Critical Systems Guidelines

Architecture, Standards and Planning Branch

Office of the CIO Province of BC

Document Version 1.5

Feb 14, 2017

Table of Contents

1.0 Document Control

Date	Author	Version	Change Reference
April 27, 2015	Tim Gagne	1.0	Published
December 14, 2015	Tim Gagne	1.1	Number of grammar and formatting changes. Material changes to Section 7 Compliance Attestation and Roadmap.
January 6, 2016	Diana Rai	1.2	Added direction in Section 7.2 to link Ministry Staff to their Ministry Coordinators. Published
March 10, 2016	Scott Johnson	1.3	Modified 7.0 activity table, updated requirements in 7.1 and added 7.2 to separate attestation and technology road map requirements.
March 23, 2016	Scott Johnson	1.4	Modified 7.2 to correct error, complete grammatical fixes and updated Table of Contents.
Feb 14, 2017	Tim Gagne	1.5	Section 3: Added role descriptions for Business Owner and MISO. Section 4: Updated registration topic to include using c55. Section 6.3.1 Added Engaging TS service providers. Section 7: Removed links to sample compliance attestation process workflow diagram and play script documents, and included as Appendix A and B.

2.0 Introduction

These guidelines are part of the developing Critical Systems Framework and to be read in conjunction with the Critical Systems Standard (the Standard).

The following sections describe proposed approaches, actions, and documentation that could meet the minimum requirements of how to meet the obligations under the Standard by:

- Aiding in the interpretation of the Standard, and,
- Outlining the minimum expectation of the specific requirements defined in the Standard.

However, the Standard can exceed these requirements and takes precedence over this guidance document.

3.0 Roles and Responsibilities

This section details the responsibilities for the roles identified in the Standard. The responsibilities described in the Standard were purposely light weight because they are somewhat generic and organic. Residing here in the guidelines permits further evolution. If there is nothing more to add to what has been expressed in the Standard for any given role, it will be noted.

Current roles identified for the purpose of the Standard include:

1. System Owner
2. Response and Recovery Director
3. Ministry Coordinator, Critical Systems Standard
4. OCIO Coordinator, Critical Systems Standard
5. Business Owner
6. Ministry Information Security Officer (MISO)

3.1 System Owner

The person who is responsible for the overall critical system's service integrity and the authority to get things done with respect to having the right people assigned when appropriate. Additionally:

- Provides Response and Recovery Director 'authority' required to be successful
- Gets the assessment and STRA done
- Raises concerns with interpretation, implementation and compliance to the Standard to the ministry coordinator.

3.2 Response and Recovery Director

The occupant of the Response and Recovery Director role is responsible for preparing the business process used to recover from a major incident and for executing it during the incident. Primary responsibilities amongst others include:

- Defining the process which will oversee the management of a major incident
- Obtaining authority to convene the team members in response to a major incident
- Lead the response and recovery effort.

3.2.1 Defining the Major Incident Management Process

The Response and Recovery Director defines and maintains a separate process (above and beyond that used for a non-critical system) to respond to a major incident that is impacting business service performance or availability.

This process should at minimum:

- Define the Response and Recovery Team roles and responsibilities matrix

- Assign primary and alternate names to the roles
- Define the procedure to escalate a major incident, through the help or service desk, to the Recovery and Response Director
- Establish authority to convene immediately the appropriate Response and Recovery Team members
- Include a communications plan (channels, medium, timing, etc.) for all stakeholders who need to know the status of the response or recovery
- Document procedures for handling vital documents generated during the response and recovery effort
- Document procedures to ensure the names in the Response and Recovery Team file are up to date.

3.2.2 Convening the Team

To establish the authority to convene the Response and Recovery Team, the Response and Recovery Director is responsible for ensuring a 'Terms of Reference' is drafted and signed by the System Owner, that at minimum:

- Names the Response and Recovery Director for said critical system
- Authorizes the named Response and Recovery Director to convene with appropriate priority, any or all of the response and recovery team members.
- Names the team members (and alternates) of the response and recovery team.

