University of Toronto

Information Risk and 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 – two documents that articulate 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

* + 1. Date:

## University of Toronto

* + 1. Sponsor’s Name:
    2. Sponsor's Department:
    3. Sponsor’s Contact Information:
    4. University of Toronto, Information + Technology Services, Information Security and Enterprise Architecture
       1. Contact Name:
       2. Contact Information:

## Company Name:

* + 1. Contact Name:
    2. Contact Information:

Contents

1. Introduction 1

2. Document Control Information 2

3. Product Summary and Asset Enumeration 4

4. Privacy Impact Assessment Questionnaire 5

5. Threat / Risk Assessment Questionnaire Introduction 11

6. TRA for Software to be managed by the University of Toronto 12

7. TRA for Networked Hardware / Appliances – to be installed on University of Toronto premises. 14

8. TRA for Outsource ('Cloud') Services – solution is hosted outside of University premises and managed by a service provider 17

9. TRA for Professional Services provided to the University 19

10. TRA for Development Services provided to the University 20

11. Additional Notes and Comments 21

# Product Summary and Asset Enumeration

## Product Summary

Please provide a description of the product or service, its purpose, how it functions and the benefits it is expected to provide to the University.

## Partners and Sub-contractors

Where aspect(s) of the product or service are not directly provided by the contracted vendor, please detail where ownership and / or responsibility resides, and for what aspects of the product or service.

## Information from Users

What information is collected from, or submitted to the system by users (user IDs, passwords, email addresses, content, etc.)?

## Information from Administrators and Operators

What information is collected from, or submitted to the system by administrators (user IDs, passwords, cryptographic keys, patches, configuration files, software updates and upgrades?

## System Generated Information

What information is created by the system as part of its operation (metadata associated with user and administrative activities, temporary system files, log files, connections to other services, etc.)

# Privacy Impact Assessment Questionnaire

A guided discussion on the use of user-associated or personally identifiable information (PII)

## Notification

* + 1. Are users notified before they sign into the service what personal information will be shared with the service?
    2. If an externally hosted service, does the service have the following:
       1. A privacy policy?
       2. A dedicated, full-time Privacy Officer position?
       3. A process to query / challenge / modify stored personal data?
       4. If so, please provide policy content, privacy officer contact info, and process info as appropriate.

## Stated uses

* + 1. What are the uses intended for requested information?
       1. How do these uses support the functionality that the University is seeking? (Note: The University must deny access to PII by default.)
    2. Is any information negotiable?

For example, the service may require certain data be required for the service to successfully authenticate the user, but that data could be a ‘dummy value’ if it is not used again, outside of the authentication process, or is not used to provide University-requested functionality

* + 1. Does the service provider intend to share University-provided PII with external partners?

If so:

* + - 1. Has the University agreed to this sharing?
      2. What is the purpose of sharing the information?
      3. Who will the information be shared with?
      4. How will the information be shared?
      5. What safeguards exist to ensure that the sharing will be limited to the stated purposes?
    1. Are there contractual terms in place to:
       1. Establish an end-of-life for data within the service and service partners’ (if any) environments?
       2. Establish that data sharing agreements with the service and the service’s partners (if any) do not out-live any part of the University’s contractual relationship with the service?
       3. Ensure the data is not re-shared by the service’s partners (if any)?
       4. Establish and enforce the University’s ownership of the data at all times and in all contexts?
       5. Please describe the process by which the University can reliably confirm the destruction of user attribute data under the following conditions:
          1. Once the information has reached its agreed end-of-life.
          2. At the termination of data sharing agreements between the University and the service, and between the service and the service’s partners (if any).
          3. Under any change in service ownership status (such as sale or bankruptcy) unless re-negotiated with the University, as per points 4.2.3 through 4.2.4.5 above.

Note: The University must prohibit sharing of released PII with service partners, except upon explicit permission of the University. Re-use of PII outside of stated and agreed-to uses must be prohibited, and all shared attribute 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 must retain ownership of shared attribute data.

* + 1. Terms for items 4.2.1 through 4.2.4 above must also be established for metadata or derivative data (such as usage or preference patterns) that is generated from PII provided by the University, when such could be associated with individual service users.

Please provide relevant information.

