Office of Inspector General

September 25, 2003
Audit Report No. 03-042

Business Continuity Planning at FDIC-Supervised Institutions

OFFICE OF INSPECTOR GENERAL
DELIVERING QUALITY TIMELINESS VALUE
OFFICE OF AUDITS

TABLE OF CONTENTS

DATE: September 25, 2003

MEMORANDUM TO: Michael J. Zamorski
Director, Division of Supervision and Consumer Protection

FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: Final Report Entitled *Business Continuity Planning at FDIC-Supervised Institutions*
(Evaluation Report No. 03-042)

This report presents the results of our evaluation of business continuity planning at Federal Deposit Insurance Corporation (FDIC)-supervised institutions. Financial institutions play a crucial role in the U.S. economy. Therefore, business operations of financial institutions must be resilient, and the effects of disruptions in service must be minimized in order to maintain public trust and confidence in our financial system.

A business continuity plan (BCP) is a comprehensive, written plan developed to maintain or resume operations, including service to customers, in the event of a disruption. Effective BCPs are building blocks for ensuring the safety and soundness of the nation's financial system. The objectives of a BCP are to minimize financial loss to the institution, continue to serve customers and financial market participants, and mitigate the negative effects disruptions can have on an institution's strategic plans, reputation, operations, liquidity, credit quality, market position, and ability to remain in compliance with applicable laws and regulations.

The objective of our evaluation was to determine the adequacy of the Division of Supervision and Consumer Protection's (DSC) approach to assessing BCPs at FDIC-supervised institutions. See Appendix I for details of our objective, scope, and methodology. Appendix II contains a glossary of terms used in our report.

BACKGROUND

Business continuity planning is important for all federally insured institutions regardless of size and complexity of the institution. According to the Federal Financial Institutions Examination Council (FFIEC), financial institutions that play significant roles in critical financial markets are those that participate in sufficient volume or value such that their failure to perform critical

activities by the end of the business day could present systemic risk. Financial institutions not directly participating in critical financial markets, but nonetheless performing financial services or supporting financial activities deemed critical to regional or national financial sectors, are also expected to establish BCPs and recovery capabilities commensurate with their role. Smaller, less complex institutions generally do not need the same level of planning, but are expected to fulfill their responsibility by developing appropriate BCPs and periodically conducting adequate tests of their readiness. The key concepts of business continuity planning should be considered in the development of every BCP, but the degree to which they are actually implemented should be relative to the risks associated with the particular entity and its size and complexity.

The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the five federal financial regulatory agencies and to make recommendations to promote uniformity in the supervision of financial institutions.

As shown in Table 1, small- and medium-size financial institutions account for 99 percent of all FDIC-insured financial institutions[1] and 31 percent of all assets held in insured financial institutions. The FDIC has primary supervisory responsibility for 5,446, or 59 percent of all small- to medium-size financial institutions, with $1.3 trillion in assets, or 47 percent of all assets held by all insured financial institutions.

Table 1: FDIC-Supervised Institutions Statistics

Category	All FDIC-Insured Institutions		FDIC-Supervised Institutions	
	Number	Percent of Total	Number	Percent of FDIC-Supervised to All Insured Institutions
Large	109	1%	19	17%
Small and Medium	9,205	99%	5,446	59%
Total	9,314	100%	5,465	59%
Category	**All FDIC-Insured Institutions**		**FDIC-Supervised Institutions**	
	Total Assets (millions)	**Percent of Total**	**Total Assets (millions)**	**Percent of FDIC-Supervised to All Insured Institutions**
Large	$5,940,053	69%	$434,353	7%
Small and Medium	$2,665,991	31%	$1,257,742	47%
Total	$8,606,044	100%	$1,692,095	20%

Source: FDIC Statistics on Banking, March 30, 2003.

The FDIC supervises the majority of small- and medium-size institutions and plays a critical role, through its supervisory examination responsibilities, in promoting safe and sound

[1] Small- to medium-size institutions are defined as having less than $10 billion in total assets.

management practices, which include assessing whether these institutions are prepared to respond to events, such as natural disasters, malicious activities, and/or technical disasters that could cause a disruption to business operations.

Business Continuity Planning: An Industry Perspective

> ***"In enterprise-wide business continuity planning an institution considers every critical aspect of its business in creating a plan for how it will respond to disruptions. It is not limited to the restoration of information technology systems and services, or data maintained in electronic form, since such actions, by themselves, cannot always put an institution back in business."***
>
> ***-- FFIEC Business Continuity Booklet***

The Year 2000 problem was technical in nature and generated much guidance from the federal government as well as the private sector on how organizations should take steps to ensure that their core business processes would not be disrupted in the event that year-date data could not be processed for years beyond 2000. After the September 11, 2001 terrorist attacks, the federal government and private sector organizations recognized that although technology was the primary basis for concern for Year 2000, an enterprise-wide, process-oriented approach that considers technology, business processes, testing, and communication strategies is critical to building a viable BCP. According to the General Accounting Office,[2] the terrorist attacks revealed limitations in many financial market participants' BCPs for addressing such a widespread disaster. These factors included a lack of backup facilities that were sufficiently geographically dispersed or comprehensive enough to conduct all critical operations, unanticipated loss of telecommunications service, and difficulties in locating staff and transporting them to new facilities.

