

IFSM 301 – Week 3 Citations

(IT Portfolio Management FAQs, 2016)

(CIO Council, 2011)

(Potts, 2010)

(Office of Information Technology, 2013)

(Government Accountability Office, 2016)

(Business Continuity Planning)

(Federal Financial Institutions Examination Council, 2019)

Bibliography

Business Continuity Planning. (n.d.). Retrieved January 25, 2021, from University of Maryland Global Campus:

<https://learn.umgc.edu/d2l/le/content/541520/viewContent/20543015/View>

CIO Council. (2011, November 4). *Portfolio Rationalization: Effective Optimization of IT Funds*. Retrieved January 25, 2021, from CIO.gov:

<https://learn.umgc.edu/d2l/le/content/541520/viewContent/20543012/View>

Federal Financial Institutions Examination Council. (2019). *Business Continuity Planning: IT Examination Handbook*. Retrieved January 25, 2021, from

https://ithandbook.ffiec.gov/media/296178/ffiec_itbooklet_businesscontinuitymanagement_v3.pdf

Government Accountability Office. (2016, November 8). *Best Practices in Information Technology Investment Management*. Retrieved January 12, 2021, from University of Maryland Global Campus:

<https://learn.umgc.edu/d2l/le/content/541520/viewContent/20543003/View>

IT Portfolio Management FAQs. (2016, November 8). Retrieved January 25, 2021, from University of Maryland Global Campus:

<https://learn.umgc.edu/d2l/le/content/541520/viewContent/20543011/View>

Office of Information Technology. (2013). *Managing Capital Investments at the Indian Health Service: A "How-To" Guide to Risk Management*. Indian Health Services, Division of Information Resource Management, Albuquerque. Retrieved January 25, 2021, from

<https://learn.umgc.edu/d2l/le/content/541520/viewContent/20543013/View>

Potts, C. (2010, April). IT Projects that Match Your Goals. *CIO*, 16. Retrieved January 25, 2021, from <https://learn.umgc.edu/d2l/le/content/541520/viewContent/20543039/View>

IT Portfolio Management

Following are two readings on Portfolio Management. The first reading was developed by the General Services Administration to explain IT Portfolio Management (ITPM) using the frequently asked questions (FAQs) format. It is written from the perspective of a federal agency, but the concepts apply to all types of organizations. In very brief form, it explains how ITPM is related to and supported by other governance processes and tools, such as strategic planning, enterprise architecture, budgeting, performance management and project management. A key concept is that "Portfolio analysis provides information demonstrating the impact of alternative IT investment strategies and funding levels, identifies opportunities for sharing resources and considers the agency's inventory of information resources." (p. 2) You only need to read the first 2 ½ pages of the document; the sections on the key stages of the CPIC lifecycle and GSA's cloud-first initiative pertain to other agency policies that are beyond the scope of this class.

The second reading, "Portfolio Rationalization," explains how the Department of Transportation (DOT) approached a review of all of their systems in an effort to maximize the business value, a process they call portfolio rationalization.

IT Portfolio Management FAQs

What is IT Portfolio Management (ITPM)?

What is the intended outcome of applying IT Portfolio Management?

What agency processes participate in the IT Portfolio Management program?

Why apply Portfolio Management to IT investment decision making?

What do the key elements to successful portfolio management include?

What are the differences and relationship between portfolio management and project management?

What are the key stages in the CPIC lifecycle?

What are the most frequently asked questions about GSA's Cloud First implementation?

What is IT Portfolio Management (ITPM)?

ITPM is a risk based approach to the selection and management of IT projects integrating business and IT planning, budgeting, standards, processes and governance.

What is the intended outcome of applying IT Portfolio Management?

The application of ITPM helps the agency achieve mission goals and accomplish agency business/performance objectives by selecting, controlling and evaluating information system projects to determine the best mix of projects and the right level of investment to make in each. Similarly, ITPM helps to balance the IT portfolio between ongoing maintenance initiatives and development/strategic (Development/Modernization/Enhancement - DME) initiatives.

What agency processes participate in the IT Portfolio Management program?

1. Strategic planning establishes the long-term vision for the agency and the supporting functions, activities, objectives and outcomes of subordinate business lines. Strategic planning also defines and

communicates the goals and objectives to be served by the IT portfolio.

2. Capital Planning and Investment Control (CPIC) establishes the processes and tools for selecting, controlling and evaluating IT projects that comprise the IT portfolio.

3. Enterprise Architecture (EA) provides IT portfolio managers and governance bodies with a better understanding of IT investment opportunities and impacts. The EA is used to help formulate and target IT initiatives, information management and sharing, application development, deployment, ongoing operation and maintenance by defining and documenting processes, technical standards, etc., which define the agency operating environment.

4. Performance management documents and tracks achievement against the outputs/outcomes/goals/objectives which define agency success.

5. Budget formulation establishes the funding baseline for approved IT projects across the agency, in accordance with agency priorities and Service/Staff Office business plans and approved IT project business cases.

6. Budget execution monitors funding expenditures against the planned expenditures.

7. IT Governance defines and enables a structured set of processes and the decision making responsibility and authority needed to formulate, manage and maintain an effective and efficient IT portfolio.

8. IT Project Management provides the planning and oversight of each IT project within the portfolio, and reporting of progress, status and results. Effective IT project management provides accountable performance monitoring and control. Periodic IT project management reporting feeds all of the ITPM processes.

Why apply Portfolio Management to IT investment decision making?

IT portfolio management is a central element of good IT investment management. GAO's IT Investment Management Framework places portfolio management at the center of its model of investment management. Portfolio analysis provides information demonstrating the impact of alternative IT investment strategies and funding levels, identifies opportunities for sharing resources and considers the agency's inventory of information resources.

What do the key elements to successful portfolio management include?

They include:

Defining goals and objectives (strategic planning, performance management);

Understanding, accepting and making tradeoffs (governance);

Identifying, eliminating, minimizing and diversifying risk (CPIC, IT Project Management, budget

formulation, governance);

Monitoring portfolio performance (IT Project Management, CPIC, budget execution, performance management, governance);

Revisiting and adjusting portfolio mix, based on goals, objectives, risk and performance (performance management, CPIC, budget formulation, governance).

What are the differences and the relationship between portfolio management and project management?

An IT portfolio is comprised of a set of IT initiatives or projects. Project management is a process that focuses on the extent to which a specific initiative establishes, maintains and achieves its intended objectives within cost, schedule, technical and performance baselines. Portfolio management focuses attention at the aggregate level; its primary objective is to identify, select, finance, monitor and maintain the appropriate mix of initiatives to achieve organizational goals and objectives. Portfolio management also involves consideration of the aggregate costs, risks and returns of all projects within the portfolio.

What are the key stages in the CPIC lifecycle?

These stages include:

1. Select Annually - during budget formulation, business cases will be prepared for proposed major IT initiatives. The business cases will be evaluated through enacted Service/Staff Office (SSO) IT governance processes, and submitted to the GSA OCIO for agency-level assessment, along with SSO-approved non-Major IT initiatives. The Information Technology Executive Council (ITEC), in conjunction with GSA's CFO and Controllers, will examine the proposed SSO portfolios from an enterprise perspective, including validating alignment with the GSA EA, with the agency strategic plan and goals, and with anticipated budget constraints. The ITEC will recommend a proposed IT portfolio to the Business Systems Council (BSC) for concurrence and submission to the GSA Administrator for approval.
2. Control - major IT initiatives in the planning, acquisition, or operations phases of the CPIC lifecycle are monitored to track actual progress against planned results. The type of monitoring and level of reporting required will vary, depending on the CPIC and System Design Life Cycle (SDLC) phase/stage of the initiative. Earned Value Management (EVM) reporting is required for major IT initiatives conducting Development/Modernization/Enhancement. Operational Analysis (OA) is required for Major IT initiatives.
3. Evaluate - IT initiatives that reach the operational phase of the SDLC will be assessed using Post Implementation Reviews (PIRs). PIRs are conducted to validate estimated benefits and costs against actual performance, and to document effective management practices for future use

What are the most frequently asked questions about GSA's Cloud First Implementation?

1. What is the Cloud First policy? Agencies must give priority to web-based applications and services. Cloud computing will allow more people to share a common infrastructure, cutting technology and support costs.

2. How is Cloud First implemented? Cloud computing should be compatible with secure, certified platforms currently provided in the private sector. Migration will build capabilities and momentum in the federal government, encourage industry to more rapidly develop initiatives and reduce operating costs.

3. What are Integrated Program Teams? Integrated Program Teams are small multi-disciplinary teams consisting of business process owners who have a clear vision of the problem they are solving. An Integrated Program Team is required prior to beginning of the investment review process. A full-time manager supported by an Information Technology Acquisition Specialist should be in place for all major programs before Office of Management & Budget approves program budgets.

4. What are data centers? A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally houses redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.

5. What are IRBs? Investment Review Boards, or IRBs, approve or disapprove funding for new systems/investments, or major modifications to existing systems/investments. The IRBs also make recommendations for continuing, modifying, or terminating existing systems or investments based on performance, cost, or schedule criteria

6. What is Modular Development? How is it implemented? Modular Development is the timeline implemented through the entire IT development process – concept, through requirement analysis development, test and delivery.

Modular Development is implemented by making sure program and business objectives have clear quantitative outcome measures for success; awarding contracts incorporating clear business objectives; delivering new working functionality to users at least every 12 months; and moving resources from one release phase to the next.

7. What is TechStat? A TechStat is a face-to-face, evidence-based review of an IT investment. A TechStat is triggered when an agency, using data from the IT Dashboard and other sources, determines that a project is under-performing. In the review session, the agency CIO and other members of an agency's leadership team meet for one focused hour. They review a briefing that highlights the management of the investment, examines program performance data and explores opportunities for corrective action. TechStat sessions conclude with clear next steps formalized in a memo and tracked to completion. Tech Stats award contracts which incorporate clear business objectives, deliver new working functionality to users at least every 12 months and move resources from one release phase to the next.

8. What is SPI (SaaS, PaaS, IaaS)? SPI is an acronym for the most common cloud computing service models: Software as a Service, Platform as a Service and Infrastructure as a Service.

Software as a Service (SaaS) is a software distribution replication in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Platform as a Service (PaaS) is a model for delivering operating systems and associated services over the Internet without downloads or installation. Infrastructure as a Service (IaaS) involves outsourcing the equipment used to support operations, including storage, hardware, servers and networking components.



[Home](#) » [CIOC Blog](#) » **Portfolio Rationalization: Effective Optimization of IT Funds**

Portfolio Rationalization: Effective Optimization of IT Funds

◀ 3



 **SUBSCRIBE by RSS**

 **FOLLOW**

 **FEEDBACK**

November 4th, 2011

[CIO Council](#)

IT portfolios in large organizations become bloated over time with an ever-increasing inventory of applications running on multiple platforms, duplicative or misaligned systems or technologies whose ability to deliver value has degraded over time. As a result, a majority of the IT budget gets allocated to “keeping the lights on” rather than investing in new strategic initiatives. This in turn results in poor business-IT alignment. As stewards of public funding, we must continuously focus on evaluating the effectiveness of our programs and systems and take action to improve our business practices when necessary in order to maximize business value. DOT IT’s process for maximizing business value is call IT portfolio rationalization.

As budgets decrease, the OCIO is focused on optimizing our best practices and adjusting or eliminating outdated systems that are no longer useful or cost effective. The OCIO’s Portfolio Rationalization project will reduce operating costs, position the department for future growth, and focus on strategic imperatives that give us new capabilities for a competitive advantage. We want to create strategic value for our IT investments and optimize our environment as a business enabler. In other words, portfolio rationalization is getting our portfolio healthy, while our governance and management will help it stay healthy. Operational efficiency is a key element of this goal, as is the effective

Archives

- » 2016 (25)
 - » November (3)
 - » October (2)
 - » September (1)
 - » August (8)
 - » July (1)
 - » June (2)
 - » May (1)
 - » March (4)
 - » February (2)
 - » January (1)
- » 2015 (90)
 - » December (4)
 - » November (3)
 - » October (6)
 - » September (9)
 - » August (7)
 - » July (11)
 - » June (4)
 - » May (14)

use of resources.

Over the course of the portfolio rationalization process we are focusing on a couple of key metrics: aligning systems with our departmental strategy and improving systems' business effectiveness. We will retain or modify systems that strongly align with one or both of these measures. This process will make strong use of customer surveys and feedback, in addition to enterprise-level analysis and review through TechStats and other methods. As we identify systems that are outdated, redundant, or provide low business value, we will either re-engineer or retire them. Our goal in this process is to rationalize our resource allocation by rewarding and upgrading high-performance systems while retiring low-performance systems.

This initiative is not exclusive to OCIO. We are relying on several partnerships to accomplish these tasks effectively. We are working with the Office of Management and Budget, Office of the Chief Financial Officer, Office of the Senior Procurement Executive, and the DOT operating agencies. A team effort is required between leadership, partners, and working groups to properly analyze and prioritize critical programs. Portfolio rationalization will address several challenges that span many DOT modes:

- Cyber security planning and execution
- Establishing a comprehensive enterprise architecture program
- Cloud first strategy and data center consolidation
- Savings through shared services
- Focus on modular development and rapid program deployment

This extensive assessment will create comprehensive measurement standards for the effectiveness of our services and ultimately allocate IT funds more efficiently. We need to get serious about addressing low-performing services by improving them, consolidating them, or retiring them. Portfolio rationalization will increase the agility and innovation potential of our IT services, and will maximize business value to the department.

[PREVIOUS](#)

[NEXT](#)

- » [April \(15\)](#)
- » [March \(5\)](#)
- » [February \(9\)](#)
- » [January \(3\)](#)
- » [2014 \(37\)](#)
 - » [December \(3\)](#)
 - » [November \(4\)](#)
 - » [October \(4\)](#)
 - » [September \(2\)](#)
 - » [August \(6\)](#)
 - » [July \(1\)](#)
 - » [June \(4\)](#)
 - » [May \(3\)](#)
 - » [April \(5\)](#)
 - » [March \(2\)](#)
 - » [February \(2\)](#)
 - » [January \(1\)](#)
- » [2013 \(21\)](#)
 - » [November \(1\)](#)
 - » [October \(1\)](#)
 - » [August \(1\)](#)
 - » [July \(2\)](#)
 - » [June \(1\)](#)
 - » [May \(7\)](#)
 - » [April \(3\)](#)
 - » [March \(1\)](#)
 - » [February \(2\)](#)
 - » [January \(2\)](#)
- » [2012 \(46\)](#)
 - » [December \(2\)](#)
 - » [November \(1\)](#)
 - » [October \(1\)](#)
 - » [September \(3\)](#)
 - » [August \(6\)](#)
 - » [July \(3\)](#)
 - » [June \(14\)](#)
 - » [May \(4\)](#)
 - » [March \(1\)](#)
 - » [February \(4\)](#)
 - » [January \(7\)](#)
- » [2011 \(150\)](#)

- » December (5)
- » November (10)
- » October (8)
- » September (12)
- » August (8)
- » July (10)
- » June (35)
- » May (16)
- » April (13)
- » March (16)
- » February (8)
- » January (9)
- » 2010 (93)
 - » December (12)
 - » November (6)
 - » October (14)
 - » September (6)
 - » August (7)
 - » July (13)
 - » June (15)
 - » May (9)
 - » April (4)
 - » March (3)
 - » February (2)
 - » January (2)
- » 2009 (27)
 - » December (2)
 - » September (1)
 - » August (1)
 - » May (1)
 - » April (1)
 - » January (21)

About

- » Leadership
- » Members
- » Groups

Agenda

- » World-Class Digital Services
- » Driving Value in Federal IT

CIOC Blog

- » Current Year 2015
- » Archives 2014
- » Archives 2013
- » Archives 2012

Resources

- » Accessibility Webinars
- » Document Library
- » IT Policy Library
- » Project Open Data

- » [Protecting Federal IT](#)
- » [National Initiatives](#)

- » [Archives 2011](#)
- » [Archives 2010](#)
- » [Archives 2009](#)

- » [U.S. Digital Services Playbook](#)

CIO.GOV

[Privacy Policy](#) • [Accessibility Statement](#) • [USA.GOV](#)

GROWTH FACTOR

IT Projects that Match Your Goals

The best technology investments don't always have the largest ROI. Your portfolio needs to account for the future shape of your enterprise. **BY CHRIS POTTS**

The fundamental principle of portfolio management is that you first choose the goals for your portfolio and then select the investments that will achieve them. For investments in change, these goals are expressed as the results you want to accomplish (with corresponding measures and milestones) and the shape of the enterprise that the investments must deliver.

