6.4. Business Continuity and Disaster Recovery

Objective

6.4.1. To ensure business continuity and disaster recovery processes are established to assist in meeting the agency's business requirements, minimise any disruption to the availability of information and systems, and assist recoverability.

Context

Scope

6.4.2. This section covers information on business continuity and disaster recovery relating specifically to systems.

References

6.4.3. Additional information relating to business continuity is contained in:

Reference	Title	Publisher	Source
ISO 22301:2019	**Security and resilience — Business continuity management systems — Requirements**	ISO	https://www.iso.org/standard/75106.html
ISO/IEC 27001:2013	**Information Technology – Security Techniques - Information Security Management Systems - Requirements**	ISO	https://www.iso.org/standard/54534.html
ISO/IEC 27002:2022	**Information security, cybersecurity and privacy protection — Information security controls**	ISO	https://www.iso.org/standard/75652.html
ISO/IEC 27005:2018	**Information Technology – Security Techniques - Information Security Risk Management**	ISO	https://www.iso.org/standard/75281.html
ISO/IEC 27031:2011	**Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity**	ISO	https://www.iso.org/standard/44374.html
SAA/SNZ HB 221:2004	**Business Continuity Management**	Standards NZ	https://standards.govt.nz/

PSR references

6.4.4. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, GOV7, INFOSEC1 and PHYSEC1	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements/ Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Availability requirements

6.4.5.R.01. **Rationale**

Availability and recovery requirements will vary based on each agency's business needs and are likely to be widely variable across government.

Agencies will determine their own availability and recovery requirements and implement measures consistent with the agency's SRMP to achieve them as part of their risk management and governance processes.

6.4.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1120]

Agencies MUST determine availability and recovery requirements for their systems and implement measures consistent with the agency's SRMP to support them.

Backup strategy

6.4.6.R.01. **Rationale**

Having a backup strategy in place is a fundamental part of business continuity planning. The backup strategy ensures that critical business information is recoverable if lost. Vital records are defined as any information, systems data, configurations or equipment requirements necessary to restore normal operations.

6.4.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1123]

Agencies SHOULD:

- Identify vital records;
- backup all vital records;
- store copies of critical information, with associated documented recovery procedures, offsite and secured in accordance with the requirements for the highest classification of the information; and
- test backup and restoration processes regularly to confirm their effectiveness.

Business Continuity plan

6.4.7.R.01. **Rationale**

It is important to develop a business continuity plan to assist in ensuring that critical systems and data functions can be maintained when the system is operating under constraint, for example, when bandwidth is unexpectedly limited below established thresholds.

6.4.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1126]

Agencies SHOULD develop and document a business continuity plan.

Disaster recovery plan

6.4.8.R.01. **Rationale**

Developing and documenting a disaster recovery plan, will reduce the time between a disaster occurring, and critical functions of systems being restored.

6.4.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1129]

Agencies SHOULD develop and document a disaster recovery plan.