Information security consultants, business continuity consultants, and the FFIEC agree that business continuity planning should be conducted on an enterprise-wide basis. Without a BCP that considers every critical business unit, including personnel, physical workspace, and similar issues, an institution may not be able to resume servicing its customers at acceptable levels.

Business continuity planning is the process of proactively developing, documenting, and integrating processes and procedures and enabling technologies that will allow an organization to respond to a disruption in such a manner that critical business functions will continue with minimal, if any, interruption or significant changes until such time as normal facilities are restored. Industry consultants agree that business continuity planning takes into account the recovery of the business, not just information technology (IT) systems. Conversely, disaster recovery planning is an IT function. A disaster recovery plan documents the actions that will be taken to restore computer processing, applications, telecommunications services, and data after a disruption or disaster event to prevent, or at least minimize, the relative impacts on a business. Business continuity planning focuses on avoiding or mitigating the impact of a risk; whereas disaster recovery focuses on restoring the organization to business as usual after a disruption occurs.

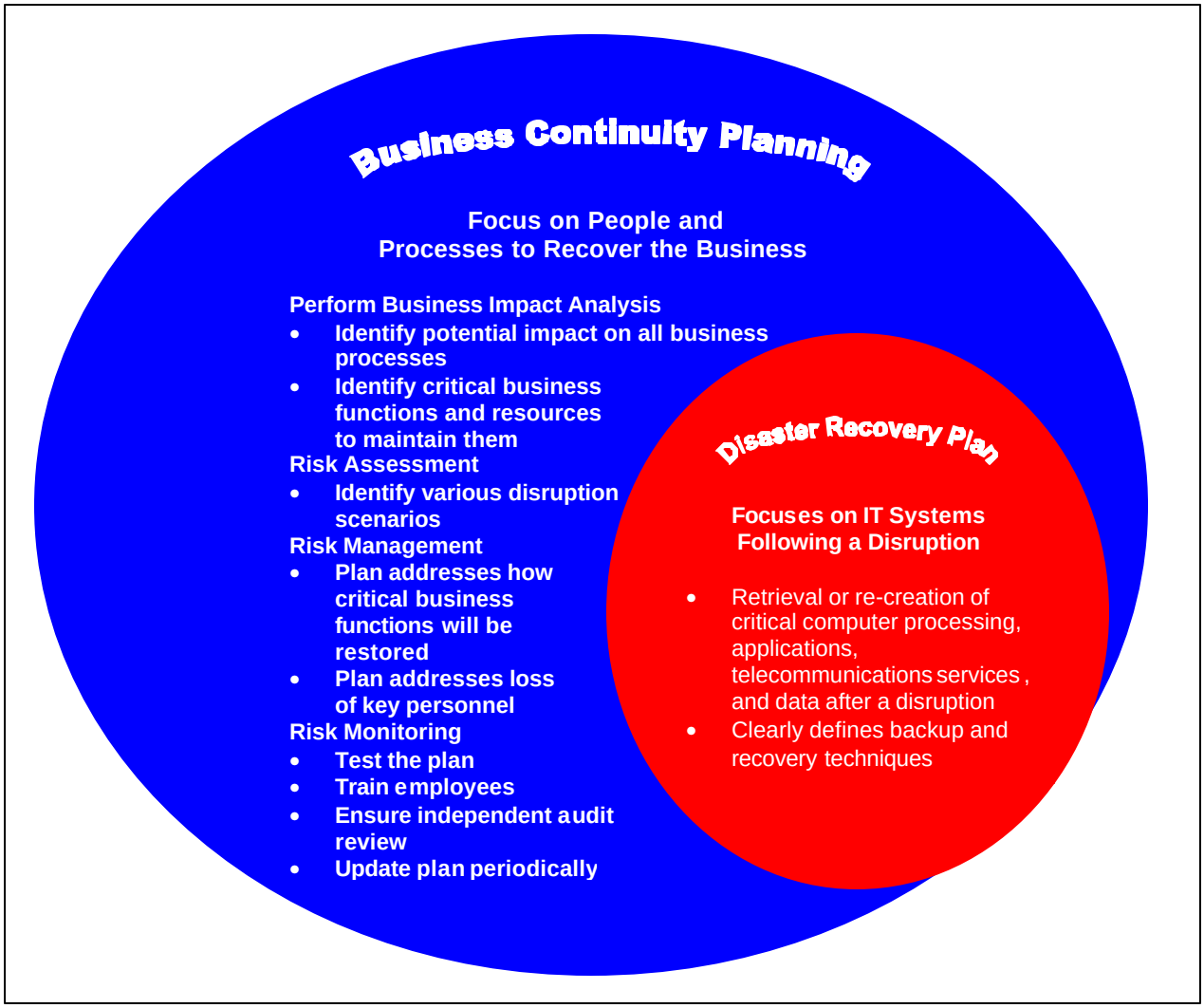
---

[2] GAO-03-414, *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, dated February 2003.

The FFIEC's *Business Continuity Planning* booklet[3] discusses four basic components to business continuity planning: the business impact analysis, risk assessment, risk management, and risk monitoring. This planning framework is usable regardless of the size of the financial institution. Business continuity planning encompasses the full restoration process of all business operations, including IT, and is a function and responsibility of the entire organization.