You can use these signs to assess whether your enterprise manages its investments in change as a portfolio:

- As your goals change—for example, from efficiency to growth—so does your portfolio.
- You select projects based on their contributions to the portfolio, rather than their standalone merits. This means turning down proposals that have positive ROI individually but don't fit the goals of the portfolio.
- You explore what each proposal would mean for the shape of the enterprise, considering factors other than cost.

This can mean investing in projects—such as redesigning a pivotal process—that have a low or negative return but are key to the enterprise's future. It can also mean rejecting projects that would undermine the organization's direction.

Better Investment Decisions

It's common for enterprises to treat the cost of a portfolio as the primary constraint when making decisions. But this approach can conceal other, possibly more significant, factors that drive the portfolio's success. These include the overall value that the portfolio is expected to deliver and the enterprise's capacity to make and exploit the changes that the portfolio represents. Exploring other prioritization criteria can result in a more productive and efficient portfolio and a higher project success rate.

Chris Potts is corporate IT strategist and CIO futurist with Dominic Barrow.

NEW MARKETS

More Help for When You're Hacked

Forensics tools let companies investigate intrusions remotely



How it works: Forensics software from vendors such as Guidance Software and Mandiant let companies remotely examine machines for evidence of intrusion. These applications help security professionals find signs that other tools miss—checking registry files, hard drives, even a computer's memory.

Who is doing it: Google's break with China in January over compromised e-mail accounts highlighted the need for global companies to adopt more sophisticated methods of protecting data. Gary Warner, director of research in computer forensics at the University of Alabama at Birmingham, says antivirus and anti-malware software isn't enough because hackers tailor malware for specific victims. China isn't the only worry, he adds, especially for companies in industries such as defense.

Growth potential: Forensics software represents a fraction of the security market, which IDC estimates is worth \$24.5 billion, but Guidance Software says its products are used by 20 percent of the Fortune 500. As western companies take a hard look at their security postures, forensics may become key to survival, say analysts. Today, if you work for the government or a company with sensitive business, "You don't take your own computer when you go to China because of the likelihood of intrusion," Warner notes.

—Robert McMillan

Copyright of CIO is the property of CXO Media Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.



Managing Capital Investments at the Indian Health Service

A “How-To” Guide to Risk Management

February 2013

Office of Information Technology (OIT)
Division of Information Resource Management
Albuquerque, New Mexico

ACKNOWLEDGEMENT

The Indian Health Service gratefully acknowledges the assistance of the National Institutes of Health, Office of the Deputy Chief Information Officer, in the preparation of this document.

Document Change History

Version Number	Release Date	Summary of Changes
1.0	July 14, 2006	Initial release
2.0	February 14, 2013	Updated document to be consistent with the Department of Health and Human Services Project and Portfolio Management tool and added questions to assist in the risk assessment.

Contents

PURPOSE	1
THE BASICS	2
What Is Risk?	2
What Is Risk Management?.....	2
How Do You Manage Risk?.....	3
DRAFT A RISK MANAGEMENT PLAN	3
ASSESS YOUR RISK.....	4
TRACK AND REPORT PROGRESS.....	7
Executing Risk Management Activities.....	7
Reporting Risk Management Progress.....	7
Reevaluating Project Risk	8
Conducting Lessons Learned Sessions	8
Documenting Lessons Learned Activities	9
RISK MANAGEMENT ROLES AND RESPONSIBILITIES	9
APPENDIX A. RISK MANAGEMENT PLAN TEMPLATE	A-1
APPENDIX B. CONDUCTING AN OPEN AND COMPREHENSIVE RISK REVIEW	B-1
APPENDIX C. SAMPLE RISK INVENTORY AND ASSESSMENT	C-1

Figures

Figure 1. Overview of Risk Management.....	2
Figure 2. The Risk Management Process.....	4

A “How-To” Guide to Risk Management

PURPOSE

This guide is intended to be used by project managers and project team members to manage the risks associated with their projects.¹ The purpose of this guide is to provide a basic, easy, step-wise method for managing the risks associated with a project; a method that is consistent with federal and Indian Health Service (IHS) requirements. *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, ANSI/PMI 99-001-2008 published by the Project Management Institute can provide a more comprehensive reference guide.

All information technology projects have risk. Risk management provides a means to identify the potential problems before they occur. Activities addressing these problems are planned and executed, as needed, across the life of the project to mitigate adverse impacts on achieving the project’s objectives. The purpose of Risk Management is to proactively identify and manage potential problems that may occur during a project’s implementation lifecycle. Risk management is a continuous process that will occur throughout the project lifecycle. Effective risk management includes early and aggressive risk identification through the collaboration of relevant project stakeholders.

The output of this process is a risk management approach to be used as part of the overall project management process.

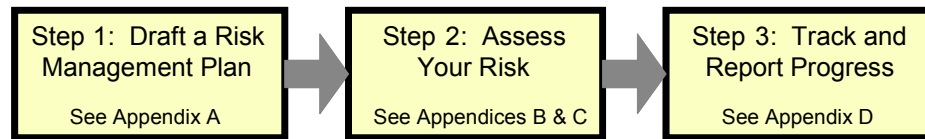
This process describes the following four activities and the steps involved in these activities:

- Identify and analyze risks early and determine their relative importance.
- Provide a tracking system to document, monitor, and update risks systematically.
- Manage risks by handling them appropriately.
- Make timely and appropriate decisions based on risk assessment and monitoring.

This guide first presents the basics of risk management, defining the terms and then providing a step-by-step approach to managing risks, following the steps shown in Figure 1.

¹ OMB uses the term “investment” to incorporate the projects, programs, systems, etc., that fall under the purview of the Capital Planning and Investment Control (CPIC) process. Because this guide supports the CPIC process, in this document, this document uses the term “project” to be synonymous with the term “investment.”

Figure 1. Overview of Risk Management



Appendix A contains a template for a draft risk management plan. Appendix B tells how to conduct a comprehensive risk review and Appendix C contains an example of a comprehensive risk review.

THE BASICS

What Is Risk?

A risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective, such as time, cost, scope, or quality. A risk may have one or more causes and one or more impacts.² For reasons of simplicity, we are only considering risks with negative outcomes. A risk is any factor that has the potential to interfere with the successful completion of the project. Risks are not events that have already occurred, but events that might occur and that have the potential to adversely impact the project in some way..

What Is Risk Management?

Risk management is an organized method of identifying, prioritizing, and measuring the impact of project risks and developing, selecting, and managing options for handling those risks—not necessarily to eliminate them entirely, but to minimize their impact on the project.

Managing project risk is a key component of good project management. Risks that are managed are minimized. Understanding and communicating risks help manage the expectations of senior management and other stakeholders. One such stakeholder, the Office of Management and Budget (OMB), requires a formal risk management plan for major projects and has in the past required annual reporting of risks and risk mitigation progress before approving requested project funding.³

² *A Guide to the Project Management Body of Knowledge*, Fourth Edition (PMBOK Guide), ANSI/PMI 99-001-2008, Project Management Institute, Inc, Newton Square, PA, 2008.

³ OMB does not specify a risk management plan format or content, but the previous reporting requirements of the Exhibit 300 imply obvious plan elements. These elements are also selection elements in the ProSight tool.

How Do You Manage Risk?

The appropriate level of risk management for any project depends on many factors (e.g., size, complexity, life-cycle phase, and stability) and determining that level requires candid management judgment. For example, a stable, straightforward application using established technology in the maintenance phase of its life cycle needs a far less extensive risk management program than a large, complex agency-wide system just beginning the development phase.

No one risk management approach is appropriate for all projects. Managers of smaller projects can profitably use elements of these risk management guidelines without the administrative burden of reporting risks to OMB. Those subject to OMB or HHS oversight *must* satisfy OMB requirements; risk status and mitigation must be well documented to be assured that the project manager is managing risks sufficiently well that project success is probable.

DRAFT A RISK MANAGEMENT PLAN

The risk management planning process begins with the selection of a risk management process model. One such model is shown in Figure 2. The risk management process model in Figure 2 is straightforward, and its elements are readily adaptable to the range of projects at IHS. The first four activities of the risk management process model depicted in the figure, designated as the planning phase and presented in the top row, specify the actions required to complete Step 2 of Figure 1, *Assess Your Risk*. The last three activities of the risk management process model, designated as the execution phase and presented in the bottom row of the figure, specify the actions required to complete Step 3 of Figure 1, *Track and Report Progress*.

Step 1: Draft a Risk
Management Plan

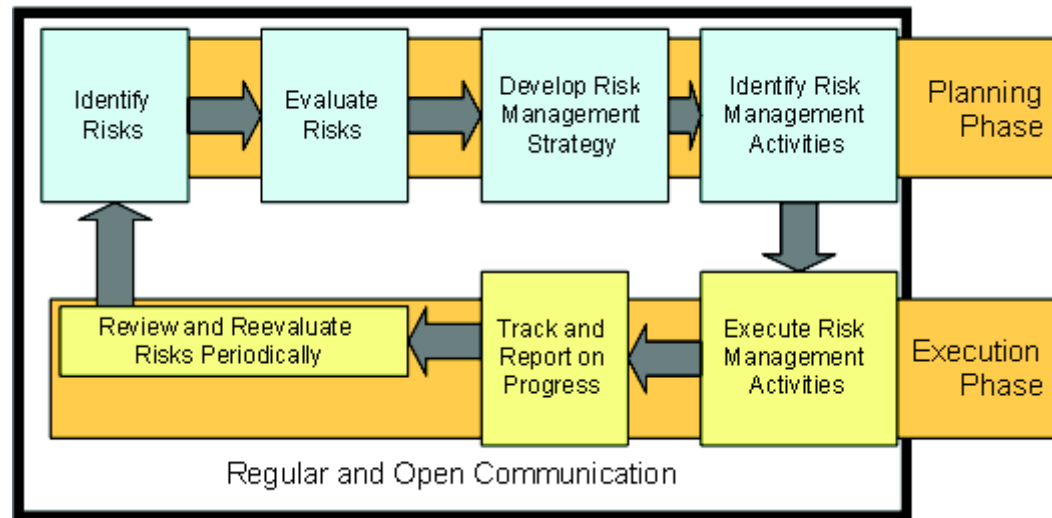
See Appendix A

To draft a plan for your project, you will have to consider what level of detail is required to identify risks, what methods are appropriate for evaluating the risks, who will be responsible for developing strategies to manage the risks, and how risk management actions will be developed, monitored, and reported. The level of funding, impact, or complexity of a project will determine how fully and detailed the risks are identified, managed, and tracked.

When completed, the risk management plan for your project should be dated and published. It should be made available to all project personnel, oversight and audit personnel, project sponsors, and other interested stakeholders.

A template for a risk management plan is presented in Appendix A.

Figure 2. The Risk Management Process



ASSESS YOUR RISK

The planning phase of the risk management process model provides an assessment of project risks, including understanding the nature, likelihood, and potential impact of risk. It has four discrete elements:

Step 2: Assess Your Risk

See Appendices B & C

- *Identify risks.* The risks inherent in your project should be defined in two ways: (1) they should be part of a continuous, ongoing part of project management so that risks are managed as risks arise; and (2) there should be a periodic, independent, comprehensive assessment of potential risks to assure that potential new risks are fully identified and managed.

As discussed in Appendix B, OMB has identified 19 risk categories, that provide a minimum set of risk areas to be considered by the project risk assessment team:

- 1) Schedule
- 2) Initial cost
- 3) Life-cycle cost
- 4) Technical obsolescence
- 5) Feasibility
- 6) Reliability of systems
- 7) Dependencies and interoperability
- 8) Surety (asset protections)
- 9) Risk of creating a monopoly

-
- 10) Capability of agency to manage the investment
 - 11) Overall risk of investment failure
 - 12) Organizational and change management
 - 13) Business
 - 14) Data/information
 - 15) Technology
 - 16) Strategic
 - 17) Security
 - 18) Privacy
 - 19) Project resources

- *Evaluate risks.* Once the risks have been identified, the Project Team will analyze those risks by determining how they might impede the overall success of the project if they occur. Each risk should be rated in terms of (1) the likelihood that the risk will occur and (2) its potential impact on the project if it does occur. This rating can be expressed as high, medium, or low for both probability of occurrence and for the potential impact. Then, a level of magnitude can be computed by assigning a numerical score to each risk by multiplying the numerical score of the risk's likelihood of occurrence by its potential impact score. By formally evaluating the risks in this way, the project team can determine how each risk should be managed, depending on its magnitude. Risks with a high magnitude should receive greater management attention than those with a low magnitude.

Risks with a high magnitude represent those risks that are deemed to pose the greatest threat to program success and accomplishment, i.e., the high-risk items. These items are typically reviewed at all internal program status reviews. Once a high magnitude risk is sufficiently mitigated that it can be closed out, it is reduced in priority and moved to an appropriate spot on the watch list. Caution must be exercised when closing out any risk from the high magnitude list. Closure does not mean file and forget. A closed risk may resurface and should continue to be observed, tracked, and documented.

After quantifying each high magnitude risk, the risks should be prioritized from the most to least important. This allows the team to focus on the most important risks first.

The Risk Assessment process should begin with the project team; however, all project stakeholders should have input. During regularly scheduled risk reviews, the project team will reassess risks previously identified, as well as newly identified risks.

-
- *Develop risk management strategy.* The most appropriate strategy for managing each risk should be determined. If a negative risk can be avoided (e.g., changing the project plan), if it is transferred (e.g., through the use of a firm fixed-price contract), or if it is accepted (e.g., there is no other suitable response strategy), it need no longer be part of the on-going risk management strategy, although it should be identified and the action taken on documented. The remaining risk management strategy for a negative risk should be to develop a mitigation strategy, which is what you do to try to keep the risk from occurring in the first place. For a positive risk (i.e., an opportunity), the risk management strategy may include exploiting it by insuring that the opportunity will definitely happen; sharing or transferring it to another organization that can best take advantage of it; or enhancing it or increasing the probability of the opportunity occurring. Regardless of whether the risk is positive or negative, if it is of medium or of high magnitude, you should also develop a risk management strategy or contingency plan, which is what you plan to do if the risk occurs.

