

Appendix D. Auditor's Recommendations

This appendix contains the detailed reviews of auditor reports that contained business continuity-relevant references. The applicable statements are captured in the following tables along with MITRE's assessment of whether the statement is a Requirement (R) that must be addressed, or Advice (A) that should be considered, or just a Comment (C) to put the information into context.

Table of Contents

D.1	General Accounting Office Reports and Testimony	3
D.1.1	GAO-00-33 Information Security Risk Assessment	3
D.1.2	GAO-00-295, INFORMATION SECURITY	5
D.1.3	GAO-01-1168T, CRITICAL INFRASTRUCTURE PROTECTION.....	7
D.1.4	GAO-02-24 INFORMATION SHARING	10
D.1.5	GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets	11
D.1.6	GAO-02-586, INFORMATION MANAGEMENT	13
D.2	Treasury Inspector General for Tax Administration Audits.....	14

D.1 General Accounting Office Reports and Testimony

D.1.1 GAO-00-33, Information Security Risk Assessment

Ref #	GAO-00-33, Information Security Risk Assessment: Practices of Leading Organizations, November 1999	Applicable BC Process	Applicable BC Plans	Statement Class
1.	<p>Regardless of the types of risk being considered, all risk assessments generally include the following elements:</p> <ul style="list-style-type: none"> • Identifying threats that could harm and, thus, adversely affect critical operations and assets. • Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals. • Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important. • Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs. • Identifying cost-effective actions to mitigate or reduce the risk. • Documenting the results and developing an action plan. 	2. Risk Evaluation and Control	All Plans	A
2.	<p>Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing. For example:</p> <ul style="list-style-type: none"> • Data are limited on risk factors, such as the likelihood of a sophisticated hacker attack and the costs of damage, loss, or disruption caused by events that exploit security weaknesses; • Some costs, such as loss of customer confidence or disclosure of sensitive information, are inherently difficult to quantify; • Although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented; • And even if precise information were available, it would soon be out of date due to fast-paced changes in technology and factors such as improvements in tools available to would-be intruders. 			C

Ref #	GAO-00-33, Information Security Risk Assessment: Practices of Leading Organizations, November 1999	Applicable BC Process	Applicable BC Plans	Statement Class
3.	Critical Success Factors: <ul style="list-style-type: none"> • Obtain senior management support and involvement • Designate focal points • Define procedures • Involve business and technical experts • Hold business units responsible • Limit scope of individual assessments • Document and maintain results 			C

Statement Class

A – Advice

C – Comment

R – Requirement

D.1.2 GAO-00-295, INFORMATION SECURITY

Ref #	GAO-00-295, INFORMATION SECURITY: Serious and Widespread Weaknesses Persist at Federal Agencies, September 2000	Applicable BC Process	Applicable BC Plans	Statement Class
1.	<p>In February 2000, we reported that significant weaknesses in the Internal Revenue Service's (IRS) computer security controls continued to place taxpayer and other data in IRS' automated systems at serious risk of unauthorized disclosure, modification, or destruction. Specifically, IRS continued to have serious weaknesses with general controls designed to protect computing resources such as networks, computer equipment, software programs, data, and facilities from unauthorized use, modification, loss, and disclosure. IRS did not always: (1) effectively implement controls to prevent, limit, or detect access to computing resources, (2) adequately segregate system administration and security administration responsibilities, (3) optimally configure system software to ensure the integrity of system programs, files, and data, (4) sufficiently plan or test the activities required to restore critical business systems when unexpected events occur, and (5) routinely monitor key networks and systems to identify unauthorized activities and inappropriate system configurations.</p>			C
2.	<p>Entity-wide Security Program Planning and Management. Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses.</p>	1. Project Initiation and Management	BCM	R
3.	<p>Access Controls. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and to keep records of individual user's actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and terminated employees and changes in users' responsibilities and related access needs.</p>	2. Risk Evaluation & Control	Security	A

Ref #	GAO-00-295, INFORMATION SECURITY: Serious and Widespread Weaknesses Persist at Federal Agencies, September 2000	Applicable BC Process	Applicable BC Plans	Statement Class
4.	Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented.			C
5.	Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection.			C
6.	System software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation.			C
7.	Service continuity controls ensure that, when unexpected events occur, critical operations continue without undue interruption and that critical and sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications.	3. Business Impact Analysis 4. Business Continuity Strategies	BCM, BRP, COG, CIP, COOP, DRP, IMP, OEP, Security, COOP [Test, Training & Exercise Plan]	R
8.	To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.	7. Awareness and Training Program	BCM, COOP [Test, Training & Exercise Plan]	R
9.	Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location.	3. Business Impact Analysis 4. Business Continuity Strategies	BCM, BRP, COG, CIP, COOP, DRP, IMP	R