Disaster recovery planning enables business continuity planning and, as shown below, is a critical component of the business continuity planning process.

Business Continuity and Disaster Recovery



Source: OIG Analysis of Industry Sources.

[3] In May 2003, the FFIEC issued revised guidance for examiners and financial institutions on business continuity planning. The guidance is contained in the booklet, entitled, *Business Continuity Planning* (BCP Booklet). The BCP Booklet provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services.

DSC's Approach to Examining Business Continuity Planning at FDIC-Supervised Institutions

DSC reviews BCP as part of its IT examinations of FDIC-supervised institutions and its examinations of organizations that provide IT services to FDIC-supervised institutions. DSC revised its IT examination approach in September 2002 as a result of an initiative undertaken to improve the effectiveness and efficiency of IT examinations of the least complex financial institutions. As part of its revision, DSC implemented new IT examination guidance and two new related work programs that were designed toward a more risk-focused IT examination approach:

- The IT-MERIT (Maximum Efficiency, Risk-Focused, Institution Targeted) Procedures were developed for examiners conducting technology risk reviews at FDIC-supervised financial institutions with the least technology risk.

- The IT General Work Program was developed for examiners conducting technology risk reviews at FDIC-supervised financial institutions with low to moderate technology risk.

For financial institutions with greater technology risk, examiners are expected to continue using guidance and work programs issued by the FFIEC (FFIEC Work Programs) that are found in the 1996 FFIEC Information Systems Examination Handbook (Handbook). The FFIEC is updating the Handbook to address significant changes in technology since 1996 and to incorporate a more risk-based examination approach. The FFIEC's updates are being issued in separate booklets that will ultimately replace all chapters of the Handbook and comprise the new FFIEC Information Technology Examination Handbook. The BCP Booklet is one in a series of updates being made to the Handbook. The BCP Booklet rescinded and replaced Chapter 10, *Corporate Contingency Planning*, of the Handbook.

To address the different levels of technology risk at financial institutions, DSC defined four "types" of financial institutions based on their technology risk profile and implemented the Technology Profile Script (TPS) to assist in determining an institution's technology risk profile type. Before beginning an IT examination, DSC responds to questions in the TPS based on DSC's review of an institution's core processing systems, networks, electronic banking (E-Banking) products, and other technology components. The responses to the TPS yield a numeric score that correlates to the assigned type of the institution. This measurement of technological complexity is intended to allow examiners to focus examination efforts on high-risk institutions. The determination of an institution's type is the key factor in determining which examination procedures (IT MERIT, IT General Work Program, or FFIEC Work Programs) will be used. Further, managers may use the TPS to allocate examination resources, such as matching examiner skills to the complexity of the institution, or determining training needs. Table 2 shows the examination procedures to be used for each technology type.

Table 2: Technology Risk Profile and Applicable Examination Procedures

TPS Type	Description	IT Examination Procedures Used
Type I	Limited Networking and E-Banking; No in-house programming or core processing; Minimal external threats; Primary risks: Core banking system or vendor management; Does not have an examination history of less than satisfactory ratings.	IT-MERIT Procedures
Type II	Same as Type I, except that the institution has an examination history of less than satisfactory ratings.	IT General Work Program
Type III	Fully integrated networking; Increased external threats from E-banking and Internet connections; Increased operational risks from limited programming activities or servicing responsibilities.	IT General Work Program, supplemented with FFIEC Work Programs, as needed
Type IV	Reliance upon networks and other communication systems as a critical element of operations; Networking and Internet connectivity relied upon as critical communications medium; Risk of compromise or access to critical systems resulting from Internet and other wide-area network connections, is present; Complex technology.	FFIEC Work Programs

Source: DSC Examination Guidance, September 2002.

RESULTS OF EVALUATION

DSC has actively promoted sound business continuity planning practices in financial institutions. Through its participation in the FFIEC, DSC was the primary author of interagency guidance on business continuity planning. This guidance organizes key elements of business continuity planning into an easily readable and usable format that will assist bankers in developing, and examiners in assessing, BCPs at financial institutions. DSC also examines the services performed for FDIC-supervised institutions by technology service providers (TSP).[4] These examinations include an assessment of the TSP's business continuity planning. Through its participation in the Financial and Banking Information Infrastructure Committee (FBIIC),[5] DSC has worked to assess the vulnerabilities and risks facing the banking industry. DSC has also incorporated key elements of business continuity planning into the curriculum of its in-house training program for examiners. Further, for a sample of IT examinations we reviewed, we concluded that DSC examiners generally used the appropriate work programs and adequately documented the procedures performed and the conclusions reached, in accordance with DSC's approach to IT examinations **(See Finding A: DSC Actively Participates in Efforts to Address Business Continuity Planning)**.

[4] TSPs are third-party companies that provide information technology support to financial institutions.
[5] The FBIIC was created by Executive Order 13231. The FBIIC is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system. The Department of the Treasury's Assistant Secretary for Financial Institutions chairs the committee.