The risk management strategy is expressed in a short statement that describes the approach to managing the risk. For a risk with a high magnitude, a specific risk owner may be assigned to manage the risk and its mitigation activities. For negative risks that cannot be mitigated or which are too expensive to mitigate, a risk response or contingency plan should be developed and documented in the risk log. The risk management strategy, along with any related work, e.g., controls, should be agreed to via consensus techniques.

Acceptable risk management options are:

- **Accept** – Accept the risk when there are no viable options to mitigate or avoid the risk, or where the management or avoidance of the risk is not economically practical. In situations where nothing can realistically be done to prevent a risk from happening, the project risks should have a higher degree of scrutiny so that the probability or impact of occurrence is minimized. The Project Sponsor will formally accept the potential impact of this risk on the project. There may be contingency plans or reserves developed for these types of risks. A contingency plan is a pre-defined action that can be implemented in the event that a previously identified risk occurs, in order to diminish impact on the project (i.e., “What should the team do if...?”).
- **Manage** - Reduce the expected impact associated with the risk through mitigation and contingency techniques. Mitigation is a preventative action, e.g., controls, that are performed to reduce the probability of the occurrence, increase the visibility of the risk, or reduce the seriousness of the impact should the risk occur (i.e., “What should the team do now to minimize or prevent the risk and to minimize its impact?”). There is usually a cost associated with a risk mitigation

approach. The estimated cost of such mitigation should be identified and documented in the Risk Log. Contingency outlines a “plan of action” to take if the risk occurs and becomes an event to be dealt with.

- **Avoid** - Eliminate the impact of the risk upon the project by formally transferring this risk to another party. This is usually accomplished through some form of contractual agreement.
- *Identify risk management activities.* The project manager, or risk owner if one is assigned, should develop an approach and action plan to implement the risk management strategy.

A guide for conducting an open and comprehensive risk review is presented in Appendix B and an example of a comprehensive Risk Log is contained in Appendix C.

TRACK AND REPORT PROGRESS

The execution phase of the risk management process model provides a periodic review of the status of risk management activities. Tracking and reporting progress on the actions taken to manage the risks include both monitoring the progress toward mitigating the risk and periodically reassessing risk..

Step 3: Track and Report Progress

See Appendix D

Executing Risk Management Activities

Overall execution of the risk management strategy and the corresponding management activities is managed by the risk owner. Risk management status is tracked against the planned risk management activities developed for each risk. HHS uses a commercial software package, currently Primavera ProSight, as its portfolio management tool (PMT) to track information technology investments that are subject to HHS review. The PMT provides forms to use for reporting project risks, their levels of magnitude, and their risk management strategies.

Reporting Risk Management Progress

Risk owners regularly report on their progress in implementing the risk management strategies and the current status of the risk management activities. These reports are presented to the other members of the project team at a level of detail commensurate with the risk magnitude and in the format prescribed by the project manager.

Progress may also be reported regularly to senior management outside the project team if appropriate.

Examples of reporting measures to be used can include:

- Number of risks identified, managed, tracked, and controlled.
- Monitoring the indicators that will trigger thresholds.
- Risk exposure and changes to the risk exposure for each assessed risk (as a summary percentage of management reserve).
- Change activity for the risk (e.g., processes, schedule, funding).
- Occurrence of unanticipated risks.
- Risk categorization volatility.
- Comparison of estimated versus actual risk management effort and impact.

Earned value management metrics can be used as “risk triggers” to predict when cost and schedule risks are likely to occur or whether they are sufficiently under control. Most projects are required to use earned-value management to track and report on cost and schedule performance. HHS has developed a three-tiered definition of projects that are required to report cost and schedule variances.

Reevaluating Project Risk

A comprehensive review and assessment should occur frequently, as determined by the Project Manager, but at least once per year. Reviews can be timed to provide current comprehensive information to assist the project manager with preparing reports, and as a minimum, for the annual IHS or HHS business case review and prioritization process.

During the reevaluation process, it may be determined that some risks that were identified in past evaluations, or as part of the ongoing risk identification process, have been successfully mitigated. These risks should still be listed on the risk inventory with an annotation that no action is necessary, the risk has been successfully mitigated. This will demonstrate that the risk was identified and managed at some time as part of the risk identification and assessment process.

Conducting Lessons Learned Sessions

The lessons learned activity involves determining the causes of variances in performance, the reason behind corrective actions chosen, and project activities that worked well and those that did not. Lessons learned should be documented as part of the historical record for the current project and as a “best practice” reference for future projects. The lessons learned review should be conducted following completion of each major lifecycle phase. At a minimum, projects perform a lessons learned review at the end of each phase and at project completion.

A lesson learned session serves as a valuable phase closure activity. The session provides an opportunity for public praise and recognition for project team members, allows the team to acknowledge what worked well, and offers an opportunity to discuss ways to improve processes and procedures.

Participants of a lessons learned session are typically the Project Manager and project team. It may also include the customer and/or external stakeholders as appropriate. Some typical questions to answer include the following:

- In this process or sub process, what did we do well? What could we have changed?
- Did the delivered product meet the specified requirements and goals of the project?
- Was the customer satisfied with the end product?
- Did the project stay within scope?
- Were cost budgets met?
- Was the schedule met?
- Were risks identified and mitigated?
- Were problems or issues resolved timely and adequately?
- Did all of the components of the project management methodology work? If not, which ones did not, and why?
- What could be done to improve the process?

Documenting Lessons Learned Activities

Lessons learned are captured and documented to be housed with other project files and closure documentation. At a minimum, projects should perform a lessons learned review at the end of each major lifecycle phase and at project completion.

RISK MANAGEMENT ROLES AND RESPONSIBILITIES

The project manager is responsible for overseeing, monitoring, and assigning all risk management activities, among other project management responsibilities.

The risk owner is responsible for overall execution of the risk management strategy and the corresponding risk management activities, including the following:

- Proposing a strategy for mitigating the assigned risk and getting the strategy approved by the project team and project manager.
- Developing an approach and action plan to execute the management strategy.
- Tracking and reporting on the progress in mitigating the risk.

APPENDIX A. RISK MANAGEMENT PLAN TEMPLATE

This appendix contains an annotated outline of a risk management plan adaptable to individual projects.⁴ Use the outline headings for your risk management plan and follow the guidance under the headings:

- *Red italicized text* describes what should be in each section of the risk management plan.
- Black text may be used in your plan as is, or with minor modification.
- Blue underlined text indicates that you “fill in the blank.”

⁴ Risks should be managed for all projects, regardless of size, and the processes for doing so should be documented. Smaller projects may require a lesser degree of risk management than do larger projects.



Project Name

Risk Management Plan

Version 1.0

DATE

Organizational Unit

Location

UPDATE HISTORY

Version	Date	Nature of Change	Comment
1.0	Date	Initial Draft	

TABLE OF CONTENTS

I. Purpose	1
II. Background	1
A. Organizational Mission	2
B. Project Description	2
III. The Project Name Risk Management Process	2
A. Planning Phase	3
B. Execution Phase	10
IV. Risk Management Roles and Responsibilities	12
A. Project Manager	13
B. Risk Owner	13

I. PURPOSE

To introduce the plan, provide a short statement of the purpose, such as the following:

The purpose of this risk management plan is to provide a framework for managing the risks that could hinder the success of [Project Name](#). This risk management plan provides guidelines for identifying, analyzing, documenting, mitigating, and monitoring events that might adversely affect the project. Specifically, this plan provides procedures that

- serve as a basis for identifying, documenting, analyzing, and prioritizing risks associated with the project and for developing management strategies to handle those risks, and
- enable Indian Health Service (IHS), [Area Office](#), and [Organization Unit](#) executives and the project team to monitor the health of the project throughout its life cycle.

All information technology projects have risk. Risk management provides a means to identify the potential problems before they occur. Activities addressing these problems are planned and executed, as needed, across the life of the project to mitigate adverse impacts on achieving the project's objectives. To ensure the lowest possible risk in the performance of project efforts, the established goals for this Risk Management Plan are to:

- Identify and analyze risks early and determine their relative importance.
- Provide a tracking system to document, monitor, and update risks systematically.
- Manage risks, if necessary, by handling them appropriately.
- Make timely and appropriate decisions based on risk assessment and monitoring.

II. BACKGROUND

If the risk management plan is a component of the project management plan, this section may be omitted as it is superfluous. If the risk management plan is a stand-alone document, include a Background Section to place the plan in its context.

A. Organizational Mission

In this section, describe the mission of the organization or operating unit. The mission of the organization or operating unit can probably be extracted from the IHS website and should be edited to focus on that part of the mission that is most relevant to the project's scope and objectives. The description of the mission should be no more than one page.

The Indian Health Service (IHS), an agency within the Department of Health and Human Services, is responsible for providing federal health services to American Indians and Alaska Natives. The provision of health services to members of federally-recognized tribes grew out of the special government-to-government relationship between the federal government and Indian tribes. This relationship, established in 1787, is based on Article I, Section 8 of the Constitution, and has been given form and substance by numerous treaties, laws, Supreme Court decisions, and Executive Orders. The IHS is the principal federal health care provider and health advocate for Indian people and its goal is to assure that comprehensive, culturally acceptable personal and public health services are available and accessible to American Indian and Alaska Native people. The IHS currently provides health services to approximately 2 million American Indians and Alaska Natives who belong to more than 566 federally recognized tribes in 35 states.

Describe the mission of the organizational unit that is or will be using the system. This description should put the system in its proper context and should be about one page.

B. Project Name Description

Describe the project's purpose, history, scope, concept of operations, future plans, and life-cycle phase. This should be about one or two pages.

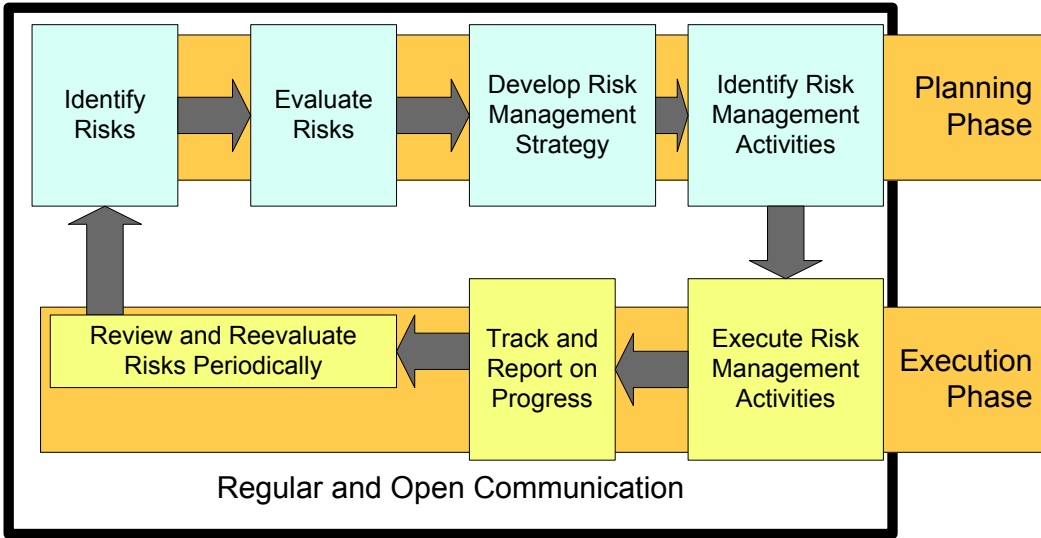
III. THE PROJECT NAME RISK MANAGEMENT PROCESS

Select a risk management model to be followed. Several are available, including one from the Software Engineering Institute of Carnegie Mellon University.

Describe the model and show it graphically.

Figure 1 depicts the process used to manage risks associated with Project Name. As the figure shows, the process has two phases: a planning phase, and an execution phase. Risk management activities are conducted in an overall atmosphere of regular and open communication within the project team and among stakeholders and users.

Figure 1. Project Name Risk Management Process



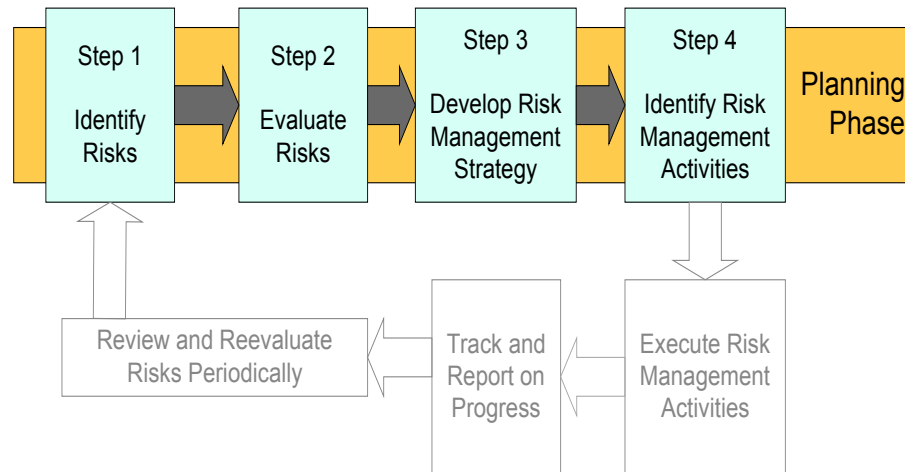
A. Planning Phase

The planning phase of the risk management process has four steps:

- Identify risks
- Evaluate risks
- Develop risk management strategy
- Identify risk management activities

Figure 2 highlights the four steps in the planning phase.

Figure 2. Project Name Risk Management Process—Planning Phase



1. IDENTIFY RISKS

Define risks and describe the process for identifying risks. The following is an example.

Risk identification involves recognizing the critical events that, if they occurred, would prevent the project from achieving its objectives. These events may be related to technological or process uncertainty, cultural resistance to change, lack of progress, failure to achieve critical metrics, or many other factors.

The first step in preparing for risk management is to determine risk sources and categories. Sources are both internal and external to the project. Internal risks are assumed to be capable of being mitigated by the project manager and team. External risks are usually assumed to be outside the control of the project manager and team and will usually need to be elevated to a higher level of management for action or a contingency plan may need to be developed in the event the risk occurs. Due to the dynamic nature of most projects, risk sources can change over the life of the project and will need to be reviewed periodically.

One key factor in recognizing and communicating risk is to state it properly. Best practice is to define specific risks in cause-and-effect statements. State your intent to do so and give a few examples of risk statements that are relevant to the project and its current life-cycle phase. Here are two examples:

“If data supporting the legacy system are not accurate and complete, then successful transition to the new system will be jeopardized. “

“If the acquisition process does not include detailed selection criteria and an evaluation plan, then the selection may not be the ‘best value’ for IHS, and it will not be legally defensible. “

Describe both continuous and periodic, comprehensive processes for identifying risks. First, introduce the subject.

- Throughout the project's life cycle, risks will be identified in two ways: (1) they will be part of a continuous, ongoing part of project management so that risks are identified and managed as risks arise; and (2) there will be an annual independent, comprehensive assessment of potential risks to assure that potential new risks are fully identified and managed.