* + 1. The University will not share attributes of exceptional sensitivity (such as plain-text passwords, or a users’ Social Insurance Number – i.e. any attribute that could lead to user impersonation or identity theft) under any circumstances.
       1. Are any attributes of this nature currently required for the service?
       2. If any such attributes are, please state which attributes are required, why they are required and what measures are in place to protect them.

## Changes to Use

* + 1. If an externally hosted service, does the service provider have a process whereby users can query the service provider as to what data is stored, and update that information for accuracy?
       1. If so, the service provider must supply details of the query and update processes.
    2. Is there a notification and opt-out process in the event of proposed new uses of PII by either the service or the service’s partners (if applicable)?
       1. If so, the service provider must supply details of the notification process.
    3. Can users opt-out of the service’s or service partner’s (individually or in whole, if applicable) products at any time?
       1. If so, the service provider must supply details of the opt-out process.
    4. Will the users’ attribute data be provably destroyed in both the service and the service partners’ (if applicable) environments when a user chooses to opt-out of the service or service partners’ products?
       1. Please provide details of how this will be done.
    5. Terms for items 4.3.1 through 4.3.4 above must be established for metadata or derivative data (such as usage or preference patterns) that is generated from PII provided by the University, when such could be associated with individual service users.
       1. Please provide relevant information.

## Security

* + 1. The service provider must provide a copy of their Information Security Policy, or similar document that describes the practices and procedures put in place to protect the confidentiality, integrity, availability, and accountability for use of collected attribute data.
    2. The service provider must provide annual, successful, audits of the above policy or similar document (i.e. SAS 70 type II or equivalent audit) and practical network intrusion-testing audits. Does the service provider currently have such audits performed?
       1. If so, please provide details.
    3. Terms for items 4.4.1 and 4.4.2 above must be established for any partners with whom the service provider shares PII, or PII-derived data / PII metadata, or who develop their own metadata or derived data from supplied PII when such could be associated with individual service users. Does the service provider currently have such audits performed?
       1. If so, 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 service or 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’.

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.

# TRA for Software to be managed by the University of Toronto

## Information Security

## Access Controls

* + 1. Does the solution use Active Directory (AD) and / or Kerberos to authenticate users?
    2. If the solution provides a web interface, is it Security Assertion Markup Language 2.0 (SAML 2.0) compliant (i.e. will it work with Shibboleth federated access control software) for the purpose of authenticating users?

## Change Controls

## Authorization

* + - 1. Does the solution use Lightweight Directory Access Protocol (LDAP) or AD to manage roles and permissions?
      2. What degree of granularity does the solution offer in defining roles?
      3. Does the solution require a schema extension to support role management?

## Isolation

* + - 1. Does the solution work with / come with a guide for configuring its use with a firewall?
      2. Does the solution come with a hardening / security practices guide?
      3. Does the solution support encryption of data while in transit?

## Business Continuity Practices

* + 1. Does the solution have a recommended backup and recovery strategy? If so, what is it?
    2. Are backups capable of being encrypted? How are encryption keys managed?
    3. Is the solution compatible with Hardware Security Modules for the purpose of key management?

## Access, Change, and Fault Reporting

* + 1. Does the solution integrate with log monitoring services? If so, which? What information is provided to the monitoring service?
    2. If the solution does not integrate with log monitoring services, what internal activity and resource consumption reports does it provide?

## Enterprise Architecture

## Capacity and Scalability

* + 1. Does the solution support High Availability (HA); does it support live fail-over?
    2. Does the solution work with load balancers?
    3. Does the solution work in a virtual environment - if so, is any particular vendor's virtual environment preferred?
    4. What Service Level options are available?
    5. What are the limitations on solution capacity including, but not limited to: memory, CPU, simultaneous connections, storage, and throughput.

## Inter-Operability

* + 1. Does the solution follow web standards, such as REpresentational State Transfer (REST), or Open Web Application Security Project (OWASP)?
    2. Does the solution comply with the Accessibility for Ontarians with Disabilities Act (AODA) accessibility requirements?
    3. Does the solution comply with the Learning Tool Inter-operability (LTI) standard?
    4. Does the solution comply with the IMS Common Cartridge format?
    5. Does the solution comply with the Question and Test Inter-operability (QTI) standard

## Maintainability

* + 1. Does the solution offer a choice of databases, or is one preferred? If so, which?
    2. Does the solution work with a Storage Area Network (SAN)?
    3. Does the solution offer a choice of operating systems? If so, which?
    4. Can the solution be remotely administered?