DSC's newly implemented examination work programs, however, do not always address certain key elements that should be included in every BCP, regardless of the size and complexity of the financial institution being examined. Specifically, the IT MERIT Procedures and IT General Work Program, used for IT examinations of Type I, Type II, or Type III institutions, focus largely on disaster recovery planning (an IT function) as opposed to enterprise-wide business continuity planning (overall business concerns, such as the people, management succession, and backup sites). As a result, DSC supervisory examinations may not be adequately assessing whether most FDIC-supervised institutions would be able to effectively respond to a disruption and maintain critical business functions until those functions are fully restored **(See Finding B: DSC's Examination Approach to Business Continuity Planning)**.

FINDINGS AND RECOMMENDATION

FINDING A: DSC ACTIVELY PARTICIPATES IN EFFORTS TO ADDRESS BUSINESS CONTINUITY PLANNING

DSC has actively promoted sound business continuity planning practices in financial institutions through its involvement in the FFIEC and FBIIC and through its in-house examiner training program. Further, we determined that, generally, DSC's assessments of BCPs at FDIC-supervised institutions and TSPs were conducted and adequately documented in accordance with established guidelines.

DSC Participation in the FFIEC

Members of DSC's E-Banking Branch, through their affiliation with the FFIEC's Task Force on Supervision, were the primary authors of the BCP Booklet. DSC's approach to IT examinations requires examiners to consider using FFIEC Work Programs for IT examinations of Type III and Type IV institutions. Therefore, with the release of the FFIEC updated guidance, the BCP Booklet has become the examiner's primary source of guidance in assessing business continuity planning at these financial institutions and TSPs.

In July 2002, DSC circulated the draft BCP booklet to examiners for field testing in a coordinated effort with other FFIEC agencies. DSC examiners were asked to incorporate the work steps into their IT examinations conducted through August 2002 and to provide feedback on the following:

- Relevance and accuracy of subject
- Definitions of BCP concepts
- Length of booklet
- Clarity of material
- Adequacy of information to assess risk
- Length of time to complete steps
- Helpfulness in setting exam scope
- Necessity of training

DSC incorporated the feedback into the final BCP booklet, which was issued in May 2003. As discussed later in our report, we found that the BCP booklet addresses all of the key elements of

business continuity planning that we identified from our research of industry sources. The BCP booklet also organizes the elements into an easily readable and usable work program format that will assist bankers and examiners in developing and assessing, respectively, BCPs at financial institutions.

Also through its membership in the FFIEC, DSC participates in various other non-bank IT examinations. Two noteworthy reviews are the TSP and Multi-Regional Data Processing Servicers (MDPS) Examinations. The FFIEC agencies examine TSPs to identify existing or potential risks that could adversely affect serviced financial institutions. When a large TSP is regional or national in scope and services more than one class of financial institutions, the FFIEC evaluates the TSP for selection into the MDPS program. The FFIEC agencies examine MDPS organizations because these entities pose a systemic risk to the banking system should one or more have operational or financial problems or fail. When conducting these IT examinations, examiners focus on the underlying risk issues that are common to all IT activities, including the availability of services that the TSP or MDPS organization is providing to the financial institution. During these examinations, the effectiveness of the organization's business continuity program and adherence to service-level agreements is reviewed. Therefore, DSC's participation in these examinations helps to ensure that key service providers of FDIC-supervised institutions are maintaining adequate BCPs for key processes that will facilitate the serviced institutions' ability to provide critical services to their customers in the event of a disruption.

DSC Participation in the Financial and Banking Information Infrastructure Committee

DSC officials also participate in various working groups within the FBIIC. The FBIIC has taken actions designed to assess potential systemic vulnerabilities of the U.S. financial system to disruptions caused by electronic or physical destruction of critical sector assets. Understanding these systemic vulnerabilities will enhance a financial institution's ability to appropriately identify how its business processes and customers would be affected by such disruptions, which is a key element in developing a BCP.

One ongoing FBIIC initiative is the development of a vulnerability assessment that will assess the resilience of the retail banking system in the post-September 11 environment. Retail banking services are services offered by or through federally insured depository institutions, such as most FDIC-supervised institutions, to individuals and households. The objective of the vulnerability assessment is to determine whether key single points of failure exist that would have a material effect on the retail financial system. Although these initiatives are led by the Department of the Treasury, DSC's role is to meet periodically with the members of the Vulnerability Assessment Working Group and to review and provide comments on the draft report. The vulnerability assessment for the retail banking system is slated to be finalized in the fall of 2003.

DSC also participated in FBIIC's Telecommunications Working Group, which was responsible for developing two programs, described below, to enhance communication between financial institution regulators and sponsored affiliated institutions in the event that important telecommunication services are disrupted:

- Government Emergency Telecommunications Service (GETS) Card Program, which allows priority of telecommunication services to qualified users; and

- Telecommunications Service Priority Program, which allows sponsored institutions priority service restoration or provisioning of telecommunication circuits.

DSC's role in these programs has been to review applications for sponsorship submitted by FDIC-supervised institutions and to make recommendations to the Department of the Treasury for sponsorship, in accordance with policy established by the FBIIC.

DSC officials are also members of other FBIIC working groups, including the Communications Working Group. The Communications Working Group is responsible for the FBIIC's Web site and the speaker's bureau and outreach and for communicating U.S. Department of Homeland Security information to the banking sector.