Team members named in the Terms of Reference that form the response and recovery team must be capable of meeting the responsibilities defined in the roles and responsibilities matrix. Training and succession plans should be identified by the Response and Recovery Director and committed to by the System Owner. Where internal capabilities do not exist, the Response and Recovery Director should ensure that an appropriate level of support agreements and funding are in place with service support partners.

3.2.3 Leading the Response and Recovery

Upon receiving an escalation of an incident to a major incident (as defined above in 3.2.1), the Response and Recovery Director leads the actions of the team and is the primary liaison with executives:

- Convene appropriate team members and communicate to their supervisors
- Validate the impact is real
- Execute the communications plan
- Direct the actions from problem analysis to resolution
- Lead recovery if required as documented in the Disaster Recovery Plan
- Lead review of any process issues and identify lessons learned
- Continuously improve process.

3.3 OCIO Coordinator

Upon approval of the Standard by the GCIO, the single point of contact for OCIO will be named and communication channels will be described to the Ministry Coordinators.

The OCIO Coordinator will be responsible for responding to Ministry concerns with required clarifications and ensuring the completeness and accessibility of the critical systems register.

3.4 Business Owner

The person, who is responsible for delivery of the program that depends on the system, and:

- Signs off the independent review along with System Owner and reviewer.

3.5 MISO

The person who is responsible to manage **security** programs in their **ministry**, and for the critical system standard:

- Guides the completion of the STRA .

3.6 Ministry Coordinator, Critical Systems Standard

Presently, the Ministry Coordinator role has three primary responsibilities:

1. Acting as the single point of contact for their Ministry and the OCIO for matters surrounding the Standard,
2. Providing details for their Ministry's identified critical systems as described in Section 4.0 below, and,
3. Maintaining the Ministry's critical systems register.

The Ministry Coordinator is to identify themselves by emailing the OCIO Critical Systems Coordinator (CSS.OCIO.Coordinator@gov.bc.ca)

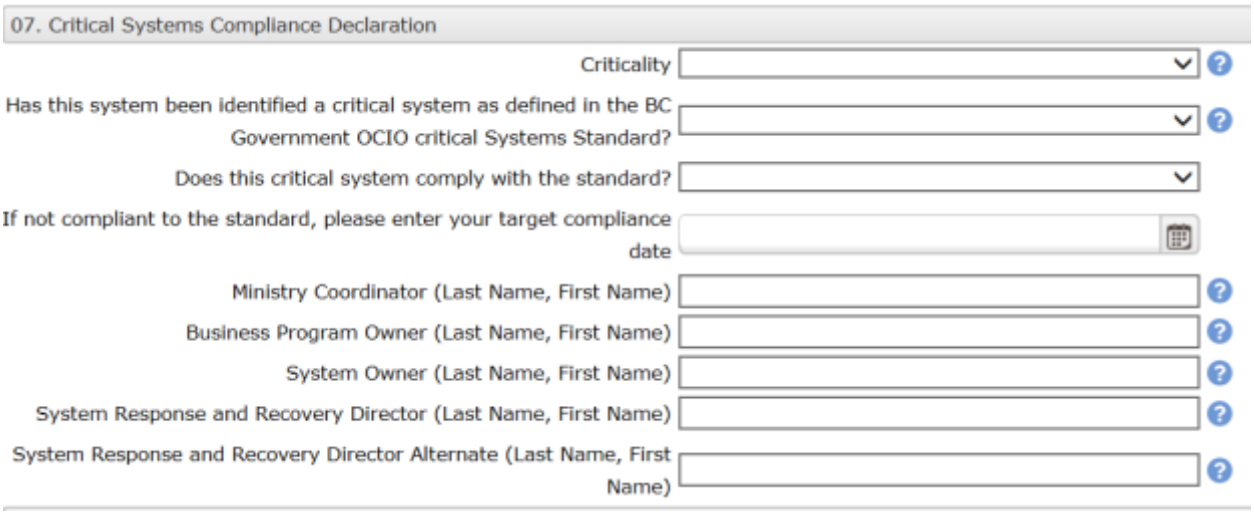
4.0 Critical System Registration

OCIO will maintain the single source of truth identifying all of the registered critical systems.