Statement Class

A – Advice

C – Comment

R - Requirement

D.1.3 GAO-01-1168T, CRITICAL INFRASTRUCTURE PROTECTION

Ref #	GAO-01-1168T, CRITICAL INFRASTRUCTURE PROTECTION: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks, September 26, 2001	Applicable BC Process	Applicable BC Plans	Statement Class
1.	<p>Security Program Management. Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses.</p>	1. Project Initiation and Management	BCM	A
2.	<p>Access Controls. Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.</p> <p>For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions.</p>			C
3.	<p>Software Development and Change Controls. Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before they are implemented, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and ensure that different versions are not misidentified.</p>			C
4.	<p>Segregation of Duties. Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection.</p>			C

Ref #	GAO-01-1168T, CRITICAL INFRASTRUCTURE PROTECTION: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks, September 26, 2001	Applicable BC Process	Applicable BC Plans	Statement Class
5.	<p>Operating System Software Controls. Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation.</p> <p>Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired.</p>			C
6.	<p>Service Continuity Controls. Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected.</p>			C
7.	<p>Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location. It is also essential that the related controls be understood and supported by management and staff throughout the organization.</p>	2. Risk Evaluation and Control	BCM	R
8.	<p>Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing.</p>	1. Project Initiation & Management	BCM	R
9.	<p>To establish effective service continuity controls, agencies should first assess the criticality and sensitivity of their computerized operations and identify supporting resources. At most agencies, since the continuity of certain automated operations is more important than others, it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them.</p>	3. Business Impact Analysis	BCM	R
10.	<p>Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. This plan should be documented, tested to determine whether it will</p>	6. Develop and Implement BC Plans	BCM, BRP, COG, CIP, COOP, DRP	R

Ref #	GAO-01-1168T, CRITICAL INFRASTRUCTURE PROTECTION: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks, September 26, 2001	Applicable BC Process	Applicable BC Plans	Statement Class
	<p>function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. The plan itself should identify and provide information on supporting resources that will be needed, roles and responsibilities of those who will be involved in recovery activities, arrangements for off-site disaster recovery location and travel and lodging for necessary personnel, off-site storage location for backup files, and procedures for restoring critical applications and their order in the restoration process.</p>			
11.	<p>Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes. Federal agencies depend not only on their own internal systems, but also on data provided by their business partners and services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications).</p>	4. Business Continuity Strategies	BCM, CIP, BRP	A

Statement Class

A – Advice

C – Comment

R - Requirement

D.1.4 GAO-02-24, INFORMATION SHARING

Ref #	GAO-02-24, INFORMATION SHARING: Practices That Can Benefit Critical Infrastructure Protection, October 2001	Applicable BC Process	Applicable BC Plans	Statement Class
1.	Accordingly, the federal government's strategy for protecting the nation's critical computer-dependent infrastructure sectors includes efforts to establish information sharing and analysis centers (ISACs) within both the federal government and individual industry sectors.	9. Public Relations and Crisis Coordination 10. Coordination with Public Authorities	COOP, CIP	R
2.	All of the organizations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships.	9. Public Relations and Crisis Coordination	COOP, CIP	A
3.	Other critical success factors identified included (1) establishing effective and appropriately secure communication mechanisms , such as regular meetings and secure Web sites, (2) obtaining the support of senior managers at member organizations regarding the sharing of potentially sensitive member information and the commitment of resources, and (3) ensuring organization leadership continuity.	1. Project Initiation and Management	COOP, CIP	A
4.	Among the challenges identified, one of the most difficult was overcoming new members' initial reluctance to share information. Other challenges included (1) developing agreements on the use and protection of shared information , (2) obtaining adequate funding to cover the cost of items such as Web sites and meetings while avoiding seeking contributions intended primarily to promote the interests of an individual organization, (3) maintaining a focus on emerging issues of interest to members, and (4) maintaining professional and administrative staff with appropriate skills.	1. Project Initiation and Management	COOP, CIP	A

Statement Class

A – Advice

C – Comment

R – Requirement

D.1.4 GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets

Ref #	GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets Statement of Robert F. Dacey, Director, Information Security Issues November 9, 2001	Applicable BC Process	Applicable BC Plans	Statement Class
1.	...the terrorist events that began on September 11, 2001, have redefined the disasters that must be considered in identifying and implementing service continuity controls to ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected.			C
2.	Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location.	2. Risk Evaluation and Control	All Plans	A
3.	Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing.	1. Project Initiation and Management	All Plans	A
4.	... it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them.	3. Business Impact Analysis	All Plans	R
5.	Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed.	3. Business Continuity Strategies	All Plans	R
6.	This plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations.	8. Maintain and Exercise BC Plans	All Plans	R
7.	Both user and data processing departments should agree on the plan, and it should be communicated to affected staff.	7. Awareness and Training Program	All Plans	A

