

FCA Essential Practices for Information Technology

Based on Industry Standards and FFIEC Examination Guidance

Table of Contents

	Page
Business Continuity	
Introduction	BC - 1
Examination Objectives.....	BC - 1
Examination Procedures	BC - 1
<u>Essential Practice Statements</u>	BC - 2
Risk Assessment (Business Impact Analysis)	BC - 2
Business Continuity Plan	BC - 2
Defined Recovery Process.....	BC - 3
Training	BC - 3
Testing.....	BC - 3
Backup and Offsite Storage	BC - 4
Insurance.....	BC - 5

Business Continuity

Introduction:

All institutions are required to develop, maintain, and test a business continuity plan. These plans enable mission critical systems and functions to be resumed in the event of a disruption. The planning process evaluates an institution's various departments, business units, or functions to identify critical information systems and business functions. A well researched, current, and comprehensive continuity plan will greatly aid management in selecting reasonable cost solutions in highly stressful disaster situations. Effective business continuity planning should:

- Minimize disruptions of service to the institution and its customers;
- Ensure timely resumption of operations; and
- Limit financial loss.

Examination Objectives:

Determine if the board and management have established and maintained effective business continuity processes. This is accomplished through the following examination objectives:

- **Board and Management Oversight** – Evaluate board and management oversight of business continuity activities (e.g. planning, management reporting, policies and procedures, audit, etc.).
- **Plan Assessment** – Assess the effectiveness of the institution's business continuity planning process (development, maintenance, testing, and training).

Examination Procedures:

Examination activities should be based on the criticality and complexity of the business functions present at the institution. The examination should begin with a review of audit activities and the risk assessment for business continuity. At a minimum, the **Essential Practices** for Business Continuity should be clearly documented and functioning within the internal control environment. More in-depth examination procedures (such as those found in the [FFIEC Business Continuity Planning Booklet](#)) should be evaluated and incorporated into the examination scope as an institution's size, risk, and complexity increases.

Business Continuity

Element		
Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Risk Assessment (Business Impact Analysis)		
<p>Conduct a risk assessment to develop response strategies, which:</p> <ul style="list-style-type: none"> • Identify events and likelihood of those events that could cause interruptions to business processes and services; • Assess impacts from loss of information and services from both internal and external sources; • Assess the criticality of all business areas; and • Identify and prioritize critical services, operations, and personnel provided by internal and external service providers. <p><u>Reason:</u> <i>Prior to developing the business continuity plan, the criticality of information resources (applications, data, networks, system software, facilities) that support an organization's critical business process must be determined. With management support, both information systems processing and end user personnel should participate in this analysis.</i></p>	<p>ISO/IEC 27002:2005, Section 14.1.2, "Business Continuity and Risk Assessment."</p>	<p>Business Continuity Planning Booklet (Mar. 2003) pp. 6, 8-9.</p> <p>Management Booklet (Jun. 2004) p. 10.</p> <p>Information Security Booklet (Jul. 2006) p. 78 - 79.</p>
Business Continuity Plan		
<p>Establish and maintain an organization-wide business continuity plan that addresses:</p> <ul style="list-style-type: none"> • Critical services and operations provided by internal and external sources; • Resources needed to support the critical functions; • Steps to be taken in a business disruption; • Coordination with outside parties where necessary; • Board approval and annual review; • Defined Business Continuity and Recovery Teams; • Responsibility for Disaster Declaration; • Notification Tree (Employees, Customers, FCA, vendors, local authorities, etc.); and • Testing process and schedule. <p><u>Reason:</u> <i>A Business Continuity Plan provides the vital preplanned framework for initiating recovery operations immediately following a disruption. It also provides guidance for damage assessment and the planned actions that must be taken to resume critical services and restore full business operations with minimum delay.</i></p>	<p>ISO/IEC 27002:2005, Section 14.1.4, "Business Continuity Planning Framework."</p> <p>FCA Informational Memorandums, "Reassessment of Business Continuity Plan" (Oct. 18, 2001); "Rescission of Information Systems Bulletin No. 89-2" (April 5, 2000).</p>	<p>Business Continuity Planning Booklet (Mar. 2003) pp. 10-11 and Appendix E.</p> <p>FedLine Booklet (Aug. 2003), p. 11.</p> <p>Outsourcing Technology Services Booklet (Jun. 2004), pp. 25-28.</p>

