IT SECURITY RISK MANAGEMENT IN THE GOVERNMENT OF CANADA

JULY 2016 | EXECUTIVE SERIES | ITSE.10.033

With today's dynamic threat environment and Government of Canada (GC) fiscal constraints, information technology (IT) security can no longer be an afterthought, but rather needs to be a vital component in both departmental and IT project plans.

IT security risks can result in exposure of sensitive government information, a loss in productivity, an inability to meet organizational objectives, or damage to the GC's reputation, all of which can be costly to the GC.

IT security risk management is the process by which organizations manage IT security risks and is achieved through the management and application of security controls, solutions, tools, and techniques to protect IT assets against compromises.

CSE's IT security risk management framework can help outline a risk strategy that will align with GC priorities and resource allocation so that departmental objectives can be met.

Departmental Responsibility

The following actions should be performed by the **business owner** of the IT system when making IT security risk management decisions:

- ✓ Determine the highest level of risk that can be tolerated;
- ✓ Consult with business continuity planning, privacy, information management, and other functional specialists to ensure that risks within these areas of responsibility are identified and managed;
- ✓ Provide IT security risk decisions to the Departmental Security Officer;
- ✓ Grant **Authority to Operate** once risks have been identified and mitigated or accepted; and
- ✓ Ensure that risk assessments are re-evaluated in light of changes to asset value, threats, or vulnerabilities to maintain the authority of IT systems to operate.

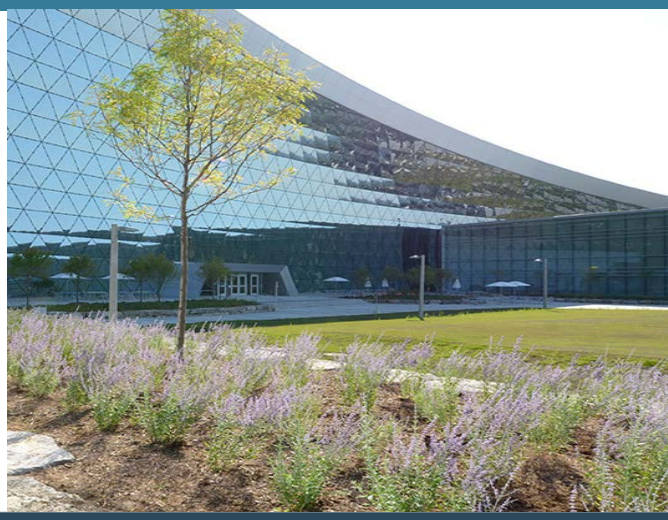
Authority to Operate is the business owner's approval to allow a project, program, facility, or system to operate using a particular set of safeguards within an acceptable level of residual risk.

Build and Strengthen

Since IT security is an iterative process that evolves as the threat landscape changes, departments should take a holistic and strategic look at how their IT security is implemented.

Departments need to continually assess, plan, build, and execute effective IT security programs that consider IT risk management as well as governance, operational requirements, and compliance.

IT risk management addresses the legal, financial, compliance, reputational, policy, operational, and privacy risks organizations face.



A Business Enabler

CSE's *ITSG-33 - IT Security Risk Management: A Lifecycle Approach* has been developed to help GC departments ensure security is considered right from the start. ITSG-33 is a framework to help organizations assess and mitigate risks through the effective application of security controls that protect information against a compromise of confidentiality, integrity, or availability. By following its principles, you not only help ensure predictability and cost-effectiveness, you also help ensure that there are no hidden surprises preventing you from obtaining and maintaining **authority to operate** from the designated business owner of the IT system.

Want to Learn More?

Take the Executive Overview of IT Security Management offered by CSE's IT Security Learning Centre (Course #604).

According to TBS's ***Operational* Security STANDARD: MANAGEMENT OF IT SECURITY**, program and service delivery managers must ensure an appropriate level of security for their programs and services.

An Integrated Approach

IT security risk management identifies the roles, responsibilities, and activities that will help GC departments manage IT security risks. When GC departments follow the risk management strategies outlined in CSE's *ITSG-33 - IT Security Risk Management: A Lifecycle Approach*, departments will:

- ✓ Address all aspects of IT security in an efficient manner;
- ✓ Satisfy department-wide business needs for security;
- ✓ Improve risk management decision making; and
- ✓ Comply with GC policies and standards.

If you would like to read more about IT Security Risk Management, visit:

www.cse-cst.gc.ca/its

Questions?

Contact ITS Client Services
itsclientservices@cse-cst.gc.ca
613-991-7654

IT Security Risk Management: A Lifecycle Approach

Adhering to ITSG-33 guidelines has many benefits for departments, including compliance with the overall risk management strategy and objectives established by TBS, addressing key aspects of IT security in an efficient manner, and consistently and cost-effectively managing IT security risks.