a sub-section is relevant but no response available, please indicate with ‘**No Answer**’.

(ID.RA-5)

The subsections are

8 TRA for Applications or Systems (Internal or External) 17

9 TRA for Networked Hardware / Appliances 33

10 TRA for Professional Services provided to the University 42

11 TRA for Development Services provided to the University 46

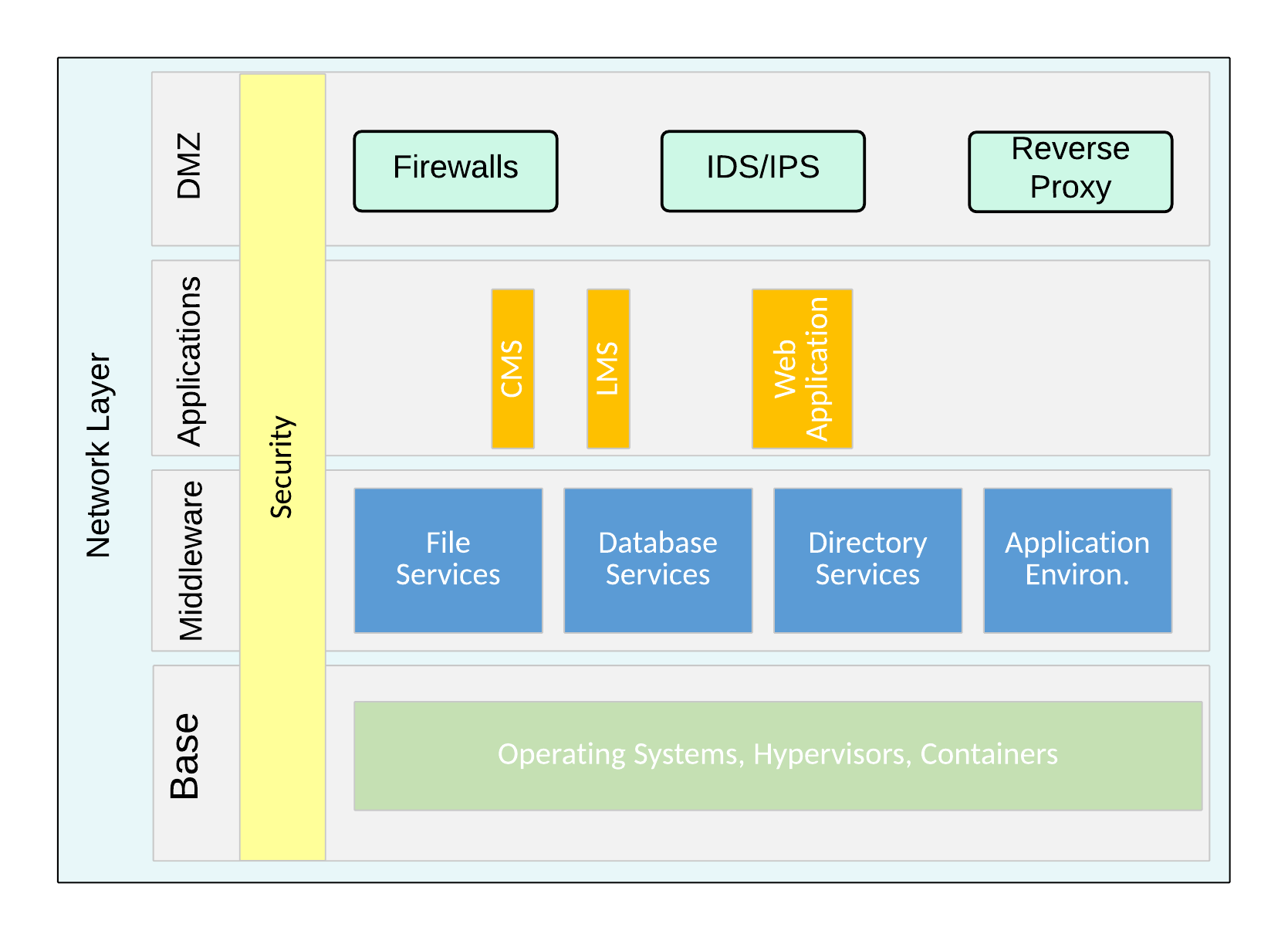
12 Additional Notes and Comments 51

In order to expedite the completion of the Threat and Risk Assessment, please provide supporting details where appropriate rather than simple Yes or No answers. This is especially important if your answers indicate that a threat or risk exists.

**If the answer is found in the documentation provided in section 6, refer to the document, and please provide the section in the document.**

# TRA for Applications or Systems (Internal or External)

Simplified Security Stack



The simplified security stack in the diagram indicates, for example, how a web application may depend on a database that depends on an operating system, and the dependence of these on the network layer. If any layer is inadequately protected, the services provided at the other layers might be at risk. The questions below should be answered to provide details of controls for all layers.

If answers are provided in the documentation referred to in Section 6, please provide the reference.

If another group manages a layer for you, answer this (e.g. 8.1.1.2), and leave the rest of the relevant column blank.

## Identification and Authentication

Please answer as appropriate to your responsibilities in the relevant columns.

