Security Standard

Business Continuity Management

Information security aspects of business continuity management

Version: 1.0
Status: Approved: 06/22/11
Contact: Chief Information Security Officer

PURPOSE

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information stems or disasters and to ensure their timely resumption.

SCOPE

A business continuity management process will be implemented to minimize the impact on VCCS and recover from loss of information assets to an acceptable level through a combination of preventive and recovery controls. In accordance with ISO/IEC 27002:2005(E), § 14.1, the consequences of disasters, security failures, loss of service, and service availability will be implemented to ensure timely resumption of essential operations. This process will identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

Information security will be an integral part of the overall business continuity process, and other management processes within VCCS. Business continuity management will include controls to identify and reduce risks, and in addition to the general risks assessment process defined in ISO/IEC 27002:2005(E), § 4.1 and § 4.2 will limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.
APPLICABILITY

This Information Security Aspects of Business Continuity Management standard is applicable to the System Office and all Colleges.

STANDARD

The standards identified in this document define the minimum requirements for the controls that must be in place to provide business continuity management to VCCS. This document comprises the following topics:

- Including information security in the business continuity management process;
- Business continuity and risk assessment;
- Developing and implementing continuity plans including information security;
- Business continuity planning framework;
- Testing, maintaining and re-assessing business continuity plans

The following requirements must be addressed in the plan.


A managed process must be developed and maintained for business continuity throughout the VCCS that addresses the information security requirements needed for the System Office and College business continuity.

The process must bring together the following key elements of business continuity management:

a. Understanding the risks the System Office or College is facing in terms of likelihood and impact in time (Recovery Point Objective (RPO) and Recovery Time Objective (RTO), including identification and prioritization of critical business processes from the Business Impact Analysis process.

b. Identifying all System Office and College assets involved in critical business processes including all the necessary information to recovery from a disaster.

c. Understanding the impact which interruptions caused by information security incidents are likely to have on the System Office and College (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the System Office or College), and establishing the objectives of information processing facilities.

d. Considering the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management.
e. Identifying and considering the implementation of additional preventive and mitigating controls.

f. Identifying sufficient financial, organizational, technical, and environmental resources to address the identified information security requirements.

g. Ensuring the safety of personnel and the protection of information processing facilities and organizational property.

h. Formulating and documenting business continuity plans addressing information security requirements.

i. Regular testing and updating of the plans and processes.

j. Ensuring that the management of business continuity is incorporated in the System Office or College processes and structure; responsibility for the business continuity management process should be assigned at an appropriate level within the organization.

**Requirement:** (Business Continuity and Risk Assessment- §14.1.2)

The System Office and Colleges will identify events that may cause interruptions to the business processes, along with the probability and impact of such interruptions and their consequences for information security.

Information security aspects of business continuity must be based on identifying events (or sequence of events) that can cause interruptions to the System Office or College business processes, e.g. equipment failure, human errors, theft, fire, natural disasters and acts of terrorism. This must be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period.

Business continuity risk assessments must be carried out with full involvement from owners of business resources and processes. This assessment will consider all business processes and should not be limited to the information processing facilities, but must include the results specific to information security. It is important to link the different risk aspects together, to obtain a complete picture of the business continuity requirements of the System Office or College. The assessment must identify, quantify, and prioritize risks against criteria and objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

Depending on the results of the risk assessment, a business continuity strategy must be developed to determine the overall approach to business continuity. Once this strategy has been created, endorsement must be provided by management, and a plan created and endorsed to implement this strategy.

**Requirement:** (Developing and Implementing Continuity Plans Including Information Security- §14.1.3)

The System Office and Colleges will develop and implement plans to maintain or restore operations and ensure availability of information at the required level and in the required time frames following interruption to, or failure of, critical business processes.
The business continuity planning process should include the following:

- a. Identification and agreement of all responsibilities and business continuity procedures.
- b. Identification of the acceptable loss of information and services.
- c. Implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place.
- d. Operational procedures to follow pending completion of recovery and restoration.
- e. Documentation of agreed procedures and processes.
- f. Appropriate education of staff in the agreed procedures and processes, including crisis management.
- g. Testing and updating of the plans.

