Standard: Threat Risk Assessment (IT)

Effective Date:	2020.02.06
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Director, Information Security and Compliance
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The purpose of this standard is to describe Threat Risk Assessment activities at a high level and applicable terminology. An IT Threat Risk Assessment is an activity used to identify risks and threats that may impact the security of information systems and the data processed by them in the context of business and compliance requirements.

Who/what does the standard apply?

The requirements in this standard apply to assets owned by the University of Manitoba.

Definitions

- **Asset:** components that comprise the value of an information system. The value of an asset is typically expressed in the context of Confidentiality, Integrity and Availability.
- **IT Threat Risk Assessment:** An activity used to identify risks and threats that may impact the security of information systems and the data processed by them in the context of a business or compliance requirement.
- **Risk:** The potential for losing something of value.
- **Stakeholder:** People participating in the TRA.
- **Threat:** an event with the potential to adversely impact the value of an asset.
- **Threat Landscape:** A collection of threats and trends collected from trusted public sources.
- **Tools:** Are used to conduct TRA activities and include but are not limited to: matrices, questionnaires, guides and technical tools.
- **Vulnerability:** A state or condition in an asset that when combined with an action or change in the form of a threat event contributes to risk.

Compliance

Threat Risk assessment activities must align to the requirements and specifications outlined in this standard. Where systems and applications are not able to comply, please refer to the Information Security Policy for guidance on exceptions.

Specifications

Requirement	Specifications
TRAs will be conducted on IT systems.	Information Security guidelines will be used to conduct assessment work.
All request will be triaged.	Information collected during intake will be used to determine whether a TRA is required. TRAs required for high risk systems or systems that integrate with a higher risk. Lower risk systems may not require a TRA.
Assessment work will be recorded	Information collected during and derived from assessment work will be stored and maintained in systems under the control of the University.
Risk assessment tools will be used to conduct assessment work	The TRA guideline documentation will describe tools and their appropriate use. The guidelines and tools will be updated based on industry standard methodologies, stakeholder feedback, management directives, organizational change and changes in the Threat Landscape.
Risks will be reported to stakeholders for response. Risks requiring remediation will be followed up on.	Risks and resulting recommendations will be communicated to stakeholders based on guidelines. Risks identified as Critical will be raised to stakeholders immediately. Identified risks and remediation activities will be stored and maintained in systems under the control of the University.
Risks identified in TRAs will be represented in the Risk Register	Risks identified during TRA activities will be aggregated for representation in the Risk Register. Risk Register activities will be guided by the Risk Register guideline.
Stakeholder participation.	A stakeholder with a leadership role or management authority will act as a point of contact during assessment work. Stakeholders with leadership duties will provide a point of contact for issues to be escalated to. Issues include but are not limited to: Identified Critical Risks, non-responsive stakeholders, incomplete information and scheduling conflicts.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	