| Are you responsible for: | An Application? | Middleware? | Underlying Operating System? | Other? [[6]](#footnote-6) |
| --- | --- | --- | --- | --- |
| * + - 1. **If yes**, provide details of all that you are responsible for: | Yes/No  <Name of Application> | Yes/No  <Which Middleware> | Yes/No  <Which Operating systems; what version> | Yes/No |
| * + - 1. **If no**, detail which group is managing the system, and (if applicable) the name of the service provider. |  |  |  | ID.BE-4 |
| * + 1. Is the identity of user accounts obtained from an existing central University system? | Yes/No | Yes/No | Yes/No | Yes/No |
| * + - 1. **If yes:** |  |  |  | PR.AC1 |
| * + - * 1. Which system? |  |  |  |  |
| * + - * 1. Is full authentication (identity and password) obtained from this system? Yes/no |  |  |  |  |
| * + - * 1. If no, describe how access controls (such as passwords) are applied. |  |  |  |  |
| * + - 1. **If no:** |  |  |  | PR.AC1 |
| * + - * 1. Describe how users are identified and authenticated. |  |  |  |  |
| * + - * 1. Are all users uniquely identified? |  |  |  | PR.AC-4 |
| * + - * 1. What are the authentication requirements (such as passwords:length; complexity, quality etc.?) |  |  |  | Does this pass UofT minimum? |
| * + - * 1. Could this solution support authentication through SAML. |  |  |  |  |
| If so, does the SAML implementation support multiple authentication contexts? E.g. two factor authentication. |  |  |  |  |
| * + 1. **Continue for all** |  |  |  |  |
| * + - 1. Is two-factor authentication available? |  |  |  |  |
| * + - 1. **If so**, under what conditions are users required / able to use two-factor authentication? |  |  |  | PR.AT-2 |
| * + - 1. **If not,** will two-factor authentication be available in the future? Please provide details. |  |  |  |  |
| * + - 1. Is the solution compatible with Hardware Security Modules for the purpose of key management? |  |  |  |  |
| * + - 1. Describe controls applied to service / local / default accounts   *(disabled/ deleted / changed default passwords etc.).* |  |  |  | PR.AC-1  PR.PT-3 |
| * + - 1. Who has access to the passwords of service / local / default / accounts. |  |  |  | PR.AT-2 |
| * + - 1. Are there processes in place to change passwords / recover multi-factor authentication assets / reset access controls when these individuals leave or change roles within the group / organization? |  |  |  | PR.AC-1  PR.IP-3 |
| * + - 1. **Specific Middleware Questions. Answer if managing Middleware / if an Application accesses Middleware** |  |  |  |  |
| * + - * 1. Which Middleware is used?   *For example: Tomcat, WebSphere Application Server, WebSphere MQ, Rabbit MQ, etc.* |  |  |  |  |
| * + - * 1. Detail how access to the Middleware is managed: |  |  |  |  |
| From the application perspective. |  |  |  | PR.AC-1 |
| From the Middleware server perspective. |  |  |  | PR.AC-1 |

## Authorization

Please answer as appropriate to your responsibilities in the relevant columns.

| Continued | Application | Middleware | Underlying Operating System | Other |
| --- | --- | --- | --- | --- |
| * + 1. Is the authorization of the user managed through an existing University system? | Yes/No | Yes/No | Yes/No | Yes/No |
| * + - 1. **If yes:** |  |  |  | ID.BE-4 |
| * + - * 1. Which system? |  |  |  |  |
| * + - * 1. What degree of granularity does the solution offer in defining roles? |  |  |  | PR.AC-4 |
| * + - * 1. Does this level of granularity require any additions / modifications to existing University identification / authentication systems?   If so, detail the changes required. |  |  |  |  |
| * + 1. **If no:** |  |  |  |  |
| * + - 1. Describe the authorization system used. |  |  |  | PR.AC-1 |
| * + - 1. What degree of granularity does the solution offer in defining roles? |  |  |  | PR.AC-4 |
| **Continue for all** |  |  |  |  |
| * + 1. Are roles based on the principle of least privilege in practice / by default? Explain. |  |  |  | PR.AC-4  PR.PT-3 |
| * + 1. Is access reviewed and reauthorized on a periodic basis? If so, how often, and by whom? |  |  |  | PR.AC-1  PR.IP-3 |
| **Remote Session Management** |  |  |  |  |
| * + 1. Is remote administration of applications, systems and/ or system components performed over an encrypted network connection? Provide details. |  |  |  | PR.DS-2  PR.DS-5  PR.MA-2 |
| * + 1. **Application Session controls – answer if managing an application** |  |  |  | Thanks to CMU [[7]](#footnote-7) |
| * + - 1. How are sessions uniquely associated with an individual or system? |  |  |  | CMU.AS-8 |
| * + - 1. How are session identifiers generated in a manner that makes them difficult to guess? |  |  |  | CMU.AS-9 |
| * + - 1. How long does it take for active sessions to time out after a period of inactivity? |  |  |  | CMU.AS-11 |
| * + - 1. Explain the time chosen in relation to requirements of your system. |  |  |  |  |
| * + 1. **Middleware Controls – Answer if managing Middleware / if the Application accesses Middleware** |  |  |  |  |
| * + - 1. Detail how authorization to the Middleware is managed: |  |  |  |  |
| * + - 1. From the application perspective |  |  |  | PR.AC-1 |
| * + - 1. From the Middleware server perspective. |  |  |  | PR.AC-1 |

