INFORMATION SECURITY THREAT AND RISK ASSESSMENT STANDARD (STRA)

Architecture, Standards and Planning Branch
Office of the CIO • Province of BC

People • Collaboration • Innovation

Version 2.0

23 July, 2010 – V1.6 (For Review)
Copyright notice
This document is a Provincial Architecture/Standard proposal and is copyright-protected by the province. Except as permitted under the applicable laws of the user's country, neither this draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured. Requests for permission to reproduce should be addressed to the Office of the CIO.

Document Control

[Drafts start at 0.1 whereas a document ready for signature becomes version 1.0]

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Change Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 Feb – 17 May 2010</td>
<td>Steven Hunt</td>
<td></td>
<td>Updates after several meetings with ISB</td>
</tr>
<tr>
<td>06 May 2010</td>
<td>Steven Hunt</td>
<td>1.4</td>
<td>Updates after several meetings with STRA Working team</td>
</tr>
<tr>
<td>27 May 2010</td>
<td>Karen Bolch</td>
<td>1.4</td>
<td>Updates after MISO feedback</td>
</tr>
<tr>
<td>23 June 2010</td>
<td>Karen Bolch</td>
<td>1.5</td>
<td>Clarified minimum STRA standard requirements</td>
</tr>
<tr>
<td>19 July 2010</td>
<td>Steven Hunt</td>
<td>1.6</td>
<td>Review of feedback from Cindy Madden</td>
</tr>
<tr>
<td>23 July 2010</td>
<td>Karen Bolch / Steven Hunt</td>
<td>1.6</td>
<td>Review of feedback from MOH, FIN, CS and STED.</td>
</tr>
</tbody>
</table>
Table of Contents

1 FOREWORD ................................................................................................................................................. 3
2 INTRODUCTION ............................................................................................................................................ 3
2.1 Classification........................................................................................................................................... 4
3 SCOPE ......................................................................................................................................................... 5
4 NORMATIVE REFERENCES ..................................................................................................................... 5
5 REQUIREMENTS ......................................................................................................................................... 7
5.1 Basis of Evaluation (BoE) Table ........................................................................................................... 8
6 GENERAL CHARACTERISTICS .............................................................................................................. 11
6.1 Characteristics and Standard ............................................................................................................... 11
6.2 Security Control Objectives ............................................................................................................... 11
6.3 Information Characteristics .............................................................................................................. 11
7 EVALUATION CRITERIA ......................................................................................................................... 12
7.1 Enquiry Scope ...................................................................................................................................... 12
7.2 Analysis/Acceptance .......................................................................................................................... 12
7.3 Response ............................................................................................................................................. 12
8 TERMS AND DEFINITIONS .................................................................................................................... 12
9 BIBLIOGRAPHY ....................................................................................................................................... 12
ANNEX A. SECURITY THREAT RISK ASSESSMENT STANDARD ......................................................... 13
ANNEX B. STRA PROCESS .......................................................................................................................... 19
ANNEX C. FUNDAMENTAL INFORMATION RISK MANAGEMENT (FIRM) ............................................ 30
ANNEX D. HARM REFERENCE TABLE ...................................................................................................... 32
ANNEX E. STRA BOE (SCORECARD) TABLE .............................................................................................. 33
ANNEX F. HIGH LEVEL RISK SCORECARD – ISMART ............................................................................ 34
ANNEX G. STRA TECHNICAL DIAGRAMS ................................................................................................ 36
ANNEX H. STRA PROCESS CHECKLIST ................................................................................................. 43
ANNEX I. DETERMINATION OF ACCEPTABLE RISK ............................................................................... 44
ANNEX J. TERMS AND DEFINITIONS ........................................................................................................ 46

Table of Figures
Figure 1: Enterprise Risk Management Components .................................................................................. 5
Figure 2: Standard Classification Table ....................................................................................................... 5
Figure 3: STRA BoE (Scorecard) Table ......................................................................................................... 9
Figure 4 'Issues' data field within Citicus .................................................................................................... 23
Figure 5 Levels of HARM ........................................................................................................................... 25
Figure 6 'Action Plan' data fields within Citicus ......................................................................................... 27
Figure 7: Constructive Risk Management Process .................................................................................... 31
Figure 8: BC Provincial Government customised HARM Reference Table v4 ........................................... 32
Figure 9: STRA BoE (Scorecard) Table ....................................................................................................... 33
Figure 10: Information Security Assessment Architecture Documentation ............................................. 36
Figure 11: Infrastructure Review ................................................................................................................ 37
Figure 12: Sample Process- Service for Granting Access ........................................................................... 38
Figure 13: Sample Process - Service for Granting Access .................................................................... 38
Figure 14: Information Flow presented in Tabular Form ........................................................................... 39
Figure 15: Sample Process - Expansion of the registration process from information flow .................... 40
Figure 16: Sample Tabular View - Data flow could also be presented as a Table ..................................... 41
Figure 17 Acceptable Risk for the BC Government .................................................................................... 44
Figure 18 Acceptable Risk BC Government Basis of Evaluations (BoE’s) .................................................... 45
1 Foreword

The Government Chief Information Officer (GCIO) is responsible for ensuring the management of information and the use of technology to support government’s Five Great Goals and Strategic Investments for the Future to assist in achieving secure client-centered service delivery. One of the roles of the GCIO is to promote and guide government’s management of information as a strategic business asset and to enable information use and sharing while protecting privacy and maintaining a secure environment.

Information Management/Information Technology (IM/IT) security governance and policy frameworks have been established to ensure that the Province complies with international standards, guidelines, policies, and legislation related to information privacy and security within provincial jurisdiction. Information about the rationale for achieving full compliance is available in the Core Policy Procedure Manual (http://gww.cio.gov.bc.ca/policy/).

The Office of the Chief Information Office (OCIO), Information Security Branch is responsible for the development and maintenance of a Security Threat and Risk Assessment (STRA) standard to measure, report on, and monitor information risk and compliance to the IM/IT security governance and policy framework.

The Ministry Information Security Officer (MISO) is responsible for assisting business areas in conducting Security Threat and Risk Assessments.

Information owners and information custodians must conduct a STRA to ensure that information system development or acquisition activities are done in accordance with documented requirements, standards, and procedures. The STRA process is intended to address these issues and to establish compliance practices that are in line with the IM/IT security governance and policy frameworks. It also includes assessments of legal and regulatory requirements applicable to government.

2 Introduction

The Government of British Columbia takes a corporate view of managing risks and threats to its programs, operations, systems, networks and other components of its activities. It can be described as one in which risks/threats/vulnerabilities (collectively referred to as risks) are analyzed by:

- Identifying the context in which the risk exists
- The nature of the risk itself
- The analysis of the impacts and likelihoods of the risk
- Identification and analysis of the ways in which the risks can be reduced, mitigated, accepted, eliminated, or how the risk will be managed

All of this is undertaken within a framework of consultation and communication and ongoing monitoring and review referred to as a Security Review. The Security Review is aligned with the government’s Enterprise Risk Management (ERM) Model. The Security Threat and Risk Standard outlined herein is a subset of the Security Review - Information Security Threat and Risk Assessment Methodology and Process Supplementary document and focuses on the STRA process to be followed when assessing an IM/IT project for risk and compliance to government policy and standards. The Security Review - Information Security Threat and Risk Assessment Methodology and Process Supplementary document provides more detailed elements of the information security threat and risk assessment (STRA) methodology and process.

This information security threat and risk assessment methodology and process focuses primarily on the security component of ERM as seen below in Figure 1: Enterprise Risk Management Components. The methodology can be
applied to the four key elements of security (personnel, physical, records/information and information technology) and is particularly appropriate to complex situations where a detailed examination is required. These specialized areas bring their own criteria and resources to bear upon the process. Risk Management Branch can assist with many of these specialized sub-disciplines.

Figure 1: Enterprise Risk Management Components

2.1 Classification

The proposed standard is classified as follows:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Type</th>
<th>Nature</th>
<th>Review</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Threat and Risk Assessment Standard (STRA)</td>
<td>Process</td>
<td>Strategic</td>
<td>Annual</td>
<td>The standard is meant for any ministry, other public agency or external service provider that is considering undertaking a STRA.</td>
</tr>
</tbody>
</table>

Figure 2: Standard Classification Table
3 Scope

The standard is meant for any ministry, public agency or external service provider that is responsible for managing B.C. Government’s information. For maximum effectiveness, STRAs must be done on every IM/IT project involving a new application, service, system, and/or environment or whenever a major change (i.e.: new information systems) is proposed.

This STRA standard document is intended for those individuals who are responsible for measuring and controlling information risk as outlined in the Core Policy and Procedures Manual, Information Security Policy and legislation. Information security threat and risk assessments are to be carried out using the BC Government’s Information Security Management and Risk Tool (iSMART).

iSMART will enable information security risks to be identified, measured using the risk register (refer to Annex D: HARM Reference Table), and mitigated. iSMART establishes an information security risk monitoring capability in government and serves as a repository for STRAs. It also enables authorized personnel to view individual STRA results, ministry-wide results and cross-government results.

