BRITISH COLUMBIA | Ministry of Citizens' Services

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0

Published: September 2019

Table of Contents

I Introduction, Scope, Background 3

II Glossary, Terms and definitions, List of commonly used references 3

1 Information Security Aspects of Business Continuity Management 4

1.1 Information security continuity 4

1.2 Redundancies.. 7

I Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

II Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references “ sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.

1 Information Security Aspects of Business Continuity Management

This chapter provides direction from a security focus for planning the resumption of business or services where a man-made or natural disaster has occurred. Government organizations are required to be prepared and to re-establish business or services as swiftly and smoothly as possible. Business continuity plans include the evaluation of security risks in line with the directions set by Emergency Management BC and the BC government. More comprehensive policy on business continuity management is described in Chapter 16 of the government Core Policy and Procedures Manual.

1.1 Information security continuity

1.1.1 The organization must determine its requirements for information security and the continuity of information security management in adverse situations.

a) Business continuity planning

b) Business continuity risk assessment

c) Business continuity strategy

d) Business continuity plans

e) Coordination of business continuity plans

Purpose: ***To ensure government can continue to deliver essential services despite damage, loss, or disruption of business processes.***

1.1.1 a) Business continuity planning

Information Owners and Information Custodians must ensure business continuity and recovery plans address information security requirements consistent with the classification of the information. Processes for establishing business continuity and recovery plans are detailed in the Business Continuity Management Program Guidelines.

- Information Owners must perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations; and,
- Information security requirements remain the same in adverse situations, compared to normal operational conditions.

The Information Custodian must maintain the business continuity and recovery plans for information systems as part of the System Security Plan.

Government policy on business continuity programs is defined in Core Policy and Procedures Manual 16 – Business Continuity Management.

1.1.1 b) Business continuity risk assessment

The process for identifying, analyzing and evaluating risks, including information security risks, is detailed in the Business Continuity Management Program Guidelines, section 2 – Identify, Analyze and Evaluate Risks.

The process for analyzing and assessing business impacts, including those for information security risks, is detailed in the Business Continuity Management Program Guidelines, section 3 – Review Business Functions and Analyze Business Impacts.

1.1.1 c) Business continuity strategy
The process for developing a business continuity strategy is detailed in the Business Continuity Management Program Guidelines, section 4 – Plan Mitigation Strategies and, section 5 – Plan Business Continuity Strategies.

1.1.1 d) Business continuity plans
Requirements for business continuity plans are defined in Core Policy and Procedures Manual 16 – Business Continuity Management. The process for developing and maintaining business continuity plans is detailed in the Business Continuity Management Program Guidelines.

1.1.1 e) Co-ordination of business continuity plans
Information Owners and Information Custodians must ensure business continuity plans:

- Include the classification of information assets to identify critical business operations;
- Use government-wide frameworks and processes; and,
- Use information security processes which maintain approved security levels.

The Emergency Management BC must coordinate government-wide business continuity plans to reconcile recovery priorities, business impacts, security impacts and business resumption processes.

The Government Chief Information Officer is responsible for protecting the privacy, confidentiality, integrity and availability of government's electronic information. This responsibility includes providing expert advice to Emergency Management BC on information security aspects of business continuity plans.

Recommended Tests:
Note: 1.1.1 is reported on as part of the annual information security review.

- Demonstrate a documented business continuity plan that is current, reviewed regularly and is aligned with government strategic objectives.

1.1.2 The organization must establish, document, implement and maintain processes, procedures and controls to ensure the required level of information security for business continuity during an adverse situation.
a) Implement required level of continuity
b) Information security continuity requirements
c) Processes and procedures
d) System redundancy

Purpose: ***To ensure the required level of continuity for information security is maintained during an adverse situation.***

1.1.2 a) Implement required level of continuity
Information Owners and Information Custodians must ensure that:

- An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using employees with the necessary authority, experience and competence;
- Incident response employees with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated; and,
- Documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on approved information security continuity objectives.

1.1.2 b) Information security continuity requirements

According to the information security continuity requirements, Information Owners and Information Custodians must establish, document, implement and maintain:

- Information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
- Processes, procedures and implementation changes to maintain existing information security controls during an adverse situation; and,
- Compensating controls for information security controls that cannot be maintained during an adverse situation.

1.1.2 c) Processes and procedures

Within the context of business continuity or disaster recovery, specific processes and procedures have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them must be protected. Information Owners and Information Custodians must involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures.

1.1.2 d) System redundancy

Information security controls that have been implemented must continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls must be established, implemented and maintained to achieve an acceptable level of information security.

Recommended Tests:

Note: 1.1.2 is reported on as part of the annual information security review.

- Demonstrate a management structure is in place to mitigate and respond to adverse situations.
- Demonstrate documented plans, response and recovery procedures are developed and approved.
- Demonstrate compensating controls for information security controls that cannot be maintained during an adverse situation have been developed.

1.1.3 Business continuity plans must be regularly exercised and updated.
a) Business continuity plan exercising and maintenance

Purpose: ***To ensure business continuity plans are current, functional and address information security requirements.***

1.1.3 a) Business continuity plan exercising and maintenance

Information Owners and Information Custodians must review business continuity plans annually to ensure they are current, valid and readily accessible during a business interruption. Business Continuity Plans must be coordinated with security management and emergency preparedness and response plans.

Business Continuity Plans must be exercised at least annually to the extent necessary to confirm plan effectiveness and to ensure employees are prepared and trained. All employees and key stakeholders must be aware of the Ministry Business Continuity Management Program and understand its contents and their role. Information Owners and Information Custodians must report the number and type of exercises completed, the training conducted and the status of the business continuity plans to Emergency Management BC semi-annually.

Requirements for exercising business continuity plans are defined in Core Policy and Procedures Manual 16 – Business Continuity Management. The processes for exercising business continuity plans are detailed in the Business Continuity Management Program Guidelines, section 8 – Train and Exercise. Requirements for the maintenance of the business continuity plan are detailed in Business Continuity Management Program Guidelines, Section 10 – Monitor and Review.

Recommended Tests:
Note: 1.1.3 is reported on as part of the annual information security review.

- Demonstrate the business continuity plan is reviewed and tested annually.
- Demonstrate employees are made aware of their roles and responsibilities as part of the business continuity plan.

1.2 Redundancies

1.2.1 Information processing facilities must be implemented with redundancy sufficient to meet availability requirements.
a) Availability requirements

Purpose: To ensure the availability of information systems without interruption.

1.2.1 a) Availability of information processing facilities
The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems. Information Owners and Information Custodians must identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.

Where applicable, redundant information systems must be tested to ensure the failover from one component to another component works as intended.

Recommended Tests:
Note: 1.2.1 is reported on as part of the annual information security review.

- Demonstrate system redundancy capacity is adequate to meet system service business requirement.