## Isolation

| Continued | Application | Middleware | Underlying Operating System | Other |
| --- | --- | --- | --- | --- |
| * + 1. Is the system fully managed for you by one of the central services on one of the campuses of the University of Toronto? | Yes/No | Yes/No | Yes/No | Yes/No |
| * + 1. **If Yes**, please record which group is managing the system, and the name of the solution provider. |  |  |  | ID.BE-4 |
| * + 1. **If no**, please answer questions below (refer to answers in documents in section 6, if present and convenient). |  |  |  |  |
| * + - 1. Detail the hardening process followed. |  |  |  | PR.MA-1  PR.PT-3 |
| * + - 1. Detail the procedure followed for deploying updates/patches. |  |  |  | PR.MA-1 |
| * + - 1. If the system is multi-tenanted, detail the controls / security checks / hardening followed to prevent unauthorized access to data of one tenant by users from other tenants, for both the data store and the application. |  |  |  | PR.MA-1  PR.PT-3 |
| * + 1. **Operating System Questions** |  |  |  |  |
| * + - 1. Are host based firewall/s run? | Yes/No |  | Yes/No | PR.PT-4  DE.AE-1 |
| **If yes**, please answer the questions below |  |  |  |  |
| * + - * 1. Are there controls for both ingress and egress of IPV4 traffic? |  |  |  |  |
| * + - * 1. Are there controls for both ingress and egress of IPV6 traffic? |  |  |  |  |
| * + - * 1. Are ports / protocols / traffic sources blocked by default? |  |  |  |  |
| * + - * 1. Detail the procedure followed for identifying and testing / periodically re-validating allowed ports and protocols. |  |  |  | PR.IP-3 |
| * + 1. **Application Questions** |  |  |  | Thanks to CMU for some controls. [[8]](#footnote-8) |
| * + - 1. Is the development and testing environment separate from the production environment? |  |  |  | PR.DS-7 |
| * + - 1. How is data created for testing? |  |  |  | PR.DS-5 |
| * + - 1. What is the process for identifying new vulnerabilities in the application? |  |  |  | DE.CM-8  ID.RA-2  RS.MI-3 |
| * + - 1. How are input data validated and restricted to types known to be correct? |  |  |  | CMU.AS-4 |
| * + - 1. How is proper error handling executed so that error messages do not reveal potentially harmful information to unauthorized users? |  |  |  | CMU.AS-5 |
| * + - 1. What standards are followed when developing applications? |  |  |  | OWASP / ? |
| * + - 1. How are vulnerabilities in the code tested for, and how frequently? |  |  |  | DE.CM-4  DE.CM-8  CMU.AS-12 |
| * + 1. **Middleware Question** |  |  |  |  |
| * + - 1. Detail how the database is managed.   *(updates / backups/ restores/ protection of backups).* |  |  |  | PR.MA-1  PR.IP-4 |
| * + - 1. If other Middleware, detail how it is managed |  |  |  |  |
| * + 1. **Data Isolation Questions** |  |  |  |  |
| * + - 1. Where is the data located / stored (include country if a cloud service)? |  |  |  | Privacy Commissioner |
| * + - 1. How is data at rest protected? |  |  |  | PR.DS-1 |
| * + - 1. Is data in transit encrypted? Please provide details of the protocols used for user interaction, and if applicable, for system to system data transfers. |  |  |  | PR.DS-2 |
| * + - * 1. If the protocol depends on SSL / TLS, provide the versions of SSL / TLS you support, and your process for upgrading the protocol strength and versions. |  |  |  |  |
| * + - 1. How are backups secured (If encrypted, include management of keys)? |  |  |  |  |
| * + 1. **Network Isolation Questions** |  |  |  |  |
| * + - 1. Describe the network segmentation |  |  |  | PR.AC-5 |
| * + - 1. If firewalls are used: |  |  |  | PR.PT-4  DE.AE-1 |
| * + - 1. Is both ingress and egress controlled for IPV4 traffic? Expand. |  |  |  |  |
| * + - 1. Is both ingress and egress controlled IPV6 traffic? Expand. |  |  |  |  |

## Continuity

| Continued | Application | Middleware | Underlying Operating System | Other |
| --- | --- | --- | --- | --- |
| * + 1. Detail the effects of interruptions of this solution to the sponsoring unit, and to the University as a whole.   *Provide details relating to the effects of planned maintenance, and of unplanned interruptions.* |  |  |  | ID.RA-4 |
| * + 1. What are the SLA’s for this solution? Are they sufficient to offset negative results of interruptions, as detailed above? |  |  |  | ID.BE-5 |
| * + 1. Is adequate capacity to ensure availability provided?   *Describe whether the limitations on solution capacity (including, but not limited to: memory, CPU, simultaneous connections, storage, and throughput) meet the SLA’s / Service Level requirements?* |  |  |  | PR.DS-4  ID.BE-5 |
| * + 1. Detail how this solution interoperates with systems within the University. |  |  |  | ID.BE-4 |
| * + 1. Does the solution support High Availability (HA); does it support live fail-over, if needed? |  |  |  | PR.DS-4  ID.BE-5 |
| * + 1. Is a disaster plan documented? If so, where? |  |  |  | PR.IP-9  PR.IP-10 |
| * + 1. Are backup and recovery procedures documented? If so, where? |  |  |  | PR.IP-4 |
| * + 1. Are backup and recovery procedures tested periodically? How often? |  |  |  | PR.IP-4 |
| * + 1. Are backup copies of data accurately and reliably inventoried? |  |  |  |  |
| * + 1. What data retention policy is followed for the data collected or processed? |  |  |  | PR.IP-6 |
| * + 1. What process is followed to securely delete this data at the end of the retention period? |  |  |  | PR.IP-6 |
| * + 1. What policy is followed for the destruction of electronic media? |  |  |  | PR.IP-6  PR.DS-3 |
| * + 1. What change management procedures are followed? |  |  |  | PR.IP-1  PR.IP-3 |
| * + 1. Are access, change and availability controls tested on a periodic basis or after every significant change to the solution? |  |  |  | PR.IP-3 |
| * + 1. Detail the Solution Development Lifecycle policy.   *How is the solution kept current? How are maintenance concerns addressed?* |  |  |  | PR.DS-7  PR.IP-2 |

## Monitoring

| Continued | Application | Middleware | Underlying Operating System | Other |
| --- | --- | --- | --- | --- |
| **Logs** |  |  |  |  |
| * + 1. Detail what is logged. |  |  |  |  |
| * + 1. Are logs integrated with log monitoring services? | Yes/No | Yes/No | Yes/No | Yes/No |
| * + - 1. **If Yes:** |  |  |  | PR-PT-1 |
| * + - * 1. Which monitoring service? |  |  |  |  |
| * + - * 1. What logs are provided to the service? |  |  |  |  |
| * + - * 1. What reports does the service provide? |  |  |  |  |
| * + - 1. **If no:** |  |  |  | PR-PT-1 |
| * + - * 1. Detail the log monitoring procedure. |  |  |  |  |
| * + - * 1. Detail controls to protect logs from tampering. |  |  |  |  |
| **Continue for all** |  |  |  |  |
| * + 1. Detail how problems with the system/application would be detected. |  |  |  | DE.AE-1  DE.AE-2  DE.AE-3  DE.AE-4 |
| * + 1. Detail how a breach of data / a compromise of the system or application would be detected. |  |  |  | DE.CM-1  DE.CM-7  DE.DP-1  PR.DS-5 |
| * + 1. Do the logs include sufficient information to permit incidence analysis? |  |  |  | DE.AE-2 |
| * + 1. Detail how you would notify the University in the event of a security breach in the solution and/or of the data. Include the timeframe. |  |  |  |  |
| * + 1. Detail incidence response management procedures. How often are they practiced? |  |  |  | RS.RP-1  RS.CO-1  PR.IP-9  PR.IP-10  DE.DP-1  DE.DP-5 |
| **Compliance** |  |  |  |  |
| * + 1. Is compliance with internal security standards assessed in an audit, at least annually? Which type of audit? Please supply details or Attestation Letters. |  |  |  | DE.DP-2 |