Risk sources identify common areas where risks may originate. The following are considered when developing the source lists:

- Changing uncertain requirements
- Change in business need
- Organizational change
- Unprecedented efforts – estimates unavailable
- Infeasible design
- Unavailable technology
- Unrealistic schedule estimates or allocation
- Inadequate staffing, skills, or tool resources
- Cost or funding issues
- Uncertain or inadequate new subcontractor capability
- Uncertain or inadequate new vendor capability
- Other risks outside of the realm of technology.

a. Continuous Risk Identification

Because continuous methods of identifying risk are the first line of defense for a project or program, the project team must maintain an atmosphere of open, candid communication.

Continuous risk identification procedures may vary considerably, from one in which any project team member or stakeholder can formally identify a perceived risk by sending the project manager an e-mail, to procedures involving formal risk identification documentation and a risk committee to evaluate and accept them. Determine the most appropriate level of continuous risk identification for

your project and describe it in a few paragraphs. A smooth-running project in its steady-state phase will require a lesser degree of continuous risk identification than a complex, mission-critical project just beginning the development phase. Use your own judgment to define the best risk identification procedures for your project.

b. Periodic, Comprehensive Risk Identification

In addition to continuous methods of assessing risk, a comprehensive risk assessment should be a regular part of the project's risk management process. At least annually (and more often if necessary, such as at a significant project milestone), the project team should conduct a comprehensive review of project risks. For example, the review could correlate with the agency budget process and the review and prioritization of agency business cases. Review Appendix B, "Conducting an Open and Comprehensive Risk Review" of this document to determine the appropriate level and schedule for your project. Then describe the chosen approach in a few paragraphs.

2. EVALUATE RISKS

Introduce risk evaluation.

During the risk evaluation process, the project team will assess all suggested risks, assign each to a risk owner, and enter the risk into the risk tracking process.

a. Risk Rating Method

Describe the method to be used to rate the risks. The following paragraphs describe a two-stage method by first assessing the probability that the risk will occur and the impact of the risk. We then calculate the risk magnitude. Risk Magnitude (=Risk Probability of Occurrence times Risk Impact) is used by the portfolio management tool (PMT) that HHS and IHS use to evaluate the projects for investments that require HHS review and to track those projects. A scoring scheme of High=3, Medium=2, Low=1 is used.

Risk evaluation is an assessment of the magnitude of the identified risks. The [Project Name](#) team will measure the risk magnitude by combining estimates of the estimated probability of the risk occurring and the risk's potential impact. The management of risks with a greater magnitude receives more management attention than the management of risks with lesser levels of magnitude.

Table 1 provides the ratings and guidelines for the estimated probability that the risk situation will occur. Table 2 provides the ratings and guidelines for estimating the degree of impact on the project if the risk is not mitigated.

Table 1. Probability of Occurrence

Probability	Rating	Guideline
Low	1	Below 30% probability of occurrence
Medium	2	Between 30% and 70% probability of occurrence
High	3	Greater than 70% probability of occurrence

Table 2. Degree of Impact

Impact	Rating	Guideline
Low	1	Will have minor impact on system development or operation
Medium	2	Will likely cause delay in one or more functions required to develop or operate the system
High	3	Will likely cause a significant delay and/or stoppage in system development or operation

The magnitude for each risk is then calculated by multiplying its rating for degree of impact by its probability of occurrence rating:

$$\text{Risk Magnitude} = \text{Probability} \times \text{Impact}.$$

Table 3 shows the guidelines used to determine the risk magnitude for each attribute.

Table 3. Risk Magnitude

Magnitude	Rating	Guideline
Low	1 or 2	Low likelihood of the risk moderately impacting one or more factors.
Medium	3 or 4	Medium likelihood of the risk moderately impacting one or more factors.
High	6 or 9	High likelihood of the risk severely affecting one or more factors. May have a high potential of causing program stoppage.

b. Actions for Different Risk Magnitude Ratings

Different risk magnitude ratings may require the project manager and the risk owner to apply different risk management actions, such as the following:

- Notifying senior management of project risk. A risk with a probability of occurrence of High = 3 and potential impact on the program of High = 3,

resulting in a risk magnitude of High = 9 might be required to be reported as soon as possible to senior management officials (the project sponsor and the IHS Chief Information Officer (CIO), for example).

- Assigning a risk owner. A risk with a medium or high magnitude (risk magnitude = 3, 4, 6, or 9) might have a risk owner assigned and have risk management activities developed for it. Risks with a lower risk magnitude might be handled in a less intensive manner.
- Developing a risk management strategy and plan. A risk with a low magnitude (risk magnitude = 1 or 2) might be tracked by the project manager but not have an assigned risk owner or risk management activities.

Appropriate risk management action depends on risk magnitude, the nature and complexity of the project itself, and good management judgment.

Determine the appropriate level of risk tracking for your project and describe it in a few paragraphs.

3. DEVELOP RISK MANAGEMENT STRATEGY

The most appropriate strategy for managing each risk should be determined. If a negative risk can be avoided (e.g., changing the project plan), if it is transferred (e.g., through the use of a firm fixed-price contract), or if it is accepted (e.g., there is no other suitable response strategy), it need no longer be part of the on-going risk management strategy, although it should be identified and the action taken on documented. The remaining risk management strategy for a negative risk should be to develop a risk management strategy, which is what you do to try to keep the risk from occurring in the first place.

For a positive risk (i.e., an opportunity), the risk management strategy may include exploiting it by insuring that the opportunity will definitely happen; sharing or transferring it to another organization that can best take advantage of it; or enhancing it or increasing the probability of the opportunity occurring.

Regardless of whether the risk is positive or negative, if it is a risk that is being managed and is of medium or of high magnitude, you should also develop a risk response or contingency plan, which is what you plan to do if the risk occurs. The risk management strategy is expressed in a short statement that describes the approach to managing the risk. For a risk with a high magnitude, a specific risk owner may be assigned to manage the risk and its management activities. For negative risks that cannot be mitigated or which are too expensive to mitigate, a risk response or contingency plan should be developed.

Give one or two examples that are relevant to your project. An example follows:

It is the responsibility of the risk owner to develop an appropriate risk management or risk management strategy and to get it approved by the [Project Name](#) team.

The risk management strategy is a short statement that describes the approach to managing the risk. For example, the statement below describes a mitigation strategy for a system interface risk:

“The organization will acquire an independent validation and verification (IV&V) contractor to assist with developing interface test requirements and an integrated test plan, and it will perform interface testing before acceptance.”

The statement below is an example of a mitigation strategy for the risk of declining system effectiveness from the perspective of users:

“Continuous assessment of program usability and effectiveness will be maintained through open communication and regular user group meetings. Users will participate in annual program risk assessment exercises.”

Management strategies may be even more concise. Here’s an example of a security risk mitigation statement:

“The project manager will implement the security protocols provided by IHS and NIST.”

There are other approaches to risk management other than mitigation that may be appropriate. Any of these approaches could be a risk management strategy that should be documented in the risk management plan:

- Changing the project plan to eliminate the risk altogether
- Transferring the risk impact to a third party
- Accepting that there is no cost-effective approach to mitigation and that contingency planning will be the best way to manage the risk. Active acceptance may involve the creation of contingency plans and passive acceptance may leave actions to be determined as needed. A decision to accept a risk must be communicated to stakeholders.

4. IDENTIFY RISK MANAGEMENT ACTIVITIES

Describe how you plan to have risk management actions developed by the risk owner (or whomever else might be assigned responsibility for developing the plans), and how risk management activities are approved, tracked and reported.

A variety of approaches are possible depending on the complexity and life-cycle phase of the project and the complexity of the risk management strategy. For example, for simple risk management strategies, a list of actions with due dates and responsibilities may suffice. Or, for complex or high-magnitude risks, a detailed plan for risk management might be needed. Using Microsoft Project as a tool to help manage the risk management activities may be appropriate.

Determine the best approach for your project and describe it in a few paragraphs. Say something like the following.

Once the risk management strategy is approved by the project team, the risk owner will develop an approach and propose actions to execute the risk management strategy. The proposed actions are defined in a work plan, unless a more detailed approach is directed by the project manager.

With the help of the project manager, appropriate members of the team and others as necessary, the risk management actions will be assigned to specific individuals and formalized.

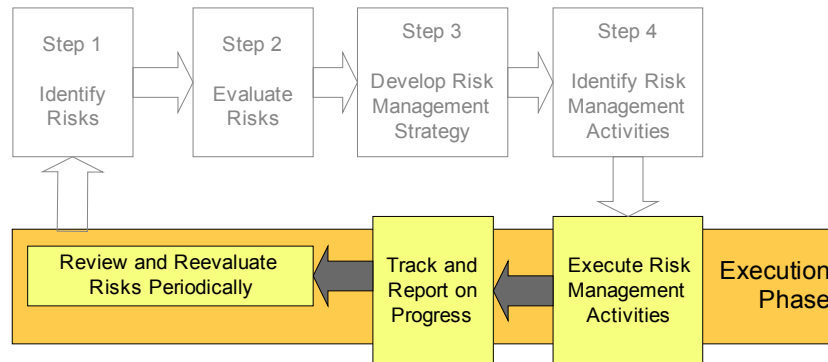
The risk owner tracks and reports on progress toward risk management at predetermined risk review sessions conducted by the project team—at least monthly.

B. Execution Phase

Figure 3 highlights the execution phase of the risk management process. This phase has three steps:

- Execute risk management activities
- Track and report on progress
- Review and reevaluate risks periodically

Figure 3. Project Name Risk Management Process—Execution Phase



1. EXECUTE RISK MANAGEMENT ACTIVITIES

Describe responsibilities for execution of the risk management activities in a few paragraphs. Say something like the following.

Those responsible for executing the risk management activities will execute them in accordance with the plans managed by the risk owners.

The risk owner maintains responsibility for overall execution of the risk management strategy and the corresponding risk management activities.

2. TRACK AND REPORT ON PROGRESS

Describe how information on risks and risk management planned activities will be tracked. Begin by stating something like the following.

Performance and progress on mitigating the risks are tracked against the risk management activities. Progress against the risk management plan is available for review by the project manager and designated members of the project team at any time.

Then, describe the reporting schedules and venues for reporting by the risk owners. Many reporting options are possible depending on the nature of the project and the severity of the risk. Low-severity risks on stable operating systems may be reviewed by the project team at a regularly scheduled meeting at least once each quarter. For complex or high-magnitude risks or for risks associated with a large, complex, and mission-critical project, more frequent reporting is warranted. In some cases, it may be appropriate to hold a weekly or monthly ad hoc project risk meeting that is attended by stakeholders and senior managers, as well as team members.

In all situations, information on risks, their risk management strategies, risk management activities, and progress toward mitigation should be available to appropriate staff and managers.

Progress toward mitigating risks will be reported annually to senior [Area Office/Organization Unit](#) and IHS management and to OMB through the CPIC process and the OMB Exhibit 300.

If you plan to report high risks to senior management as soon as they are identified, as discussed in the Evaluate Risks section (III. A. 2. b), include this reporting requirement here as well. The following is an example.

The IHS CIO will be notified and briefed whenever a high-magnitude risk is identified.

3. REVIEW AND REEVALUATE RISKS PERIODICALLY

Describe plans for periodic review and reevaluation of risks. It should be done at least annually but should also be performed at significant project milestones, such as after selection of a system integrator or at completion of end-to-end testing. Describe what is appropriate for your project. The following is an example.

The project team, led by the project manager, will assist with a periodic comprehensive review of the risk posture of the [Investments](#). This review will take place at least once each year in preparation for the annual business case review and prioritization by the IHS Information Technology Investment Review Board (ITIRB).

During the reevaluation process, it may be determined that some risks that were identified in past evaluations, or as part of the ongoing risk identification process, have been successfully mitigated. These risks will still be listed on the risk inventory with an annotation that no action is necessary, the risk has been successfully mitigated. This will demonstrate that the risk was identified and managed at some time as part of the risk identification and assessment process.

IV. RISK MANAGEMENT ROLES AND RESPONSIBILITIES

Describe the risk management roles and responsibilities for your project. Include at least the project manager and the risk owner. Review and cite the roles and responsibilities sections for the CPIC program contained in Capital Planning and Investment Control Policy and Guidelines issued by the Office of the CIO. Say something like the following.

The project manager and the risk owner have specific risk management responsibilities for project risk management.

A. [Project Name](#) Project Manager

The project manager is responsible for overseeing, monitoring, and assigning all risk management activities.

The project manager will schedule a periodic independent review of program risks at least once each year. This review will cover the perspectives of all program stakeholders. It will result in identified risks, risk ratings, and suggested risk management strategies.

B. Risk Owner

The risk owner has the following responsibilities:

- Propose a strategy for mitigating the assigned risk and get the strategy approved by the team and project manager
- Develop an approach and action plan to execute the risk management strategy
- With the help of the project manager, assign responsibility for completion of the action plan steps
- Track and report on progress in mitigating the risk

APPROVALS:

Jonas Salk
Project Investment Manger

Date

Howard Hays
Chief Information Officer (Acting)

Date

Samuel Mudd
Project Sponsor

Date

APPENDIX B. CONDUCTING AN OPEN AND COMPREHENSIVE RISK REVIEW

Risk management includes assessment of risk, development and execution of risk management strategies, and monitoring of progress. This appendix provides guidance on how to conduct a risk assessment.

Risk assessment involves identifying and understanding the potential risks during project development and implementation: the events that, if they occurred, would prevent the project from achieving its cost, schedule, or performance objectives. These events may be related to technological or process uncertainty, cultural resistance to change, lack of progress, failure to achieve critical metrics, or many other factors.

One effective way of assessing risk is through a periodic, open and comprehensive risk review.⁵ The risk review team normally consists of a leader and one or two team members. The team convenes representatives from the project staff, users, and stakeholders in an environment of open communication. The risk review must be comprehensive so that the full spectrum of risks from all sources is considered. During a risk review, the risk assessment team must ask the right questions and ask the right people, as shown in Figure B-1.

Figure B-1. Two Elements of Effective Risk Assessment



Ask the Right Questions

Risks that are managed are minimized. Understanding and communicating project risks help manage the expectations of senior management and other stakeholders. One such stakeholder, OMB, may ask for the formal risk management plan and annual reporting of project risks and risk management progress before approving requested project funding.

OMB's risk management reporting requirements for large projects are useful for managing risk in projects of all sizes because they contain a broad, comprehensive set of risk categories that are useful to project managers as a starting point for defining their project risks.

⁵ Two important ways of identifying risk are continuous risk identification, which requires an open and honest exchange of ideas as part of daily project management, and comprehensive risk identification, which entails a periodic assessment of risk on a project-wide basis. For additional information on these types of risk identification, see Appendix A, Section III.A.1, Identify Risks.

OMB has identified 19 risk categories, presented in Figure B-2, that provide a minimum set of risk areas to be considered by the project risk assessment team.

Figure B-2. OMB’s 19 Risk Categories

Risk Categories for All Investments	Risk Categories for IT Investments
1) Schedule	12) Organizational and change management
2) Initial cost	13) Business
3) Life-cycle cost	14) Data/information
4) Technical obsolescence	15) Technology
5) Feasibility	16) Strategic
6) Reliability of systems	17) Security
7) Dependencies and interoperability	18) Privacy
8) Surety (asset protections)	19) Project resources
9) Risk of creating a monopoly	
10) Capability of agency to manage the investment	
11) Overall risk of investment failure	

The figure separates the risks into two categories: (1) those for all investments and (2) those for IT investments. There are similarities between those in the first set of risk categories and those in the second. It is helpful to consider the risks grouped according to their overall management-related area. Reordering the risk categories into related risk areas, as shown in Figure B-3, makes them more user friendly and more meaningful to technical personnel, functional users, and senior management.