## Client Integration

* + 1. Does the solution have any client-specific requirements including, but not limited to: hardware, operating system, software or software components / frameworks (such as Silverlight, Adobe Flash, or Microsoft .NET), authentication or authorization membership (such as Active Directory domain membership), protocols, and

## Business Integration

* + 1. Is the solution obliged to comply with functionality requirements that may be present in jurisdictions other than Ontario, Canada?
    2. Are users required to accept click-through Terms of Service agreements? Can these be disabled for users affiliated with the University of Toronto?
    3. If handling credit card data, is the solution Payment Application Data Security Standard (PA-DSS) compliant?
    4. Does the solution support application of separation of duties and need-to-know rules, or any other solution-specific GAAP or IFRS rules?

## Academic Objectives

* + 1. What tools does the solution provide to assess the effectiveness of learning outcomes both for administrators / educators and for students?
    2. Does the solution support adaptive release functionality?

# TRA for Networked Hardware / Appliances

## Information Security

## Access Controls

* + 1. Does the solution use Active Directory (AD), Kerberos, or Remote Access Dial In User Service (RADIUS) to authenticate users?
    2. If the solution provides a web interface, is it Security Assertion Markup Language 2.0 (SAML 2.0) compliant (i.e. will it work with Shibboleth federated access control software) for the purpose of authenticating users?

## Change Controls

## Authorization

* + - 1. Does the solution use Lightweight Directory Access Protocol (LDAP) or AD to manage roles and permissions?
      2. What degree of granularity does the solution offer in defining roles?
      3. Does the solution require a schema extension to support role management?

## Isolation

* + - 1. Does the solution work with / come with a guide for configuring its use with a firewall?
      2. Does the solution come with a hardening / security practices guide?
      3. Does the solution support encryption of data while in transit?

## Business Continuity Practices

* + 1. Does the solution have a recommended backup and recovery strategy? If so, what is it?
    2. Does the solution have dual power supplies and / or dual Network Interface Cards (NICs)?

## Access, Change and Fault Reporting

* + 1. Does the solution integrate with log monitoring services? If so, which? What information is provided to the monitoring service?
    2. If the solution does not integrate with log monitoring services, what internal activity and resource consumption reports does it provide?

## Enterprise Architecture

## Capacity and Scalability

* + 1. Does the solution support High Availability (HA); does it support live fail-over?
    2. Does the solution work with load balancers?
    3. What Service Level options are available?
    4. What are the limitations on solution capacity including, but not limited to: memory, CPU, simultaneous connections, storage, and throughput.

## Inter-Operability

* + 1. Does the solution follow web standards, such as REpresentational State Transfer (REST), or Open Web Application Security Project (OWASP)?
    2. Does the solution comply with the Accessibility for Ontarians with Disabilities Act (AODA) accessibility requirements?

## Maintainability

* + 1. Does the solution offer a choice of databases, or is one preferred? If so, which?
    2. Does the solution work with a Storage Area Network (SAN)?
    3. Does the solution offer a choice of operating systems? If so, which?
    4. Can the solution be remotely administered?

## Client Integration

* + 1. Does the solution have any client-specific requirements including, but not limited to: hardware, operating system, software or software components / frameworks (such as Silverlight, Adobe Flash, or Microsoft .NET), authentication or authorization membership (such as Active Directory domain membership), protocols, and

## Business Integration

* + 1. Is the solution obliged to comply with functionality requirements that may be present in jurisdictions other than Ontario, Canada?
    2. Are users required to accept click-through Terms of Service agreements? Can these be disabled for users affiliated with the University of Toronto?
    3. If handling credit card data, is the solution Payment Application Data Security Standard (PA-DSS) compliant?

# TRA for Outsource or 'Cloud' Services (non-University managed software solutions)

## Information Security

## Access Controls

* + 1. Does the solution use Active Directory (AD) and / or Kerberos to authenticate users?
    2. If the solution provides a web interface, is it Security Assertion Markup Language 2.0 (SAML 2.0) compliant (i.e. will it work with Shibboleth federated access control software) for the purpose of authenticating users?