# 

## Interoperability

|  |  |  |
| --- | --- | --- |
| **For each of the following, if provided / available, and if applicable, detail how the data is protected in transit; in storage; detail the granularity of control.** | |  |
| **Authentication / Authorization Interoperability components** | |  |
| * + 1. SAML 2.0 **compatibility** |  |  |
| * + 1. Active Directory **compatibility** |  |  |
| * + 1. **OAuth 2.0 compatibility, and scopes** |  |  |
| * + 1. OpenID compatibility |  |  |
| * + 1. LDAP **compatibility** |  |  |
| * + 1. Kerberos **compatibility** |  |  |
| * + 1. MFA and / or X.509 authentication **compatibility** |  |  |
| * + 1. **SAML Federation compatibility**   ***(e.g. Canadian Access Federation)*** |  |  |
| **Others** | |  |
| * + 1. Application Programming Interface (API) |  |  |
| * + 1. **ROSI/ACORN/NGSIS compatibility** |  |  |
| * + 1. **SAP compatibility** |  |  |
| * + 1. **Kuali compatibility (specify modules)** |  |  |
| * + 1. **Compatibility with common client relationship management (CRM) systems** |  |  |
| * + 1. **Informatica compatibility** |  |  |
| * + 1. **Cognos compatibility** |  |  |
| **Teaching and Learning Interoperability Components. In addition to detailing how the data is protected in transit; in storage; detailing the granularity of control (if applicable), provide the IMS or other certification.** | |  |
| * + 1. Learning Tool Inter-operability (LTI) standard? |  |  |
| * + 1. **Common Cartridge compliant** |  |  |
| * + 1. **QTI compliant** |  |  |
| * + 1. **SCORM compliant** |  |  |
| * + 1. **AICC compliant** |  |  |
| * + 1. **CALIPER compliant** |  |  |
| * + 1. **xAPI compliant** |  |  |
| * + 1. **TIN CAN compliant** |  |  |
| **General Interoperability Questions** | |  |
| * + 1. **Which browsers does your solution support?** |  |  |
| * + 1. Does your solution support the latest commonly used operating systems, including Windows, Mac OS X, and Linux? |  |  |
| * + 1. **Does your solution require** client side Java plugins / applications? If so, detail the requirements. |  |  |
| * + 1. **Mobile Access -** Does your solution have the ability to access the full product interface on the native browsers of mobile devices? | Provide details of which browsers on which classes of devices, and any additional requirements. |  |

# TRA for Networked Hardware / Appliances

## Identification and Authentication

|  |  |  |
| --- | --- | --- |
| * + 1. Will the identity of user accounts be obtained from an existing central University system? | Yes/No | ID.BE-4 [[9]](#footnote-9) |
| * + - 1. **If yes:** |  | PR.AC1 |
| * + - * 1. Which system? |  |  |
| * + - * 1. Will full authentication (identity and password) be obtained from this system? Yes/no |  |  |
| If no, describe how access controls (such as passwords) are applied. |  |  |
| * + - 1. **If no:** |  | PR.AC1 |
| * + - * 1. Describe how users will beidentified and authenticated. |  |  |
| * + - * 1. Will all users be uniquely identified? |  |  |
| * + - * 1. What are the authentication requirements (such as passwords:length; complexity, quality etc.?) |  | Does this pass UofT minimum? |
| * + - * 1. Which Identity Access Management systems is the appliance compatible with? |  |  |
| **Continue for both** |  |  |
| * + 1. Will two-factor authentication be used? |  |  |
| * + - 1. If so, under what conditions are users are required to use two-factor authentication? |  | PR.AT-2 |
| * + 1. Describe controls to be applied to the default accounts *(disabled/ deleted / changed default passwords etc).* |  | PR.AC-1  PR.PT-3 |
| * + 1. Who has / will have access to the passwords of service / local / default accounts. |  | PR.AT-2 |
| * + 1. Are there processes in place to change passwords / recover multi-factor authentication assets / reset access controls when these individuals leave or change roles within the group / organization? |  | PR.AC-1  PR.IP-3 |

## Authorization

|  |  |  |
| --- | --- | --- |
| * + 1. Will the authorization of users be managed through an existing University system? | Yes/No |  |
| * + - 1. **If yes:** |  | ID.BE-4 |
| * + - * 1. Which system? |  |  |
| * + - * 1. What degree of granularity will the solution offer in defining roles? |  | PR.AC-4 |
| * + - * 1. Does this level of granularity require any additions / modifications to existing University identification / authentication systems?   If so, detail the changes required. |  |  |
| * + - 1. **If no:** |  |  |
| * + - * 1. Describe the authorization system to be used. |  | PR.AC-1 |
| * + - * 1. What degree of granularity will the solution offer in defining roles? |  | PR.AC-4 |
| **Continue for both** |  |  |
| * + 1. Can the appliance be set up to provide access for users with multiple roles, and in context, provide for the principle of least privilege? |  | PR.AC-4  PR.PT-3 |
| * + 1. Is access reviewed and reauthorized on a periodic basis? If so, how often, and by whom? |  | PR.AC-1  PR.IP-3 |

