

Appendix C. IRS Requirements

This appendix contains the detailed review of the Internal Revenue Manual. 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.

C.1 Internal Revenue Manual – 25.10.1 IT Security Policy and Guidance

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
1.	The Chief, Information Technology Services shall ensure the capability to implement the IRS business continuity planning program policy.	1. Project Initiation & Management	BCM	R
2.	The Director, Office of Security is responsible for managing core security operations , which include the systems security certification and accreditation process, computer security incident response capabilities (CSIRC), Critical Infrastructure Protection (CIP) program , security awareness program, and existing and planned business resumption/disaster recovery/continuity of operations capabilities.	1. Project Initiation & Management	BCM	R
3.	The Director, Office of Cyber Security is responsible for working with Information Technology Services (ITS) Operations and business units to identify existing and planned business resumption/disaster recovery/continuity of operations capabilities, including the establishment of executable/tested business resumption plans.	1. Project Initiation & Management	BCM	R
4.	General Support System Security Plans shall include the following controls: establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.	6. Develop & Implement BC Plans 7. Awareness & Training Program 8. Maintain & Exercise BC Plans	BCM, Security	R
5.	The National Security Officer (NSO) shall provide and maintain documentation of the communications network at off-premises locations sufficient to meet the requirements of the Business Continuity Program addressed in the IRM.	4. Business Continuity Strategies 6. Develop & Implement BC Plans 8. Maintain & Exercise BC Plans	BCM, BRP, DRP	R
6.	Security and Telecommunications personnel shall ensure timely maintenance of communications network documentation in suitable off-premises locations to meet the requirements of the Business Continuity Program of this manual.	4. Business Continuity Strategies 8. Maintain & Exercise BC Plans	BRP, DRP	R

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
7.	Business continuity planning is based on laws enacted by Congress, OMB, NIST, GSA, and the Department of the Treasury that have established policies and guidelines to manage Federal information resources.			C
8.	Department of Treasury Information System Life Cycle Manual TD P 4-01 provides guidelines for ensuring that contingency plans are developed for each mission critical system; those systems that significantly affect bureau programs, property, finances, and other resources. Each plan must be tested at a frequency commensurate with the risk and magnitude of loss or harm that could result from the disruption of systems operation.	8. Maintain & Exercise BC Plans	BCM, BRP, DRP, IMP, OEP	R
9.	Department of Treasury Security Manual TD P 71-10 provides uniform policies and general procedures to be used by the bureaus to carry out their respective responsibilities in the areas of personnel, physical, telecommunications, IT systems security, and emergency preparedness.	6. Develop & Implement BC Plans	BCM, BRP, DRP, IMP, OEP	A
10.	Disaster Recovery and Business Resumption Plans are the major components of the sites Business Continuity Plan. These combined plans provide for the resumption of all critical processes within an organization. In the event of a disaster, the most critical applications and systems identified by the site will be recovered first.			C
11.	Business Resumption Plans shall be developed, tested, implemented, and maintained for all essential IT systems.	6. Develop & Implement BC Plans 8. Maintain & Exercise BC Plans	BCM, BRP	R
12.	The Commissioner of the IRS shall: a. designate senior management officials to establish and manage the Business Continuity Planning Program for the IRS, and b. establish policy and ensure compliance with those directives identified in this section.	1. Project Initiation & Management	BCM	R
13.	The senior executive responsible for an IRS business function shall initiate and ensure that the Business Continuity Planning Program policy established by the Commissioner is followed , and delegate implementation of the Business Continuity Program to Heads of Office. The senior executive shall also cooperate among various business units to develop, maintain, and validate effective, comprehensive plans.	1. Project Initiation & Management	BCM, BRP, DRP, IMP, OEP	R