Examiner Training Stresses Enterprise-Wide Business Continuity Planning

The FDIC's Corporate University, School of Supervision and Consumer Protection, offers technical training programs for risk management and compliance. One of the risk management training courses is the *Information Technology Exam Course* (ITEC). This training program provides an opportunity for participants to take part in a series of case studies designed to reinforce concepts and techniques that will further an examiner's ability to assess a financial institution's technology risk through use of the IT General Work Program and other IT examination tools. The course includes a segment on the evaluation of the adequacy of business continuity planning/disaster recovery planning processes. The course content adequately addressed the concepts of enterprise-wide business continuity planning, including concepts contained in the FFIEC's BCP Booklet. Therefore, DSC provides training to its IT examiners that stresses the importance of enterprise-wide business continuity planning at financial institutions and the examination procedures that should be applied in assessing an institution's business continuity planning.

IT Examiner's Implementation of DSC's Approach to Business Continuity Planning at FDIC-Supervised Institutions

We reviewed IT examination workpapers for 10 judgmentally selected IT examinations. The purpose of our review was to determine whether the examiners' reviews of BCPs at FDIC-supervised institutions were consistent with DSC's IT examination approach that was implemented in September 2002. Based on our review of examination workpapers, we concluded that DSC examiners used the TPS to determine the technology risk profile type of the institution and used the appropriate work program(s) to complete the examination. We did not test the accuracy of the responses to the TPS because those tests would have been outside the scope of this evaluation.

Although there is no written requirement for DSC examiners to review business continuity planning at each IT exam, senior management at the regional offices we visited told us that they require their examiners to review BCPs as part of each IT exam. For each of the 10 examinations reviewed, we were able to determine from the examination workpapers: the procedures performed by the examiner, the conclusions reached, and any matters that warranted discussion in the Report on Examination regarding business continuity planning. Therefore, we are reasonably assured that DSC examiners are conducting their reviews of business continuity planning in accordance with DSC's established guidance.

FINDING B: DSC'S EXAMINATION APPROACH TO BUSINESS CONTINUITY PLANNING

DSC's examination approach to assessing business continuity planning at FDIC-supervised institutions does not address certain key elements that should be included in every BCP, regardless of the size and complexity of the financial institution. DSC reviews business continuity planning at FDIC-supervised institutions as part of its IT examination program. The IT MERIT Procedures, used for IT examinations of Type I institutions, and the IT General Work Program, used for IT examinations of Types II and III institutions, focus on disaster recovery planning not business continuity planning. DSC was aware of the FFIEC's efforts to develop a BCP Booklet at the time that the IT MERIT and IT General Work procedures were being developed. However, DSC focused solely on developing procedures for IT-related functions because the procedures were for IT examinations. As a result, DSC's supervisory examinations may not be adequately assessing whether most FDIC-supervised institutions would be able to effectively respond to a disruption and maintain critical business functions until those functions are fully restored.

Key Elements of Business Continuity Planning

We researched business continuity planning guidance from a variety of industry sources. These sources included a cross-section of government, private consultants, and federal financial regulatory agencies that identified common elements of business continuity planning that should be addressed by a business entity, regardless of its size and complexity. In July 2003, we provided 14 common business continuity planning elements to DSC management officials in the Washington and Regional Offices for their review and comment. DSC officials agreed that the 14 elements should be included in a financial institution's BCP and that the degree to which they are implemented is determined by the risks associated with the particular entity and its size and complexity. Table 3 identifies the business continuity planning elements, the industry sources, and whether the concepts were included in the published guidance.

Table 3: Common BCP Elements

Common Elements of Business Continuity Planning	FISCAM[a]	Interagency Paper[b]	FEMA[c]	NIST[d]	ISACA[e]	FFIEC[f]
Board of Directors and senior management are involved in and committed to business continuity planning.	X	X	X	X	X	X
Plan is documented and made policy.	**X**	**X**	**X**	**X**	**X**	**X**
Addresses various business threat/ disruption scenarios.	X	X	X		X	X
Business Impact Analysis is performed on an enterprise-wide basis. All critical business functions/assets are identified and prioritized, not just technology function/assets.	**X**	**X**	**X**	**X**	**X**	**X**
Is updated as changes in technology/business processes warrant.	X			X	X	X
Provides for alternate telecommunication services/interoperable communications.	**X**	**X**	**X**		**X**	**X**
Provides for alternative processing sites located an appropriate distance away.	X	X	X	X	X	X
Critical data files are backed up appropriately and stored off-site an appropriate distance away from the data processing facility.	**X**	**X**	**X**	**X**	**X**	**X**
Includes a plan for succession and/or loss or inaccessibility of key staff.	X	X	X	X	X	X
Staff is aware of responsibilities under the plan and is adequately trained.	**X**		**X**	**X**	**X**	**X**
Key contractors/service providers are identified; backup arrangements are in contract.	X			X	X	X
Insurance coverage adequately mitigates risk.					**X**	**X**
Plan is routinely tested, results are analyzed, and corrective actions are taken.	X	X	X	X	X	X
BCP and test results are subject to independent audit.					**X**	**X**

Source: OIG Analysis.

Notes:

[a] The General Accounting Office, Accounting and Information Management Division issued, *"Federal Information System Controls Audit Manual"* (FISCAM) in January 1999.