## Isolation

|  |  |  |
| --- | --- | --- |
| * + - 1. Will remote administration by default be performed over an encrypted network channel? Provide details. |  | PR.DS-2  PR.DS-5  PR.MA-2 |
| * + - 1. Will the solution be fully managed by one of the central services on one of the campuses of the University of Toronto? | Yes/No |  |
| * + - 1. **If Yes**, please record which group is managing the system, and the name of the solution provider. |  | ID.BE-4 |
| * + - 1. **If no**, please answer questions below (refer to answers in documents in section 6, if present). |  |  |
| * + - * 1. Detail the system hardening process followed. |  | PR.MA-1  PR.PT-3 |
| * + - * 1. Detail the procedure followed for deploying operating system and security patches? |  | PR.MA-1 |
| * + - * 1. Detail the process to identify new vulnerabilities in the appliance? |  | DE.CM-8  ID.RA-2  RS.MI-3 |
| * + - * 1. Are host based firewall/s run? | Yes/No | PR.PT-4  DE.AE-1 |
| If yes, please answer the questions below |  |  |
| Are there controls for both ingress and egress of IPV4 traffic? |  |  |
| Are there controls for both ingress and egress of IPV6 traffic? |  |  |
| Are ports / protocols / traffic sources blocked by default? |  |  |
| Detail the procedure followed for identifying and testing / periodically re-validating allowed ports and protocols. |  | PR.IP-3 |

## Continuity

|  |  |  |
| --- | --- | --- |
| * + 1. What are the SLA’s / Service Level requirements for these appliances/ hardware |  | PR.DS-4 |
| * + 1. Detail the effects of downtime / failures of these appliances / hardware to individual units and to the University as a whole. |  |  |
| * + 1. Do you provide metrics showing Probability of Failure? Please provide document/ URL. |  |  |
| * + 1. Does the appliance have any propriety implementations that are non-standard based? What are they? |  |  |
| * + 1. Is adequate capacity to ensure availability maintained?   *Describe whether the limitations on solution capacity (including, but not limited to: memory, CPU, simultaneous connections, storage, and throughput) meet the SLA’s / Service Level requirements?* |  | PR.DS-4  ID.BE-5 |
| * + 1. Does the solution support High Availability (HA); does it support live fail-over, if needed? |  | PR.DS-4  ID.BE-5 |
| * + 1. Is a disaster plan documented? If so, where? |  | PR.IP-9  PR.IP-10 |
| * + 1. Are backup and recovery procedures documented? Please provide the documents or the URL. |  | PR.IP-4 |
| * + 1. Are backup and recovery procedures tested periodically? How often? |  | PR.IP-4 |
| * + 1. Are backups accurately and reliably inventoried? |  |  |
| * + 1. What change management procedures are followed for systems? |  | PR.IP-1  PR.IP-3 |
| * + 1. Are access, change and availability controls tested on a periodic basis or after every significant change / update? |  | PR.IP-3 |
| * + 1. If any data is collected, what data retention policy is followed for the data collected or processed? How is the data securely destroyed at the end of the retention period? |  | PR.IP-6 |

## Monitoring

|  |  |  |
| --- | --- | --- |
| **Logs** |  |  |
| * + 1. What degree of granularity does the solution offer in logging events? |  |  |
| * + 1. Are logs / can logs be integrated with log monitoring services? | Yes/No |  |
| * + - 1. **If Yes:** |  | PR-PT-1 |
| * + - * 1. Which monitoring service? |  |  |
| * + - * 1. What logs are provided to the monitoring service? |  |  |
| * + - * 1. What reports do they provide to you? |  |  |
| * + - 1. **If no:** |  | PR-PT-1 |
| * + - * 1. Detail the log monitoring procedure. |  |  |
| * + - * 1. Detail controls to protect logs from tampering. |  |  |
| **Continue for both** |  |  |
| * + 1. Detail how problems with the appliance would be detected? |  | DE.AE-1  DE.AE-2  DE.AE-3  DE.AE-4 |
| * + 1. Detail how a breach of data / a compromise of the system or application would be detected. |  | DE.CM-1  DE.CM-7  DE.DP-1  PR.DS-5 |
| * + 1. Do the logs include sufficient information to permit incidence analysis? |  | DE.AE-2 |
| * + 1. Detail incidence response procedures? How often are they practiced? |  | RS.RP-1  RS.CO-1  PR.IP-9  PR.IP-10  DE.DP-1  DE.DP-5 |
| **Compliance** |  |  |
| * + 1. Is compliance with internal security standards assessed in an audit, at least annually? Which type of audit? |  | DE.DP-2 |

# TRA for Professional Services provided to the University

## Identification and Authentication

|  |  |  |
| --- | --- | --- |
| * + 1. Please identify the team members who will manage this service? |  | ID.AM-6 [[10]](#footnote-10) |
| * + 1. Will team members continue to be part of the service offering, or are they only part of the deployment / transition team? How will the University be advised if team members are replaced? |  | ID.GV-2  PR.AC-1  DE.CM-6 |

## Authorization

|  |  |  |
| --- | --- | --- |
| * + 1. What certifications are required by the University for the maintenance of this solution? |  |  |
| * + 1. Please detail how the University will be advised of the certifications of new team members. |  |  |
| * + 1. How does the team propose to manage access permissions, incorporating the principles of least privilege and separation of duties? |  | PR.AC-1  PR.AC-4 |

## Isolation

|  |  |  |
| --- | --- | --- |
| * + 1. Have the proposed team members undergone background checks? Please specify the type of background checks. |  |  |
| * + 1. How does the team propose to control remote access to the managed service in a manner that prevents unauthorized access? |  | PR.AC-3 |
| * + 1. Does the vendor intend to apply an information security standard to components they will manage? If so, which standard(s)? |  | ID.GV-1 |
| * + 1. What hardening guidelines will the team members use to harden the managed backend environment components? Please supply references to the guidelines used. |  |  |
| * + - 1. If the team uses their own guidelines, would the team be willing to use the University’s guidelines, should the University’s guidelines exceed their own? |  |  |
| * + 1. What data would travel between the University network and the vendor infrastructure? How is it protected? |  | PR.AC-5 |
| * + 1. If 3rd parties are used for any part of the professional service offered, what procedures are followed to ensure 3rd party personnel and procedures are of the same standard or higher than your own? |  | PR.AT-3  ID.AM-6 |

