Critical Systems Guidelines

Enterprise Architecture Branch

Office of the Chief Information Officer

Province of British Columbia

Document Version 3.1

May 28, 2021

Table of Contents

1.0 Document Control

Date	Author	Version	Change Reference
April, 2015	Tim Gagne	1.0	Initial version
December, 2015	Tim Gagne	1.1	Updates to Section 7 Compliance Attestation and Roadmap
January, 2016	Diana Rai	1.2	Linked Ministry Staff to their Ministry Critical Systems Coordinators
March, 2016	Scott Johnson	1.3	Updated 7.0, 7.1 and added 7.2
July, 2019	Stuart Cayzer, Theresa Parkin	3.0	Add Compliance Checklist, and synchronize versioning with the Critical Systems Standard
May, 2021	R. Jim Rabb	3.1	Add single point to list of "documentation must describe" in section 5.0 to address Recommendation 6 in the audit of "IT Asset Management in B.C. Government" of November 2020 ,on recommendations of the Office of the CISO. Also added NIST YouTube reference. Changed branch name and document version number on the title page.

2.0 Introduction

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

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

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

3.0 Roles and Responsibilities

Current roles identified in support of the Standard include:

1. Business Owner;
2. System Owner;
3. Response and Recovery Director (and alternate);
4. Ministry Coordinator, Critical Systems Standard;
5. OCIO Coordinator, Critical Systems Standard.

The responsibilities for each of these roles are described fully in the Standard.

Recommendations on the assignment of the supporting roles:

- MCIO collaborate with Business Owners to appoint a single Ministry Critical Systems Coordinator (and, ideally, an alternate);
- MCIO collaborate with Business Owners to appoint, for each critical system, a Response and Recovery Director and alternate.

4.0 Critical System Registration

OCIO will maintain a Critical Systems Registry, as a single source of truth, identifying all registered critical systems.

The Ministry Critical Systems Coordinator is required to provide their contact details to the OCIO Critical Systems Coordinator, and maintain accurate information on their ministry's critical systems at all times, as follows:

- System name and business function description
- Name and contact details for:
    - Ministry Critical Systems Coordinator;
    - Business Owner;
    - System Owner;
    - System Response and Recovery Director;
    - System Response and Recovery Director alternate.

- Target Date for Compliance

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, ..);
- 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;
- Maps of key organizational communication and data flows that include key information; *(NEW point, see also this supporting video)* (this may also be addressed by other points, but is essentially a physical architecture, showing servers, networks, ports, and protocols)
- 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

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

A process should be put in place to ensure that support documents are annually reviewed and signed off as accurate and current.

5.3 Accessible

A copy of all support documents should be stored in a single location that is available to the team members and essential service support partners.

6.0 Systems Management

Above and beyond normal service desk or operation functions, the following requirements should apply in overseeing the 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 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.

Change Management processes should also:

- Be performed initially on a test system that is reflective of the production environment;
- Be performed in identified production change windows;
- Log all changes and maintain history;
- For changes that require extra-ordinary services from OCIO or would benefit with a restriction on changes to infrastructure services or other dependent systems: coordinate with OCIO change management function - refer to Request for Special Processing (RSP) for engagement instructions;
- Update System Design and Support documentation following changes;
- Update problem log and close appropriate problems addressed in each 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 and record baseline metrics for normal business operating performance and availability;
- Establish performance and availability impact tolerance thresholds;
- Continuously monitor actual performance and keep history for trend analysis and capacity planning;
- Raise alerts pro-actively, and independent of user experiences and calls, when impact tolerance threshold is experienced.

6.3 Service Provider Support Management Requirements

The System Owner should ensure support agreements are in place for critical systems:

- Days of week and 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.

6.4 Incident Management Requirements

Maintain the capability to recognize an incident that could impact availability of a critical system, by ensuring:

- Escalation of a major incident is clearly defined by the Response and Recovery Director;
- 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 function (e.g. if service is until 8pm, then single point of contact should be offered until 8pm);
- All incidents are recorded and history is maintained;

- Trouble tickets are generated, severity assigned, and alerts sent to designated support personnel;
- Incidents are reviewed daily, and action is taken to address any trends identified (problem management).