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
14.	Each Head of Office shall: a. ensure an Executive Steering Committee is established to make site-specific policy/business decisions regarding development of the site Business Continuity Plan;	1. Project Initiation & Management	BCM	R
15.	Each Head of Office shall: b. utilize the results of the site's Risk Assessment to develop disaster scenarios and establish the basis for conducting a Business Impact Analysis (BIA);	2. Risk Evaluation & Control	BCM	R
16.	Each Head of Office shall: c. conduct a BIA to establish recovery priorities for business processes and their required information systems;	3. Business Impact Analysis	BCM	R
17.	Each Head of Office shall: d. establish a roster of knowledgeable personnel to serve on recovery teams (i.e. management team, damage assessment team, operations team, restoration team);	6. Develop & Implement BC Plans	COOP, IMP	R
18.	Each Head of Office shall: e. ensure that Performance Measures are followed for the planning, implementation, testing, review, and maintenance of Business Continuity Plans for all critical business functions;	1. Project Initiation & Management 8. Maintain & Exercise BC Plans	BCM	R
19.	Each Head of Office shall: f. establish and periodically test the capability to perform the agency functions that significantly effect IRS programs, property, finances, information systems, and other systems;	7. Awareness & Training Program 8. Maintain & Exercise BC Plans	BCM	R
20.	Each Head of Office shall: g. implement emergency response procedures appropriate to government laws, regulations, and directives;	5. Emergency Response & Operations	COOP, CIP, OEP, IMP,	R
21.	Each Head of Office shall: h. develop exercise plans that include an agenda of anticipated accomplishments, a list of participants, methodology for proceeding, and requirements for vendors, alternate sites, and off-premises storage facilities. All subsequent exercises will follow the plans verbatim to determine if they are complete and correct, or need modification;	8. Maintain & Exercise BC Plans	BCM, BRP, COG, CIP, COOP, DRP, IMP, OEP, Security, COOP [Test, Training & Exercise Plan]	R
22.	Each Head of Office shall: i. develop exercise plans in accordance with the American National Standards Institute (ANSI)/Institute	8. Maintain & Exercise BC Plans	BCM, BRP, COG, CIP, COOP, DRP, IMP, OEP, Security,	R

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
	of Electrical and Electronics Engineers (IEEE) Standard Software Test Documentation 829. The test case is explained in IRM Exhibit 25.10.1-16 and the exercise plan format is provided in Exhibit 25.10.1-17;		COOP [Test, Training & Exercise Plan]	
23.	Each Head of Office shall: j. perform at least one exercise of the Business Continuity Plan each year. Exercises must include one business process and one IT system. Exercises will not be used to evaluate the plans on a pass or fail basis, but will serve as an opportunity to enhance the plans and improve organizational recovery readiness;	8. Maintain & Exercise BC Plans	BCM, BRP, COG, CIP, COOP, DRP, IMP, OEP, Security, COOP [Test, Training & Exercise Plan]	R
24.	Each Head of Office shall: k. ensure that only backup files retrieved from the off-premises storage site are used for the recovery exercises. Backup files will not be pre-positioned at the recovery site; and	8. Maintain & Exercise BC Plans	BCM, BRP, COG, CIP, COOP, DRP, IMP, OEP, Security, COOP [Test, Training & Exercise Plan]	R
25.	Each Head of Office shall: l. forward [to Treasury] within thirty (calendar) days of any exercise, a description of the events, results, problems encountered and recommended solutions to the Office of Security Evaluation and Oversight for review. Accomplish all modifications to the Business Continuity Plan in the same time frame.	8. Maintain & Exercise BC Plans	BCM, BRP, DRP, IMP, OEP	R
26.	Each site , based on National business function objectives, will define their overall Business Processes and Mission Critical Application(s) MCA(s), this should include National PDD-63, Critical Assets, recovery priorities.	3. Business Impact Analysis	BCM	R
27.	Business Continuity Plan resource requirements will be identified to support the recovery of critical processes and applications.	1. Project Initiation & Management	BCM	R
28.	Business Continuity Plans shall be comprehensive, reviewed quarterly, tested annually, and updated as needed , to provide for the reasonable restoration of operations.	8. Maintain & Exercise BC Plans	BCM, BRP, DRP, IMP, OEP	R