## Continuity

|  |  |  |
| --- | --- | --- |
| * + 1. Do the proposed team members have IT security certification such as Certified Information Systems Security Professional (CISSP) and architecture certification, such as The Open Group Architecture Framework (TOGAF)? |  | PR.AT-1 |
| * + 1. Do the proposed team members have vendor or technology-specific certifications (e.g. Microsoft, Java, Oracle, IBM, CISCO etc.)? |  | PR.AT-1 |
| * + 1. Have the proposed team members worked on projects of similar size / nature / complexity in past? |  | PR.AT-1 |
| * + 1. Detail the effects of interruptions of this service to the sponsoring unit, and to the University as a whole.   *Provide details relating to the effects of planned maintenance, and of unplanned interruptions* |  | ID.RA-4 |
| * + 1. What are the proposed SLAs for this service? Are they sufficient to offset negative results of interruptions, as detailed above? |  | ID.BE-5 |
| * + 1. What service will be provided in the case of a disaster? Is this documented? |  | PR.IP-9  PR.IP-10 |
| * + 1. Detail backup and restore procedures. Are backups encrypted? How are they protected from unauthorized restoration? |  | PR.IP-4 |
| * + 1. What configuration change control processes will the team use? |  | RC.RP-1 |
| * + 1. How does the team continuously improve protection processes? |  | RS.MI-3  RS.IM-1  RS.IM-2  RC.CO-3 |

## Monitoring

|  |  |  |
| --- | --- | --- |
| * + 1. How will access (authorized or unauthorized) be audited? |  | PR.PT-1 |
| * + 1. What metrics are monitored to ensure the managed backend environment meets SLAs? |  |  |
| * + 1. Is any additional software installed to enable monitoring of metrics? |  |  |
| * + 1. What metrics are monitored to identify security incidents? |  |  |
| * + 1. Detail incidence response management procedures? How often are they practiced? |  | RS.RP-1  RC.CO-1  PR.IP-9  PR.IP-10  DE.DP-1  DE.DP-5 |

# TRA for Development Services provided to the University

## Identification and Authentication

|  |  |  |
| --- | --- | --- |
| * + 1. Please identify the proposed team members who will develop this service? | Yes/No | ID.AM-6 [[11]](#footnote-11) |
| * + 1. How will the University be advised if team members are replaced with others? |  | ID.GV-2  PR.AC-1 |
| * + 1. How is access to development of the proposed service managed? |  | PR.AC-3 |
| * + 1. Will the service integrate with existing Identity and Access Management systems within the University? |  | ID.BE-4 |
| * + 1. **If yes:** |  | PR.AC1 |
| * + - 1. Which system? |  |  |
| * + - 1. Will full authentication (identity and password) be obtained from this system? Yes/no |  |  |
| * + - 1. If no, describe how access controls (such as passwords) are applied. |  |  |
| * + - 1. What are the authentication requirements (such as passwords:length; complexity, quality etc.?) |  | Does this pass UofT minimum? |
| * + 1. **If no, and if applicable:** |  | PR.AC1 |
| * + - 1. Describe the authentication system to be used. |  |  |
| * + - 1. Will all users be uniquely identified? |  |  |

## Authorization

|  |  |  |
| --- | --- | --- |
| * + 1. What certifications are required by the University for the development of this solution? |  |  |
| * + 1. Please detail how the University will be advised of the certifications of new team members. |  |  |
| * + 1. How is authorization to the development environment of the proposed service managed? |  | PR.AC-4  PR.DS-7 |
| * + 1. Will authorization for users of the service be managed through an existing University system? | Yes/No | ID.BE-4 |
| * + 1. **If yes:** |  |  |
| * + - 1. Which system? |  |  |
| * + - 1. What degree of granularity does the solution offer in defining roles? |  |  |
| * + - * 1. Does this level of granularity require any additions / modifications to existing University identification / authentication systems?   If so, detail the changes required. |  |  |
| * + 1. **If no, and if applicable:** |  |  |
| * + - 1. Describe the authorization system to be used. |  |  |
| * + - 1. What degree of granularity does the solution offer in defining roles? |  |  |
| **Continue for all** |  |  |
| * + 1. Are roles based on the principle of least privilege in practice / by default? |  | PR.AC-4  PR.PT-3 |
| * + 1. **Are you developing an Application?** |  |  |
| * + 1. **If Yes** |  |  |
| * + - 1. How do you uniquely associate a session with an individual or system? |  |  |
| * + - 1. How do you generate session identifiers in a manner that makes them difficult to guess? |  |  |
| * + - 1. Will active sessions time out after a period of inactivity? |  |  |
| * + - 1. If so, explain the time chosen. |  |  |

## Isolation

|  |  |  |
| --- | --- | --- |
| * + 1. Have the proposed team members undergone background checks? Please specify the type of background checks. |  |  |
| * + 1. Are security standards (such as Open Web Application Security Project (OWASP)) and architectural standards (such as TOGAF) followed in development of solutions? |  |  |
| * + 1. Is the development and testing environment separate from the production environment? |  | PR.DS-7 |
| * + 1. How is data created for testing? |  | PR.DS-5 |
| * + 1. How are vulnerabilities in the code tested for, and how frequently? |  | DE.CM-4  DE.CM-8 |
| * + 1. Has the developer anticipated the need to perform a Privacy Impact Assessment (PIA) and Threat and Risk Assessment (TRA)? Has the developer budgeted time to do so? |  |  |
| * + 1. How has the PIA and TRA process been integrated into the development process? |  |  |
| * + 1. If 3rd parties are used to develop any part of the professional service offered, what procedures are followed to ensure 3rd party personnel and procedures are of the same standard or higher than your own? |  | PR.AT-3 |