Figure B-3. Restructured OMB Risk Categories

Restructured Investment Risk Categories	
<u>Business Impact</u> 16—Strategic 13—Business 5—Feasibility 9—Risk of creating a monopoly	<u>Resource Availability</u> 19—Project resources 1—Schedule 2—Initial cost 3—Life-cycle cost
<u>Management and Oversight</u> 10—Capability of agency to manage the investment 12—Organization and change management 7—Dependencies and interoperability	<u>Technical Issues</u> 4—Technical obsolescence 15—Technology 6—Reliability of systems 14—Data/information
<u>Security</u> 17—Security 8—Surety 18—Privacy	<u>Summary of Risk</u> 11—Overall risk of investment failure

The order of assessing these risks doesn't matter. However, it improves the ability of the risk assessment team to identify risks if the assessment starts with those areas that are broadest in scope. The risk assessment leader should start the assessment with Business Impact; the highest level, least technical of the risk areas. Next the risk assessment leader should address the other areas according to Resource Availability, Management and Oversight, Technical Issues, and Security, the most narrow and specialized area. The risk assessment leader should address the Summary of Risk last. Table B-1 lists the order in which the risks should be addressed and provides some examples of topics that may be considered while assessing risk in each risk category.

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Business Impact	16—Strategic	Risk associated with strategic/government-wide goals top management support and communication, consistency with strategic plans, high-level visibility with outside stakeholders such as OMB or Congress, and other political impacts. Risk that the proposed alternative fails to result in the achievement of those goals or in making contributions to them. Risk that strategic goals and objectives, including PMA goals or HHS priorities, may change. Risk that the objectives of the project are not clearly linked to program needs, to the agency's overall strategies, and to government-wide policies and standards. Risk that the initiative is not based on clearly understood needs or opportunities and is inconsistent with the overall strategies and architectures used by the agency and the federal government (i.e., Federal Enterprise Architecture).	• Does this project support a government wide initiative? • Does this project support the strategic goal(s) of HHS or of the OPDIVs? • Have stakeholders (e.g., OPDIVs) been engaged? Do stakeholders have buy-in with scope and requirements?
	13—Business	Risk associated with the validity of the business case for the project, the completeness and validity of the specified functional requirements, and the need for reengineering subject business processes. Risk that the business goals of the program or initiative will not be achieved. Risk that the program effectiveness targeted by the project will not be achieved.	• Is the business need and project scope well-defined? • Have the planned improvements/benefits to business operations or customer results been documented? • Have operational performance measures been identified and signed-off by the sponsor and (OPDIVs) major stakeholders? • Has an Operational Analysis been performed at least annually? • Have any shortcomings been identified?
	5—Feasibility	Risk associated with the feasibility of the requirements from a technical and performance point of view and the organization's familiarity with the project life-cycle method used within the organization or as implemented by others. Risk of insufficient ability to successfully develop and implement the project within defined technical, scope, cost, and schedule parameters to successfully meet the performance goals.	• Is the proposed technology involved feasible? • Has an alternatives analysis been performed, is it less than 3 years old? Does/did the alternatives analysis examine use of other technologies (e.g., different COTS products and/or different hosting solutions: Cloud Computing/private cloud)? • Is the proposed solution feasible? • Is the solution as simple as possible?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Business Impact	9—Risk of creating a monopoly	Risk associated with the over-reliance on a particular vendor or on proprietary or specialty software that would limit project expansion or flexibility.	Does the technology/vendor selected trigger a risk that the Department/OPDIV will be locked in to a specific set of vendors and their products?
Resource Availability	19—Project resources	Risk associated with the stability and adequacy of project staff and project budget for today and the future. Include resources that might be available from contractors. Risk that the availability of people, funds, schedule, and tools that are the necessary ingredients for successfully implementing the project will be inadequate (if any are inadequate, including the qualifications of the people, there is risk). Risk that appropriate training will not be available in a timely fashion.	- Do the COTS vendors have an established reputation of delivering quality product on time? - Are the contractors qualified for this type of work; do they have an established track record? - Are requirements/scope, cost and schedule well defined? - Are necessary algorithms or work flows well understood? - Do the contract vehicles provide cost controls; are they appropriate to the product and/or service to be provided? - Has the project management team worked with the business owners/stakeholders to identify capabilities or components that might need to be reschedule or delayed in the event that budget cuts affect the ability to authorize and execute tasks as planned?
	1—Schedule	Risk associated with the stability, reality, and validity of the time estimated and allocated for the development, deployment, and operation of the system. Include the cost or impact of not meeting the schedule. Two risk areas bearing on schedule risk are (1) the risk that the schedule estimates and objectives are not realistic and (2) the risk that program execution will fall short of the schedule objectives.	- Does the project have an Integrated Master Schedule? - Is there a high level of confidence in the schedule for the project? - Does the schedule address all of the EPLC documentation in addition to the functional deliverables? - If processes and procedures are being affected is delivering training and developing the related documentation included in the schedule?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Resource Availability	2—Initial cost	Risk associated with the adequacy, completeness, accuracy, and validity of the initial funding estimates, the supporting information that justifies those initial funding estimates, and their relationship to longer term funding needs.	• Is there a high level of confidence in the estimates for the project? • Is the project scope sufficiently defined to identify size/scale/complexity of the project effort? • Are the estimates based on two or more reliable estimating techniques? • Have management and oversight requirements, such as workflow/status reporting, identified? • Are the requirements well understood and well developed? • Are security requirements well established? • Do security requirements include audit logging and regular analysis of audit logs? • In addition to the functionality and security requirements, have all of the “ility” requirements been identified (i.e., reliability, availability, maintainability, usability, supportability, etc.)?
	3—Life-cycle cost	Risk associated with the adequacy, completeness, accuracy, and validity of life-cycle cost estimates, the supporting information that justifies those life-cycle funding estimates, and the likely stability of longer term availability of funds. This includes the impact of errors in the cost estimating technique(s) used (given that the technical requirements were properly defined). Lifecycle costs include planning, development, operations, and retirement costs.	• If this project is going to be followed by additional functionality • Is there a good understanding of the projects/enhancements that are needed? • Has the additional functionality been considered in the design? • Is the system solution designed to be maintainable • Is the design and acquisition structured so the solution is not a proprietary solution that can only be supported by one vendor/competitor? • Are training and maintenance costs considered in the life cycle cost analysis? • Will the planned solution/system be supportable, and maintainable? • What is the plan for maintaining the system once it is deployed? • Is there funding to maintain this system?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Management and Oversight	10—Capability of agency to manage the investment	Risk associated with the experience of the project manager and staff in the development or operation of systems with similar complexity and/or size, the application domain, and the functional business processes involved. Risk associated with the existence of an experienced project management team, appropriate project management structures, executive management support, governance, clear and defined responsibilities, as well as demonstrated experience in managing the development or operation of projects of similar complexity and/or size, the application domain, and the functional business processes involved. Also relates to the degree to which program plans and strategies exist and are realistic and consistent.	- Does the project have a PM with experience in this type and/or size of project? - Does the PM have certification and/or appropriate training? - Does the project have team members with appropriate experience to manage, track progress and ensure quality deliverables (e.g., PM, EPLC or technical expertise appropriate to type of project)? - Are good project management, acquisition management, requirements management, etc., controls in place? - Are there adequate tools for planning and managing the project?
	12—Organization and change management	Risk associated with the willingness and ability of the organization/agency to accept the cultural, process, and procedural changes required by the project. Include the existence or adequacy of the change management plan, communications plan, and user training plan. Risk associated with bypassing, lack of use, improper use, or adherence to new systems and processes due to organizational structure and culture; inadequate training.	- Is organizational change required? - Is reengineering/ reorganizing of business processes or workflows required? - Is there adequate backing by sponsors and key stakeholders? - Are planned changes well communicated? - Is training for new system as well as new processes planned?
	7—Dependencies and interoperability	Risk associated with the dependence of the project on data from other systems and processes (existing and planned) (existing or in development) within the Agency and across the Federal Government (e.g. technical interfaces, schedule dependencies). Risk associated with the requirement for the project to operate in concert with other programs. Include related schedule and funding concerns. Risk is increased if the success of a project is directly linked to the success/ implementation or on-going maintenance of other systems.	- Are the internal and external interfaces identified and well understood? - Are dependencies and interoperability requirements well defined? - Is there an Interface Control Document (ICD) for each interface/connection between communicating systems that specifies the data, format, communications protocol, periodicity, expected volumes, etc? - Are there signed Service Level Agreements (SLAs) or Memoranda of Understanding (MOUs) that address reliability, availability, security data integrity, etc?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Technical Issues	4—Technical obsolescence	Risk associated with the likelihood of the technology becoming obsolete because of changing technology or requirements. Include technology support from the existing supplier and ability of in-house staff to manage support. Risk that strategies for avoiding the use of outdated technical resources over the system life are not planned for and implemented. A plan for regular technology upgrade or refresh is one way to avoid obsolescence by ensuring the use of advanced versions of equipment or software when they become available.	• Is the technology “aging” and in danger of obsolescence? • Is there a danger that the development language or other COTS products are so old that it would be difficult to get and/or maintain a qualified team for the project as well as the anticipated life cycle of the system? • If this project provides an upgrade or replacement to an existing system, are there plans for retirement and disposition of the current system/solution?
	15—Technology	Risk associated with the existing or chosen software, hardware, and network reliability, maintainability, and security. Include technology documentation, testability, and appropriateness for the functional need in the existing or future environment. Risk associated with immaturity of commercially available technology. Risk of technical problems/failures with applications and their ability to provide planned and desired technical functionality. Technical risk addresses the possibility that the application of software engineering theories, principles, and techniques will fail to yield the appropriate software product. Technical risk is comprised of the underlying technological factors that may cause the final product to be overly expensive, delivered late or otherwise unacceptable to the customer.	• Is the technology bleeding edge? • Is the technology considered mature enough to be reliable? • Are there multiple vendors that are able to provide the support/services needed on this technology? • Do the team members have appropriate expertise? • Is the technology mature enough?
	6—Reliability of systems	Risk associated with the defined response time and throughput requirements as needed and expected. Include system contingency plans, continuity of operations plans, disaster recovery plans and tests of those plans. Risk of inability of the system to provide planned and desired functionality.	• Does the proposed solution provide a sufficiently robust and/or redundant solution that system and data availability requirements are met? • Are physical and IT security measures sufficient to ensure the security of the IT system and the integrity of the data?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Technical Issues	14—Data/information	Risk associated with the clarity, completeness, validity, sources, and feasibility of data requirements. Include data interface and data conversion complexities. Include data collection, storage, integrity, and availability. Risk associated with the loss/misuse of data or information, risk of increased burden on citizens and businesses due to data collection requirements if the associated business processes or the project require access to data from other sources (federal, state and/or local agencies).	• Has a Privacy Impact Assessment (PIA) been performed or revisited in the last 2 years? • If any Personally Identifiable Information (PII) is collected, has the need for that information been established? • Have the requirements for the analysis, reporting and or other use of this data been well established? • If multiple sources of PII are combined, has that been announced in a System of Records Notice (SORN)? • Are processes and security controls in place to ensure authorized users have a need for access to the system/data and that the users are granted only the (role-based) access they need? • Are there controls in place to prevent unauthorized access/viewing, combination, and/or analysis of the PII? • Are data being supplied by trusted sources? • Is there a way to check the integrity and/or validity of the data? Are interfaces and data feeds/pulls well defined? • Is there a data migration plan for transition of data from legacy to replacement system(s)? • Is there an approved records management plan?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Security	17—Security	Risk associated with the security/vulnerability of systems, websites, information and networks; risk of intrusions and connectivity to other (vulnerable) systems Risk associated with the misuse (criminal/fraudulent) of information Risk associated with the validity and effectiveness of the organization security plan, the plan's compliance with NIST requirements, associated plans to certify and accredit the IT system prior to implementation, and the organization's ability to implement the plan. [Note: This risk category must include in the risk description the level of risk (high, medium, or low) and what aspect of security determines the level of risk, e.g. need for confidentiality of information associated with the project/system, availability of the information or system, or reliability of the information or system.]	• Are physical security controls in place? • Are adequate personnel checks in place? • Is there role-based access control and separation of responsibilities to ensure adequate information security controls are in place? • Do the COTS products provide tools that support FISMA requirements? • Does/will the system have current Certification and Accreditation (C&A) and/or Authority To Operate (ATO)? • Are interfacing systems subject to security checks and access controls?
	8—Surety (asset protection)	Risk associated with the impact of loss, damage, or theft and the adequacy of physical protection, continuity of operations, and disaster recovery plans, and operations for the system. Risk associated with the nature, value, and security of physical assets (government or contractor owned) and the contingency plans to protect the project in the event of asset loss or failure.	• Are there adequate checks/controls to ensure data integrity and appropriate level of access control? • Are the selected systems/technologies reliable? • Are processes in place to ensure transfer of data is reliable, and to ensure that transmitted/transferred data reaches only the intended recipient system(s)?
	18—Privacy	Risk associated with the vulnerability of the collection, use, storage, transmission, and disposal of personally identifiable or proprietary information. Risk associated with the compliance with the Privacy Act and the privacy impact assessment. Include the effectiveness and cost of the project's documented standards for submission and use of personal information.	• Has a Privacy Impact Assessment (PIA) been performed? • If this is a project related to a legacy system, has the PIA been revisited in the last 2 years? • Does/will the system contain Personally Identifiable Information (PII) of the general public or of employees?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Summary of Risk	11—Overall risk of investment failure	Risk associated with any risks, including other risks not already discussed, that have the greatest potential for causing system failure or that have a negative impact resulting from the occurrence of one or more identified or unidentified risks, leading to catastrophic results for the project. It refers to the aggregation of identified risks associated with this initiative and the likelihood (probability and impact) that one or more occurrences of risk will cause this initiative to fail. It also includes the risk that unidentified activities occur that lead to the project becoming obsolete. Include the effectiveness and use of the risk management plan.	• Is there a business need for this project? • Does the product/system support the business goals and objectives? Is this project a business priority? • Has the sponsor/business owner been identified? • Does the sponsor/business owner his/her recognize role and responsibilities with the project? • Is there sufficient support for completing this effort and backing to get allocation of funds? • Are there political issues that might affect the direction and/or priority of this effort? • Are the requirements well understood and well managed? • Is the design well documented? • Is the test plan well-documented? • Do the tests map to the requirements? • Is there a sound implementation plan? • Is there a sound training plan? • Are there adequate tools for executing the project, for requirements analysis and management, design, development, test, implementation/deployment? • Do team members have adequate training to use the tools and perform their job/role? • Are roles and responsibilities within the project team clear? • Is there a training plan? • Do key individuals have backup/shadow personnel? • Is there any succession planning?