- In late 2016 OCIO implemented Copperleaf's asset management system C55 to maintain BC Government's Application Health-Check (AppHC) details.
- The Critical Systems registry data items were added as attributes of an AppHC record and thus AppHC became the repository of the Critical Systems Registry.

The Ministry Coordinator is required to maintain a registry of their Ministry's critical systems using C55.

For each system deemed by the Ministry as critical, the Ministry Coordinator must register the system and ensure the required registration information contained in Section-7 of the AppHC record is current.



4.1 Register a Critical System

To register a critical system, set the value of the field 'Has this system been identified a critical system as defined in the BC Government OCIO critical systems standard?' to Yes.

Note that setting the legacy field 'Criticality' to a value of Mission Critical or Business Priority does not register that system as a deemed critical system by the standard.

4.2 De-Register a Critical System

To remove the designation of being deemed a critical system by the Standard, set the value of the field 'Has this system been identified a critical system as defined in the BC Government OCIO critical systems standard?' to No.

Note that setting the legacy field 'Criticality' to a value of non-Critical does not de-register that system as deemed a critical system by the standard.

Be aware that each Ministry will have an AppHC/C55 process and critical systems coordinators will need to engage their Ministry's AppHC coordinator to keep the registry data current.

5.0 System Design and Support Documentation

Each critical system's support documentation must describe:

- Designs incorporating business, system, technical and over-arching security
- Corporate Infrastructure Services (e.g. identity management, payment, etc.)
- The Application platform
- Communications infrastructure
- Application platform interface
- Communications infrastructure interface
- Special qualities (e.g. security, application management, etc.)
- Physical components making up the system
- The logical relationships/data and process flows
- Each business process that is supported or potentially impacted by the system
- For each software product:
    - Software title
    - Software version
    - Software functional description
    - Software vendor
    - SLA reference if applicable.
- For each hardware product:
    - Hardware component name
    - Hardware functional description
    - Hardware operating system version if applicable
    - Hardware vendor
    - SLA reference if applicable

5.1 Validity

The support Documentation lifecycle must be owned, managed and maintained to be effective in supporting a major incident.

To keep support documents valid it is recommended that at least the following control information is present in each document:

- Current document owner, and their organization
- Update history, author, and author's organization
- Last reviewed date, and who reviewed
- Next Review Date

5.2 Accurate and Current

Staff called in to support a critical system major incident response and recovery need the support documents to accurately portray current state of the system, that they are complete and indeed the latest version.

A process should be put in place to ensure that support documents are reviewed and signed off as accurate and current as prescribed in the next review date (described above in 5.1) or annually whichever is sooner.

5.3 Accessible

Response and recovery team members called in to support a major incident need to have immediate access to the current system design and support documentation.

A copy of all support documents is to be stored in a single location that is available to the team members and essential service support partners as appropriate. The location must be recorded in the registration record described earlier.

6.0 Systems Management

Above and beyond normal service desk or operation functions the following requirements shall apply in overseeing the daily overall health of a critical system.

6.1 Change Management Process

- A procedure should be established to review and approve all proposed changes
- Change requests should at minimum include the following information:
    - change requestor, approval chain
    - component(s) being changed
    - changes to be performed (include documented MOP - method of procedures)
    - start time, end time, duration
- Perform initially on a test system that is reflective of the production environment
- Perform in identified production change windows
- Log all changes and maintain history
- Coordinate changes with OCIO change management function that require extra-ordinary services from OCIO or would benefit with a restriction on changes to infrastructure services or other dependant systems. Refer to Request for Special Processing (RSP) for engagement instructions
- Update appropriate support documentation following the changes
- Update problem log and close appropriate problems addressed in change
- Include internal event logging to support determination of ‘who did what and when they did it’

6.2 Performance Baseline, Monitoring and Alerting

- Understand what normal is:
    - establish actual normal business operating performance and availability baseline metrics
- Establish performance and availability impact tolerance thresholds
- Continuously monitor actual performance and keep history for trend analysis and capacity planning

- Raise alerts pro-actively, that is independent of user experiences and calls, when impact tolerance threshold is experienced

6.3 Service Provider Support Management Requirements

The System Owner shall ensure support agreements in place for critical systems match the appropriate level of support required:

- the days of week or hours of service
- Level of expertise expected
- On-site requirement

Service partner support specialists will rely on the support documentation to effectively assist in major incident response and recovery. To ensure effectiveness the System Owner should provide service partners the opportunity to attest that design support documents are complete and meaningful and current configuration or use of their services is supportable.