## Continuity

|  |  |  |
| --- | --- | --- |
| * + 1. Do the proposed team members have IT security certification, such as Certified Information Systems Security Professional (CISSP) and architecture certification, such as The Open Group Architecture Framework (TOGAF)? |  |  |
| * + 1. Do the proposed team members have vendor or technology-specific certifications (such as: Microsoft, Java, Oracle, IBM, CISCO, etc.)? |  |  |
| * + 1. Have the proposed team members worked on projects of similar size / nature / complexity in past? |  |  |
| * + 1. What coding methodology / review practices / are followed in the development of solutions? |  |  |
| * + 1. What configuration change control processes will the team use? |  | PR.IP-1  PR.IP-3 |
| * + 1. If required, how will patches/ updates to the application/ code / service be managed? |  | PR.MA-1 |

## Monitoring

|  |  |  |
| --- | --- | --- |
| * + 1. What logging capabilities will the service provide? |  |  |
| * + 1. Detail how a compromise of the service would be detected. |  | DE.CM-1  DE.CM-7  DE.DP-1  PR.DS-5 |
| * + 1. What application scanning / code review / penetration tests are you planning to run against the service as you develop it? Please provide the results. |  | DE.CM-7  DE.CM-8 |

# Additional Notes and Comments

If there is any information that you think is relevant to the assessment that has not been addressed above, please provide it here.

# Appendix NIST CyberSecurity Framework Controls

The following controls were selected from the NIST Cybersecurity Framework [[12]](#footnote-12). They have been broken down here into their stated categories: Identify, Protect, Detect, Respond, Recovery.

This selection is intended to **illustrate** the relationships between the questions in this IRMQ and various security controls. These are not intended to be prescriptive, authoritative, or exhaustive, and there is not exact correspondence in some cases. Units may decide to use any standard they prefer. NIST provided References to other standards. The COBIT, ISO and NIST references are included.

|  |  |  |
| --- | --- | --- |
| **IDENTIFY** | | |
| *Control* | *Definition* | *References* |
| ID.AM-3 | Organizational communication and data flows are mapped | **COBIT 5** DSS05.02  **ISO/IEC 27001:2013** A.13.2.1  **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 |
| ID.AM-6 | Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. | **COBIT 5** APO01.02, DSS06.03  **ISO/IEC 27001:2013** A.6.1.1 |
| ID.BE-4 | Dependencies and critical functions for delivery of critical services are established | **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3  **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-1 |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established | **COBIT 5** DSS04.02  **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1  **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14 |
| ID.GV-1 | Organizational information security policy is established | **COBIT 5** APO01.03, EDM01.01, EDM01.02  **ISO/IEC 27001:2013** A.5.1.1  **NIST SP 800-53 Rev. 4** -1 controls from all families |
| ID.GV-2 | Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | **COBIT 5** APO13.12  **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 |
| ID.GV-3 | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | **COBIT 5** MEA03.01, MEA03.04  **ISO/IEC 27001:2013** A.18.1  **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1) |
| ID.GV-4 | Governance and risk management processes address cybersecurity risks | **COBIT 5** DSS04.02  **NIST SP 800-53 Rev. 4** PM-9, PM-11 |
| ID.RA-2 | Threat and vulnerability information is received from information sharing forums and sources | **ISO/IEC 27001:2013** A.6.1.4  **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5 |
| ID.RA-4 | Potential business impacts and likelihoods are identified | **COBIT 5** DSS04.02  **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14 |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | **COBIT 5** APO12.02  **ISO/IEC 27001:2013** A.12.6.1  **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 |

|  |  |  |
| --- | --- | --- |
| **PROTECT** | | |
| *Control* | *Definition* | *References* |
| PR.AC-1 | Identities and credentials are managed for authorized devices and users | **COBIT 5** DSS05.04, DSS06.03  **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 |
| PR.AC-3 | Remote access is managed | **COBIT 5** APO13.01, DSS01.04, DSS05.03  **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 |
| PR.AC-4 | Access permissions are managed, incorporating the principles of least privilege and separation of duties | **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 |
| PR.AC-5 | Network integrity is protected, incorporating network segregation where appropriate | **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 |
| PR.AT-1 | All users are informed and trained | **COBIT 5** APO07.03, BAI05.07  **ISO/IEC 27001:2013** A.7.2.2 |
| PR.AT-2 | Privileged users understand roles & responsibilities | **COBIT 5** APO07.02, DSS06.03  **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2  **NIST SP 800-53 Rev. 4** AT-3, PM-13 |
| PR.AT-3 | Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | **COBIT 5** APO07.03, APO10.04, APO10.05  **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 |
| PR.DS-1 | Data-at-rest is protected | **COBIT 5** APO01.06, BAI02.01, BAI06.01,  DSS06.06  **ISO/IEC 27001:2013** A.8.2.3 |
| PR.DS-2 | Data-in-transit is protected | **COBIT 5** APO01.06, DSS06.06  **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 |
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | **COBIT 5** BAI09.03  **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | **COBIT 5** APO13.01  **ISO/IEC 27001:2013** A.12.3.1 |
| PR.DS-5 | Protections against data leaks are implemented | **COBIT 5** APO01.06  **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | **COBIT 5** BAI07.04  **ISO/IEC 27001:2013** A.12.1.4 |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained | **COBIT 5** BAI10.01, BAI10.02, BAI10.03,  BAI10.05  **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | **COBIT 5** APO13.01  **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5  **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8 |
| PR.IP-3 | Configuration change control processes are in place | **COBIT 5** BAI06.01, BAI01.06  **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 |
| PR.IP-4 | Backups of information are conducted, maintained, and tested periodically | **COBIT 5** APO13.01 |
| PR.IP-5 | Policy and regulations regarding the physical operating environment for organizational assets are met | **COBIT 5** DSS01.04, DSS05.05  **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 |
| PR.IP-6 | Data is destroyed according to policy | **COBIT 5** BAI09.03  **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 |
| PR.IP-9 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | **COBIT 5** DSS04.03  **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 |
| PR.IP-10 | Response and recovery plans are tested | **ISO/IEC 27001:2013** A.17.1.3  **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14 |
| PR.MA-1 | Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | **COBIT 5** BAI09.03  **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5  **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5 |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | **COBIT 5** DSS05.04  **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1  **NIST SP 800-53 Rev. 4** MA-4 |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | **COBIT 5** APO11.04  **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 |
| PR.PT-3 | Access to systems and assets is controlled, incorporating the principle of least functionality | **COBIT 5** DSS05.02  **ISO/IEC 27001:2013** A.9.1.2  **NIST SP 800-53 Rev. 4** AC-3, CM-7 |
| PR.PT-4 | Communications and control networks are protected | **COBIT 5** DSS05.02, APO13.01  **ISO/IEC 27001:2013** A.13.1.1, A.13.2.  **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7 |