The scope of the STRA standard is to assess an IM/IT project’s use of resources and controls, either implemented or planned to eliminate and/or manage vulnerabilities exploitable by threats internal and external to government. If exploited, these vulnerabilities could result in:

- Unauthorized disclosure of data
- Unauthorized modification to the system, its data, or both
- Denial of service, access to data, or both to authorized users

A completed STRA within iSMART provides reports which illustrate the confidentiality (protection from unauthorized disclosure of system and data information), integrity (protection from improper modification of information), and availability (loss of system access) of the system. The reports show the risks associated with the IM/IT project being reviewed, compliance to policy and standards when assessed and an overall project action plan to address risks and recommendations. Recommended security safeguards will allow management to make informed decisions about security-related initiatives.

4 Normative references

International Standards
- ISO/IEC 27002 information security standard published by the International Organization for Standardization (ISO)

Standards Manual
- Core Policy and Procedures Manual:
  http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm

Information Management Standards
- Information Security Policy:
  http://www.cio.gov.bc.ca/cio/informationsecurity/policy/securityinformationpolicy.page

• STRA Methodology and Process
Page 5
5 Requirements

This Standard puts into effect the B.C. Government’s policy requirements as outlined in Annex A: Security Threat Risk Assessment Standard:

- All IM/IT projects must select any one of the Basic of Evaluation (BoE) scorecards listed, and complete the top-level sections (A through I – 61 statements) within the risk tool located in iSMART. (Each response to a question should be substantiated by adding comments, and attaching or providing a reference to the supporting documentation.)
- Any identified issues, risks and recommendations are to be entered into the issues log and action plan and remediation action provided. (This requirement can be met by attaching or providing a reference to the supporting documentation within the issues log and action plan.)

iSMART Basis of Evaluation (BoE) Scorecards:

<table>
<thead>
<tr>
<th>CSV Row</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 or Information Risk Assessment (IRA) or Standard of Good Practice (SoGP)</td>
<td></td>
</tr>
</tbody>
</table>

The Basis of Evaluation (BoE) Matrix (seen below in Figure 3: STRA BoE (Scorecard Table) is intended to assist ministries in selecting the most suitable scorecard to meet their IM/IT project requirements.

It is highly recommended that further analysis of risk and compliance be undertaken by completing the underlying questions associated with the scorecard chosen.
## 5.1 Basis of Evaluation (BoE) Table

This table summarizes the basic requirements for IM/IT projects and recommended use each scorecards.

(All estimates for resourcing are dependent on scenario or complexity of IM/IT project).

<table>
<thead>
<tr>
<th>Target Type</th>
<th>BoE Name</th>
<th>ID &amp; Example</th>
<th>Purpose</th>
<th>Description</th>
<th>Suitable for Evaluation of</th>
<th>Project Size &amp; Complexity</th>
<th>Level of Review</th>
<th>Depth &amp; Detail Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Resource</td>
<td>BoE U 11</td>
<td>Security Review (Confidentiality, Integrity and Availability)</td>
<td>Based on ISO 27001 - 27002 Standards. Provides self-validation tests. Static checklist containing up to 123 control review questions.</td>
<td>• Applications&lt;br&gt;• Program Areas&lt;br&gt;• Systems and Services&lt;br&gt;• Sites</td>
<td>Small Size Project&lt;br&gt;• Less than one application and/or system&lt;br&gt;• No significant interfaces to other applications or systems&lt;br&gt;• 3 - 6 hours of effort</td>
<td>High Level Review</td>
<td>Less Detailed</td>
<td></td>
</tr>
<tr>
<td>Information Resource</td>
<td>BoE U 18</td>
<td>Security Review (Confidentiality, Integrity and Availability)</td>
<td>The selection of questions are based on Citius Ltd. research and analysis of the effectiveness of industry best practice security controls. Provides self-validation tests. Static checklist containing up to 221 control review questions.</td>
<td>• Applications&lt;br&gt;• Program Areas&lt;br&gt;• Systems and Services</td>
<td>Medium Size Project&lt;br&gt;• More than one application and/or system&lt;br&gt;• Significant interfaces to other applications or systems&lt;br&gt;• 6 - 12 hours of effort</td>
<td>Medium Level Review</td>
<td>Moderately Detailed</td>
<td></td>
</tr>
<tr>
<td>Information Resource</td>
<td>BoE U 35</td>
<td>Security Review (Confidentiality, Integrity and Availability)</td>
<td>Based on the Information Security Forum (ISF) Standard of Good Practice (SoGP 2007). Checklist can be customised with specific questions relevant to the information being evaluated. Checklist can use up to 36 different “Attributes” containing up to 1572 control review questions.</td>
<td>• Applications&lt;br&gt;• Systems and Services&lt;br&gt;• Alternative Service Delivery (ASD)</td>
<td>Large Size Project&lt;br&gt;• More than one application and/or system&lt;br&gt;• Significant interfaces to other applications or systems&lt;br&gt;• 12 - 25 hours of effort</td>
<td>Low Level Review</td>
<td>Very Detailed</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: STRA BoE (Scorecard) Table
6 General characteristics

6.1 Characteristics and Standard

While there are a variety of risk management methodologies, many options are substantially the same or simply variations on a common theme. To provide a meaningful framework for analysis, the STRA standard provides an analytical approach to information security risk management.

The STRA standard is aligned with the government’s Enterprise Risk Management (ERM) Model and provides additional specific details on IM/IT security threats and risks. It is tightly integrated with other government related policies, such as the Core Policy and Procedures Manual Chapter 12 Supplemental, Information Security Policy and IM/IT Manual.

Information owners and information custodians must conduct a STRA to ensure that IM/IT projects involving information system development or acquisition activities are done in accordance with documented requirements, standards, and procedures. The STRA process is intended to address this and to establish compliance practices that are in line with the Information Management / Information Technology (IM/IT) security governance and policy frameworks. It also includes assessments of legal and regulatory requirements applicable to government.

6.2 Security Control Objectives

There is currently no government standard that articulates the expectations and the level of depth on how security reviews are to be undertaken. In order to address these concerns and promote the use of the STRA Standard the OCIO ISB has initiated the implementation of the information Security Management and Risk Tool (iSMART). iSMART encompasses the requirements for completing a security review including the STRA methodology, process and the assessment tool to be used.

The recommended approach to completing a security review is broad in scope and evaluates the security vulnerabilities affecting confidentiality, integrity, and availability. Once the security review is completed, the STRA reports outline the recommended / appropriate security safeguards, permitting those involved to make knowledge-based decisions about security-related initiatives.

The STRA methodology addresses the following types of controls:

- **Management Controls:** Management of the information technology (IT) security system and the management and acceptance of risk

- **Operational Controls:** Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls

- **Technical Controls:** Hardware and software controls providing automated protection to the system or applications (Technical controls operate within the technical system and applications.)

6.3 Information Characteristics

An ‘information resource’ is the collective term used to describe information and its associated IT facilities, such as a business application system, a computer installation, a network, or a system development activity.

According to the Deloitte report commissioned by the Security Enhancement Project, “52% of ministry programs (out of 118) rely on sensitive information and 24% rely on medium sensitive information. After only 1 day of loss of availability, greater than 30 ministry programs (25%) consider the impact to be related as major or catastrophic”\(^1\).

---

\(^1\) Province of BC: Security Enhancement Project (SEP) – Business Requirements Definition Final Report, April 19, 2005, Deloitte
7 Evaluation criteria

7.1 Enquiry Scope
This STRA standard will be reviewed by the STRA Working Group as referenced in the supplemental document, the Information Security Advisory Committee (ISAC), Ministry Chief Information Officers (MCIOs) and Information Security Branch (ISB) prior to presentation at ASRB. All teams encompass government-wide ministry sector representation.

7.2 Analysis/Acceptance
The material contained in this document was recommended for approval by the ASRB.
Possible impacts of the implementation of this standard are:

- Time, cost and resource increases to system development projects.
- Increased expectation of security training and certification of government and contracted development team members and government information security staff.

7.3 Response
The standard was has been reviewed by the STRA Working Group, Information Security Branch, Ministry Information Security Officers, and Ministry Chief Information Officers and is recommended for approval.

8 Terms and Definitions

Annex J: Terms and Definitions contain the key terms and definitions used in this document.