Ref #	GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets Statement of Robert F. Dacey, Director, Information Security Issues November 9, 2001	Applicable BC Process	Applicable BC Plans	Statement Class
8.	Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred.	8. Maintain and Exercise BC Plans	All Plans	R
9.	Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes.	3. Business Impact Analysis	All Plans	R
10.	During the Year 2000 computing challenge, it was essential that agencies develop business continuity and contingency plans for all critical core business processes and supporting systems regardless of whether these systems were owned by the agency.	3. Business Impact Analysis	All Plans	R

Statement Class

A – Advice

C – Comment

R – Requirement

D.1.5 GAO-02-586, INFORMATION MANAGEMENT

Ref #	GAO-02-586, INFORMATION MANAGEMENT: Challenges in Managing and Preserving Electronic Records, October 2001	Applicable BC Process	Applicable BC Plans	Statement Class
1.	Part of the problem is that records management guidance is inadequate in the current technological environment of decentralized systems producing large volumes of complex records.			C
2.	NARA's responsibilities stem from the Federal Records Act, which requires each federal agency to make and preserve records that (1) document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and (2) provide the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities.	3. Business Impact Analysis	All Plans	R
3.	First, agencies are required to maintain an inventory of all agency information systems. The inventory should identify (1) the system's name; (2) its purpose; (3) the agency programs supported by the system; (4) data inputs, sources, and outputs; (5) the information content of databases; and (6) the system's hardware and software environment.	3. Business Impact Analysis	All Plans	R
4.	Second, NARA requires agencies to schedule the electronic records maintained in its systems. Agencies must either schedule those records under specific schedules, completed through submission and approval of Standard Form 115 (SF 115), <i>Request for Records Disposition Authority</i> , or pursuant to a general records schedule.	3. Business Impact Analysis	All Plans	R

Statement Class

A – Advice

C – Comment

R – Requirement

D.2 Treasury Inspector General for Tax Administration Audits

The Treasury Inspector General for Tax Administration (TIGTA) has completed several audits on the IRS's ability to respond to disasters and protect its assets. These reports may have recommendations that need to be considered when developing business continuity management capabilities. The following list of TIGTA reports are all issued as Limited Official Use (LOU) only documents. As such, their content is not represented within this report. However, MITRE suggests that the IRS conduct their internal review to determine applicability of TIGTA's recommendations. The following TIGTA reports should be considered for review.

1. 2000-20-031: The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans, March 2000
2. 2000-20-039: The Internal Revenue Service Can Improve Information Systems Physical Security, February 2000
3. 2000-20-072: The General Controls Over a Critical Internal Revenue Service Tax Processing Computer System Can Be Strengthened, May 2000
4. 2001-20-020: Computer Security Controls Should Be Strengthened in the Former Brooklyn District, November 2000
5. 2001-20-036: Computer Security Controls Should Be Strengthened in the Former Northern California District, January 2001
6. 2001-20-072: Disaster Recovery Plans for Mainframe Systems at the Tennessee Computing Center Have Improved, But Mid-Range Systems Still Need Attention, April 2001
7. 2001-20-092: Controls Over The IRS' Masterfile System Are Generally Adequate, But Some Improvement Is Needed, June 2001
8. 2001-20-108: Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources, July 2001
9. 2002-20-007: The Internal Revenue Service Encrypts Data Transmitted Between Its Facilities, But Controls Over Cryptography Can Be Improved, October 2001
10. 2002-20-044: The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made, January 2002
11. 2002-20-045: Controls Over the Procurement Web Site Should Be Improved to Better Deter and Detect External Attacks, January 2002
12. 2002-20-057: Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems, March 2002

13. 2002-20-064: Controls Over the Excise Files Information Retrieval System Web Site Should Be Improved to Better Deter and Detect External Attacks, April 2002
14. 2002-20-082: System-Level Controls Over the Detroit Computing Center Mainframe Computers Are Generally Adequate, But Some Improvement Is Needed, April 2002
15. 2002-30-054: The Centralization of Business Tax Return Processing to Two Submission Processing Centers Is on Schedule, but Disaster Contingency Plans Must Be Updated and Tested, February 2002
16. 2003-20-026: The Internal Revenue Service Has Made Substantial Progress in Its Business Continuity Program, but Continued Efforts Are Needed, December 2002