[b] "*Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*" was issued by the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission in April 2003.

[c] Federal Emergency Management Agency, "*Federal Preparedness Circular 65*," July 26, 1999.

[d] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, Special Publication 800-34, *"Contingency Planning Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology,"* dated June 2002.

[e] Information Systems Audit and Control Association (ISACA), *"Certified Information Systems Auditor Review Manual."*

[f] "FFIEC Business Continuity Handbook" issued in May 2003.

We concluded that DSC's approach to reviewing BCPs at FDIC-supervised institutions does not always incorporate the more enterprise-wide elements of business continuity planning and instead focuses on the IT aspects of disaster recovery planning. As Table 4 shows, our evaluation of DSC's approach to assessing business continuity planning indicates that 7 of the 14 BCP common elements identified in Table 3 either are not adequately addressed in the IT MERIT and IT General Work Program procedures or are not addressed at all.

Table 4: BCP Common Elements That Need To Be Addressed in DSC's Approach

BCP Common Elements	IT Merit Procedures	IT General Work Program
Business Impact Analysis is performed on an enterprise-wide basis. All critical business functions/assets are identified and prioritized, not just technology function/assets.	Not adequately addressed	Not adequately addressed
Updates to BCP should be made as changes in technology/business processes warrant.	Not adequately addressed	Not adequately addressed
BCPs should provide for alternate telecommunication services, interoperable communications, and utilities.	Not addressed	Not addressed
BCPs should provide for alternate processing sites located an appropriate distance away.	Not addressed	Adequately addressed
BCPs should address a plan for management succession or loss or inaccessibility of key staff.	Not addressed	Not adequately addressed
BCPs should ensure that employees are aware of responsibilities under the BCP and are adequately trained to carry out the plan and procedures.	Not adequately addressed	Adequately addressed
Key contractors and service providers are identified and backup arrangements are in the contract.	Not adequately addressed	Not adequately addressed

Source: OIG Analysis of BCP Common Elements and IT Examination Guidance.

Because the underlying purpose of business continuity planning is the resumption of *business* operations, it is essential to consider the entire organization, not just technology, when developing the plan. Further, BCPs should be reviewed periodically and updated to reflect and respond to changes in the financial institution or its TSP, business processes, technology, changes in key personnel, and the internal and external environments of the institution. Financial institutions should plan for alternative telecommunication services and utilities and alternative processing site(s) if the primary sources become inaccessible and/or unavailable for use. Further, in making the arrangements for alternative telecommunications, utilities or physical work sites, BCPs should ensure that alternative telecommunications and utilities are not susceptible to single points of failure and that alternative facilities are not vulnerable to the same set of risks as the primary location.

Additionally, BCPs should include management succession plans and plans for loss or inaccessibility of key staff. Cross-training of employees should be utilized, and backup roles and responsibilities should be clearly defined in the BCP should key personnel not be available to restore operations. Further, staff should be fully aware of their responsibilities under the BCP and should be aware of the risks of not fulfilling those duties. Finally, institutions should ensure

that all key contractors, vendors, suppliers, and service providers are identified and that the BCPs include provisions if accessibility to these outsourced services becomes unavailable.

DSC officials agreed that the IT MERIT Procedures and IT General Work Program focus more on IT than enterprise-wide aspects of business continuity planning. The FFIEC's draft BCP booklet was circulated to DSC examiners for field testing in July 2002, or 2 months before the September 2002 release of DSC's revised IT examination guidance. According to DSC officials, it was not DSC's intention to exclude enterprise-wide business continuity planning in DSC's IT examination guidance. In fact, the authors of the IT examination guidance were aware that the BCP booklet was being drafted, but were unaware of the detailed concepts that were being developed in the BCP booklet. Also, DSC officials stated that it is not readily apparent where a review of business continuity planning should occur in DSC's supervisory examination program. DSC officials stated that it would make sense that the BCP review occur during a safety and soundness examination (instead of an IT examination) as part of the assessment of an institution's management practices since the development of a BCP would be the responsibility of the institution's senior management and would be incorporated into the institution's policy.

An institution's BCP is a key management control. Accordingly, a goal for DSC should be that, regardless of where the BCP review takes place, the results should be factored into the determination of the management component of the institution's CAMELS[6] rating.

Enterprise-wide business continuity planning is critical to the safety and soundness of all financial institutions, regardless of the size, complexity, and/or risk. A disruption could occur from a natural disaster (e.g., fire, flood, severe weather, chemical spills, air contaminants); malicious activity (e.g., terrorism, electronic attack, sabotage); and/or technical disasters (e.g., transportation system disruption or loss of telecommunications, equipment, software, or utilities such as power failures) that could impair the primary processing site and thereby make it unavailable for use. Moreover, a disruption could make key personnel and/or decision-makers inaccessible for maintaining the operations and services performed by the institution. Because DSC's approach is not designed to address the business or enterprise-wide aspects of business continuity planning for most FDIC-supervised institutions, DSC may not be adequately assessing whether most FDIC-supervised institutions would effectively respond to a disruption and maintain critical business functions until those functions are fully restored. An institution's inability to resume business operations could result in an adverse effect on the regional economy, reputation damage, operational downtime, and in the worst of circumstances, failure of the bank.