Ask the Right People

WHOM TO ASK

Whose opinion of project risk is the best to solicit? The answer is anyone who has a stake in the project's success. No one group of people is best for every project or every life-cycle phase of a single project. The appropriate people include individuals selected from this list:

- Project or investment management
- Project staff
- Organization or operating unit security officer
- Organization or operating unit and/or IHS chief enterprise architect
- Agency support staff such as the budget officer and the contracting officer
- Contractor management
- Contractor staff
- Users or potential users
- Senior functional management and senior technical management
- Other members of the Integrated Project Team (IPT)
- Other stakeholders that have an interest in the success of the project and a perspective about risk.

Do not exclude people because they are not supporters of the project or because you think you already understand their opinions. These may be the most important people to include. Getting potential real or perceived risks out in the open early is often the best way to manage or mitigate them.

It is best to gather opinions of risk in an open forum so all players can hear and learn from the ideas of others. For this reason, a facilitated workshop is recommended.

DON'T ATTEMPT TOO MUCH

While a group is gathered to identify and evaluate project risk, it may be tempting to try to cover too much ground—for example, to also develop risk management strategies and discuss risk management action steps. These are best postponed until a later meeting or until the risk owner is ready to discuss them. A more limited agenda works best. Suggestions for an agenda are listed below:

- Describe the purpose of risk management and the risk management model. Introduce the risk categories.
- Address each risk category. You may not have a risk in every category; however, every category should be reviewed. State each risk as a cause-and-effect statement.
- When all risks have been identified, consider them in their entirety. Then evaluate each risk—one at a time—for its potential impact on the project and the likelihood of occurrence as described in your risk management plan.

If time permits, consider risk management strategies for the most serious risks. If appropriate, assign risks to risk owners as described in the risk management plan.

A sample risk inventory and assessment, the results of conducting an open and comprehensive risk review, is presented in Appendix C.

APPENDIX C. SAMPLE RISK INVENTORY AND ASSESSMENT

This Appendix provides a sample risk inventory and assessment.

When entered into the HHS project and Portfolio Management Tool, Oracle Primavera ProSight, a unique identifier for each risk identifier will be assigned by the tool

Within a risk category, there can be more than one risk (see risk category 4) *Technical Obsolescence*, for example).

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment As of February 14, 2013									
Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Schedule data	10 Jan 2013	1) Schedule	If the project manager does not have the appropriate information to track actual progress against planned milestones, then the project may fall behind schedule.	Low	Low	1	None required. Risk is minimal.	Schedule issues involving system modification are managed through regular weekly team meetings.	10 Jan 2013: Risk initially identified.
Initial cost data	10 Jan 2013	2) Initial Costs	If the initial cost estimate is not accurate, then the lifecycle costs and future estimates will not be accurate.	Low	Low	1	None required. Risk is minimal.	GSA purchase.	10 Jan 2013: Risk initially identified. 16 Jan 2013: Purchase completed.
Life-cycle cost data	10 Jan 2013	3) Life-cycle Costs	If life-cycle costs are estimated incorrectly, then project may not be completed within the specified budget.	Low	Low	1	None required. Risk is minimal.	COTS product; GSA purchase. System is primarily in the steady-state phase of its life cycle and DME costs are relatively low. Those requesting enhancements participate in funding justifications.	10 Jan 2013: Risk initially identified.
Maintenance costs	10 Jan 2013	4) Technical obsolescence	If the Investment relies on technology that is not open or widely supported, then the maintenance may become cost-prohibitive.	Low	Low	1	None required. Risk is minimal.	Auto-refresh with contractor.	10 Jan 2013: Risk initially identified.
Oracle migration	10 Jan 2013	4) Technical obsolescence	If the standard Oracle migration path is not followed, the system could become technologically obsolete, more expensive to maintain, and/or lose functionality.	Low	Low	1	None required	The Oracle contractor attends weekly ITDS team meetings and reports on Oracle technology change issues. Project personnel have extensive experience with the Oracle products.	10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Design complexity	10 Jan 2013	5) Feasibility	If the implementation of the design is difficult or impossible to test, the project may be accepted when it does not meet user-defined functional requirements.	Low	Low	1	None required. Risk is minimal.	COTS product; GSA purchase.	10 Jan 2013: Risk initially identified.
System restoration	10 Jan 2013	6) Reliability of systems	If the staff has limited expertise with technology, then the ability to quickly restore and repair systems could be impacted.	Low	Low	1	None required. Risk is minimal.	COTS product; meets business need.	10 Jan 2013: Risk initially identified.
Software / hardware reliability	10 Jan 2013	6) Reliability of systems	If the software places unexpected stress on the hardware and other infrastructure, the system may fail.	Low	Low	1	None required	The software, hardware, and infrastructure have proven their ability to support the system. The system has a continuity of operations plan and a disaster recovery site. System reliability has not been an issue.	10 Jan 2013: Risk initially identified.
Shared system	10 Jan 2013	6) Reliability of systems	If a change is made in the hardware or software to accommodate other work without evaluating its impact on all systems, ITDS may fail.	Medium	Low	2	None required	System is primarily in the steady-state phase of its life cycle and hardware and software changes are coordinated among affected parties. Risk is continuous and will be regularly monitored.	10 Jan 2013: Risk initially identified.
Planned interoperation	10 Jan 2013	7) Dependencies/ interoperability	If the internal and external system dependencies and ability to interoperate are not adequately planned for, the system may not be as effective and costs could increase.	Low	Low	1	None required. Risk is minimal.	No dependencies and interoperability risks have been identified. ITDS is a stand-alone application.	10 Jan 2013: Risk initially identified.
Asset protection	10 Jan 2013	8) Surety	If the fixed, intellectual, and human assets are not protected adequately from harm, then the investment may be impacted.	Low	Low	1	None required. Risk is minimal.		10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Monopoly avoidance	10 Jan 2013	9) Risk of Creating a Monopoly	If the investment relies on one or two vendors, then the risk of creating a monopoly increasing and innovation may be stifled.	Low	Low	1	None required. Risk is minimal.	IHS uses full and open competition. Some contracts, by the nature of the technology, are dependent on a particular company – i.e., Cisco Routers, MCI backbone.	10 Jan 2013: Risk initially identified.
Project management skills	10 Jan 2013	10) Capability of Agency to Manage the Investment	If project managers are not sufficiently skilled in project management, software development, software management, or the development process, the project could fail.	Medium	Medium	4	Laura Lee Hope 301-443-1234	Project manager is an experienced federal manager. Project manager is taking project management training and will be certified by December 2013.	10 Jan 2013: Risk initially identified. 14 Feb 2013: Project manager is taking project management courses as scheduled. Expected certification by December 2013. Continue monitoring.
Project monitoring	10 Jan 2013	11) Overall project failure	If Inadequate attention is paid to monitoring cost, schedule, and performance goals, then the investment may be impacted.	Low	High	3	Capt. Mark Twain will monitor EVM variances monthly.	COTS product; planned use similar to previous use	10 Jan 2013: Risk initially identified. 14 Feb 2013: Project schedule variance i-3.37% Project cost variance is - 4.05%. Continue monitoring.
Stakeholder support	10 Jan 2013	12) Org/Change Management	If the stakeholders do not support the investment or major organizational changes occur, the investment may not meet performance goals.	Low	Low	1	None required. Risk is minimal.	The program conducts regular performance reviews with management and key users.	10 Jan 2013: Risk initially identified.
Sponsor support	10 Jan 2013	13) Business	If the investment does not have active project sponsor support, then resources, funding, schedule, and management support could be impacted.	Low	Low	1	None required. Risk is minimal.	The investment manager meets regularly with key business managers and the CIO's office.	10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Poorly defined field names	10 Jan 2013	13) Business	If the end user is unable to easily understand the field name semantics, data may become inconsistent.	Medium	Medium	4	Flossie Bobbsie 505-248-1234	Critical data elements for ITDS are being defined and will be converted into Common Data Elements (CDEs). The CDEs created for ITDS will be added to the Infrared Terosis Standards Repository (ITSR) as they are finalized. The estimated completion date is December 29, 2013. CDEs from other IHS context areas will be reused where appropriate. Meetings will be held with key staff members for IHS entities that manage protocols to develop a core set of CDEs that will accommodate the processing of protocols and related documents. The estimated completion date is December 29, 2013.	10 Jan 2013: Risk initially identified. 14 Feb 2013: First meeting is scheduled for 1 April 2013.
Data loss	10 Jan 2013	14) Data/Info	If the investment incurs data loss, then dependent systems could be compromised.	Low	Low	1	None required. Risk is minimal.	Regularly monitoring of data.	10 Jan 2013: Risk initially identified.
Data requirements	10 Jan 2013	14) Data/Info	If data requirements are unclear to data suppliers, data collected may be inconsistent, incomplete, and inaccurate. (See risk "Poorly Defined Field Names" 13—Business.)	Medium	Medium	4	Flossie Bobbsie 505-248-1234	Train data suppliers. When the severity of adverse events for Vioxx was identified, 26 prevention trials were underway. It took four staff members more than a week to gather the necessary data to expeditiously notify investigators and participants, stop the trials, and stop the drug shipments.	10 Jan 2013: Risk initially identified. 14 Feb 2013: Orientation meeting scheduled for data suppliers on 1 April 2013. Continue monitoring.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment
As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Bleeding edge	10 Jan 2013	15) Technology	If the investment is developed with new performance-enhancing technology, then the investment may incur additional training, testing, and implementation activities.	Low	Low	1	None required. Risk is minimal.	Tested and commonly used applications/COTS products used to meet requirements where possible Staff has access to training in new technology. The investment has built the risk of any new technology into cost and schedule projections.	10 Jan 2013: Risk initially identified.
Strategic direction	10 Jan 2013	16) Strategic	If changes in HHS IT goals or federal health architecture mandates occur, the investment will be impacted.	Low	Low	1	None required. Risk is minimal.	The investment manager continually monitors upcoming HHS and HHS IT initiatives for impact on program.	10 Jan 2013: Risk initially identified.
Data response	10 Jan 2013	16) Strategic	If ITDS is not able to provide the data to quickly respond to congressional inquiries, it may lose stakeholder support.	Low	Low	1	None required. Risk is minimal.	System is primarily in the steady-state phase of its life cycle. Risk is continuous and will be regularly monitored.	10 Jan 2013: Risk initially identified.
User access	10 Jan 2013	17) Security	If user access is not well maintained, unauthorized users may have access to sensitive data. ITDS contains patient data and prognostic data. The need for confidentiality of the information in ITDS makes the risk level high.	H=2	Low	2	Laura Lee Hope 301-443-1234	Classification of users is being reviewed currently and will be finalized by March 1, 2014.	10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

As of February 14, 2013

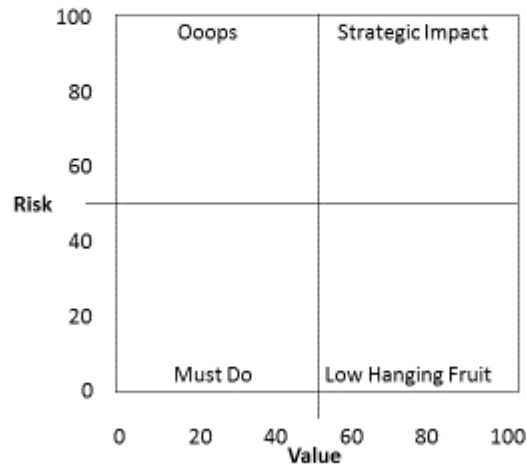
Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Super users	10 Jan 2013	17) Security	If too many users have access to the system as super users, sensitive data may become accidentally corrupted. The need for the availability of accurate, comprehensive information makes the risk level medium.	Medium	Medium	4	Laura Lee Hope 301-443-1234	Classification of users is being reviewed currently and will be finalized by March 1, 2014.	10 Jan 2013: Risk initially identified. 17 Jan 2013: No risk occurrence. Continue monitoring. 24 Jan 2013: No risk occurrence. Continue monitoring. 31 Jan 2013: No risk occurrence. Continue monitoring. 7 Feb 2013: No risk occurrence. Continue monitoring. 14 Feb: No risk occurrence. Continue monitoring
System integrity	10 Jan 2013	17) Security	If the Information Security considerations have not been adequately addressed, then confidentiality, availability and integrity of the systems could be impacted.	Medium	High	6	Capt. Mark Twain will discuss C&A with the ISSO.	The investment is closely monitored for NIST 800-53 compliance. HHS is implementing specific security training in FY2013 for those employees and contractors with significant security responsibilities.	10 Jan 2013: Risk initially identified. 17 Jan 2013: Training on schedule. Continue monitoring. 24 Jan 2013: Training on schedule. Continue monitoring. 31 Jan 2013: Training on schedule. Continue monitoring. 7 Feb 2013: Training on schedule. Continue monitoring. 14 Feb: Training on schedule. Continue monitoring

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Privacy	10 Jan 2013	18) Privacy	If the privacy issues have not been addressed, then patient information, employee information, and other sensitive information may be compromised.	Medium	High	6	Capt. Mark Twain will discuss PIA with the IHS Privacy Officer.	Make employees and contractors aware of proper use of systems and privacy protection. Implement and maintain adequate controls to protect privacy as mandated in NIST 800-66 and 800-53. An IHS HIPPA privacy officer conducts awareness program. HIPPA officer conducts awareness program. Investment conducts annual privacy impact assessment.	10 Jan 2013: Risk initially identified. 17 Jan 2013: Training on schedule. Continue monitoring. 24 Jan 2013: Training on schedule. Continue monitoring. 31 Jan 2013: Training on schedule. Continue monitoring. 7 Feb 2013: Training on schedule. Continue monitoring. 14 Feb: Training on schedule. Continue monitoring.
Staff expertise	10 Jan 2013	19) Project Resources	If staff members do not have the right expertise, maintenance activities may be delayed and costs may increase.	Low	Medium	2	None required	Staff has demonstrated appropriate capability, although depth in experience is lacking.	10 Jan 2013: Risk initially identified.
Staff turnover	10 Jan 2013	19) Project Resources	If there is major staff turnover (either government or contractor staff), maintenance activities may be delayed as replacement personnel are oriented and educated.	Low	Medium	2	None required	Staff has undergone major turnover in the past year, and training and project orientation have proven adequate for transition. New staff qualifications are carefully reviewed for appropriate expertise.	10 Jan 2013: Risk initially identified. 25 Jan 2012: Risk has been mitigated.

IT Decision Quadrant



The value and risk for all IT investments (new proposals, projects in development, and operations and maintenance activities) are scored, and the projects' benefit/risk is plotted on a graph like the one shown above. The results can be analyzed as: (1) the “must do” (low risk/low value) projects should be examined to be sure they really require funding and support; (2) the “low hanging fruit” (low risk/high value projects) identifies additional opportunities for funding; (3) the “strategic impact” (high risk/high value) investments should be evaluated for possible funding for strategic purposes; and (4) the “oops” category (high risk/low value projects) should be reviewed to be sure the projects that ended up there really belong there, and then terminating support and funding may be considered.

Business Continuity Planning

The National Institute of Standards and Technology has published a number of guides related to contingency planning and IT system security planning. The NIST publication, Contingency Planning Guide for Federal Information Systems, discusses the various types of Information Systems Contingency Plans (ISCP) and processes that are needed to fully protect information systems. We are focusing on the planning that is most closely aligned with the business processes – the Business Continuity Plan. Its relationship to the closely related Continuity of Operations Plan is also presented. The following sections are directly quoted from the first two chapters of the Guide. The entire NIST publication is available at: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>

"Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

Purpose

This publication assists organizations in understanding the purpose, process, and format of ISCP development through practical, real-world guidelines. While the principles establish a baseline to meet most organizational needs, it is recognized that each organization may have additional requirements specific to its own operating environment. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle (SDLC). The document provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities...Considerations for impact levels and associated security controls for contingency planning are presented to assist planners in developing the appropriate contingency planning strategy. Although the information presented in this document is largely independent of particular hardware platforms, operating systems, and applications, technical considerations specific to common information system platforms are addressed.