The planning process will focus on the required business objectives. The services and resources facilitating this must be identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities.

The System Office and College business continuity plans must address vulnerabilities and therefore may contain sensitive information that needs to be appropriately protected. Copies of business continuity plans must be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. The System Office and College will ensure copies of the business continuity plans are up-to-date and protected with the same level of security as applied at the main site. Other material necessary to execute the continuity plans should also be stored at the remote location. If alternative temporary locations are used, the level of implemented security controls at these locations should be equivalent to the main site.

It should be noted that crisis management plans and activities may be different from business continuity management; i.e. a crisis may occur that can be accommodated by normal management procedures.

**Requirement: (Business Continuity Framework- §14.1.4)**

A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

Each business continuity plan should describe the approach for continuity, for example the approach to ensure information or information system availability and security. Each plan should also specify the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures, e.g. evacuation plans or fallback arrangements, will be amended as appropriate. Procedures will be included within the System Office and College change management program to ensure that business continuity matters are always addressed appropriately.
The System Office and Colleges will address the identified information security requirements and will consider the following:

a. The conditions for activating the plans which describe the process to be followed (e.g. how to assess the situation, who is to be involved) before each plan is activated.
b. Emergency procedures, which describe the actions to be taken following an incident, which jeopardizes business operations.
c. Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales.
d. Temporary operational procedures to follow pending completion of recovery and restoration.
e. Resumption procedures which describe the actions to be taken to return to normal business operations.
f. A maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan.
g. Awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective.
h. The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
i. The critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

Consideration and consistency, as applicable, should be given to the Virginia Department of Emergency Management’s requirements for continuity of operations planning. Public colleges and universities are subject to the provisions of Executive Order 44, which directs “all executive branch agencies, including institutions of higher education, to include emergency preparedness planning, training and promotion as a core component of their mission.” And further, to “create or update Continuity of Operations Plans to conform to the template produced by VDEM, and utilize the resources available from VDEM for creating or updating Continuity of Operations Plans.” Therefore, the System Office and College’s should refer to the Virginia Department of Emergency Management manual as needed in conjunction with this Standard.

VDEM Templates may be found at:

Requirement: (Testing, Maintaining, and Reassessing Business Continuity Plans- §14.1.5)

The System Office and Colleges will test business plans periodically to ensure that they are up to date and effective. “Periodically” must be defined in the System Office or College security plan but should be as a minimum on an annual basis.

Business continuity plan tests will ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.
The test schedule for business continuity plan(s) will indicate how and when each element of the plan should be tested. Each element of the plan(s) will be tested frequently. A variety of techniques may be used in order to provide assurance that the plan(s) will operate in real life.

These may include:

a. Table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions).
b. Simulations (particularly for training people in their post-incident/crisis management roles).
c. Technical recovery testing (ensuring information systems can be restored effectively).
d. Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site).
e. Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment).
f. Complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions).

The results of tests must be recorded and actions taken to improve the plans, where necessary.

Responsibility must be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements not yet reflected in the business continuity plans must be followed by an appropriate update of the plan. This formal change control process will ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

Examples of changes where updating of business continuity plans may be considered are acquisition of new equipment, upgrading of systems and changes in:

a. Personnel.
b. Addresses or telephone numbers.
c. Business strategy.
d. Location, facilities, and resources.
e. Legislation.
f. Contractors, suppliers, and key customers.
g. Processes or new or withdrawn ones.
h. Risk (operational and financial).

Referenced Standards:

In meeting this requirement, VCCS has adopted and implemented the following policies and procedures:

- VCCS IT Security Standard 7-2 Information classification
- VCCS IT Security Standard 7-1 Responsibility for Assets
• Business Impact Analysis Standard
• VCCS Business Impact Analysis Template Rev 1 09SEPT10
• Continuity of Operations Planning
• IT Disaster Recovery Planning
• IT System and Data Backup and Restoration

Review and Approval:

Reviewed By: [Vicky Carwile, ISO, JTCC]
Reviewed Date: 06/22/11
Next Scheduled Review: 06/21/12