6.4.1 Defining the Major Incident Management Process

The Response and Recovery Director must define and maintain a process 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.

6.4.2 Convening the Team

Members of 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 appropriate support agreements and funding are in place with service support partners.

6.4.3 Leading the Response and Recovery

Upon receiving an escalation of an incident to a major incident (as defined above), the Response and Recovery Director should lead the actions of the team and be the primary liaison with executives:

- Convene 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 the process.

6.5 Disaster Recovery Plan

The System Owner should ensure that a Disaster Recovery Plan exists, it has been tested within the past 12 months, and has been approved by the Business Owner.

6.6 Exercised

To ensure readiness, the Major Incident Management Process and Disaster Recovery Plan should be exercised before production implementation for new systems, and annually for existing systems.

7.0 Compliance Assessment and Declaration

As mentioned previously, it is the responsibility of the Ministry Critical Systems Coordinator to enter, and maintain, accurate information on the ministry's Critical Systems, in the Critical Systems Registry.

7.1 If declaring: 'No'

Enter your target date for compliance.

7. 2 If declaring: 'Yes'

Notify the OCIO Critical Systems Coordinator, update the Critical Systems Registry to indicate that the system is compliant, and ensure that the target date for compliance is set to the date on which compliance was achieved (this will set the 1-year deadline for review to ensure ongoing compliance).

7.3 Independent Review and Attestation

The adequacy of controls must be verified by recent, rigorous independent review.

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

Independent means that the review should be done by someone not in the chain of system ownership or support. Cannot be the System Owner's Ministry Information Security Officer (MISO) - another ministry's MISO is acceptable.

Appendix A: Compliance Checklist

Ministry:	**Critical System Name (as registered):**
Reviewed by: **<*Print Name Here*>**	**Review Date <dd-mmm-yyyy>:**
Reviewer's Signature:	

System Owner: **<*Print Name Here*>**	**Date <dd-mmm-yyyy> signed:**
Signature:	

Business (Program) Owner: **<*Print Name Here*>**	**Date <dd-mmm-yyyy> signed:**
Signature:	

Controls	**Evidence Good Y/N**	**Comments/Gaps**	**Compliance Target Date** <dd-mmm-yyyy>
UP-TO-DATE STRA The SYSTEM OWNER MUST ensure that this system has an up-to-date STRA.			
Describe how you meet the requirement.			
Tell me/show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
CRITICAL SYSTEM REGISTRATION: The required information has been registered with the OCIO and the named persons are aware of their roles and responsibilities and feel capable of doing so: **Click here for the full list.**			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

SYSTEM DESIGN AND SUPPORT DOCUMENTATION All required elements are available. **Click here for the full list.**			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

SYSTEM DESIGN AND SUPPORT DOCUMENTATION VALIDITY: Required control information provided in each document. **Click here for the full list.**			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
SYSTEM DESIGN AND SUPPORT DOCUMENTATION **CURRENT and ACCURATE:** Support documents are reviewed and signed off annually as accurate and current.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

SYSTEM DESIGN AND SUPPORT DOCUMENTATION **ACCESSIBLE:** Support documentation accessible to all supporting roles.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

CHANGE MANAGEMENT PROCESS: Process in place, and meets requirements. **Click here for the full list.**			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
PERFORMANCE BASELINE, MONITORING AND ALERTING: Process in place, and meets requirements. **Click here for the full list.**			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			
CAPACITY PLANNING: Process in place, and meets requirements.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

SERVICE PROVIDER SUPPORT MANAGEMENT: Process in place, and meets requirements. **Click here for the full list.**			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
INCIDENT MANAGEMENT: Process in place, and meets requirements. **Click here for the full list.**			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

MAJOR INCIDENT MANAGEMENT: Process in place, and meets requirements. • **Click here for the full list.**			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

CONVENING THE TEAM Terms of Reference in place, and meets requirements. **Click here for the full list.**			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
DISASTER RECOVERY PLAN:			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
Plan in place, tested annually, and meets requirements. **Click here for the full list.**			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

RESPONSE AND RECOVERY EXERCISED: Plan in place, tested annually, and meets requirements.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			