Chapter 7 – Business Continuity and Risk Management

Section 01 Business Continuity Management

070101 Initiating the Business Continuity Plan (BCP)

Purpose: To establish the appropriate level of business continuity management to sustain the operation of critical business services following a disaster or adverse event.

POLICY

1. Agencies must maintain a business and disaster recovery plan with respect to information technology. Business and disaster recovery plans shall be provided to the Office of the State CIO.
2. Agencies, through their management, must implement and support an appropriate information technology business continuity program to ensure the timely delivery of critical automated business services to the State's citizens.
3. A management team composed of representatives from all the agency organizational areas has primary leadership responsibility to identify information technology risks and to determine what impact these risks have on business operations.
4. Management must also plan for business continuity, including disaster recovery, based on these risks and document continuity and recovery strategies and procedures in a defined business continuity plan that is reviewed, approved, tested and updated on an annual basis.

ISO 27002 REFERENCES
14.1.04 Business continuity planning framework

070102 Assessing the BCP Risk

Purpose: To require that State agencies manage information technology risks appropriately as required in GS 147-33.89.

POLICY

1. Agencies shall identify the potential risks that may adversely impact their business in order to develop continuity and recovery strategies and justify the financial and human resources required to provide the appropriate level of continuity initiatives and programs.
2. Agencies shall conduct business risk impact analysis activities that include the following:
   - Define the agency's critical functions and services.
   - Define the resources (technology, staff and facilities) that support each critical function or service.
   - Identify key relationships and interdependencies among the agency's critical resources, functions and services.
   - Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact. (See also Statewide Glossary for Recovery Time Objective)
   - Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service. (See also Statewide Glossary for Recovery Point Objective)
   - Document any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority (for example, tax filing dates, reporting deadlines, etc.).

- Identify any critical non-electronic media required to support the agency’s critical functions or services.
- Identify any interim or workaround procedures that exist for the agency’s critical functions or services.

GUIDELINES

The following items should be considered:

- Estimate the decline in effectiveness over time of each critical function or service.
- Estimate financial losses over time resulting from the inoperability of each critical function or service.
- Estimate tangible (non-financial) impacts over time resulting from the inoperability of each critical function or service.
- Estimate intangible impacts over time resulting from the inoperability of each critical function or service.

ISO 27002 REFERENCES

14.1.02 Business continuity and risk assessment
14.1.04 Business continuity planning framework

070103 Developing the BCP

Purpose: To require that the appropriate level of information technology business continuity management is in place to sustain the operation of critical information technology services to support the continuity of vital business functions.

POLICY

1. Management shall develop a business continuity plan (BCP) that covers all of the agency’s essential and critical business activities and that includes references to procedures to be used for the recovery of systems that perform the agency’s essential and critical business activities.
2. At a minimum, an agency’s business continuity plan must:
    - Help protect the health and safety of the employees of the State of North Carolina.
    - Protect the assets of the State and minimize financial, legal and/or regulatory exposure.
    - Minimize the impact and reduce the likelihood of business disruptions.
    - Create crisis teams and response plans for threats and incidents.
    - Include communication tools and processes.
    - Require that employees are aware of their roles and responsibilities in the BCP and in plan execution.
    - Include training and awareness programs.
    - Require simulations and tabletop exercises.
    - Have a documented policy statement outlining:
        - Framework and requirements for developing, documenting, and maintaining the plans.
        - Requirements for testing and exercising.
        - Review, sign-off and update cycles.

- Require senior management oversight and approval.
- Assess the professional capability of third parties and ensure that they provide adequate contact with the agencies.
- Review dependence on third parties and take actions to mitigate risk associated with dealing with third parties.
- Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.
- Set forth procedures to be followed for restoring critical systems to production.

3. Training and awareness programs shall be undertaken to ensure that the entire agency is confident, competent and capable and understands the roles each individual within the agency must perform in a disaster/or adverse situation.
4. The person(s) designated as the agency business continuity plan (BCP) coordinator(s) has the responsibility of overseeing the individual plans and files that constitute the BCP and ensuring that they are current, meet these standards and are consistent with the agency's overall plan. At the direction of the State Chief Information Officer, an agency's BCP shall be reviewed annually by the Office of Information Technology Services and recommendations shall be made for improvement, if necessary.
5. The agency business continuity plan shall be tested annually, at a minimum. All critical applications shall be tested annually.

GUIDELINES

The following methods are recommended:

- Tabletop testing (walk-through of business recovery arrangements using example interruptions).
- Simulations (especially for post-incident / post-crisis management roles).
- Technical recovery testing.
- Testing recovery at an alternate site.
- Testing of hot-site arrangements, complete rehearsal (testing organization, personnel, equipment, facilities and processes).
- Updating of plan as necessary.

Additional steps that may be taken include the repetition of the test to validate any updated procedure(s) and the addition or removal of application backup procedures. Agency management should define, document, and approve what type of testing methodology to use.