Business Continuity

Element		
Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Defined Recovery Process		
<p>Establish IT recovery strategies and procedures for mission critical systems, which:</p> <ul style="list-style-type: none"> • Prioritize system recovery; • Define responsibilities; • Establish expectations for recovery time; and • Allow flexibility by providing alternate solutions when necessary. <p><i>Reason:</i> <i>Recovery strategies are necessary to limit the consequence of damaging events and ensure the timely resumption of critical operations. There are various strategies for recovering critical information resources. The appropriate strategy is the one that is most efficient and effective based on the relative risk level identified in the business impact analysis. This strategy is often dictated by the defined recovery timeline and expectations.</i></p>	<p>ISO/IEC 27002:205, Section 14.1.3, “Developing and Implementing Continuity Plans Including Information Security”; and Section 14.1.4, “Business Continuity Framework.”</p>	<p>Business Continuity Planning Booklet (Mar 2003) pp. 15-20.</p>
Training		
<p>Train personnel involved in executing the Business Continuity Plan and recovery strategies. Review and update training needs as changes in plans occur—at least annually.</p> <p><i>Reason:</i> <i>Regular training should be conducted in the agreed emergency procedures and processes, including crisis management. This should ensure that the execution of the Business Continuity Plan is effective when a disruption occurs. It is also important that an effective cross training program be in place to ensure that vital functions can be effectively performed if key personnel are unavailable at the time of a disruption.</i></p>	<p>ISO/IEC 27002:2005, Section 14.1.4, “Business Continuity Framework.”</p>	<p>Business Continuity Planning Booklet (Mar 2003) pp. 13-14.</p> <p>Information Security Booklet (Jul. 2006) p. 78 - 79.</p>
Testing		
<p>Test the plan(s) at least annually. The testing process includes:</p> <ul style="list-style-type: none"> • Scope, goals and objectives commensurate with defined risk; • Reporting to management/board; • Corrective action(s); and • Plan updates to incorporate test results. 	<p>ISOIEC 27002:205, Section 14.1.5, “Testing, Maintaining, and Re-assessing Business Continuity Plans.”</p>	<p>Business Continuity Planning Booklet (Mar. 2003) pp. 15-21.</p> <p>FedLine Booklet (Aug. 2003), pp. 11-12.</p>

Business Continuity

Element		
Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
<p>Based on the risk assessment, consider the following types of testing methodologies:</p> <ul style="list-style-type: none"> • Desk review; • Simulation; • Technical recovery; • Testing at alternative site; and • Comprehensive Business Continuity Plan Test (include all critical functional areas). <p><u>Reason:</u> <i>The Business Continuity Plan should be tested using a fully developed test scenario, a simulated disruption, planned monitoring of results, and appraisal of the entire process with plan revisions, as necessary. Since emergencies do not happen often, periodic testing of the plan is needed to ensure that it is still adequate and that there are skilled personnel to implement it. Tests also serve as training in emergency, backup, and recovery procedures. One of the purposes of the business continuity test is to determine how well the plan works or which portions of the plan need improvement.</i></p>		
Backup and Offsite Storage		
<p>Develop and implement backup, storage, and rotation procedures of critical systems including hardware, software, and documents.</p> <p>Consider the following in the backup and storage process:</p> <ul style="list-style-type: none"> • Location of backup media (in-house and offsite); • Physical and data security at the backup site; • Backup routines for corporate and branches; and • Current list of personnel authorized to access the off-site storage location. <p><u>Reason:</u> <i>To ensure that critical business activities are not interrupted, secondary storage media (tape reels, tape cartridges, removable hard disk or cassettes) are used to store and backup programs and associated data. This media is stored offsite to ensure that it will be available for restoration if the primary business location is inaccessible. The location of and controls over the offsite facility are important to ensure the security of sensitive information.</i></p>	<p>ISO/IEC 27002:2005, Section 15.1.3, "Protection of Organizational Records."</p>	<p>Business Continuity Planning Booklet (Mar. 2003) pp. 12-13;</p> <p>Appendix E, E4-7.</p> <p>FedLine Booklet (Aug. 2003), pp. 5-6, 8, 12.</p> <p>Operations Booklet (Jul. 2004), pp. 29-30.</p>

Business Continuity

Element		
Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Insurance		
<p>Obtain insurance coverage to guard against risk of loss that exceeds the board and organization’s risk tolerance.</p> <p><i>Reason:</i> <i>Insurance is an effective method to transfer risk from the institution to insurance companies. It guards against loss from risk that cannot be completely prevented. Generally, coverage is acquired for events with little probability of occurring, but with significant potential for financial loss or other disastrous consequences. Insurance should cover physical losses such as building, equipment, software, etc., and also the costs of business disruption.</i></p>	<p>ISO/IEC 27002:2005, Section 14.1.1, “Including Information Security in Business Continuity Management Process.”</p>	<p>Information Security Booklet (Jul. 2006), pp. 79-80.</p> <p>Business Continuity Planning Booklet (Mar. 2003) p. 14.</p>