Critical Systems Standard FAQs:

(Click+Link) on each question to go to the corresponding answer.

Q: What is the Critical Systems Standard?

A. The Critical Systems Standard is an OCIO standard that governs roles and responsibilities in addition to response/recovery requirements in the event of unplanned system outages for government's most critical hardware and software applications.

Q: Who is the Standard written for?

A. The Critical Systems Standard was written for use by anyone involved in response and recovery efforts during an unplanned Critical System outage. Specific target audiences include:

- Business Owners
- System Owners
- Ministry Chief Information Officers (MCIO)
- Response and Recovery Directors and their alternates
- Ministry Critical Systems Coordinators
- OCIO Coordinator, Critical Systems Standard
- Ministry Information Security Officers (MISO)
- NEW: Product Owners and Scrum Master (these roles are directly responsible for overseeing teams conducting new application development at the Lab)

Q: What characteristics are used to determine whether a system should be declared a Critical System under the Standard?

A. 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 considered to be a critical system for the purposes of the 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.

MISSION CRITICAL - Indicates 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.

BUSINESS PRIORITY - Indicates processes that are not MISSION CRITICAL, but, should they not be performed, could lead to the loss of a major business function.

For more information, visit the Standard **here**.

Q: Who is ultimately responsible for determining whether a system should be registered as a Critical System?

A. Under the Standard, the SYSTEM OWNER role is assigned accountability for the overall state of the system, including determining whether a system should be formally declared as a Critical System. SYSTEM OWNERS often work with BUSINESS OWNERS and MCIOs to assess their systems before making this determination.

Q: Why is the Standard important to development teams working at the CSI Lab?

A. Version 2.01 of the Standard (released in Oct. 2017) sets out compliance requirements for new application compliance. These requirements outline that all new applications must be evaluated against the definition of a Critical System in the Standard. Any new application whose SYSTEM OWNER determines that it will be registered as a Critical System MUST ensure it is designed and built in compliance with the Critical Systems Standard prior to release into a production environment.

As such, efforts to reach compliance with the Standard for a new Critical System application must now be made, in part, at the development team level and under direction of the Product Owner responsible for overseeing that team.

Q: How is the CSI Lab supporting implementation of the Standard?

A. The CSI Lab is currently working with the OCIO to embed various activities found in the Critical Systems Compliance Checklist directly within the Lab's development environment. The goal is to make the road towards reaching compliance a regular part of the 'start-up' package that new development teams will use to get up and running quickly on the Lab's Devops Platform.

Presently, this initiative is in its initial stage of development and not yet fully implemented. To assist development teams achieve compliance in the interim, Product Owners may contact their Ministry Critical Systems Coordinator for further assistance. If you are not aware who your Ministry Critical Systems Coordinator is, check **here**.

Q: How do I register my system as a Critical System?

A. Once a SYSTEM OWNER has determined that a system shall be declared a Critical System, the System Owner (or their designate) shall use Section 7.0 of the C55 Data Repository Application to formally conduct the required declaration to register their system. Please note that when you register a system, you MUST provide a compliance Target Date.

Q: Once I register my system, what are the next steps?

A. As outlined above, the CSI Lab is currently in the initial stages of setting up the ability to manage the road towards reaching compliance by embedding the compliance process into their development environment. As such, all work outlined in the **Critical Systems Standard Compliance Checklist** must presently be done manually.

Working with the assistance of your Ministry Critical Systems Coordinator, Product Owners will use the Compliance Checklist to manage completion and review of all tasks need to reach compliance.

Q: What does being compliant with the Standard mean?

A. Compliance with the Standard can only be achieved once all work outlined in the **Critical Systems Standard Compliance Checklist** has been fully completed and an independent review has been successfully conducted. The checklist must then be properly signed off by the Independent Reviewer, System Owner and Business Owner in order for compliance with the Standard to be achieved.

Q: What does 'independent review' mean?

A. An Independent Review is a verification review conducted once all work outlined in the **Critical Systems Standard Compliance Checklist** has been completed as required. The intent of the review is to ensure that the work has been completed fully and that all artifacts have been made easily accessible (whether digitally or in hard copy) for use by the Response and Recovery Team. The review is not intended to audit the quality, relevancy or validity of the artifacts covered in the Compliance Checklist.

The term '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 acceptable.

Q: What are some of the best practices for becoming compliant?

A. Several best practices have been identified which can assist your efforts towards quickly reaching compliance:

i. Depending on how many Critical Systems your Ministry has declared, it may be beneficial to establish or participate within a working group to better manage the collective workload associated with completing one or more **Critical Systems Standard Compliance Checklists**.

ii. If you are simultaneously completing Compliance Checklists for multiple Critical Systems, consider first tackling sections that allow you to address tasks within the checklists that may be common to each system in order to maximize your use of available resources.

iii. When compiling system documentation and other important artifacts required under the Compliance Checklist, ensure that everything is housed in one location (whether digitally or manually) that is easily accessible to the Independent Reviewer. Doing so will significantly speed up the Independent Review process.

iv. Product owners are strongly encouraged to tap into the expertise of the Critical Systems Community of Practice. This group can connect you to other teams within government who are much closer to reaching compliance who may be willing to share their experiences and other best practices gained. Contact the **OCIO Critical Systems Coordinator** for an introduction.

Q: Where can I go if I need other questions answered regarding the Standard?

A. Development teams working through the CSI Lab have multiple options to seek further assistance. These include contacting:

- Ministry Critical Systems Coordinators (**contact list**)
- OCIO Coordinator, Critical Systems Standard (**email link**)
- Ministry Chief Information Officers (MCIO)
- Ministry Information Security Officers (MISO)

Product owners may also contact the OCIO Coordinator, Critical Systems Standard to request access to the Critical Systems SharePoint site for more information.