## Change Controls

## Authorization

* + - 1. What degree of granularity does the solution offer in defining roles?

## Isolation

* + - 1. What security standards are followed in the operation of the service? Please indicate where the service is protected via firewalls, and data protected via encryption.
      2. Is compliance with internal security standards assessed via a SAS 70 Type II or a CSAE 3416 (formerly CICA 5970) compliance audit, at least annually?
      3. What external application vulnerability scans / assessments / audits are done? How often?
      4. Does data transit non-Canadian networks? If so, where?
      5. Is data stored outside of Canadian borders? If so, where?

## Business Continuity Practices

* + 1. What provisions are in place to exit the service?
    2. What provisions are in place to protect intellectual property?
    3. What provisions exist for decryption key escrow, for encrypted solutions?
    4. Are backups encrypted? How are the encryption keys managed?
    5. Are backups and recovery procedures tested?

## Access, Change and Fault Reporting

* + 1. Does the solution integrate with log monitoring services? If so, which? What information is provided to the monitoring service?
    2. If the solution does not integrate with log monitoring services, what internal activity and resource consumption reports does it provide?

## Enterprise Architecture

## Capacity and Scalability

* + 1. What Service Level options are available?
    2. What are the limitations on solution capacity including, but not limited to: memory, CPU, simultaneous connections, storage, and throughput.

## Inter-Operability

* + 1. Does the solution follow web standards, such as REpresentational State Transfer (REST), or Open Web Application Security Project (OWASP)?
    2. Does the solution comply with the Accessibility for Ontarians with Disabilities Act (AODA) accessibility requirements?
    3. Does the solution comply with the Learning Tool Inter-operability (LTI) standard?
    4. Does the solution comply with the IMS Common Cartridge format?
    5. Does the solution comply with the Question and Test Inter-operability (QTI) standard

## Maintainability

* + 1. Does the solution offer a choice of databases, or is one preferred? If so, which?
    2. Does the solution work with a Storage Area Network (SAN)?
    3. Does the solution offer a choice of operating systems? If so, which?
    4. Can the solution be remotely administered?

## Client Integration

* + 1. Does the solution have any client-specific requirements including, but not limited to: hardware, operating system, software or software components / frameworks (such as Silverlight, Adobe Flash, or Microsoft .NET), authentication or authorization membership (such as Active Directory domain membership), protocols, and

## Business Integration

* + 1. Is the solution obliged to comply with functionality requirements that may be present in jurisdictions other than Ontario, Canada?
    2. Are users required to accept click-through Terms of Service agreements? Can these be disabled for users affiliated with the University of Toronto?
    3. If handling credit card data, is the solution Payment Card Industry Data Security Standard (PCI-DSS) compliant?
    4. Does the solution support application of separation of duties and need-to-know rules, or any other solution-specific GAAP or IFRS rules?
    5. What auditable, IT standards are followed (such as operational or security standards)? How often are the audits performed?
    6. Are the results of audits communicated to service clients upon completion?

## Academic Objectives

* + 1. What tools does the solution provide to assess the effectiveness of learning outcomes both for administrators / educators and for students?
    2. Does the solution support adaptive release functionality?

# TRA for Professional Services provided to the University

## Certifications / Qualifications

* + 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)?
    2. Have proposed team members worked on projects of similar size / nature / complexity in past?
    3. Do the proposed team members have vendor or technology-specific certifications (such as: Microsoft, Java, Oracle, etc.)?

# TRA for Development Services provided to the University

## Certifications / Qualifications

* + 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)?
    2. Have proposed team members worked on projects of similar size / nature / complexity in past?
    3. Do the proposed team members have vendor or technology-specific certifications (such as: Microsoft, Java, Oracle, etc.)?

## Standards

* + 1. Are security standards (such as Open Web Application Security Project (OWASP)) and architectural standards (such as TOGAF) followed in development of solutions?
    2. What coding methodology / review practices / are followed in the development of solutions?

## Review

* + 1. Has the developer anticipated the need to perform a Privacy Impact Assessment (PIA) and Threat and Risk Assessment (TRA), and has budgeted time to do so?
    2. If so, how much time has been reserved?
    3. How has the PIA and TRA process been integrated into the development process?

# 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.