ISO 27002 REFERENCES

14.1.03 Developing and implementing continuity plans including information security
14.1.04 Business continuity planning framework
14.1.05 Testing, maintaining and re-assessing business continuity plans

070104 Disaster Recovery and/or Restoration

Purpose: To restore the operability of the systems supporting critical business processes and return to normal agency operations as soon as possible.

POLICY

The agency is responsible for maintaining its ability to recover in the event of an outage. Agencies must ensure that business continuity and/or disaster recovery plans are developed, maintained, tested on a prescribed basis and subjected to a continual update and improvement process. Agencies shall conduct the following disaster recovery and/or restoration activities:

1. Define the agency's critical operating facilities and mission essential service(s) or function(s).

2. Define the resources (facilities, infrastructure, and essential systems) that support each mission critical service or function.
3. Define explicit test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration.

ISO 27002 REFERENCES
14.1.3 Developing and implementing continuity plans including information security

---

Section 02 Information Technology Risk Management Program

070101 Implementing a Risk Management Program

Purpose: To ensure that state agencies manage risks appropriately. Risk management includes the identification, analysis, and management of risks associated with an agency's business, information technology infrastructure, the information itself, and physical security to protect the state's information technology assets and vital business functions.

POLICY

1. The State of North Carolina recognizes that each agency, through its management, must implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to the state's citizens.
2. The risk management program must identify and classify risks and implement risk mitigation as appropriate.
3. The program must include the identification, classification, prioritization and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.
4. In general, "risk" is defined as a condition or action that may adversely affect the outcome of a planned activity. Some types of risk are as follows:
    - o Business Risk – The cost and/or lost revenue associated with an interruption to normal business operations.
    - o Organizational Risk – The direct or indirect loss resulting from one or more of the following:
        - Inadequate or failed internal processes
        - People
        - Systems
        - External events
    - o Information Technology Risk - The loss of an automated system, network or other critical information technology resource that would adversely affect business processes.
    - o Legal – Parameters established by legislative mandates, federal and state regulations, policy directives and executive orders that impact delivery of program services.
    - o Reputation – General estimation, by the public, on how state services are delivered (integrity, credibility, trust, customer satisfaction, image, media relations, political involvement.)
    - o Citizen Services - Program services mandated by charter, legislation, or policy that provides for the delivery of the state's business (education, human services, highways, law enforcement, health and safety, unemployment benefits, vital records, etc.)

GUIDELINES

Agencies are encouraged to select and use guidelines that support industry best practices for risk management relative to business continuity planning and security as appropriate. Some suggested guidelines are listed below.

Risk Management Program Activities:

Agency risk management programs at a minimum should focus on the following four types of activities:

- **Identification of Risks:** A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.
- **Analysis of Risks:** An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.
- **Mitigation Planning:** Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For moderate or high rated risks, mitigation plans should be developed, documented and assigned to managers. Plans should include assigned manager's signatures.
- **Tracking and Controlling Risks:** Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

Business Continuity Risk Management Processes:

For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt agency business. Agencies should identify the potential impacts in order to develop the strategies and justify the resources required to provide the appropriate level of continuity initiatives and programs.

Agencies should conduct business risk impact analysis activities that include the following:

- Define the agency's critical functions and services.
- Define the resources (technology, staff, and facilities) that support each critical function or service.
- Identify key relationships and interdependencies among the agency's critical resources, functions, and services.
- Estimate the decline in effectiveness over time of each critical function or service.
- Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact.
- Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
- Estimate financial losses over time of each critical function or service.
- Estimate tangible (non-financial) impacts over time of each critical function or service.
- Estimate intangible impacts over time of each critical function or service.
- Document any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority. (For example - tax filing dates, reporting deadlines, etc.)
- Identify any critical non-electronic media required to support the agency's critical functions or services.
- Identify any interim or workaround procedures that exist for the agency's critical functions or services.

Security Risk Process:

The focus of security risk management is an assessment of those security risk outcomes that may jeopardize agency assets and vital business functions or services. Agencies should identify those impacts in order to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical agency functions and services in the event of a security incident. The lack of appropriate security measures would jeopardize agency critical functions and services.

Security risk impact analysis activities include the following:

- Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for agency functions or services.
- Identification of confidential information stored in the agency's files and the potential for fraud, misuse, or other illegal activity.
- Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical agency functions and services.
- Identification of the processes used to monitor and report to management on whatever applications, tools and technologies the agency has implemented to adequately manage the risk as defined by the agency (*i.e.,* baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).
- Identification of the agency's IT Change Management and Vulnerability Assessment processes.
- Identification of what security mechanisms are in place to conceal agency data (Encryption, PKI, etc.).

For more information on implementing a risk management program, including the Risk Management Guide and the Risk Assessment Questionnaire, please refer to the Risk Management Services page found on the Enterprise Security and Risk Management Office (ESRMO) web site:

http://www.esrmo.scio.nc.gov/riskManagement/default.aspx

ISO 27002 REFERENCES

4.1 Assessing security risks
4.2 Treating security risks