|  |  |  |
| --- | --- | --- |
| **DETECT** | | |
| *Control* | *Definition* | *References* |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | **COBIT 5** DSS03.01 |
| DE.AE-2 | Detected events are analyzed to understand attack targets and methods | **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 |
| DE.AE-3 | Event data are aggregated and correlated from multiple sources and sensors | **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR5, IR-8, SI-4 |
| DE.AE-4 | Impact of events is determined | **COBIT 5** APO12.06  **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI 4 |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | **COBIT 5** DSS05.07 |
| DE.CM-2 | The physical environment is monitored to detect potential cybersecurity events | *N/A* |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | **COBIT 5** DSS05.01  **ISO/IEC 27001:2013** A.12.2.1 |
| DE.CM-4 | Malicious code is detected | **COBIT 5** DSS05.01  **ISO/IEC 27001:2013** A.12.2.1 |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | **COBIT 5** APO07.06  **ISO/IEC 27001:2013** A.14.2.7, A.15.2.  **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA9, SI-4 |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 |
| DE.CM-8 | Vulnerability scans are performed | **COBIT 5** BAI03.10  **ISO/IEC 27001:2013** A.12.6.1 |
| DE.DP-1 | Roles and responsibilities for detection are well defined to ensure accountability | **COBIT 5** DSS05.01  **ISO/IEC 27001:2013** A.6.1.1  **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 |
| DE.DP-2 | Detection activities comply with all applicable requirements | **ISO/IEC 27001:2013** A.18.1.4  **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4 |
| DE.DP-5 | Detection processes are continuously improved | **COBIT 5** APO11.06, DSS04.05  **ISO/IEC 27001:2013** A.16.1.6  **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 |

|  |  |  |
| --- | --- | --- |
| **RESPOND** | | |
| *Control* | *Definition* | *References* |
| RS.RP-1 | Response plan is executed during or after an event | **COBIT 5** BAI01.10  **ISO/IEC 27001:2013** A.16.1.5 |
| RS.CO-1 | Personnel know their roles and order of operations when a response is needed | **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 |
| RS.IM-1 | Response plans incorporate lessons learned | **COBIT 5** BAI01.13  **ISO/IEC 27001:2013** A.16.1.6 |
| RS.IM-2 | Response strategies are updated | *N/A* |
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks | **ISO/IEC 27001:2013** A.12.6.1 |

|  |  |  |
| --- | --- | --- |
| **RECOVERY** | | |
| *Control* | *Definition* | *References* |
| RC.RP-1 | Recovery plan is executed during or after an event restoration of systems or assets affected by cybersecurity events. | **COBIT 5** DSS02.05, DSS03.04  **ISO/IEC 27001:2013** A.16.1.5 |
| RC.IM-1 | Recovery plans incorporate lessons learned | **COBIT 5** BAI05.07 |
| RC.CO-3 | Recovery activities are communicated to internal stakeholders and executive and management teams | *N/A* |

1. See [Appendix](#_Appendix___1) for controls [↑](#footnote-ref-1)
2. This information includes all data in section 4.1 above. The University requires notification of all external / third-party data sharing agreements. The University prohibits sharing of released PII / PHI with solution partners, except upon explicit permission of the University. Re-use of data outside of stated and agreed-to uses is prohibited, and all data must be verifiably destroyed / returned to the University in event of the sale or change in ownership status of the firm (e.g. bankruptcy). The University at all times retains ownership of solution data. [↑](#footnote-ref-2)
3. Some of the questions are taken from the Privacy Commissioner of Ontario’s Planning for Success: Privacy Impact Assessment Guide <https://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=1616> [↑](#footnote-ref-3)
4. The University must ensure that the institution (or any service endorsed by the institution) collects personal information only if it has the authority to do so and that notice of collection is provided to the individual in accordance with FIPPA. For more information on collection regulations as it is governed in FIPPA please see sections 38 and 39 of the Act. [↑](#footnote-ref-4)
5. See appendix for controls [↑](#footnote-ref-5)
6. This column has also been used to illustrate relationships between the questions and various security controls. These are not intended to be prescriptive, authoritative or exhaustive, and there is not exact correspondence in some cases. Please see the [Appendix](#_Appendix__) for descriptions and crosswalks. [↑](#footnote-ref-6)
7. With thanks to Carnegie Mellon University for the Application Security Controls listed at <https://www.cmu.edu/iso/governance/guidelines/data-protection/application-security.html>, May 10, 2016. [↑](#footnote-ref-7)
8. With thanks to Carnegie Mellon University for the Application Security Controls listed at <https://www.cmu.edu/iso/governance/guidelines/data-protection/application-security.html>, May 10, 2016. [↑](#footnote-ref-8)
9. This column has also been used to illustrate relationships between the questions and various security controls. These are not intended to be prescriptive, authoritative or exhaustive, and there is not exact correspondence in some cases. Please see the [Appendix](#_Appendix__) for descriptions and crosswalks. [↑](#footnote-ref-9)
10. This column has also been used to illustrate relationships between the questions and various security controls. These are not intended to be prescriptive, authoritative or exhaustive, and there is not exact correspondence in some cases. Please see the [Appendix](#_Appendix__) for descriptions and crosswalks. [↑](#footnote-ref-10)
11. This column has also been used to illustrate relationships between the questions and various security controls. These are not intended to be prescriptive, authoritative or exhaustive, and there is not exact correspondence in some cases. Please see the [Appendix](#_Appendix__) for descriptions and crosswalks. [↑](#footnote-ref-11)
12. <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> downloaded May 10, 2016. [↑](#footnote-ref-12)