9 Bibliography

ISB Security Review, (STRA Methodology and Process Supplementary document - Placeholder)
Annex A. Security Threat Risk Assessment Standard

<table>
<thead>
<tr>
<th>IM/IT Architecture &amp; Standards Manual</th>
<th>Effective Date: 2010-MM-DD</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD</td>
<td>Scheduled Review: Annual</td>
</tr>
<tr>
<td>Office of the Chief Information Officer</td>
<td>Last Updated: 2010-MM-DD</td>
</tr>
<tr>
<td>Province of British Columbia</td>
<td>Last Reviewed: 2010-MM-DD</td>
</tr>
<tr>
<td></td>
<td>Type: Process</td>
</tr>
</tbody>
</table>

6.0 Information and Technology Security (CPPM 12.3.6)

6.11 Standard for Information Security Threat and Risk Assessment Methodology, Process and Assessment Tool

Keywords: Risk, Assessment, Risk Assessment, Compliance, Criticality, STRA, iSMART

Description of Standard

This Standard defines the methodology, process and tools for performing a Security Threat and Risk Assessment (STRA). The STRA methodology is aligned with the government’s Enterprise Risk Management (ERM) Model and provides additional specific details on Information Management/Information Technology (IM/IT) security threats and risks.

As per the government information security policy chapter 2.1.3 b, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister. Information Owners have the responsibility and decision making authority for information throughout its life cycle, including:

- Be involved with security reviews and/or audits;
- Define security requirements during the planning stage of any new or significantly changed information system; and
- Ensure information and information systems are protected commensurate with their information classification and value.

Information Owners and Information Custodians must conduct a STRA to ensure that projects involving information system development or acquisition activities are completed in accordance with documented requirements, standards, and procedures. The STRA standard is intended to address these issues and to establish compliance practices that are in line with the IM/IT security governance and policy frameworks. It also includes assessments of legal and regulatory requirements applicable to government.

The Ministry Information Security Officer (MISO) is responsible for assisting business areas in conducting Security Threat and Risk Assessments.

The STRA standard used by government is supported through the Information Security Management and Risk Tool (iSMART). The Fundamental Information Risk Management (FIRM) methodology is used herein for managing information risk through a practical and constructive approach of evaluating risk and driving risk down to acceptable levels. The FIRM methodology
is used in monitoring of the effectiveness of information security management that enables information risk to be managed systematically across the B.C. government.

iSMART allows Ministry Information Security Officers (MISOs) and the Office of the Chief Information Officer (OCIO) to identify information security issues, monitor mitigation activities, ensure compliance to standards and policies and report on the governments information security posture.

iSMART enables information security risks to be identified and measured using the Risk Register referred to as the HARM Table. Referenced in Annex D: HARM Reference Table. The HARM table is used as an objective basis for assessing the worst-case business impact and the level of harm that has been – or could be – caused by a disruption to or loss of the confidentiality, integrity or availability of business information. It can also be used to provide a common basis for evaluating other risks.

iSMART is also used to assist in mitigating and establishing an information security risk monitoring capability in government. The risk tool serves as a repository for STRAs and enables authorized personnel to view individual organization results, ministry results and cross-government results.

The minimum STRA Standard requirement is:

1. **All IM/IT projects must select any one of the Basic of Evaluation (BoE) scorecards listed, and complete the top-level sections (A through I – 61 statements) within the risk tool located in iSMART.** (Each response to a question should be substantiated by adding comments, and attaching or providing a reference to the supporting documentation.)

2. **Any identified issues, risks and recommendations are to be entered into the issues log and action plan and remediation action provided.** (This requirement can be met by attaching or providing a reference to the supporting documentation within the issues log and action plan.)

**iSMART Basis of Evaluation (BoE) Scorecards:**

<table>
<thead>
<tr>
<th>ISO 27001 or</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Risk Assessment (IRA) or</td>
</tr>
<tr>
<td>Standard of Good Practice (SoGP)</td>
</tr>
</tbody>
</table>

*It is highly recommended that further analysis of risk and compliance be undertaken by completing the underlying questions associated with the BoE scorecard chosen.*

An Information Owner or Custodian may choose to complete a more detailed assessment based on the initial risk review and risk tolerance/acceptance of the ministry. When the initial risk assessment reports a high or medium risk to a system, a more detailed review as described in Annex B: STRA Process is required.

For further supplemental information relating to the STRA Standard, refer to:
Where to Apply This Standard

The standard is meant for any ministry, public agency or external service provider that is responsible for managing B.C. Government’s information. For maximum effectiveness, STRAs must be completed on every IM/IT project involving a new application, service, system, and/or environment or whenever a major change is proposed.

This STRA standard is intended to be used government-wide as a guide to understand and generate their project specific STRA’s using the iSMART tool. It is intended primarily for Information Owners and Information Custodians and those individuals who are responsible for measuring and controlling information risk.

Authority and Exemptions

If there are, compelling business reasons why an organization is unable to comply with this standard, the organization’s CIO may authorize a submission for exemption through the OCIO.

Metrics and Enforcement

All required documents in the STRA Process Checklist (Annex H) should be completed, reviewed and signed off.

The intention of the OCIO is to advertise and promote this STRA standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other government agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

When requested, the OCG’s Internal Audit group and the Office of the Auditor General will be provided with high-level or detailed reports. These reports may assist them in determining how Information Security related risks are being addressed within government.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in Annex J: Terms and Definitions.
References

1. Core Policy and Procedures Manual:
   http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm

   12 Information Management and Information Technology Management
   13.4.2 Risk and Controls Review
   15 The Environmental Stewardship and Technical Value department of
       Citizens’ Services is responsible for providing advice and assistance on
       security of physical facilities, design services, and the plant and
       equipment necessary to meet the security needs as identified by
       government policy, security threat and risk assessments, and from other
       approved sources.

2. Information Security Policy:
   http://www.cio.gov.bc.ca/cio/informationsecurity/policy/securityinformationpolicy.page?

   2.1.1 Management direction and support for information security.
   2.1.2 Implementation of information security activities across government.
   2.1.4 Formal management authorization for new information systems.
   2.2.1 Assessment of risks from external party access.
   2.2.2 Granting external parties access to government information and
   information systems.

   5.1 Physical and Environmental Security – Secure Areas
   5.1.1b Government information processing by appropriate entry controls to
       ensure that only authorized personnel are allowed access.
   5.1.2.b Secure areas must be protected by appropriate entry controls to ensure
       that only authorized personnel are allowed access.
   5.1.4.a Physical and Environmental Security, Design and Site Selection.
   5.1.6.b Security controls for co-located information processing facilities and
       loading areas.
   5.2.2.b Equipment must be protected from power supply interruption and other
       disruptions caused by failures supporting utilities maintenance.

   6.1.2 Controlling changes to information systems.
   6.3.2 Acceptance criteria for new or upgraded information systems.
   6.7.1 Media handling.
   6.8.2 Information and software exchange agreements between the Province
       and other organizations must be documented.
   6.9.1 Information in electronic commerce information systems must be
       protected from fraudulent activity, contract dispute, unauthorized
       disclosure and modification.

   7.7 Mobile Computing and Tele-working security controls.
   7.4.5 Access Control – Network access control - Groups of information
       services, users and information systems must be segregated on
       networks.
8.1.1 Security controls identified as part of business requirement for new or modified information systems.

8.3 Information Systems Acquisition, Development and Maintenance – Cryptographic controls.

8.6 Information Systems Acquisition, Development and Maintenance – Vulnerability management. “Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.”

9.1.1 Information Security Incident Management - Reporting information security events and weaknesses.

11.1 Compliance – Compliance with legal requirements, statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained.


4. Security Review Information Security Threat and Risk Assessment Standard (STRA) document (to be linked directly to the Compliance Web Site – currently under construction)

Additional Information

Information security Branch – Compliance Website link
- Security Review - STRA Methodology and Process Supplementary
iSMART Prod Link - https://gww.iscm.cio.gov.bc.ca/
Annex B - STRA Process
Annex C - Fundamental Information Risk Management (FIRM)
Annex D - HARM Reference Table
Annex E - STRA BOE (SCORECARD) TABLE
Annex F - RISK SCORECARD
Annex G - STRA TECHNICAL DIAGRAMS
Annex H - STRA PROCESS CHECKLIST
Annex I - DETERMINATION OF ACCEPTABLE RISK
Annex J - TERMS AND DEFINITIONS

Contact

Karen Bolch, Manager, Compliance
Office of the Chief Information Officer
Information Security Branch
Phone: 250 952-6403
e-mail: Karen.Bolch@gov.bc.ca
Annex B. STRA Process

STRA Process Flow Diagram

Note: Upload results from the blue boxes into iSMART

Legend:
- All
- Applications / Systems
- Financial

Note: SADPS (Secure Application Development Process Standard - DRAFT)
STRA Process

Pre-assessment (Dry Run)

Requirements Phase  (As per Secure Application Development Process Standard (SADPS) (currently in draft) and the System Development Life Cycle (SDLC).)

1) Initial Assessment iSMART BoE Scorecard (Required for all projects)

This is the B.C. Government Information Security Threat and Risk Assessment standard, based on the ISF Fundamental Information Risk Methodology (FIRM). The information security management and risk tool (iSMART) is used to undertake the assessments needed. The MISO and MCIO in each ministry is responsible to ensure that the STRAs are planned and undertaken for each IM/IT project requiring one. The MISO can also oversee the STRA scorecard distribution, facilitating workshops and/or provide training or other assistance in the preparation of an STRA. iSMART will enable a full assessment of an application or service’s level of risk.

