UNIVERSITY OF
SASKATCHEWAN

IT Risk Management Procedure

A key objective of the IT Risk Management Procedure is to reduce the risk (i.e., likelihood and impact) of a security incident incurred by the university or the university community.

The risk management process considers the information (in IT assets or IT systems) at risk, determines the consequence of compromise, identifies threats, recommends appropriate security controls and safeguards, and determines the reduced residual risk remaining after the controls and safeguards are implemented. Controls can also be designed to demonstrate compliance to a set of security requirements or regimes.

The following scenarios are examples of activities that would need to follow the IT risk management procedure.

- Need to share information or collaborate using information technology
- Need to purchase IT assets, including computers, mobile devices, servers, network-enabled devices, etc.
- Need to purchase IT services or systems, either locally hosted or cloud based

Contact the ICT Service Desk at servicedesk@usask.ca to start the IT risk management procedure. The process is summarized in the three-steps below:

1. **Occurrence of an Initiating Activity or Decision**
   As identified in the IT Security Policy, the IT risk management procedure is initiated when units or individuals need to work with ICT to implement alternative mitigation strategies for IT services and university-owned IT end-point devices to ensure that the overall risk to the university is being maintained at an acceptable level.

   a) **Assessment of Risk**
   For each initiating activity, the risk to the university must be assessed. ICT will work through a Threat and Risk Assessment and a Privacy Impact Assessment with the units or individuals. Once assessed, a risk management approach will be designed.

   b) **Assessment of Security Controls and Safeguards (Mitigation Alternatives)**
   Once the risk to the university has been assessed, , the risk needs to be mitigated (managed). Working with ICT, mitigation alternatives will be explored. Examples of strategies and controls available to mitigate risk include segmenting the network to limit exposure, requiring two-factor authorization, or modification of the business process making using of the IT, or modification of the type of information captured.

2. **Implementation of Mitigation Strategies**
   Once the mitigation strategies have been assessed, the ones that reduce the risk to an acceptable level will be implemented by ICT. The reduced level of risk remaining is known as the residual risk (Threat – Controls = Residual Risk). The mitigation strategies need to be assessed after they've been implemented to ensure they provide the expected result.

3. **Maintenance of Security Controls and Safeguards**
   Once the security controls and safeguards have been implemented, the security of the information, IT assets, and IT services must be maintained.

To start the IT risk management procedure, or if you have questions or comments, contact the ICT Service Desk at servicedesk@usask.ca.