Unsupported configurations must be identified in a risk management plan along with mitigation strategy.

If there's privacy or exceptional security surrounding any system data, a process should be put in place that reviews and approves access or describes alternate solutions.

6.3.1 Engaging TS service providers

Some TS service delivery units will construct templates that ministry can complete and submit to have their service-usage configuration reviewed. If you have capability to engage directly with service contacts then please do. For further details contact Lisa.Koorbatoff@gov.bc.ca.

6.4 Incident Management Requirements

Ensure capability to recognize an incident that could impact business service availability of a critical system:

- There is a single point of contact (help desk, an email inbox or a phone number) for users to raise incidents with the critical system and the hours of service match the criticality of the business (e.g. if service is until 8pm, then single point of contact should be offered until 8pm)
- That all incidents are recorded and history is maintained
- That trouble tickets are generated, severity assigned and alerts sent to designated support personnel
- Escalation of a major incident as defined by the Response and Recovery Director
- Reviews incidents daily and follows up on trends (problem management)

6.5 Disaster Recovery Plan

System Owner shall ensure that (tested within 12 months) Disaster Recovery Plan exists and has been approved by the appropriate business owner. Take note; unless specifically stated in the OLA/SLA with your provider, it is not likely there is any commitment by them to have a DRP.

6.6 Exercised

To ensure readiness, the major incident management process and disaster recovery plan should be exercised before production implementation on new systems and immediately for existing systems. Take note; unless specifically stated in the OLA/SLA with your provider, it is not likely there is any commitment by them to have exercised their DRP.

7.0 Compliance Assessment and STRA Sub-Section/Roadmap

Based on an effective date of April 2016 the following schedule defines the target deadlines for submission of critical systems compliance assessments and compliance roadmaps.

Note that, the Ministry Coordinator can engage the OCIO Coordinator at any time.

Activity	Complete by	Responsible
Register critical systems with OCIO Coordinator.	Oct 31, 2015	Ministry Coordinator
You must declare 'No' or 'Yes' in regards to whether your critical system is compliant using the iSmart Tool.	April 1, 2016	Ministry Coordinator

NOTE: There are two hard requirements:

1. Submission MUST at minimum be the Critical Systems Standard STRA sub-section provided; additional columns or rows can be added to increase its value to you or your organization.
2. Declaration and submission MUST be done using OCIO Information Security Branch's iSmart scorecard tool.

7.1 If declaring: 'No'

1. At a minimum, upload your STRA Sub-Section/roadmap, which has been signed off by the SYSTEM OWNER and BUSINESS PROGRAM OWNER.
2. Enter your target date.

7. 2 If declaring: 'Yes'

Upload your STRA Sub-Section, which has been signed by the INDEPENDENT REVIEWER, SYSTEM OWNER and BUSINESS PROGRAM OWNER.

7.3 Sample of High-Level Process

- Download the ***Critical Systems STRA sub-section*** word document provided on the OCIO Critical Systems SharePoint site at: https://sharecio.gov.bc.ca/asb/CriticalSystems/Shared%20Documents/0_Templates/Critical%20Systems%20Standard_STRA%20SubSection%20v1.00.docx (all Ministry coordinators have access).
- Self-assess compliance (establishing target dates for controls not met)
- Work towards April 1st compliance
- Perform rigorous independent review (before April 1st 2016)
- Declare compliancy (attaching signed off STRA sub-section)

Refer to Appendix A for a more detailed sample process and workflow document that may be helpful.

Refer to Appendix B for a sample play-scripted scenario using the above detailed process and workflow, that again may be helpful.

7.4 iSmart Scorecard

The iSmart tool has been updated to incorporate the attestation of your critical system. The update includes question “Is this a critical system as defined by the Critical Systems Standard”?