All IM/IT projects must select any one of the BoE scorecards listed in Annex E: STRA BoE (Scorecard) Table and complete the top-level sections (A through I) within the risk tool located in iSMART. It is highly recommended that further analysis of risk and compliance be undertaken by completing the underlying questions associated with the BoE scorecard chosen. These specifications should be considered as Minimum requirements.

Part of the review will be done within the risk assessment tool by completing the criticality and initial risk assessment, along with mitigating risks identified in the issues plan and addressed along with the recommendations in the action plan. The reports from the risk assessment can be viewed within the tool or a PDF generated that can be signed off for acceptance by the ministry executive representative or delegate for the project.

To begin the STRA, choose one of the three Basis of Evaluation’s (BoE’s) scorecards with questions reviewed at the top level and as necessary, review questions at a lower more in-depth level. Complete the following within iSMART:

- Risk Scorecard (61 statements)
- Issue Log and Action Plan
- Reports

The 3 standard Basis of Evaluation’s (BoE’s) scorecards used to assess applications, systems and services are:

- BoE U.13 - I-risk (ISO 27001, 2005, 17 FIRM control areas) BCGOV-HTR;
- BoE U.18 - I-risk (Citicus IRA, 2008, 17 FIRM Control Areas) BCGOV HTR;

Refer to Annex E: STRA BoE (Scorecard) Table and Annex F: Risk Scorecard

After completing the initial review, the information owner and MISO should evaluate the risk identified and the value of what is being protected. If the risk is LOW and the value is LOW, an opportunity is provided to consider the STRA adequately covered, or if not, further analysis is required.
It is recommended that further analysis of risk and compliance be undertaken for all applications, systems and services. Further analysis should also be undertaken when any initial risk assessment results in a risk score of medium to high, by completing the underlying control statements / questions within each respective FIRM control category (e.g. Sections D - H of the scorecard). Each control area response should be substantiated by adding comments and / or attaching supporting documentation.

The following next 3 sub-steps are required for all applications, systems and services. They are part of iSMART, however completed outside of the risk tool.

STRAs are generally completed with the input from subject matter experts and the information owner and custodian; this area may require the assistance from technical security architects to complete.

Upload any results obtained from 1a, 1b or 1c into iSMART in the appropriate section (E.g. Section D: Vulnerability - Status of Arrangements)

1a) Technical Settings and Controls Requirements

This technical settings and controls review will include the detailed assessment of the technical controls, technical settings and technical configuration options required for the system or service from a security perspective. Included will be risks identification and risk analysis based on threat modelling with regard to technical settings, and configuration options as required. It will also include the review of network diagrams, conceptual and architecture diagrams, technical documentation, and all other necessary documentation associated with the technical settings and controls to ensure that potential risks are identified.

Refer to the ‘Information Security Assessments’ diagrams in Annex G.

1b) Management and Physical Controls and Operational/Process Requirements

The management and physical controls and operational/process review will include the detailed assessment of the controls pertaining to the information technology (IT) security system and the management and acceptance of risk. As well as the security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls.

1c) System Security Plan Development

The development of the a System Security Plan is to provide an overview of the security requirements of a system, describe the controls in place or planned, the risk assessment associated with the system and the responsibilities of personnel who manage the system. The intent of these procedures is to ensure the integrity, availability, appropriate access, and appropriate use of data and systems within the group. This plan should describe the administrative, operational, and technical security safeguards that must be implemented for systems and services that create, maintain, house, or otherwise use Public, Personal, Sensitive
and Confidential information. The Plan becomes a repository for management, technical and operational documentation related to the security of a system.

**Issues Log**

Once the controls have been identified and evaluated, and the evidence has been gathered, the MISO and information owner will need to determine where gaps exist that need to be addressed. The “Issues” field within Citicus will be used to highlight the control gaps. Items listed in the issues log that will require resources to be actioned upon to reduce risk can be automatically pre-populated into the Action Plan within the risk tool. Any recommendations to be actioned should also be added to the Action Plan. The status of the issues and actions taken should then be maintained in order to determine how they are being remediated, and when risk has been reduced to an acceptable level.

![Figure 4 'Issues' data field within Citicus](image)

**All IM/IT projects next steps:**

- Upon determining the risk level and risk tolerance, complete a mitigation strategy or choose the acceptance of risk identified.
- Triggers for more in depth analysis, (i.e. risk tolerance and/ or whether financial components exist) to be determined by ministry
- For applications or systems with initial risk reported of medium or high continue to the detailed risk assessment and compliance review – Step 2
- Create the Action Plan to mitigate risks in a timely manner. If the risk is accepted and no further assessment is required then proceed to Step 8 STRA results and sign off
Assessment

**Development Phase** (As per Secure Application Development Process Standard (SADPS) *(currently in draft)* and the System Development Life Cycle (SDLC).)

Begin with the review of documents provided by the members of the STRA team. This will include detailed interviews with members of the programs, systems and services team, which helps facilitate the completion of the scorecards (questionnaires) and identification of specific threats inadequately identified in the STRA.

**Financial Risk and Control Requirements**

All projects that are part of a financial system or that will include access to the BC Government financial system (e.g. Corporate Accounting System) must be assessed according to standards established by the Office of the Comptroller General (OCG), refer to Core Policy and Procedure Manual Chapter 13.

If the application/system/component is part of a financial system, the following two additional assessments may need to be performed: Financial Risk and Control Requirements and/or Payment Card Industry (PCI) Assessment. The initial PCI Assessment may be completed in iSMART to establish initial technical controls and requirements. However, reference to the industry specific requirements must be met. These requirements, such as when a third party review by an acquirer must be done, can be found at (www.pcisecuritystandards.org). For additional information on assessments, regarding financial systems contact Internal Audit - OCG.

2) **Detailed Risk Assessment and /or Security Compliance Review**

*(Required for Applications / Systems, Program Areas, Services and Sites)*

Based on the information gathered during the initial assessment of the STRA a more detailed risk assessment should be conducted to identify:

- Issues of non-compliance;
- Initial risk rating scored medium to high;
- While control areas were shown to be in compliance, other potential threats and vulnerabilities were observed during the initial risk assessment.

Risks and security improvements should be summarized by the ministry project team in the “Issues and Action Plan” section of the scorecard within iSMART, and should be classified according to the Information Security Classification Framework.

Using the iSMART (Citicus) HARM Reference Table (Risk Register) automatically calculates the risk, likelihood, probability with the associated cost displayed in a table giving a value from A – E. Use the HARM Reference table to help assess the potential level of harm that may exist (see Annex D HARM Reference Table).
To begin measuring risk one must identify and understand the currently and future risks as well as the classification of the information processed or stored in the system under review. First, classify the information in the system, and then identify the risks and any gaps in controls. Next, assess the likelihood or frequency of a vulnerability being exploited (i.e. threat). Once the harm (vulnerability x cost) and likelihood is known, the risk (i.e. harm x likelihood) can be measured and assigned the appropriate level using the equations below:

\[ \text{Risk Level} = \text{Harm} \times \text{Likelihood/Threat} \]
\[ \text{Harm} = \text{Vulnerability} \times \text{Cost} \]

Included below in Figure 5: Levels of HARM, is a cross reference between the B.C. Government’s newly designed security classification schema and the HARM Reference Table within iSMART (risk tool - Citicus ONE).

Understanding the information security classification and risk to the system under review will assist you in choosing the most appropriate level of HARM. The level chosen from within the HARM Reference Table will automatically populate into the BoE scorecard.

<table>
<thead>
<tr>
<th>Citicus ONE LEVELS of HARM</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Serious Harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very Serious Harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serious Harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor Harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Significant Harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Province of BC Security Classification</th>
<th>High Sensitivity Information</th>
<th>High Sensitivity Information</th>
<th>Medium Sensitivity / Information</th>
<th>Low Sensitivity Information</th>
</tr>
</thead>
</table>

Figure 5 Levels of HARM

Included in the detailed STRA are the review of current technical configuration, controls and settings, management controls and physical controls, and an operational/process review. Identification of additional controls required to mitigate identified risks will be undertaken, along with the identification of the residual risk. The assessment will also identify if modifications to current controls or processes will mitigate risks.

Within the detailed STRA is the information security compliance review, which assesses the information security environment to government information security policy and standards. The compliance questions should also be answered when the initial assessment reveals a level of risk that is unacceptable to the organisation as determined by the information owner.

If the initial STRA reveals a low level of risk, the information owner may choose to accept the residual risk, defer from performing a more in-depth STRA, and continue onto risk mitigation and recommendations – Step 6.

3) Security Documentation and Diagrams (Including Technical Controls)

**Required for Applications / Systems and Sites; upload documents to the risk tool**

Refer to the ‘Information Security Assessments’ diagrams in Annex G.