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following approaches to restore disrupted services:

- Restoring information systems using alternate equipment;
- Performing some or all of the affected business processes using alternate processing (manual means (typically acceptable for only short-term disruptions);
- Recovering information systems operations at an alternate location (typically acceptable for only long-term disruptions or those physically impacting the facility); and

- Implementing of appropriate contingency planning controls based on the information system's security impact level.

Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel, and the facility. Because there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use. Continuity planning normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. Contingency planning normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

Business Continuity Plan (BCP)

The BCP focuses on sustaining an organization's *mission/business processes* during and after a disruption. An example of a mission/business process may be an organization's payroll process or customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow. Because mission/business processes use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.

Continuity of Operations (COOP) Plan

COOP focuses on restoring an organization's *mission essential functions* (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those at a field office level, may be addressed by a BCP. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan.

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business processes at a lower or expanded level from COOP MEFs.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs.

Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions.	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
--------------------------------------	--	---	---

Conduct the Business Impact Analysis (BIA)

The BIA is a key step in ... the contingency planning process. The BIA enables the ISCP Coordinator to characterize the system components, supported mission/business processes, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The ISCP Coordinator can use the BIA results to determine contingency planning requirements and priorities. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP, BCPs, and Disaster Recovery Plan (DRP). The BIA should be performed during the Initiation phase of the System Development Life Cycle (SDLC). As the system design evolves and components change, the BIA may need to be conducted again during the Development/Acquisition phase of the SDLC.

Three steps are typically involved in accomplishing the BIA:

1. **Determine mission/business processes and recovery criticality.** Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined **along with outage impacts and estimated downtime**. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources."



FFIEC Information Technology Examination Handbook

Business Continuity Management

NOVEMBER 2019

Contents

INTRODUCTION.....	1
I BUSINESS CONTINUITY MANAGEMENT	2
II BUSINESS CONTINUITY MANAGEMENT GOVERNANCE.....	3
II.A Board and Senior Management Responsibilities	4
II.B Audit	6
III RISK MANAGEMENT.....	7
III.A Business Impact Analysis	9
III.A.1 Identification of Critical Business Functions	10
III.A.2 Interdependency Analysis	10
III.A.3 Impact of Disruption	11
III.B Risk Assessment.....	12
III.B.1 Risk Identification	13
III.B.2 Likelihood and Impact	14
IV BUSINESS CONTINUITY STRATEGIES	16
IV.A Resilience	18
IV.A.1 Physical	19
IV.A.2 Cyber Resilience	19
IV.A.3 Data Backup and Replication	19
IV.A.4 Personnel	21
IV.A.5 Third-Party Service Providers.....	22
IV.A.6 Telecommunications	23
IV.A.7 Power	24
IV.A.8 Change Management.....	24
IV.B Communications	25
V BUSINESS CONTINUITY PLAN	26
V.A Event Management.....	27
V.B Continuity and Recovery	28
V.C Facilities and Infrastructure	29
V.C.1 Data Center Recovery Alternatives	29
V.C.2 Branch Relocation	30
V.D Payment Systems.....	31
V.E Liquidity Considerations	31
V.F Other Components.....	31
V.F.1 Incident Response.....	32

V.F.2	Disaster Recovery	33
V.F.3	Crisis or Emergency Management	34
VI	TRAINING	35
VII	EXERCISES AND TESTS	37
VII.A	Exercise and Test Program	38
VII.B	Exercise and Test Policy	39
VII.C	Exercise and Test Strategies.....	39
VII.D	Exercise and Test Objectives.....	40
VII.E	Exercise and Test Plans	40
VII.F	Exercise and Test Scenarios.....	41
VII.G	Exercise and Test Methods	42
VII.G.1	Full-Scale Exercise.....	42
VII.G.2	Limited-Scale Exercise	43
VII.G.3	Tabletop Exercise.....	43
VII.G.4	Tests	44
VII.H	Industry Exercises and Resilience	44
VII.I	Third-Party Service Provider Testing	45
VII.J	Testing for Core and Significant Firms	45
VII.K	Post-Exercise and Post-Test Actions	46
VIII	MAINTENANCE AND IMPROVEMENT	47
IX	BOARD REPORTING	49
APPENDIX A:	EXAMINATION PROCEDURES	50
APPENDIX B:	GLOSSARY	70
APPENDIX C:	ABBREVIATIONS.....	77
APPENDIX D:	REFERENCES.....	78

Introduction

The “Business Continuity Management” (BCM) booklet is one in a series of booklets that comprise the *Federal Financial Institutions Examination Council (FFIEC)*¹ *Information Technology Examination Handbook (IT Handbook)*. The *IT Handbook* is prepared for use by examiners.² With the publication of this booklet, the FFIEC member agencies replace the “Business Continuity Planning” booklet issued in February 2015. The change from business continuity planning to business continuity management reflects the changes in customer and industry expectations for the resilience of operations.

The BCM booklet describes principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations. The BCM booklet also outlines BCM principles to help examiners evaluate how management addresses risk related to the availability of critical financial products and services. This booklet discusses BCM governance and its related components, including resilience strategies and plan development; training and awareness; exercises and tests; maintenance and improvement; and reporting for all levels of management, including the board of directors.

The focus of this revised booklet is on enterprise-wide, process-oriented approaches that consider technology, business operations, testing, and communication strategies critical to the continuity of the entire entity. However, business continuity should not be focused only on the planning process to recover operations after an event, but rather it should include the continued maintenance of systems and controls for the resilience of operations. Business continuity should be incorporated into the risk management life cycle of all systems, processes, and operations of an entity.

For *IT Handbook* purposes, the term “entities” includes depository financial institutions,³ nonbank financial institutions,⁴ bank holding companies,⁵ and third-party service providers.⁶

¹ The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95-630. The FFIEC members include the Board of Governors of the Federal Reserve System (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the State Liaison Committee (SLC).

² Each FFIEC member agency may use the principles outlined in this booklet, consistent with the member agency’s supervisory authority.

³ The term “depository financial institution” includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.

⁴ The term “nonbank financial institution” includes non-depository financial institutions under CFPB’s jurisdiction and subject to CFPB supervision and examination.

⁵ The term “bank holding company” includes any company which has control over any bank or over any company that is or becomes a bank holding company as defined by the Bank Holding Company Act.

⁶ The term “third-party service providers” includes those entities that provide banking services subject to examination under the Bank Service Company Act, the Home Owners Loan Act of 1933, the Dodd-Frank Wall Street Reform and Consumer Protection Act, or other relevant law.

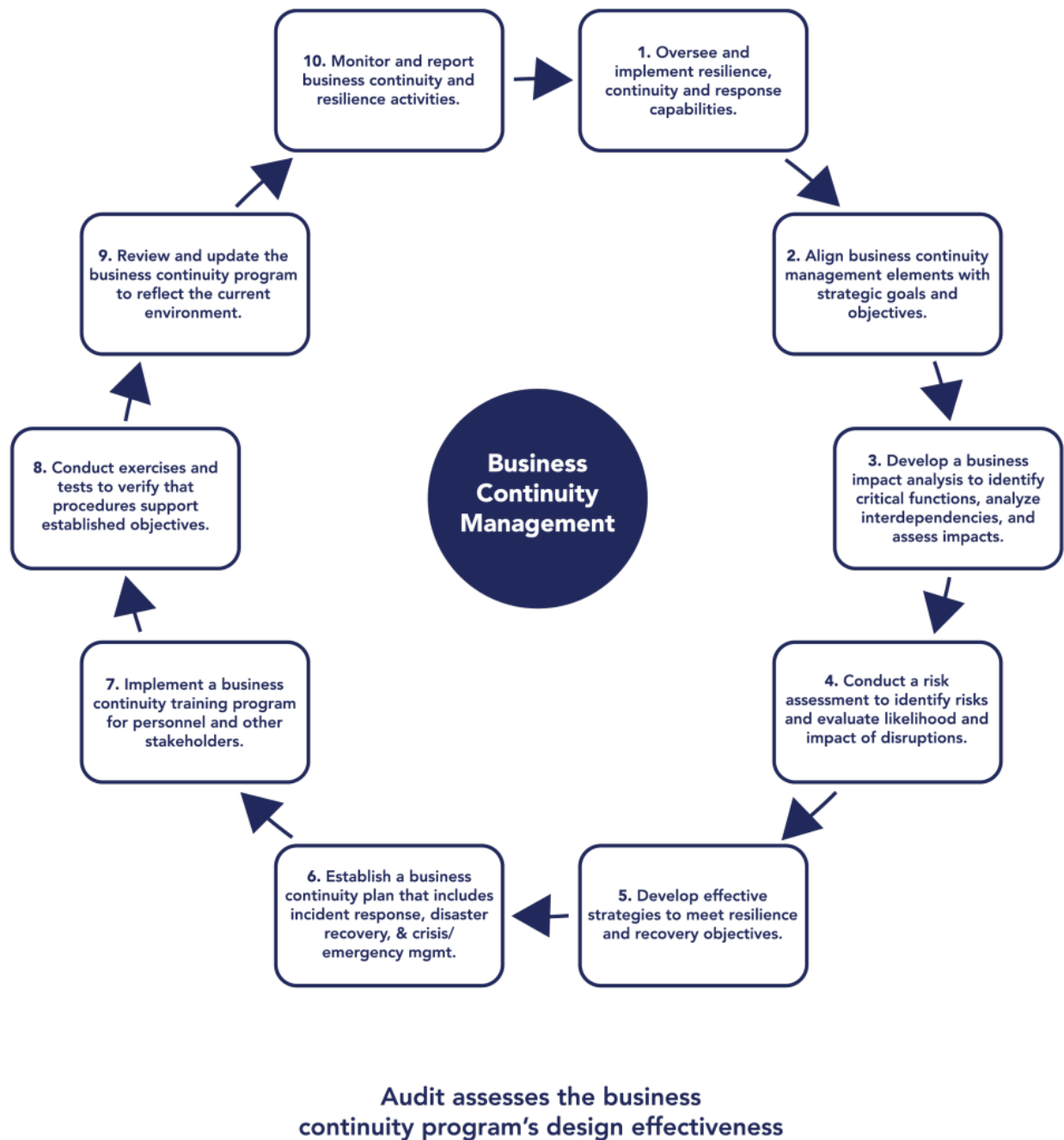
This booklet does not impose requirements on entities. Instead, this booklet describes practices that examiners may use to assess an entity's BCM function.

Appendix A of this booklet provides objectives-based examination procedures. The application of the principles and related examination procedures should vary according to an entity's complexity and risk profile. Examiners should evaluate entities in accordance with their agency's regulatory authority.

I Business Continuity Management

BCM is the process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services. Disruptions such as cyber events, natural disasters, or man-made events can interrupt an entity's operations and can have a broader impact on the financial sector. Resilience incorporates proactive measures to mitigate disruptive events and evaluate an entity's recovery capabilities. An entity's BCM program should align with its strategic goals and objectives. Management should consider an entity's role within and impact on the overall financial services sector when it develops a BCM program.

Figure 1: Business Continuity Management Cycle



II Business Continuity Management Governance

This section provides specific information about BCM governance, including board and senior management responsibilities. General information about governance and risk management is contained in the *IT Handbook's* "Management" booklet and the FFIEC members' examination handbooks.

BCM governance should include:

- Aligning BCM practices with the risk appetite.
- Identifying the continuity level needed, consistent with the operation's criticality.
- Establishing business continuity policy and plans.
- Allocating resources to BCM activities.
- Providing competent management to implement the program.
- Monitoring and assessing business continuity performance relative to these goals.

Figure 1 depicts a typical BCM cycle that entities may follow to manage business continuity risks on an ongoing basis. To manage these risks, the entity may develop a single encompassing BCM policy or individual policies and plans for different functions, depending on the size and complexity of the entity's operations. An effective practice for business continuity-related policies is to address, at a minimum, the following areas: scope and responsibilities within BCM, accountability, authority, and guidance to develop and maintain effective BCM.

II.A Board and Senior Management Responsibilities

Action Summary

The board and senior management govern business continuity through defining responsibilities and accountability, and by allocating adequate resources to business continuity.

Examiners should review for the following:

- Alignment of BCM elements with the entity's strategic goals and objectives.
- Board oversight.
- Management assignment of BCM-related responsibilities.
- Development of BCM strategies.

The board⁷ and senior management should set the “tone at the top” and consider the entity's entire operations, including functions performed by affiliates and third-party service providers, when managing business continuity. Management should evaluate continuity risk, set short- and long-term continuity objectives, adopt policies and procedures to mitigate continuity risk, evaluate continuity performance, and adjust operations in response to test results and actual events.

Management can strengthen resilience by assessing risk, planning, testing the plans, and incorporating lessons learned from tests and events. Furthermore, management should consider resilience in business functions and the design of new products and services.

⁷ Most financial institutions have boards of directors; however, not all third-party service providers do. When an entity does not have a board, the senior leaders may have the responsibilities of the board described in this booklet.

Board oversight should include:

- Assigning BCM responsibility and accountability.
- Allocating resources to BCM.
- Aligning BCM with the entity's business strategy and risk appetite.
- Understanding business continuity risks and adopting policies and plans to manage events.
- Reviewing business continuity operating results and performance through management reporting, testing, and auditing.
- Providing a credible challenge⁸ to management responsible for the BCM process.

Management oversight should include:

- Defining BCM roles, responsibilities, and succession plans.
- Allocating knowledgeable personnel⁹ and sufficient financial resources.
- Validating that personnel understand their business continuity roles and responsibilities.
- Establishing measurable goals against which business continuity performance is assessed, such as levels of preparedness and resilience targets.
- Designing and implementing a business continuity exercise strategy.
- Confirming that exercises, tests, and training are comprehensive and consistent with the BCM strategy.
- Resolving weaknesses identified in exercises, tests, and training that exceed the entity's risk appetite.
- Meeting regularly with a designated coordinator or a business continuity committee to discuss policy changes, exercises, tests, and training plans.
- Assessing and updating business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
- Coordinating plans and responses with external groups (as described in [IV.B, "Communications"](#)).

⁸ A credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment.

⁹ The term "personnel" includes both permanent and temporary staff.

II.B Audit

Action Summary

The board and senior management should engage internal audit or independent personnel to review and validate the design and operating effectiveness of the BCM program. Audit should report to the board and provide an assessment of management's ability to manage and control risks related to continuity and resilience.

Examiners should review the following:

- Scope of BCM-related audit activities.
- Audit reporting of BCM-related activities to the board.
- Board review of audit reports.
- Tracking and resolution of audit findings.
- Management's review of system and organization controls (SOC)¹⁰ and third-party service provider audit reports.