If yes:

1. the user will be asked to attest compliancy by selecting Yes or No
2. if no, user must enter compliancy target date
3. whether yes or no, user must upload the signed-off Critical Systems Standard STRA sub-section

Additional details for MISOs below.

7.4.1 Retrofitting an existing iSmart scorecard

If the critical system has a current iSmart scorecard:

- Must load a new template scorecard and import data from the old and complete the new Critical Systems section

7.4.2 No scorecard

If the critical system does not have a current scorecard:

- Log in and create a new Target of Evaluation and issue a scorecard against it

For further assistance in creating a Target of Evaluation, please email: Vulnerabilityandriskmanagement@gov.bc.ca

7.5 Independent Review and Attestation

The Standard section 8.0 states:

For each of the following sections of the STRA pertaining to critical systems, attain an "A" certification.

Sections of the STRA pertaining to critical systems are the Critical Systems Standard STRA sub-section document discussed above in 7.2.

"A" certification means adequacy of controls has been established by recent, rigorous independent review

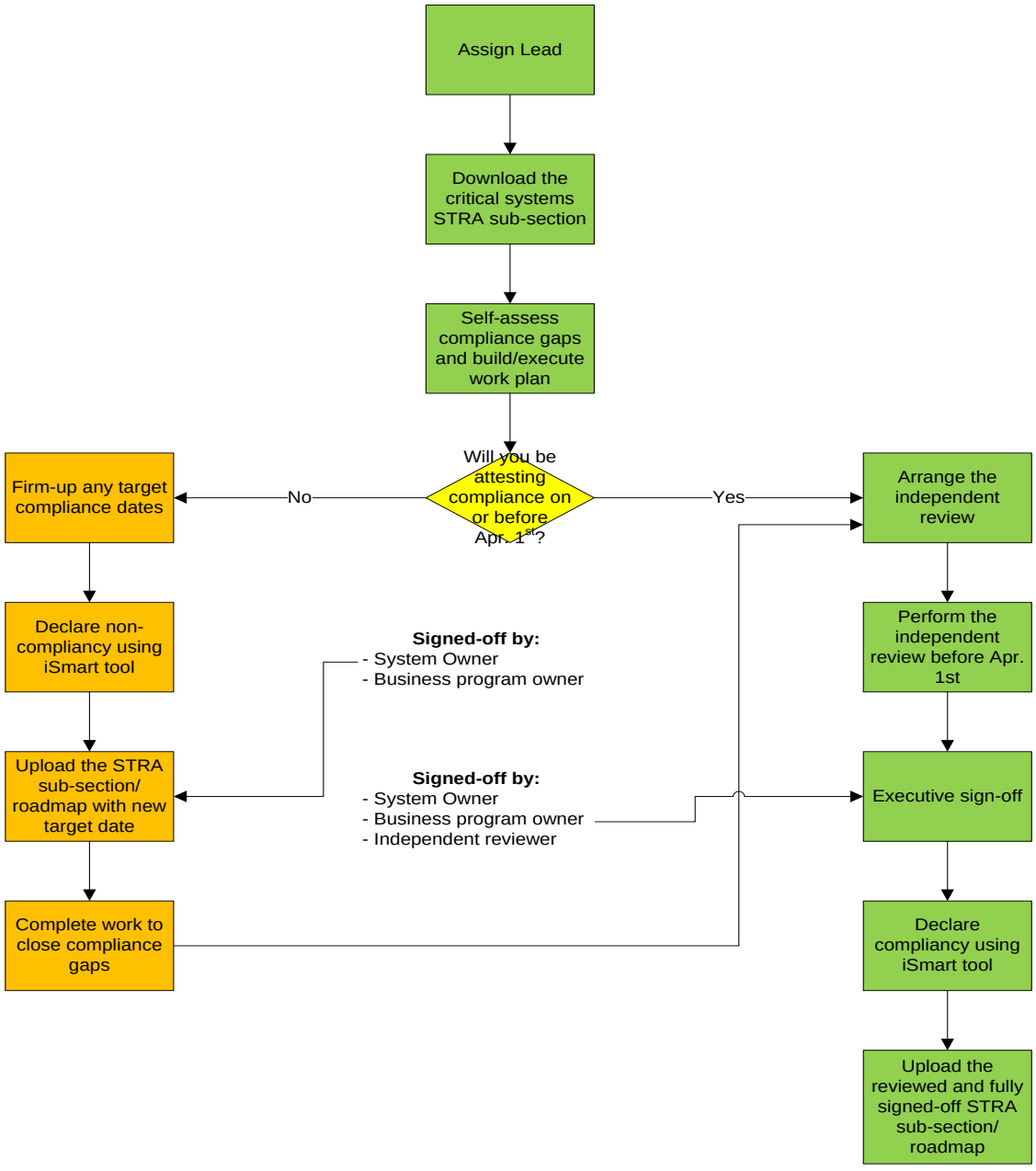
Rigorous for the purpose of the Standard means the reviewer MUST see the evidence that the control is being met.