STRAs are generally completed with the input from subject matter experts and the information owner and custodian; this area may require the assistance from the technical security architects.
to complete. The review must include all necessary diagrams and documentation associated with the technical setting and controls to ensure all potential risks are identified. An STRA requires a review of existing and proposed technical controls and technical settings.

**Special Considerations (For Real assessment in iSMART)**

Triggers for other business requirements may require separate STRAs to be completed (e.g. site review or whether financial components exist) as determined by the ministry.

**Testing Phase** (As per Secure Application Development Process Standard (SADPS) (currently in draft) and the System Development Life Cycle (SDLC).)

Upload or provide a link to any results obtained from 4, and/or 5 into iSMART in the appropriate section (E.g. Section D: Vulnerability - Status of Arrangements)

**4) Vulnerability Scan**

**Required for Applications / Systems; upload results to the iSMART risk tool.**

Vulnerability testing is needed to ensure that all necessary security controls are in place and configured adequately to prevent a security breach. Vulnerability scans should be included on applications, operating systems, routers, firewalls, and/or anywhere information is stored and transmitted; from both inside and outside the SPANBC network. Vulnerability scanning should assess the operating systems, networks, applications and if necessary application code to identify security vulnerabilities. For application assessments, specific application vulnerability scanning should be conducted based on the nature of the application. Consult the Application Security Standard for detailed testing requirements. For all other non-application specific vulnerability scans (e.g. workstation, servers, network devices, voice services, alarm systems, etc.). Analysis of the results from the vulnerability scans are to be completed by the ministry information security professionals.

**5) Security Controls ‘Validation’**

**Required for Applications / Systems and Sites; upload results to the iSMART risk tool.**

Confirmation of security controls is an essential part of the STRA process prior to any application or service being approved for production by Management. Validation and documentation of the process are essential in preparation for an audit. The confirmation or validation process will be based on the controls that were defined as applicable and necessary to manage the security of the application or service. Each control in the evaluation has a prescribed proof statement that would validate that the control exists and is functional. The testing required can be done internally or by an external party (i.e. Auditors, Penetration testing Specialist).

The level of validation required will be based on the system risk, criticality and information classification.
The status of physical security around individual assets and individual sites is assessed in this step.

**Post-assessment**

**Deployment Phase** (As per Secure Application Development Process Standard (SADPS) *(currently in draft)* and the System Development Life Cycle (SDLC).)

6) **Risk Mitigation Recommendations**

**Competed within iSMART; Required for all IM/IT Projects and Applications / Systems, Program Areas / Services and Sites at initial and detailed levels of the security review.**

During this step of the process, controls that manage the identified risks, as appropriate to the government’s operations, are provided. The goal of the recommended controls is to reduce the level of risk to the government information, programs, systems, and services to an acceptable level. The STRA team should consider the following factors when recommending controls and alternative solutions to minimize or eliminate identified risks:

- Sensitivity of the data and the system
- Effectiveness of recommended options
- Legislation and regulations
- Government/Ministry policy
- Operational impact
- Safety and reliability

Upon determining the risk level and tolerance - mitigation, avoidance, transfer or acceptance of risk is to occur. In order to assist the project and information owner in remediating the identified gaps, the “actions” field within Citicus can be leveraged. The actions allow you to prioritize and assign an issue to a responsible person to action, maintain the status of remediation (e.g. in progress, etc…), and if needed can provide details about projected costs and benefits.

**Figure 6: ‘Action Plan’ data fields within Citicus**

The Issues Log and Action Plan are developed when completing the scorecard to address risks in a timely manner. Any risks and security improvements identified should be recorded in the Issues Log within iSMART. Any activities mitigating risk are to be addressed in the Action Plan also located within iSMART. Where there are recommendations, they should also be added to the Action Plan. Triggers for more in depth analysis are also to be determined by ministry.
7) System Security Plan Review

Required for Applications / Systems and Services – completed outside of the risk tool; documents to be uploaded into or a link to the document provided within iSMART upon completion.

The system security plan needs to be reviewed and updated for the application/system with the following:

- STRA findings and recommended changes/remediation
- Privacy Impact Assessments
- Results of certification and accreditation
- Business Continuity and Disaster Recovery Plans and the
- Roles and responsibilities of personnel responsible for managing the information and associated systems.

The plan should also describe the procedures for monitoring, security event reporting and incident response. The plan includes details of legislation and regulations directly related to the system and identify policy and processes, which must be implemented to achieve system certification and accreditation. Refer to the security plan requirements listed in the System Security Plan Policy Summary No.30 and the Core Policy and Procedures manual: http://www.cio.gov.bc.ca/cio/informationsecurity/policy/isp_summaries.page

8) STRA Results

Completion of the STRA is upon acceptance of the recommendations (including residual risk) by the Information Owner, Ministry Information Security Officer, and Ministry Executive. Annex I Determination of Acceptable Risk diagram displays the acceptable levels of risk set for the B.C. Government. The ministry's acceptable risk may be different than what is displayed based on the business requirements and therefore may require more complex mitigation strategies and stronger controls to be in place.

The results of the STRA along with all the relevant documentation will be stored in iSMART (risk tool - Citicus ONE). This will include an action plan containing timelines for mitigations of risks. Any identified corporate risks should be reported within iSMART and indicated in your action plan and the CISO made aware of the issue.

Metrics and Enforcement

All required documents in the STRA Process Checklist (Annex H) should be completed and reviewed. Acceptance of the STRA is to be indicated by sign off by the Deputy Minister or delegated person(s).

In some cases, the OCIO ISB Advisory Services may request to have the remediation action that was implemented reviewed, or may wish to follow up on a particular Target of Evaluation. A re-assessment may be required in this case. In order to preserve the integrity of the initial
STRA, a new instance should be copied from the original within iSMART. The re-assessment can be carried out similarly to an initial assessment.

The STRA process within iSMART is a constructive risk management process (Figure 7: Constructive Risk Management Process) which needs to be kept up to date as long as the information, system, application or service exists.
Annex C. Fundamental Information Risk Management (FIRM)

Fundamental Information Risk Management (FIRM) is a methodology for managing information risk through a practical and constructive approach of evaluating risk and driving risk down to acceptable levels.

The FIRM methodology is used in monitoring of the effectiveness of information security that enables information risk to be managed systematically across the B.C. government. FIRM was developed in conjunction with over 60 ISF Members and an analysis of risk data on 1000 business-critical environments.

Structure of FIRM Approach:

The STRA approach is broad in scope and evaluates security vulnerabilities affecting confidentiality, integrity, and availability. The assessment recommends appropriate security safeguards, permitting management to make knowledge-based decisions about security-related initiatives.

The methodology addresses the following types of controls:

- **Management Controls**: Management of the information technology (IT) security system and the management and acceptance of risk
- **Operational Controls**: Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls.
- **Technical Controls**: Hardware and software controls providing automated protection to the system or applications (Technical controls operate within the technical system and applications.)

The core part of the FIRM methodology consists of 4 components:

1. **Coherent roles and reporting lines**: Examines the organisational structure and roles that are required to support the requirement for monitoring information security across the organisation.
2. **Defined purpose and scope**: Tackles the need to ensure there is a clear definition of the purpose and scope of risk monitoring arrangements that has been agreed with key decision-makers in the organisation.
3. **Sound fact–gathering tools**: Addresses the need for gathering realistic, complete and quantitative information on information security using forms such as the Information Risk Scorecard and Incident pro forma.
4. **Concise reporting and presentation and constructive reporting and presentation**: Deals with the structure and content of reports that are required to capture the attention of key decision makers in the organization.
Constructive Risk Management Process

The FIRM methodology and iSMART tool follow the ‘constructive risk management process,’ which is incorporated into the STRA process.

This constructive risk management process has been specifically designed to:

“Help People Succeed and not to find fault or attribute to blame...

Figure 7: Constructive Risk Management Process

...help and resources can be targeted where it is most needed.”

iSMART enables you to decide what to evaluate, with minimal effort. The preliminary screening process entails asking ‘owners’ of information resources to fill in the Criticality and Risk assessments providing a high level overview. This scorecard is best completed in a facilitated risk workshop. Completion of a scorecard yields an succinct Risk status and Criticality status reports - written in plain language - which assists the ‘owner’ in determining if a more detailed evaluation is needed or not.
Annex D. Harm Reference Table

This HARM reference table provides an objective basis for evaluating the business impact aspect of risk. It enables evaluators to gauge the nature and level of harm that could be caused by a possible incident - or that has been caused by an actual incident or series of incidents. For the purposes of evaluating risk, it is essential that the business impact of a worst-case possible incident is assessed.