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
29.	<p>Business Continuity Plans shall include at least the following:</p> <p>a. a copy of the site's Occupant Emergency Plan (OEP);</p> <p>b. recovery strategies and procedures for all MCA(s) and Business Processes;</p> <p>c. procedures to restore, once the site has been returned to normal operations, all MCA(s) and Business Processes;</p> <p>d. procedures to move critical workload or functions to other sites or Centers within the IRS;</p> <p>e. procedures to notify National Headquarters Office, external customers, emergency/evacuation personnel, contract personnel, state and local authorities, and other support personnel which may be required to assist in the sites recovery;</p> <p>f. procedures identifying responsibilities for ensuring that mission critical operations will continue if normal processing or data communications is interrupted for an unacceptable period; and</p> <p>g. a designation of OFFICIAL USE ONLY on critical portions of the plan, to ensure that only those persons who have a need-to-know will have access to the critical elements of the plan.</p>	6. Develop & Implement BC Plans	BCM, BRP, DRP, IMP, OEP	R
30.	<p>Schedules for backup frequencies and rotation schedules must be established for critical files stored off-premises.</p>	6. Develop & Implement BC Plans	DRP	R
31.	<p>Each site shall develop, maintain, and test an Incident Management Plan.</p>	6. Develop & Implement BC Plans 8. Maintain & Exercise BC Plans	IMP	R
32.	<p>All media must be properly stored and accounted for and a complete listing of the contents must be stored off-premises.</p>	6. Develop & Implement BC Plans 8. Maintain & Exercise BC Plans	DRP, COOP [Test, Training & Exercise Plan]	R
33.	<p>Audits of all off-premises storage facilities must be conducted on an annual basis.</p>	8. Maintain & Exercise BC Plans	BCM	R
34.	<p>End-users shall develop business unit plans for resumption of all critical processes within the organization.</p>	6. Develop & Implement BC Plans	BRP	R

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
35.	End-users shall review and update plans at least annually or whenever major processing environment changes occur (e.g., physical site, hardware, software, operating system, etc.).	8. Maintain & Exercise BC Plans	BCM, BRP, DRP, IMP, OEP	R
36.	Business Continuity/Business Resumption planning shall include Emergency Response, and Recovery Operations.	6. Develop & Implement BC Plans	BCM, BRP, DRP, IMP, OEP	R
37.	Before any plan can be developed, research must be done in the overall strategy of business continuity and business resumption planning to ensure that all components of the operations have been clearly defined and prioritized in terms of criticality and the impact their loss would incur to the IRS.	3. Business Impact Analysis	BCM	R
38.	An in-depth Business Impact Analysis (BIA) must be performed. This analysis must define the profile of critical business functions performed in all IRS functional areas IRS-wide . The IRS' facilities, geographical locations, sensitivity or criticality of information, and dependencies vary to such a degree that the effects of a disaster to one location will impact in a completely different manner for another.	3. Business Impact Analysis	BCM, BRP, DRP, IMP, OEP	R
39.	An assessment must be made of containment actions to be taken at the onset of an emergency to provide greater safety for personnel while decreasing the chances for major damage to equipment and facilities.	5. Emergency Response & Operations	IMP	R
40.	The IRS cannot identify all events that may occur; however, those events that are most likely to happen must be identified , as well as the most cost effective controls to minimize the impact or eliminate the event from happening.	2. Risk Evaluation & Control	BCM	R
41.	The CIO is responsible for providing guidance and direction to field personnel responsible for disaster recovery of off-premises storage activities.	1. Project Initiation & Management	BCM	A
42.	Managers of the information technology services at IRS sites will: a. establish backup frequencies and rotation schedules for critical files stored off-premises, other than those identified by National Headquarters, as stipulated in IRM 2.7.1, Information Technology Services (ITS) — Information Technology Services Operations/Inter-Centers. b. ensure that all media is properly stored and accounted for and a complete listing of the contents is stored off-premises. This information must also be included in the site's disaster recovery plans.	6. Develop & Implement BC Plans	DRP	R

