IT Service Acquisition and Outsourcing Procedure

A key objective of the IT Service Acquisition and Outsourcing Procedure is to reduce the risk (i.e., likelihood and impact) of an incident, such as disclosure of data, loss of service or loss of data, being incurred by the university or the university community as a result of using non-university IT services. IT outsourcing is defined as the use of external service providers to deliver IT-enabled business process, application service and infrastructure solutions. Outsourcing can include, but is not limited to, utility services, software as a service and cloud-enabled outsourcing.

The IT outsourcing 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 outsourcing procedure.

- Need to purchase or use IT-enabled business process, application service and/or infrastructure solutions provided by external service providers.

Contact the contact ICT Licensing and Acquisitions at ICT_acquisitions@usask.ca to start the IT outsourcing procedure. The process is summarized in the three-steps below:

1. **Decision to Acquire IT to Meet a Need or Resolve an Issue**
   As identified in the IT Security Policy, the IT outsourcing procedure is initiated when units or individuals have a need to use external service providers to deliver IT-enabled business process, application service and/or infrastructure solutions.

2. **Determination of Risk and Risk Management Strategies**
   Units or individuals need to work with ICT in order 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 assist units or individuals through a Threat and Risk Assessment and a Privacy Impact Assessment. 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 modification of the business process making using of the IT, modification of the type of information captured by the service or modification or addition of terms in the contract with the vendor.

3. **Implementation of Mitigation Strategies**
   Once the mitigation strategies have been assessed, the ones that reduce the risk to an

acceptable level must be implemented. 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 have been implemented to ensure they provide the expected result.

4. **Maintenance of the Security of the Externally Provided Services or Solutions**
   Once the security controls and safeguards have been implemented, the security of the externally provided IT-enabled business process, application service and/or infrastructure solution must be maintained.

To start the IT outsourcing procedure, or if you have questions or comments, contact ICT Licensing and Acquisitions at ICT_acquisitions@usask.ca.