[6] Under the Uniform Financial Institutions Rating System, a numeric rating is assigned to reflect the assessment of the bank's financial condition, compliance with laws and regulations, and overall operating soundness. The FDIC's rating of six elements--**C**apital adequacy, **A**sset quality, **M**anagement, **E**arnings, **L**iquidity, and **S**ensitivity to market risk--is referred to as the CAMELS rating. CAMELS component and composite ratings range from 1 to 5, with a 5 rating representing the most critically deficient level of performance.

RECOMMENDATION

We recommend that the Director, DSC, incorporate the enterprise-wide aspects of business continuity planning in DSC's supervisory approach to examinations of FDIC-supervised institutions.

CORPORATION COMMENTS AND OIG EVALUATION

The Director, DSC, provided a written response, dated September 23, 2003, to a draft of this report. DSC agreed with our recommendation. DSC's comments are presented in their entirety in Appendix III to this report. DSC's proposed action is sufficient to resolve the recommendation. Because the proposed action is subject to interagency approval, DSC could not provide a specific completion date. Accordingly, the recommendation will remain undispositioned and open for reporting purposes until we have determined that the agreed-to corrective action has been completed and is effective. Appendix IV presents a summary chart showing DSC's response to our recommendations.

APPENDIX I: OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our evaluation was to determine the adequacy of DSC's approach to assessing business continuity planning at FDIC-supervised institutions. We focused on the frequency and extent to which DSC supervisory reviews address an institution's ability to protect against, recover, and resume operations in the event of future disruptions or catastrophic events (including physical and electronic attacks).

To accomplish our objective, we performed the following work:

- Reviewed DSC's IT examination guidance, including work programs, examination procedures, Regional Director Memoranda and FDIC Financial Institution Letters, and Examination Documentation Modules, in order to gain an understanding of DSC's approach to conducting reviews of business continuity planning at FDIC-supervised institutions.

- Reviewed the FFIEC's examination guidance, specifically, the *1996 Information Security Examination Handbook*, to gain an understanding of the work programs available to DSC examiners in conducting IT examinations of Type III and Type IV institutions. We identified those procedures relevant to the review of business continuity planning. Additionally, we reviewed the BCP booklet that was released in May 2003 (after the start of our review) to gain an understanding of how the FFIEC work programs have changed regarding business continuity planning.

- Researched guidance issued by government and private industry sources on the subject of business continuity planning to gain an understanding of the key concepts or elements of business continuity planning in business entities. We focused our research on guidance that was issued in response to the lessons learned from the September 11, 2001 terrorist attacks and the importance of how BCPs contributed to the financial sector's ability to recover operations.

- Identified key elements of business continuity planning that were common to the government and private industry sources researched.

- Compared DSC's IT examination guidance to the common key elements identified by our research in order to form a basis for our evaluation of DSC's approach.

- Interviewed DSC officials from Washington, D.C., and three regional offices (San Francisco, Chicago, and Dallas/Memphis) that are responsible for implementing DSC's approach to IT examinations.

- Interviewed DSC officials from Washington, D.C., who participate in FFIEC and FBIIC activities.

- Reviewed examination workpapers for 10 sampled IT examinations. Our sample focused on IT examinations that started after January 1, 2003 and ended before May 22, 2003 in order to capture IT examinations that were conducted after issuance of the revised IT examination

guidelines in September 2002, with the exception of one examination. One examination of a TSP was performed in May 2002. We selected this May 2002 TSP examination because it was the most recent examination for which the FDIC was the lead agency. We judgmentally selected IT examinations for institutions that were located in large metropolitan areas. We also judgmentally selected institutions of various sizes and complexities to gain an understanding of the relative differences in DSC's approach. Our sample was composed of the following technology risk profile types of institutions:

Technology Risk Profile Type	Number Tested
I	1
II	1
III	4
IV	2
TSPs	2

From the sample of examinations, we reviewed, when available, the following documents in the examination workpapers:

- Report of Examination
- Technology Profile Script and Scoring Matrix
- IT Examination Questionnaire
- Request Lists and Entry Letter
- Pre-examination planning memorandum
- On-site examination procedures and work programs used and examiner's documentation of work performed.

- Interviewed examiners-in-charge, when necessary, to obtain clarifications and insights from our reviews of workpapers.

- Reviewed feedback from DSC examiners who field-tested the BCP booklet during its development phase.

- Interviewed officials from the General Accounting Office (GAO) to gain an additional understanding of their work conducted on report number GAO-03-414, *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants.*

- The nature of our objective did not require reviewing related performance measures under the Government Performance and Results Act, testing for fraud or illegal acts, or determining the reliability of computer-processed data obtained from the FDIC's computerized systems. We gained an understanding of relevant internal control activities by examining DSC's applicable policies and procedures as presented in DSC manuals, IT examination guidance, Regional Director Memoranda, and Examination Documentation Modules, when appropriate.

We decided not to test internal control activities because we concluded that the objective could be met more efficiently by conducting substantive tests (workpaper reviews) rather than placing reliance on the internal control system.

We completed field work at DSC offices located in Washington, D.C., and the San Francisco and Chicago regional offices. We conducted our evaluation from March 2003 through July 2003, in accordance with generally accepted government auditing standards.