Independent does not mean a 'hired 3rd party industry expert.' The review should be done by someone not in the chain of system ownership or support and cannot be the Ministry's MISO (Ministry Information Security Officer). Another Ministry's MISO is very acceptable.

Appendix A: Sample Compliance and Attestation Process Workflow Diagram

This is a sample process and workflow that one could use to get started on their way towards compliance to the Critical Systems Standard.

The sample process and workflow is a template and not a prescription of how. The material contained in this document can be used as is; added to, deleted, etc. or ignored completely.



Appendix B: Sample Compliance and Attestation Process Play Scripted

This document is a play script of the sample process and workflow that one could use to get started on their way towards compliance to the Critical Systems Standard.

The sample play script is a template and not a prescription of how. The material contained in this document can be used as is; added to, deleted, etc. or ignored completely.

Pre-Attestation for Compliance	
WHO	**DOES WHAT**
System Owner	**Assigns lead who is accountable to prepare the evidence for independent review.**
Lead	**Pulls down the critical systems STRA subsection and completes the template describing how the control is being met (or not) and what or where the evidence is. For the items not compliant, target estimates should be noted.**
Lead and System Owner	**Review the outcome of this initial assessment, firm up the estimated dates (this is essentially the compliance roadmap) and begin working towards compliance.**
Lead	**Notifies System Owner whether or not they are ready to attest compliance on or before the April 1st deadline.** • **If declaring 'NO', proceed to Part A below** • **If declaring 'YES', proceed to Part B below**

PART A - Declaring 'NO' to Attesting Compliance on or before April 1st	
WHO	**DOES WHAT**
Lead and System Owner	**Firm-up all necessary target dates and determines necessary work needed to declare compliance.**
Lead and MISO	**Lead meets with the MISO and uses the iSmart tool to update the STRA (or create a new STRA) to declare non-compliance. Attach the scanned signed off STRA Subsection and add target date for compliance. Two signatures are required on the STRA Subsection: System Owner and Business Program Owner.**
Lead	**Ensures work to close compliance gaps is completed as per the final target date.**
Lead and System Owner	**Lead meets with System Owner to confirm remaining compliance gaps have been addressed.**

System Owner	**Sets up meeting with Business Program Owner to review the results of the assessment and to confirm that the target dates have been met.**
OCIO	**Reviews roadmaps, ascertains risk and reports back to system owner whether the roadmap is accepted or need to explore alternate options.**
Proceed to first step in Part B below	

PART B - If declaring 'YES' to Attesting Compliance on or before April 1st	
WHO	**DOES WHAT**
System Owner	**Arranges an independent review.**
Reviewer	**Sits down with Lead and performs review (verifies things are as stated; evidence exists) noting compliance status for each of the controls documented adding comments as desired.**
Reviewer	**Reviewer either notes any remaining compliance gaps discovered or signs off on the review if no gaps are noted.**
Lead	**Meets with the MISO and uses the iSmart tool to update the STRA (or create a new STRA) to declare 'YES' for compliance. Attach the scanned signed off STRA Subsection and add target date for compliance. Three signatures are required on the STRA Subsection: Independent Reviewer, System Owner and Business Program Owner.**