Information Security

OCIO Strategy 2016:

SECURITY

Security is about safeguarding sensitive information and ensuring the confidentiality, integrity, and availability of critical systems and networks to maintain public trust in government services. Digital services, located in the cloud, often accessed using wireless devices and often involving personal information, are particularly vulnerable to cyber security threats or accidental breaches. In this context, government has a responsibility to apply the appropriate safeguards that will mitigate our risks.

Information Security

OCIO Strategy 2016:

ENABLE DIGITAL

Enabling the public service to deliver digital services that are convenient and easy to use is going to take an all-of-government approach. The OCIO will play a key enabling role in setting the B.C. government's foundation for digital service delivery.

OPERATIONAL EXCELLENCE

Striving for operational excellence is about sound management, governance and operations of IT so government services are reliable, secure and accessible. Integrating and making it easy to access the many technology choices and platforms available today, both in-house and in the cloud, ensures that government services remain sustainable and interoperable.

MAXIMIZE VALUE

Maximizing value from IT investments is about ensuring the OCIO remains focused on delivering our commitments and maintaining cost-effectiveness. In today's context of ongoing change, our investments, assets and approaches should continuously adapt to maximize business value.

How?

- How do we ensure we are **proactive** about Information Security?
- How do we ensure we are **excellent** and **maximise value** in what we do to secure information and manage our risk?

Corporate Information Security Risk Register Capability

Why?

- All corporate level InfoSec risks identified in one place, tracked over time and lets senior leadership know
  - What is happening
  - What we are doing about it
  - What the decision maker can do about it

Who?

- A project Initiated by the CISO Gary Perkins to bridge the gap between operational and corporate InfoSec risks, run out of the Information Security Branch

What?

- A corporate-level risk capability combining:
  - A tool
  - People
  - A process
  - A mandate

Corporate Information Security Risk Register

Information Security & Threat Risk Assessment – STRA

Why?

- Identifies key risk information for a Corporate Risk Registry

- Provides value to Business Owners:
  - enables them to demonstrate security features;
  - helps inform their executive and auditors;
  - helps assure their users that the system and support teams have a good understanding of the system risks and are managing them appropriately.

What?

- A STRA is a collaborative process that identifies risk and generates a report that includes an assessment of the risks, and the security controls to mitigate those risks.

Policy requires you to do a STRA, but it is your customers and users that need assurances you're actively managing security risks to *their* information.

Who does a STRA?

STRA's are a collaborative result from:

- business owners, technical leads, security leads;
- partners, vendors;
- should always include those that are (or will be) supporting the system or service on a day-to-day basis.

The true value of a STRA is in the collaborative effort – provides everyone who participates in the STRA a better understanding and a *shared knowledge* of the system environment, potential risks, and what security controls are in place to help mitigate those risks.

Where are we at with the STRA process?

- Current STRA process can be lengthy.
- Collaborative effort underway with Ministries to create a new more efficient process focused on risk management
- Currently being tested in Proof of Concept projects across multiple Ministries.

Public Service Culture

Source: "Where ideas work: A corporate plan for the BC public service, 2016"

Thank You!

Questions?

BRITISH COLUMBIA

OCIO

Office of the Chief Information Officer