<table>
<thead>
<tr>
<th>NATURE OF HARM</th>
<th>Level of Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Financial loss (loss of revenue, unforeseen costs, legal liabilities, fraud)</td>
<td>Extremely serious harm</td>
</tr>
<tr>
<td></td>
<td>$10 + million</td>
</tr>
<tr>
<td>Degraded performance (failure to achieve targets, loss of productivity)</td>
<td>10%+</td>
</tr>
<tr>
<td></td>
<td>Number of staff-hours wasted</td>
</tr>
<tr>
<td>Loss of management control (impaired oversight of government operations)</td>
<td>Key metrics not up-to-date or accurate</td>
</tr>
<tr>
<td>Damaged reputation (negative publicity, regulatory disapproval, litigation)</td>
<td>Drop in approval rating</td>
</tr>
<tr>
<td></td>
<td>Extent of negative publicity</td>
</tr>
<tr>
<td></td>
<td>Political action taken</td>
</tr>
<tr>
<td></td>
<td>Extent of litigation</td>
</tr>
<tr>
<td>Impaired growth (delayed new government initiatives)</td>
<td>Aborted initiatives or deadlines missed</td>
</tr>
<tr>
<td>Any other (ways not mentioned above)</td>
<td>Impact on health and safety</td>
</tr>
<tr>
<td></td>
<td>Impact on environment (Greenhouse gases - GHG)</td>
</tr>
<tr>
<td></td>
<td>Refer to your local co-ordinator</td>
</tr>
</tbody>
</table>

-Figure 8: BC Provincial Government customised HARM Reference Table v4
Annex E. STRA BoE (Scorecard) Table

The minimum requirement for all IM/IT projects is to complete an initial security review using one of the “Basis of Evaluation’s (BOE’s) “scorecards” listed below. (All estimates for resourcing are dependent on scenario or complexity of project).

<table>
<thead>
<tr>
<th>Target Type</th>
<th>BoE Name</th>
<th>ID &amp; Example</th>
<th>Purpose</th>
<th>Description</th>
<th>Suitable for Evaluation of</th>
<th>Project Size &amp; Complexity</th>
<th>Level of Review</th>
<th>Depth &amp; Detail Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Resource</td>
<td>BoE U 13</td>
<td>Security Review (Confidentiality, Integrity and Availability)</td>
<td>Based on ISO 27001 – 27002 Standards. Provides self-validation tests, static checklist containing up to 133 control review questions.</td>
<td>Applications • Program areas • Systems and Services • Sites</td>
<td>Small Size Project • Less than one application and / or system • No significant interfaces to other applications or systems • 3 - 6 hours of effort</td>
<td>High Level Review</td>
<td>Less Detailed</td>
<td></td>
</tr>
<tr>
<td>Information Resource</td>
<td>BoE U 23</td>
<td>Security Review (Confidentiality, Integrity and Availability)</td>
<td>The selection of questions are based on Citius Ltd. research and analysis of the effectiveness of industry best practice security controls. Provides self-validation tests. Static checklist containing up to 381 control review questions.</td>
<td>Applications • Program areas • Systems and Services</td>
<td>Medium Size Project • More than one application and / or system • Significant interfaces to other applications or systems • 6 - 12 hours of effort</td>
<td>Medium Level Review</td>
<td>Moderately Detailed</td>
<td></td>
</tr>
<tr>
<td>BCGOV: FIRM 17; SoGP 36 Attributes</td>
<td>BoE U 35</td>
<td>Security Review (Confidentiality, Integrity and Availability)</td>
<td>Based on the Information Security Forum (ISF) Standard of Good Practice (SoGP 2007). Checklist can be customized with specific questions relevant to the information being evaluated. Checklist can use up to 36 different Attributes” containing up to 2576 control review questions.</td>
<td>Applications • Systems and Services (E.g. Wireless service) • Alternative Service Delivery (ASDs)</td>
<td>Large Size Project • More than one application and / or system • Significant interfaces to other applications or systems • 12 - 25 hours of effort</td>
<td>Low Level Review</td>
<td>Very Detailed</td>
<td></td>
</tr>
</tbody>
</table>

Figure 9: STRA BoE (Scorecard) Table
Annex F.  High Level Risk Scorecard – iSMART

<table>
<thead>
<tr>
<th>BC Government Risk Scorecard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Information Resource</strong></td>
</tr>
<tr>
<td>A1. Please identify the information resource covered by this scorecard:</td>
</tr>
<tr>
<td>Resource title:</td>
</tr>
<tr>
<td>Brief description:</td>
</tr>
<tr>
<td>A2. Which of the following best describes the information resource?</td>
</tr>
<tr>
<td>Business application</td>
</tr>
<tr>
<td>A3. What is the approximate number of users?</td>
</tr>
<tr>
<td>Less than 1%</td>
</tr>
<tr>
<td>A4. Roughly what proportion of the organization's sales is supported by the information resource (if sales are not relevant, answer for an alternative activity eg purchasing, cash management, staff plant utilisation)?</td>
</tr>
<tr>
<td>Less than 1%</td>
</tr>
<tr>
<td>A5. When was the information resource last subject to a rigorous, independent review (eg using comprehensive checklists to evaluate the status of your arrangements)?</td>
</tr>
<tr>
<td>Day:</td>
</tr>
<tr>
<td>Month:</td>
</tr>
<tr>
<td>Year:</td>
</tr>
<tr>
<td>No such review conducted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1. Please identify who is the ‘owner’ of the information resource covered by this scorecard:</td>
</tr>
<tr>
<td>Owner’s name:</td>
</tr>
<tr>
<td>Job title:</td>
</tr>
<tr>
<td>Location:</td>
</tr>
<tr>
<td>Telephone number:</td>
</tr>
<tr>
<td>E-mail address:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1. What is the maximum level of harm that the business could suffer if key information held in, processed or transmitted by the information resource were to be accidentally or deliberately:</td>
</tr>
<tr>
<td>Disclosed to the wrong people?</td>
</tr>
<tr>
<td>Lost or otherwise corrupted?</td>
</tr>
<tr>
<td>Rendered unavailable for:</td>
</tr>
<tr>
<td>Less than an hour?</td>
</tr>
<tr>
<td>Half a day?</td>
</tr>
<tr>
<td>A day?</td>
</tr>
<tr>
<td>2-3 days?</td>
</tr>
<tr>
<td>A week?</td>
</tr>
<tr>
<td>A month?</td>
</tr>
<tr>
<td>Loss of confidence</td>
</tr>
<tr>
<td>Loss of availability for defined periods of time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability: Status of Arrangements</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1. What is the status of your arrangements in the following control areas:</td>
</tr>
<tr>
<td>Policies and standards (compliance with corporate requirements)?</td>
</tr>
<tr>
<td>Ownership (owner has appropriate skills and seniority)?</td>
</tr>
<tr>
<td>Organization (clear roles, responsibilities, reporting lines; sufficient staff)?</td>
</tr>
<tr>
<td>Risk identification (key risks identified and addressed)?</td>
</tr>
<tr>
<td>Awareness (people know they need to protect information)?</td>
</tr>
<tr>
<td>Service agreements (service requirements agreed in writing)?</td>
</tr>
<tr>
<td>User capabilities (sound user skills, procedures and disciplines)?</td>
</tr>
<tr>
<td>IT capabilities (sound IT skills, procedures and disciplines)?</td>
</tr>
<tr>
<td>System configuration (adequate capacity, resilience and documentation)?</td>
</tr>
<tr>
<td>Data back-up (regular cycle, secure storage)?</td>
</tr>
<tr>
<td>Contingency arrangements (plans exist and are proven to work)?</td>
</tr>
<tr>
<td>Physical security (safe site, restricted to authorised individuals)?</td>
</tr>
<tr>
<td>Access to information (access restricted to authorised individuals)?</td>
</tr>
<tr>
<td>Change management (rigorous disciplines consistently applied)?</td>
</tr>
<tr>
<td>Problem management (focal point to whom problems can be reported)?</td>
</tr>
<tr>
<td>Special controls (additional protection, eg use of cryptography)?</td>
</tr>
<tr>
<td>Audit review (independent reviews conducted periodically)?</td>
</tr>
</tbody>
</table>
| Please select one of the following in each box to indicate the maximum possible level of harm:
| A: Extremely serious harm |
| B: Very serious harm |
| C: Serious harm |
| D: Minor harm |
| E: No significant harm |
| X: Don’t know |
### BC Government Risk Scorecard

#### Vulnerability: Special circumstances
- E1. Is the information resource:
  - Subject to a high degree of change?
  - Widely extended geographically?
  - Large in scale?
  - Complex?
  - Immature?
  - Accessible by external parties?
  - Used to support call centres?

#### Level of threat
- F1. How many incidents of the following types have been experienced over the last twelve months that compromised the confidentiality, integrity or availability of key information:
  - Malfunctions of software or hardware?
  - Loss of services, equipment or facilities?
  - Overloads?
  - Human error?
  - Unforeseen effects of change?
  - Other undesirable acts?

#### Business impact
- G1. What impact, if any, did the incidents experienced over the last twelve months have on the BC Provincial Government in terms of:
  - Financial loss (loss of revenue, unforeseen costs, legal liabilities, fraud)?
  - Degraded performance (failure to achieve targets, loss of productivity)?
  - Loss of management control (impaired oversight of government operations)?
  - Damaged reputation (negative publicity, regulatory disapproval, litigation)?
  - Impaired growth (delayed new government initiatives)?
  - Any other (ways not mentioned above)?

