CRITICAL SYSTEMS STANDARD

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● *Collaboration* ● *Innovation*

Document Version 1.0
Published: APRIL 2015

Replaces: None

Critical Systems Standard

Table of Contents

1 Document Control

Date	Author	Version	Change Reference
March 26, 2015	Rutherford & Gagne	1.0	Version 1

2 Introduction

As the IM and IT operating environment continues to increase in scale, complexity, and dependencies, the risk of disruptions to business services is potentially higher. The effect of a loss of a business critical service on individuals can bring hardship and in some cases result in injury or even death. As providers of those services 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
- Reduce the probability of a preventable incident disrupting a critical system,
- Minimize the impact of a disruption to a critical system,
- Restore normal business operations as soon as possible,
- Maintain the security of information systems and communications technologies; and the availability of supporting infrastructure and services.

4 Version

This version of the standard is primarily focussed on identifying and dealing with disruptions to normal operations of critical systems. This Standard will be enhanced in the future to include requirements for the planning and build phases of systems development.

5 Conventions used

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

5.1 Notes to Reader

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 of how to meet the obligations under this standard.

A key part of the governance of compliance to this standard is achieved through the *Security Threat and Risk Assessment or STRA* process. The completed "Critical Systems" section of the STRA will be the formal record for each critical system as to its degree of compliance.

6 Definitions

6.1 Critical System

Any IM/IT service, system, or infrastructure component that is deemed necessary by the SYSTEM OWNER to deliver a MISSION CRITICAL, or BUSINESS PRIORITY 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.

6.2 Mission Critical

Processes 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.

6.3 Business Priority

Processes that are not MISSION CRITICAL, but, should they not be performed, could lead to the loss of a major business function.

6.4 Must

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

6.5 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).

6.6 The Requirement for a STRA

The *Core Policy and Procedures Manual, Chapter 12.3.6 Information and Technology Security - Policy* identifies the requirement that for "the security of information systems and communications technologies must be regularly reviewed to ensure compliance with applicable legislation, policies, standards and documented security controls". Information Security Policy 3.1.2 requires ministries to be responsible for controlling the production, development, maintenance, use and security of information and technology assets within their jurisdiction. This means that ministries MUST ensure that a STRA is performed on government information, programs, systems and services (or their environment) when designing, implementing or modifying them.

6.7 STRA

STRAs are a design review. STRAs assess the design of the information system based on a review of system design documents; specifically a STRA is used to evaluate the compliance of the information system with the government's information security policies.

6.8 The Responses to the Section(s) in the STRA dealing with Critical Systems

The responses to the section(s) in the STRA dealing with Critical Systems MUST have been established by recent, rigorous independent review and meet the following completion criteria:

- The checklist for the subsection has been completed by an independent party;
- Each control in the subsection has been tested and complies with this standard; and,
- Evidence has been supplied to support responses for each control.

7 Roles

7.1 System Owner

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.

7.2 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.

7.3 Ministry Coordinator

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

Each Ministry MUST have a *Critical Systems* MINISTRY COORDINATOR role assigned.

7.4 OCIO Coordinator

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

The OCIO MUST have a CRITICAL SYTEMS COORDINATOR role assigned.

8 Conducting a STRA

The SYSTEM OWNER MUST ensure that all *Critical Systems* for which they are accountable have an up-to-date STRA, where:

- All sections pertaining to Critical Systems are *consistent* with the *design intent* of the critical system
- For each of the following section of the STRA pertaining to critical systems, attain an "A" certification:
    - All roles have been assigned and will continue to be maintained.
    - All System and Contact details have been registered and will be maintained with the OCIO coordinator.
    - All system design documentation is complete, accurate, endorsed as current and has a process is in place to maintain their currency and accuracy.
    - A change management process is in place
    - Performance monitoring and capacity planning baselines have been established and will be actively maintained, managed and monitored
    - A Major Incident Response and Recovery process has been defined and will be maintained and continuously tested.
    - A Disaster and Recovery Plan is defined, maintained and tested.

9 Registration

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

The Ministry COORDINATOR MUST register each critical system with the OCIO COORDINATOR. A registration MUST be completed in accordance with the guidance contained in the *Critical Systems' Guidelines*.

10 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*.

11 Systems Management

11.1 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*.

11.2 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*.

11.3 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.

11.4 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*.

11.5 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*.

11.6 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*.

12 Implementation

12.1 Effective Date

This Standard is effective April 1, 2016.

12.2 Non-compliance

A SYSTEM OWNER that is unable to attest to compliance by the effective date MUST submit for endorsement a compliance assessment and roadmap as scheduled in the *Critical Systems' Guidelines*.

12.3 Annual Review

On the anniversary of the endorsement of their compliance roadmap, A SYSTEM OWNER MUST report the progress against the roadmap, any proposed revisions and an updated compliance assessment as described in the *Critical Systems' Guidelines*.