BRITISH COLUMBIA | Ministry of Citizens' Services

Critical Systems Standard

Enterprise Design Services
Office of the CIO, Province of BC

Document Version: 3.0
Published: July 2019

1 DOCUMENT CONTROL 3
2 INTRODUCTION 4
3 PURPOSE 4
4 CONVENTIONS USED 4
4.1 SUPPORTING GUIDELINES 4
5 DEFINITIONS 5
5.1 MISSION CRITICAL FUNCTION 5
5.2 CRITICAL SYSTEM 5
5.3 MUST 5
5.4 SHOULD 5
6 ROLES 5
6.1 BUSINESS OWNER 5
6.2 SYSTEM OWNER 6
6.3 RESPONSE AND RECOVERY DIRECTOR 6
6.4 MINISTRY CRITICAL SYSTEMS COORDINATOR 7
6.5 OCIO CRITICAL SYSTEMS COORDINATOR 7
7 REGISTRATION 7
8 SYSTEM DESIGN AND SUPPORT DOCUMENTATION 7
9 SYSTEMS MANAGEMENT 8
9.1 NEW APPLICATION COMPLIANCE 8
9.2 CHANGE MANAGEMENT 8
9.3 PERFORMANCE BASELINE, MONITORING AND ALERTING 8
9.4 CAPACITY PLANNING 8
9.5 SERVICE PROVIDER SUPPORT MANAGEMENT 8
9.6 INCIDENT MANAGEMENT 8
9.7 DISASTER RECOVERY PLAN 8
10 IMPLEMENTATION 9
10.1 EFFECTIVE DATE 9
10.2 NON-COMPLIANCE 9
10.3 ANNUAL REVIEW 9

1 Document Control

Date	Author	Version	Change Reference
March, 2015	Derek Rutherford, Tim Gagne	1.0	Version 1
March, 2017	Scott Johnson	2.0	Extend scope to include new and changed systems
June 2019	Stuart Cayzer, Ruonan Lou, Scott Johnson	3.0	Increase focus on Mission Critical systems

2 Introduction

This new and improved Critical Systems Standard now aligns fully with our Core Policy and Procedures Manual, Chapter 16 (Business Continuity Management) by focusing on Mission Critical Systems, which are those required for the delivery of Mission Critical Business Functions.

As the IM and IT operating environment continues to increase in scale, complexity, and dependencies, the risk of disruptions to business services is higher. The effect of a loss of a mission critical service on individuals can bring hardship, and in some cases result in injury or even death. Note also that government is increasing its reliance on service providers (internal to government as well as external contractors). This increased complexity demands higher levels of vigilance in our security posture and improved coordination to be successful in delivering stable services to citizens.

Lessons learned from recent service interruptions in government have pointed to ways of improving how we recognize and more effectively deal with these kinds of disruptions. This standard addresses the immediate concerns from lessons we have recently learned and also lays the foundations for a program of continuous improvement.

3 Purpose

The purpose of this standard is to:

- Define a critical system;
- Identify key roles and responsibilities;
- Minimize the impact of a disruption to a critical system;
- Restore normal business operations as soon as possible; and
- Maintain the security of information systems and communications technologies, and the availability of supporting infrastructure and services.

4 Conventions used

Terms used that are written in all upper case are defined within this Standard e.g. BUSINESS OWNER is a role that is defined in section 6 Roles.

4.1 Supporting Guidelines

This standard is designed to be read in conjunction with the *Critical Systems' Guidelines* published **here**. The guidelines describe proposed approaches that could meet the minimum requirements under this standard.

5 Definitions

5.1 Mission Critical Function

Defined in Core Policy, Chapter 16, and included here for ease of reference - Mission Critical functions are those that, should they not be performed, could lead to:

- Failure in meeting the legislated Emergency Program Act or any other Act
- Loss of life and/or safety
- Personal hardship to citizens
- Major damage to the environment
- Significant loss in revenue and/or assets.

5.2 Critical System

Any IM/IT service, system, or infrastructure component that is deemed necessary by the SYSTEM OWNER to deliver a MISSION CRITICAL FUNCTION, is a critical system for the purposes of this standard. The use of the word system is intended to have broad applicability and can include hardware and software implemented in numerous configurations i.e. on premise, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) whether operated under the direct control of government staff or through an outsourced service provider.

5.3 Must

The term "MUST" (when written in all upper case) is defined as an absolute requirement of this Standard.

5.4 Should

The term "SHOULD" (when written in all upper case) means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications MUST be understood and carefully weighed before choosing a different course. The use of an alternate method requires the approval of the Government Chief Information Officer (GCIO).

6 Roles

6.1 Business Owner

The BUSINESS OWNER MUST ensure that a Business Impact Analysis (BIA) is completed for each business unit or program area, as specified in Core Policy, Chapter 16.

The BIA MUST be reviewed and updated annually, as well as when changes to business operations and processes, organizational structure, critical dependencies or resources occur. Ministries are responsible for identifying and implementing operational triggers to ensure the BIA is current.

The BIA determines which business functions are Mission Critical.

6.2 System Owner

For all functions that have been deemed Mission Critical, the SYSTEM OWNER MUST identify all IM/IT services, systems, or infrastructure components that are necessary for the delivery of the Mission Critical function. These IM/IT services, systems, or infrastructure components MUST be declared as critical systems.