#### Strengthening controls
- H1. During this evaluation period, what action, if any, has been completed, initiated or planned to strengthen controls in the following areas:
  - Policies and standards (compliance with corporate requirements)?
  - Ownership (‘owner’ has appropriate skills and seniority)?
  - Organization (clear roles, responsibilities, reporting lines; sufficient staff)?
  - Risk identification (key risks identified and addressed)?
  - Awareness (people know they need to protect information)?
  - Service agreements (service requirements agreed in writing)?
  - User capabilities (sound user skills, procedures and disciplines)?
  - IT capabilities (sound IT skills, procedures and disciplines)?
  - System configuration (adequate capacity, resilience and documentation)?
  - Data back-up (regular cycle, secure storage)?
  - Contingency arrangements (plans exist and are proven to work)?
  - Physical security (safe site, restricted to authorised individuals)?
  - Access to information (access restricted to authorised individuals)?
  - Change management (rigorous disciplines consistently applied)?
  - Problem management (local point to whom problems can be reported)?
  - Special controls (additional protection, eg use of cryptography)?

#### Completion details
- I1. Please identify yourself and how you may be contacted:
  - Your name:
  - Your job title:
  - Your location:
  - Your telephone number:
  - Your e-mail address:
Annex G. STRA Technical Diagrams

An STRA requires a review of existing and proposed technical controls and technical settings. The review must include all necessary documentation associated with the technical setting and controls to ensure all potential risks are identified. The STRA analyst need not prepare documentation and diagrams on the process flows and information flows, rather, he should determine if they exist, review them, identify/confirm any potential risks or threats that may show up in the diagrams, documentation, or configuration, and ensure these have been (or will be) properly included and dealt with by the project team. With new systems or major changes to existing systems, it is often difficult to determine where threats and risks could occur; diagrams often help.

In this section, example diagrams and document are described. These descriptions represent the suggested contents for the diagrams and documents. Throughout the example, we will use the example of a “service to grant access”.

This diagram below is intended to provide guidance regarding the type of information required in order to facilitate the completion of a security threat and risk assessment.
### Information Security Assessments

<table>
<thead>
<tr>
<th>Client Document Review</th>
<th>Architecture documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Architecture</td>
</tr>
<tr>
<td></td>
<td>Application Architecture</td>
</tr>
<tr>
<td></td>
<td>Technical Architecture</td>
</tr>
<tr>
<td></td>
<td>Data model</td>
</tr>
<tr>
<td></td>
<td>Business logic</td>
</tr>
<tr>
<td></td>
<td>User interface</td>
</tr>
<tr>
<td></td>
<td>Data Flow</td>
</tr>
<tr>
<td></td>
<td>Information flow</td>
</tr>
<tr>
<td></td>
<td>Process Flow</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implementation Documents</th>
<th>Network Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Technical architecture (Servers / service providers)</td>
</tr>
<tr>
<td></td>
<td>Data Flow</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardening of Infrastructure</th>
<th>Network Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACLs, Firewall rule sets, IDS/IPS, Other active network components</td>
</tr>
<tr>
<td></td>
<td>Host based firewall / filter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Servers</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OS</td>
<td>OS</td>
</tr>
<tr>
<td></td>
<td>Services</td>
<td>Presentation</td>
</tr>
<tr>
<td></td>
<td>Provisioner</td>
<td>Thin/Fat client</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Authentication and Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Physical Security (Facilities Management)</td>
</tr>
<tr>
<td></td>
<td>BCP/DRP, Policy, Change management, SLAs with service providers, Contracts with service consumers</td>
</tr>
</tbody>
</table>

**Figure 10: Information Security Assessment Architecture Documentation**

**Infrastructure Review**

An “Infrastructure Review” consists of a number of components. Any security exposures identified during the review will be documented and mitigating strategies will be provided. A follow-up audit will occur at some to be mutually agreed upon point in the future to verify that mitigating action was taken to remediate the exposure.

**Figure 11: Infrastructure Review**
Compliance Assessment
This review is to determine if what was designed is what is implemented. Further to determine if that which was implemented complies with legislation, regulation, policy, standards and procedures. Often a diagram can help to sort out where compliance may be compromised and identify in general terms, where existing and new threats, risks and vulnerabilities may occur.

Vulnerability Assessment
This is a review for potential susceptibilities to unintentional and intentional operational breakdowns, which could lead to inadequate or inappropriate program outcomes. The vulnerability assessment can be conducted at the:
- Application layer; and / or
- Platform layer; and / or
- Network layer.

Threat Risk Assessment
This is a review to determine its susceptibility to a specific attack and the opportunities for threat agents to mount that attack. Through this process, it also identifies “most likely” system and location-specific threats.

Process Flow
Is a step-by-step description of “how you do it”. Having a diagram can often make the flow clearer and can make the identification of potential risk areas easier.

Definition Process Flow
A process flow is the depiction of the authorized paths along which communication is passed from one process step to the next. The paths indicate the order of the steps, which make up the process.

Sample Graphical View

Sample Process: Service for granting access
Information Flow
The information flow provides details of the type of communication entering and leaving a process step. The communications path is elaborated upon to providing details of the information moving along the path and what information each step takes in and produces.

Definition Information Flow:
An information flow is the depiction of the authorized paths along which information can be transferred from one step to another within process. The information flowing along a path defines the interface between processes.

Sample Graphical View

Sample Process: Service for granting access
### Sample Tabular View

Information flow could also be represented as a table

<table>
<thead>
<tr>
<th>Process #</th>
<th>Process name</th>
<th>Input</th>
<th>Output</th>
<th>Depends on</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Registration Process</td>
<td>Application Form</td>
<td>Registration</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Registration Process</td>
<td>Application Form</td>
<td>Acknowledgement</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Request Validation</td>
<td>Application Form</td>
<td>Authorization</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Authorization of request</td>
<td>Registration</td>
<td>Access Notification</td>
<td>1,2</td>
</tr>
<tr>
<td>3.1</td>
<td>Authorization of request</td>
<td>Authorization</td>
<td>Access Notification</td>
<td>1,2</td>
</tr>
</tbody>
</table>

Figure 14: Information Flow presented in Tabular Form

**Explanation of the columns:**
- **Process #:** Similar to the “step#” in process flow, this number is used to identify the process.
- **Process Name:** Name of the process.
- **Input:** Description of the interface which provides input to the process.
- **Output:** Description of the interface to which this process sends data.
- **Depends on:** Enter the process # of the predecessor processes. The processes which must be completed before this process can start.

**Data Flow**

This is a way of identifying, modeling, and documenting how data moves through a process.
Definition of Data flow

A data flow is the depiction of the authorized paths along which data can move from one step to another within a process. The data flowing along a path defines the technical interface between processes.

Sample Graphic View

Sample Process: Expansion of the registration process from information flow

Figure 15: Sample Process - Expansion of the registration process from information flow
### Sample Tabular View - Data flow could also be represented as a table

<table>
<thead>
<tr>
<th>Process</th>
<th>Process name</th>
<th>Source Step</th>
<th>Destination Step</th>
<th>Inbound Traffic</th>
<th>Outbound Traffic</th>
<th>Authentication</th>
<th>Authorization</th>
<th>Data class</th>
<th>Data source</th>
<th>Data Sink</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Registration process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Web FE</td>
<td>*</td>
<td>*</td>
<td>HTTPS 443</td>
<td>HTTPS Estab None None PI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1</td>
<td>Web FE</td>
<td>*</td>
<td>1.2</td>
<td>Estab SQL/NET 1521 TNS Update on application table PI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.2</td>
<td>Web FE</td>
<td>*</td>
<td>1.2</td>
<td>Estab Telnet 23 Known host Send mail PI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Oracle Backend</td>
<td>1.1</td>
<td>1.1</td>
<td>SQL/NET 1521</td>
<td>SQL/NET Estab TNS Update on application table PI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Mail Server</td>
<td>1.1</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.1</td>
<td>Mail Server</td>
<td>1.1.1</td>
<td>TELNET 23</td>
<td>Estab Known host Send mail PI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.2</td>
<td>Mail Server</td>
<td>*</td>
<td>Estab SMTP 25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 16: Sample Tabular View - Data flow could also be presented as a Table
### Explanation of columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process #</td>
<td>Similar to the “process #” in information flow, this number is used to identify the process.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Name of the process.</td>
</tr>
<tr>
<td>Source Step</td>
<td>The step where information for this component comes from.</td>
</tr>
<tr>
<td>Destination Step</td>
<td>The step where this component send information</td>
</tr>
<tr>
<td>Inbound Traffic Protocol</td>
<td>The type of protocol used for transmitting the information to this component. If network based transfer indicate the protocol i.e. HTTP/S for HTML web, FTP for file transfer, etc. If not network based transfer indicates transfer mechanism (courier, phone, face-to-face, etc.)</td>
</tr>
<tr>
<td>Port</td>
<td>Only valid for network based transfer this is the TCP/IP port number e.g. HTTP == 80 HTTPS == 443</td>
</tr>
<tr>
<td>Outbound Traffic</td>
<td>As for inbound Traffic. Except this represents the protocol used to send the output from this component to the next component.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Type of authentication required. If no authentication required enter NONE in this column. Otherwise indicate the type of technology used for authentication. E.g. NTLM, Kerberos, Oracle TNS, sever side cert etc.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Type of authorization the component requires to perform the task. E.g. Read, write, update on/in “object”. Where object is the database, application, etc being accessed by the component</td>
</tr>
<tr>
<td>Data Class</td>
<td>This is the classification assigned to the information by records management / privacy branch.</td>
</tr>
<tr>
<td></td>
<td>- PI personal information as defined by FOIPPA</td>
</tr>
<tr>
<td></td>
<td>- Low non-personal information low sensitivity</td>
</tr>
<tr>
<td></td>
<td>- Medium non-personal information medium sensitivity</td>
</tr>
<tr>
<td></td>
<td>- High non-personal information High sensitivity</td>
</tr>
<tr>
<td>Data Source</td>
<td>Where the data is coming from, the interface used to supply information to this component</td>
</tr>
<tr>
<td>Data Sink</td>
<td>Where data is going to, the interface to which this component is sending information</td>
</tr>
</tbody>
</table>
Annex H. STRA Process Checklist