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
43.	Business continuity planning requires cooperation among all of the business units to develop, maintain, and validate effective, comprehensive plans. The business unit Commissioners, Deputy Commissioners, and Chiefs will work together to plan for the continuity of business processes.			C
44.	Managers of the information technology services at IRS sites will coordinate the following with the appropriate business units : a. acquisition of space for alternate processing facilities, b. expeditious acquisition and transportation of replacement equipment required to restore operations, c. development of processing priorities for completion of work following emergencies that degrade computer processing capabilities, d. assessment of personnel requirements to support a distressed computer e. processing operation to include occupation of an alternate processing facility, and f. estimation of supplies and office equipment needed to support a computer processing operation occupying an alternate processing facility.	1. Project Initiation & Management 6. Develop & Implement BC Plans	CIP, DRP	A
45.	The location of the off-premises storage facility will be far enough away from the computing facility, so as to not be affected by the same threat, but close enough to allow a quick response when time is critical.	6. Develop & Implement BC Plans	DRP	R
46.	Store the items listed below at the off-premises storage facility: <ul style="list-style-type: none"> • Security Plan • Configuration Management Plan • Business Continuity Plan • DR/BR Plans • Risk Assessment Report • Security Features Users Guide • Certification and Accreditation • Trusted Facility Manual 	6. Develop & Implement BC Plans	BCM, BRP, DRP, IMP, OEP	R
47.	Each information system facility must establish a method for off-premises storage, magnetic media control and procedures for an annual audit of all media stored off-premises.	6. Develop & Implement BC Plans	DRP	R
48.	Critical information systems must have adequate backup documentation and storage.	6. Develop & Implement BC Plans	DRP	R
49.	Business Continuity plans will provide methods for	6. Develop &	DRP	R

Ref #	Internal Revenue Manual 25.10.1 IT Security Policy and Guidance January 1, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
	adjusting the use of computer and telecommunication hardware in order to continue operations, including the use of an alternate processing facility.	Implement BC Plans		
50.	Personnel considerations are a critical part of any disaster recovery and business resumption planning effort. Personnel planning needs range from cross training employees and replacement of casualties to relocation to alternate processing facilities.	6. Develop & Implement BC Plans	BRP	A
51.	Planning for supplies and office equipment is a necessary part of the disaster recovery and business resumption planning process.	6. Develop & Implement BC Plans	BRP	A
52.	Consider transportation needs to move personnel, mail, supplies, and equipment , if an alternate processing facility is activated. Include recovery procedures for damage to direct support area(s), such as the mail room or loading dock, that can create additional transportation needs.	6. Develop & Implement BC Plans	BRP	A
53.	All Business Continuity Plans for critical operations must include provisions for the appropriate level of security for both the damaged facility and any operational alternate processing facility.	5. Emergency Response & Operations	BCM, BRP, DRP, IMP, OEP	R
54.	A management team will direct all recovery operations from a pre-determined primary and alternate Command Center.	5. Emergency Response & Operations	IMP	R
55.	It is the responsibility of each Head of Office to perform at least one exercise of the Business Continuity Plan each year.	8. Maintain & Exercise BC Plans	BCM, BRP, DRP, IMP, OEP	R
56.	Plan Maintenance requires an assessment of changes to the application/system operations and environment and the effect of those changes on the performance of the plan at the time of any disruption to normal business operations.	8. Maintain & Exercise BC Plans	BCM, BRP, DRP, IMP, OEP	R
57.	It will be the responsibility of all IRS Areas Disaster Recovery Coordinators/Analysts to document the distribution of the Business Continuity Plan.	6. Develop & Implement BC Plans	BCM, BRP, DRP, IMP, OEP	R

Statement Class

A – Advice

C - Comment

R - Requirement