APPENDIX II: GLOSSARY

Term	Definition
Business Impact Analysis (BIA)	The process of identifying the potential imp act of uncontrolled, non-specific events on an institution's business process.
Disaster Recovery Plan	Disaster recovery planning is an IT function; in the IT context, disaster recovery plans document the actions that will be taken to restore computer processing applications, telecommunications services, and data after a disruption or disaster event to prevent or at least minimize the impacts that such an event will have on the business.
Financial and Banking Information Infrastructure Committee (FBIIC)	FBIIC is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system. Treasury's Assistant Secretary for Financial Institutions chairs the committee. Members of the FBIIC include representatives of the Commodity Futures Trading Commission, the Conference of State Bank Supervisors, the FDIC, the Board of Governors of the Federal Reserve System (FRB), the National Association of Insurance Commissioners, the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Office of Federal Housing Enterprise Oversight, the Offices of Homeland and Cyberspace Security, the Office of Thrift Supervision (OTS), and the Securities and Exchange Commission.
Federal Financial Institutions Examination Council (FFIEC)	The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the FDIC, FRB, NCUA, OCC, and OTS and to make recommendations to promote uniformity in the supervision of financial institutions.
Government Emergency Telecommunications Service (GETS)	GETS is an acronym for the Government Emergency Telecommunications Service card program. GETS cards provide emergency access and priority processing for voice communications services in emergency situations.
Multi-Regional Data Processing Servicers (MDPS)	TSPs who qualify for the MDPS Program. An organization is considered for the MDPS Program when it processes: mission-critical applications for a large number of financial institutions that are regulated by more than one agency, thereby posing a high degree of systemic risk; or work from a number of data centers located in different geographic regions.
Technology Profile Script (TPS)	Designed to be a basic standard measurement of the complexity and risk of a financial institution's information technology (IT) functions, the TPS is completed by DSC prior to every IT exam and is used to determine examination scope and examiner resources. Upon completion of the TPS, a score is calculated. The score becomes the primary basis for classifying an institution into one of four technology profile categories; Type I, Type II, Type III, or Type IV.
Technology Service Providers (TSP)	TSPs include independent data centers, joint venture/limited liability corporations, and bank service corporations.

APPENDIX III: CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
550 17th St. NW Washington DC, 20429
Division of Supervision and Consumer Protection

September 23, 2003

TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits

FROM: Michael J. Zamorski
Director, Division of Supervision and Consumer Protection

SUBJECT: DSC Response to OIG Draft Report Entitled *Business Continuity Planning at FDIC-Supervised Institutions* (Assignment Number 2003-006)

The subject draft report from the Office of Inspector General (OIG) contains favorable findings describing DSC's supervisory actions with regard to business continuity planning (BCP) at FDIC-supervised institutions. The report contains one recommendation to expand the coverage of the enterprise-wide aspects of BCP in our supervisory approach. It states:

> *"We recommend that the DSC, Director incorporate the enterprise-wide aspects of business continuity planning in its supervisory approach to examinations of FDIC-supervised institutions."*

DSC agrees with the OIG's finding that the examination coverage of enterprise-wide BCP could be improved and concurs with the recommendation above. As noted in the draft report, current examination procedures related to BCP are limited to planning and recovery of the information technology (IT) operations at Type I, II and III financial institutions. Enterprise-wide BCP involves much more, including such things as management succession; designation of primary spokespersons; designation of key staff; contacting staff and other parties, including regulators; identification of critical records; training and testing. Many of these are general management issues, far outside the specialized area of IT.

DSC believes the assessment of BCP should be incorporated into the management assessment in the safety and soundness (S&S) examination, with that assessment focused on two fronts – the IT area for disaster recovery and back-up issues and S&S for the remainder. Comments from the IT area, where appropriate, should be carried forward to the S&S report and both IT and S&S examiners should work together to ensure the entire plan is reviewed.

To implement the recommendation, DSC will request that the Management and Internal Control Evaluation Module, which is a key safety and soundness examination tool, be revised to incorporate the enterprise-wide aspects of BCP. This request will be presented to the Interagency Examination Documentation (ED) Module Maintenance Committee at its next meeting in November 2003.

APPENDIX IV: MANAGEMENT RESPONSES TO RECOMMENDATIONS

This table presents the management responses that have been made on recommendations in our report and the status of recommendations as of the date of report issuance. The information in this table is based on management's written response to our report and subsequent communication with management representatives.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved: [a] Yes or No	Dispositioned: [b] Yes or No	Open or Closed [c]
1	DSC will request that the Management and Internal Control Evaluation Module be revised to incorporate the enterprise-wide aspects of BCP. This request will be presented to the Interagency Examination Documentation Module Maintenance Committee at its next meeting in November 2003.	November 2003	N/A	Yes	No	Open

[a.] Resolved – (1) Management concurs with the recommendation and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation but planned alternative action is acceptable to the OIG.
(3) Management agrees to the OIG monetary benefits or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b.] Dispositioned – The agreed-upon corrective action must be implemented, determined to be effective, and the actual amounts of monetary benefits achieved through implementation identified. The OIG is responsible for determining whether the documentation provided by management is adequate to disposition the recommendation.

[c.] Once the OIG dispositions the recommendation, it can then be closed.