<table>
<thead>
<tr>
<th>Required Documents</th>
<th>Completed</th>
<th>Reviewed</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. STRA Documents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Criticality Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>High level - Risk Scorecard(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1a. Technical Settings and Controls Review (System/Services requirement)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1b. Management, Physical Controls, Operational/Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1c. System Security Plan Development</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Review</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PCI Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Assessment (Audit R&amp;C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Detailed Risk Assessments and/or Compliance Review</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Vulnerability Scans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Security Controls Validation (System / Services requirement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Risk Mitigation and Recommendations (Issues/Action Plans Completed)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Security Plan (System/Services requirement)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annex I. Determination of Acceptable Risk

**Determination of Acceptable Risk – BC Government Basis of Evaluation (BoE’s)**

Acceptable risk: The level of risk that is acceptable to the top management of each ministry representing the BC government, expressed in the form of a determination of acceptable risk.

In 2008, the STRA (Citicus ONE) working team was involved in reviewing and agreeing to what should be set for the BC government acceptable risk as it pertains to the following 5 determination areas as illustrated on the risk radar chart below.

![Risk Radar Chart](image)

**Figure 17 Acceptable Risk for the BC Government**

The STRA working team reviewed the default settings set within iSMART (risk tool - Citicus ONE application); obtained and reviewed the acceptable risk tolerance used by the Manitoba government, as well as discussed what was known of the current (ministry) government risk tolerance. The working team determined the acceptable risk tolerance that would be set and applied to targets of evaluation of the type covered by the basis of evaluation (BoE’s) scorecards used across government. The acceptable risk tolerance will be reviewed again as we get a better understanding of government’s maturity and level of risk tolerance.

Each determination defines the green area of a risk chart that appears on an Individual risk status report, Dependency risk map, Risk dashboard or other result produced by the system.
The green area on the risk radar chart depicts the level of risk acceptable to your organization, i.e. it shows your ministry’s (BC Government’s) ‘risk appetite’ and enables decision-makers to see how measured risks compare against that. The green area you see in the radar chart is comprised of the values set below.

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Acceptable Value</th>
<th>Equivalent Value For Risk Chart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criticality</td>
<td>Highly Critical</td>
<td>50%</td>
</tr>
<tr>
<td>Control Weaknesses</td>
<td>4 Weak Control Areas</td>
<td>23%</td>
</tr>
<tr>
<td>Special Circumstances</td>
<td>1 Special Circumstances Applies</td>
<td>14%</td>
</tr>
<tr>
<td>Level of Threat</td>
<td>1-10 Incidents Per Year</td>
<td>25%</td>
</tr>
<tr>
<td>Business Impact</td>
<td>Minor Harm</td>
<td>25%</td>
</tr>
</tbody>
</table>

Figure 18 Acceptable Risk BC Government Basis of Evaluations (BoE’s)
Annex J.  Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

**Accreditation** – the final approval to authorize operation of an information system and to explicitly accept the risk to Ministry operations (including mission, functions, image, or reputation), assets, or individuals, based on the implementation of an agreed upon set of security controls.

**Application** (business application) – a collection of computer hardware, computer programs, databases, procedures and knowledge workers that work together to perform a related group of services or business processes.

**Audit** - is an examination of the facts to render an opinion and would include testing evidence to support the opinion.

**Business Owner/Information Owner** - the business unit person responsible for a specific ministry programme. In cross-government situations, it is the individual with responsibility for implementing a programme or an application that supports it. The responsibility is delegated to the Minister and then to the Deputy Minister which is then further delegated to different business areas of a ministry.

**Certification** - a comprehensive assessment of the management, operational and technical security controls in an information system, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

**CIA** - An acronym that stands for confidentiality, integrity and availability.

- **Confidentiality** - Information is not made available or disclosed to unauthorized individuals, entities or processes.

- **Integrity** - The characteristic of information being accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification.

- **Availability** - Information or information systems being accessible and usable on demand to support business functions.

**Core Policy and Procedures Manual (CPPM)** - contains Treasury Board financial and general management policy and the Comptroller General's directives, combining management and financial policy with financial administration procedures. Chapter 12 outlines Information Management and Information Technology Management.

**FIRM** - Fundamental Information Risk Management is a methodology for managing information risk through a practical approach of evaluating risk and driving risk down to acceptable levels. The FIRM methodology is used in monitoring of the effectiveness of information security that enables information risk to be managed systematically across the B.C. government.

**Government Chief Information Officer (GCIO)** - senior executive who creates policies and strategies for government's information management and technology and provides the leadership to Ministry Chief Information Officers (MCIO).

**Information Custodians** - maintain or administer information assets on behalf of the Information Owners by:

- Providing and managing security for the information asset throughout its lifecycle;
- Maintaining and operating the technical infrastructure that information and information systems reside on;
• Maintaining and operating the security infrastructure protecting information and information systems.

**Information Owners** - have the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure. Within the Government of British Columbia, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

**Information Resource Management Plans (IRMP)** – Ministry plans for projects that are greater than $100,000 that need to be approved by the GCIO.

**Information Security Classification** – a system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability. (Also classification, information classification, security classification)

**Information Security Forum (ISF)** – an independent non-profit organization; a forum for the development of information security standards and best practices; an authority in information risk management.

**Information Security Policy (ISP)** - is based on the ISO 17799:2005 standard for information security management. The ISP provides the framework for government organizations to establish local policies and procedures necessary for the protection of government information resources and technology assets.

**International Organization for Standardization** - widely known as ISO, is an international standard setting body composed of representatives from various national standards organizations.

**Ministry Chief Information Officer (MCIO)** – reports to the ministry’s assistant deputy minister and is accountable for all ministry business and operational IM/IT initiatives (i.e. those which do not have cross-government implications).

**Ministry Information Security Officer (MISO)** - responsible for co-ordinating the ministry security program for protecting the confidentiality, integrity and availability of government information.

**Penetration Test** – testing to determine the possibility of exploiting vulnerabilities to gain unauthorized access and/or to perpetrate malicious activity via vulnerabilities such as system mis-configuration, hardware/software flaws, weaknesses in the perimeter defences protecting the application.

**Privacy Impact Assessment (PIA)** - is a review of information collected, used or shared by government. It is intended to identify personal information and how it is proposed to be collected, used or shared. All such activity must be in compliance with the FOIPP Act and associated policies and practices.

**Residual Risks** - Are those risks that still remain, even after relevant safeguards and/or controls have been implemented. With residual risk, management needs to implement a security strategy and security plan that documents whether they will accept, avoid/transfer, or mitigate each of the residual risks.

**Risk** – Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.

**Security Compliance Assessment** – assessment of security posture at the overall organizational level in regards to established government standards.

**Security review** – an independent review with the scope focused on the security framework over the business processes, application and operating environment. Reviews are distinguishable from audits in that the scope of a review is less than that of an audit and therefore the level of assurance provided is lower.
Security Threat and Risk Assessment (STRA) - a component of a risk analysis specifically aimed at identifying security exposures.

Source Code Review – can be performed based on results from a static analysis tool or by manually reviewing code by someone other than the person that coded e.g. the module.

System Security Plan – repository to document security information and controls (management, operational and technical) regarding an application system.

Threat – in the security context, any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin.

Threat and Vulnerability Assessment - the process that is followed once assets have been identified that require protection to determine what the threats are to those assets and what weaknesses that may be exploitable.

Vulnerability – in the security context, a weakness in security procedures, processes, or controls that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerability Scan – a tool that assesses vulnerabilities in an application and its infrastructure based on known exploitable weaknesses.