The SYSTEM OWNER role is accountable for the overall state of the system and MUST be authorized to allocate resources as appropriate to meet the obligations under this standard.

A *Critical System* MUST have a SYSTEM OWNER role assigned.

The SYSTEM OWNER MUST ensure that all critical systems for which they are accountable have:

- An up-to-date Security Threat and Risk Assessment (STRA);
- All roles required by this standard assigned, and will continue to be maintained;
- All system and contact details registered, and will be maintained in collaboration with the OCIO coordinator;
- System design documentation that is complete, accurate, up to date, and has a process in place to maintain currency and accuracy;
- A change management process;
- Performance monitoring and capacity planning baselines established and actively maintained, managed and monitored;
- A Major Incident Response and Recovery process, defined, maintained and tested at least annually;
- A Disaster and Recovery Plan defined, maintained and tested.
- Capacity Planning
- Service Provider Support Management

6.3 Response and Recovery Director

The RESPONSE AND RECOVERY DIRECTOR role defines the major incident response and recovery process and is responsible to manage, direct, and lead the actions of incident response and recovery for issues affecting normal business operating performance and availability as described in the *Critical Systems' Guidelines*.

A *Critical System* MUST have a RESPONSE AND RECOVERY DIRECTOR role and their alternate assigned.

The named Response and Recovery Director MUST have the authority to convene the necessary resources as required.

6.4 Ministry Critical Systems Coordinator

The MINISTRY CRITICAL SYSTEMS COORDINATOR role is the single point of administrative contact pertaining to the obligations under this standard.

Each Ministry MUST have a MINISTRY CRITICAL SYSTEMS COORDINATOR role assigned.

This coordinator will register each critical system with the OCIO CRITICAL SYSTEMS COORDINATOR

6.5 OCIO Critical Systems Coordinator

The OCIO CRITICAL SYSTEMS COORDINATOR role is the single point of administrative contact for all information flows between OCIO and MINISTRY CRITICAL SYSTEMS COORDINATORS.

The OCIO MUST have a CRITICAL SYSTEMS COORDINATOR role assigned.

The OCIO CRITICAL SYSTEMS COORDINATOR role MUST

maintain a register of all critical systems and

provide a quarterly report on the effectiveness of efforts made in the prior period towards achieving compliance, to:

- Ministry Chief Information Officers; and
- OCIO's CTO and ADM, Enterprise Services.

7 Registration

The OCIO CRITICAL SYSTEMS COORDINATOR MUST maintain a register of all critical systems.

MINISTRY CRITICAL SYSTEMS COORDINATORs MUST register each critical system with the OCIO CRITICAL SYSTEMS COORDINATOR. A registration MUST be completed in accordance with the guidance contained in the *Critical Systems' Guidelines*.

8 System Design and Support Documentation

For each critical system the SYSTEM OWNER MUST create and maintain as current, accurate and available, documentation for the *Critical Systems'* application; computing, data and network platform that SHOULD contain at minimum the elements as described in the *Critical Systems' Guidelines*.

9 Systems Management

9.1 New Application Compliance

All new systems developed or acquired, must be evaluated against the definition of a Critical System. Any new application whose BUSINESS OWNER determines that it will be a Critical System MUST ensure it is designed and built in compliance with the *Critical Systems Standard* prior to release into a production environment.

9.2 Change Management

The SYSTEM OWNER MUST ensure a process is in place that governs changes to a system and SHOULD ensure that such a change process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

9.3 Performance Baseline, Monitoring and Alerting

The SYSTEM OWNER MUST ensure a process is in place to manage system performance and SHOULD ensure that such a system performance process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

9.4 Capacity Planning

For each critical system the SYSTEM OWNER MUST ensure a process is in place to proactively manage system resource utilization and SHOULD review historical performance information to determine if any action is required.

9.5 Service Provider Support Management

For each critical system the SYSTEM OWNER MUST ensure a process is in place to proactively manage providers of services necessary to deliver the system and SHOULD ensure that such a service provider process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

9.6 Incident Management

The SYSTEM OWNER MUST ensure a process is in place to be able to recognize and recover from an incident that could impact business service availability and SHOULD ensure that such an incident management process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

The SYSTEM OWNER MUST ensure that their organization has a defined incident management process. The incident management process SHOULD be repeatable and MUST be exercised prior to implementation of any new critical systems and at minimum annually thereafter, in accordance with the requirements outlined in the *Critical Systems' Guidelines*.

9.7 Disaster Recovery Plan

The SYSTEM OWNER MUST ensure that a tested Disaster Recovery Plan and skilled resources are in place to be able to recover from a disruptive event that has an unacceptable impact to a business service, and MUST ensure that such a disaster recovery processes, at minimum, meet the requirements outlined in the *Critical Systems' Guidelines*.

10 Implementation

10.1 Effective Date

This Standard is effective as of April 1, 2016.

10.2 Non-compliance

If a SYSTEM OWNER is unable to attest to compliance by the effective date, the SYSTEM OWNER (or delegate) MUST submit for endorsement a compliance assessment and roadmap as scheduled in the *Critical Systems' Guidelines*.

10.3 Annual Review

On each anniversary of the endorsement of their compliance roadmap, and on or before each target date from compliance, the SYSTEM OWNER MUST report the progress against the roadmap, any proposed revisions and an updated compliance assessment as described in the *Critical Systems' Guidelines*.