The board and senior management should engage internal audit (or an independent review) to assess the BCM design effectiveness, including policies and procedures, and the effectiveness of controls. Audit should report to the board and provide an assessment of management's ability to oversee and control risks related to continuity and resilience. Auditors should be qualified and independent of BCM processes. Audit scope and frequency depend on the entity's complexity, risk profile, and changes the entity may be experiencing. Large, complex entities may have multiple audits, covering various departments or aspects of the BCM program. Less complex entities may have their business continuity activities included within an IT general controls audit.

The internal audit of the BCM program should provide an independent assessment of management's ability to oversee the entity's continuity and resilience risk. Auditors should:

- Evaluate the business impact analysis (BIA) and risk assessment for reasonableness, identification of critical functions, and the likelihood of different events and the potential impact on operations.
- Evaluate controls for reliability, adequacy, and effectiveness regarding continuity and resilience.
- Leverage SOC reports and other external artifacts from third-party service providers, as appropriate.

¹⁰ "In 2017, the American Institute of Certified Public Accountants (AICPA) introduced the term "system and organization controls" (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations." (AICPA, [SOC 2 Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions.](#))

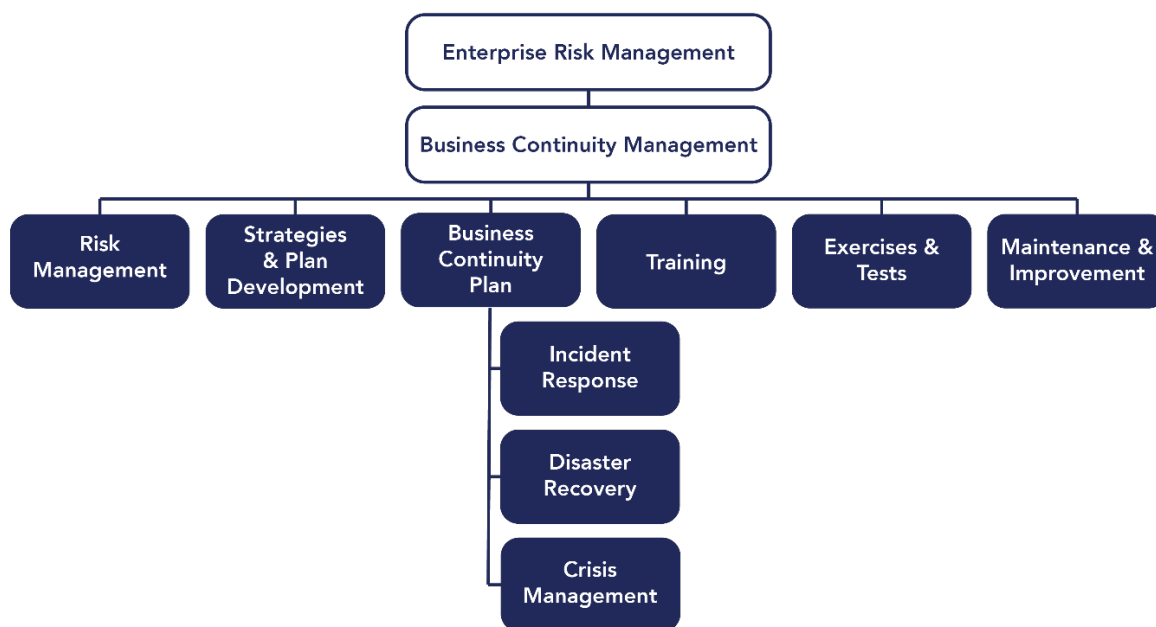
- Compare the entity's inherent risk level and the effectiveness of risk mitigation against the entity's risk appetite.
- Verify whether test plans achieve the stated objectives.
- Monitor BCM testing to verify that issues (e.g., deviation from test plans and failed objectives) are appropriately identified and escalated.
- Assess the BCM program's effectiveness.

Refer to the *IT Handbook's* "Audit" booklet for additional information.

III Risk Management

Business continuity risk management focuses on a subset of operational risk factors, against which capital and reserves alone may not protect an entity, and involves managing the possibility of an event that jeopardizes critical systems.¹¹ The BIA and risk assessment represent the foundation of BCM. As illustrated in figure 2, BCM should integrate with an entity's enterprise risk management (ERM),¹² which allows for the identification and management of risk across the entire entity. BCM allows management to set strategy to effectively mitigate risks posed by disruptive events. The level and formality of BCM and ERM integration should be commensurate with the entity's complexity and risk profile.

Figure 2: Business Continuity Management Elements (Relative to Enterprise Risk Management)



¹¹ Refer to the U.S. Department of the Treasury and the Department of Homeland Security's (DHS) [Financial Services Sector-Specific Plan 2015](#).

¹² ERM is "[a] process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (Committee of Sponsoring Organizations of the Treadway Commission (COSO), [Enterprise Risk Management – Integrated Framework \(Executive Summary\)](#), September 2004)

Management should use the BIA and risk management processes to identify and monitor continuity risks for an entity. Once management determines the risk, there are four common strategies to address that risk: risk acceptance, risk mitigation, risk transference, and risk avoidance. Risk transference, such as obtaining insurance, may allow management to recover financial losses or expenses resulting from an event and can be an effective capital management tool; however, insurance should not be a substitute for effective controls or continuity and resilience planning. Management's continuity and resilience planning efforts should focus on risk mitigation and avoidance strategies, and where appropriate, risk acceptance strategies. These strategies are covered more in depth throughout this booklet. Refer to the *IT Handbook's* "Management" booklet for additional information.

Management at large and systemically important entities whose failure could trigger a broader financial disruption should assess the likelihood and impact of a disruption, both to the entity and the entire financial sector. These entities are a critical component of the broader financial system and should incorporate scenarios of disruptions impacting the financial sector into the entity's BCM processes.

The *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Sound Practices Paper)*¹³ outlines practices for financial industry participants that perform clearing and settlement activities for critical financial markets (core firms) and institutions that process a significant share of transactions in critical financial markets (significant firms). Regulators have notified all participants that meet the definition of a core or significant firm as set forth in the *Sound Practices Paper*. Because core and significant firms participate in one or more critical financial markets, and their failure to perform critical activities by the end of a business day could present systemic risk to financial systems, their role in financial markets should be addressed as part of the business continuity planning process.

¹³ Refer to the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* issued by the [SR Letter 03-9](#) (FRB), [Bulletin 2003-14](#) (OCC), and [Release No. 34-47638](#) (U.S. Securities and Exchange Commission (SEC)). Also refer to [68 Fed. Reg. 17809](#).

III.A Business Impact Analysis

Action Summary

Management should develop a BIA that identifies all business functions and prioritizes them in order of criticality, analyzes related interdependencies among business processes and systems, and assesses a disruption's impact through established metrics. The BIA should define recovery priorities and resource dependencies for critical processes.

Examiners should review the following as part of the BIA process:

- Identification of critical business functions.
- Identification of interdependencies across business units.
- Identification and analysis of disruptive events.
- Reasonableness of recovery objectives.
- Communication of BIA results throughout the entity.
- Comprehensiveness of management's BIA review.

A BIA is the process of identifying the potential impact of disruptive events to an entity's functions and processes. A BIA allows management to identify and analyze gaps in critical processes that would prevent the entity from meeting its business requirements. The BIA generally lists recovery priorities and resources on which critical processes depend (e.g., work flow analysis¹⁴). Through the BIA process, management should identify interdependencies among critical operations, departments, personnel, services, and the functions with the greatest exposure to interruption. Management should identify resources on which these functions and processes depend and exposures that would warrant further protective measures. Furthermore, the BIA should include financial and other resource costs (e.g., the loss of business, and exposure to legal and regulatory consequences) needed to recover and restore business functions and processes.

The time and resources to complete the BIA depends on the entity's size and complexity. Complex entities may have multiple BIAs for various business lines, subsidiaries, or other organizational separations. Information from the ERM, such as business processes and risk appetites, may facilitate the BIA development.

¹⁴ The work flow analysis can assist in documenting interdependencies among critical operations, departments, personnel, and services.

III.A.1 Identification of Critical Business Functions

Completing the BIA generally involves gathering information regarding business functions, impacts from disruptions, and business interdependencies; analyzing this information; and establishing recovery objectives. Critical business functions,¹⁵ including support activities (e.g., help desk, call center, human resources, and payroll), systems, and interrelationships may be analyzed in several ways. Work flows, interviews, organizational charts, network diagrams/topologies, data flow diagrams, succession plans, or delegations of authority for key personnel may help management identify business processes and hierarchies.

Management should inventory the entity's critical assets (e.g., people, hardware, software, data, information, and cash) and infrastructure (e.g., network connectivity, communication lines, facilities, and utilities), including those provided by third-party service providers. Furthermore, management should consider supporting activities (e.g., technology support, payroll, contracting) and software (e.g., email, office productivity suites), geographic locations, and unique aspects (e.g., proprietary hardware and software, documentation, or other specialized supplies). Management should also inventory third-party service providers, including specific services they provide. The methodology used should be repeatable, allowing management to reevaluate information after significant changes.

III.A.2 Interdependency Analysis

The BIA process allows management to identify, analyze, and prioritize interdependencies among business functions and systems for alignment with resilience and recovery objectives. The analysis allows management to evaluate interdependent business functions, systems, and shared resources.

During its analysis, management should identify single points of failure, which may include telecommunication lines, network connections between branches, backups that become corrupted, reliance on one power source, or data center locations in close geographic proximity. Personnel can be a single point of failure if there are no cross-trained personnel to back up their responsibilities. Important interdependencies that should be considered include the following:

- Internal systems and business functions, which could include customer services, production processes, hardware, software, application programming interfaces (i.e., code that allows two programs to communicate with each other), data, and documentation of vital records for legal/statutory or process documentation.
- Third-party service providers (e.g., core processing, online and mobile banking, settlement activities, and disaster recovery services), key suppliers (e.g., hardware, software, and utility providers), and business partners and their roles and responsibilities for resilience and recovery.

The BIA will assist management in forming contract and service-level agreement (SLA) requirements for availability and reliability of each service. For pre-existing contracts and SLAs,

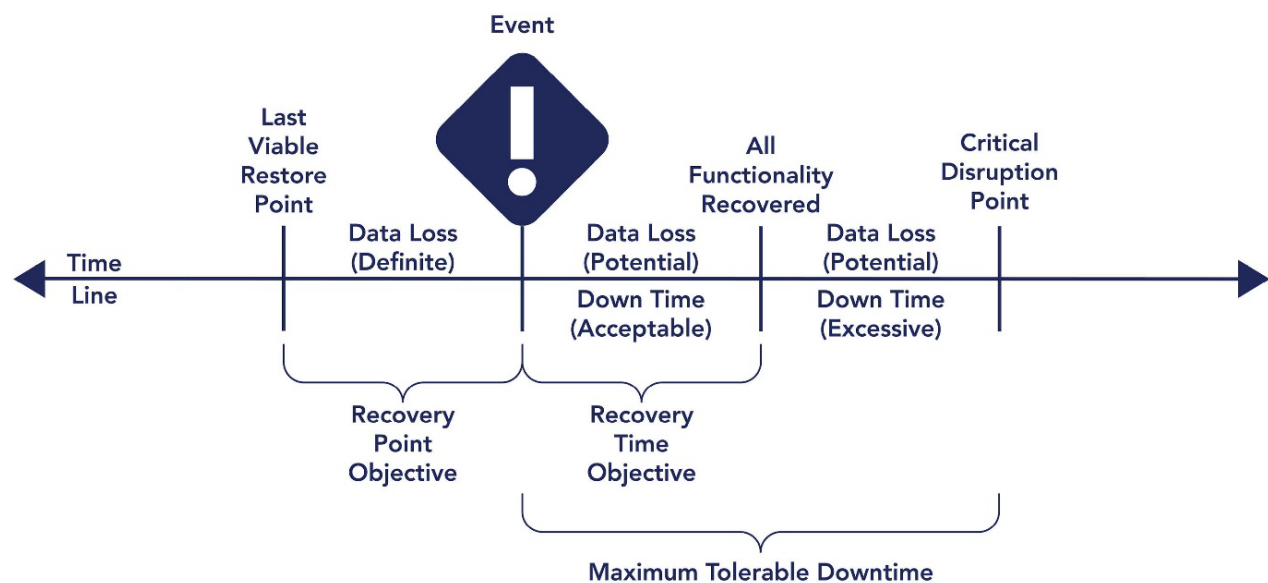
¹⁵ The term "function" can consist of one or more processes.

management should confirm that the contract and SLA requirements align with management's and the customer's continuity and resilience expectations.

III.A.3 Impact of Disruption

Through the BIA process, management should evaluate the potential impact of disruptive events, including operational, financial, and reputational impacts. Management should establish recovery objectives after determining a disruption's impact. Common measurements include recovery point objective (RPO), recovery time objective (RTO), and maximum tolerable downtime (MTD). Where applicable, these measurements should be evaluated for alignment with third-party service providers' contracted recovery expectations.

Figure 3: Recovery Objectives (Relative to an Event)



As illustrated in figure 3, the RPO represents the point in time, before a disruption, to which data can be recovered (given the most recent backup copy of the data) after an outage. Refer to section [IV.A.2, “Cyber Resilience,”](#) for additional information regarding backups.

As illustrated in figure 3, the RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and business processes. Determining the RTO is important for selecting appropriate technologies and strategies. When it is not feasible to meet an RTO, management should verify whether the RTO is realistic, initiate an action plan and milestone(s) to document the situation, and, when appropriate, plan for its mitigation. Management should consider interrelated RTOs for each business function to determine the total downtime caused by a disruption. Establishing realistic RTOs assists management in determining a critical path and hierarchy for recovery. For example, a process with a shorter RTO that is dependent upon on a process with a longer RTO may indicate a gap that should be analyzed further.

Whether driven by customer expectations or technological advancement, previously established RTOs that were a few hours in duration may now require near real-time recovery. Therefore, it may be appropriate for management to reevaluate currently acceptable RTOs.

As illustrated in figure 3, the MTD represents the total amount of time the system owner or authorizing official is willing to accept for a business process disruption and includes all impact considerations. The MTD is important for contingency planners when selecting an appropriate recovery method and developing the scope and depth of recovery procedures. Examiners may encounter other terminology to describe MTD (e.g., maximum allowable downtime).

Failure to meet established metrics, such as RPO, RTO, and MTD, may have operational impacts, including discontinued or reduced service levels, inability to meet security requirements, workflow disruptions, supply chain disruptions, and delays of business initiatives. The financial impact could include the loss of revenue, increased costs, or fines and penalties.

III.B Risk Assessment

Action Summary

Management should evaluate the likelihood and impact of potential disruptions and events. As part of this evaluation, management should consider the geographical area where the entity operates. Additionally, management should consider the risks and threats that could affect the entity's third-party service providers. Once management identifies scenarios; evaluates specific threats to the controls, strategies, and plans; and understands the entity's risk exposure, management should develop risk treatment strategies (including risk acceptance or risk transfer) based on the entity's risk appetite.

Examiners should review the risk assessment and determine whether it addresses the impact and likelihood of disruptions of the entity's information services, technology, personnel, facilities, and services provided by third parties. Specifically, examiners should review whether the following types of events are included in the risk assessment:

- Natural events such as fires, floods, severe weather, air contaminants, and hazardous spills.
- Technical events such as communication failure, power failure, equipment and software failure, transportation system disruptions, and water system disruptions.
- Malicious activity, including fraud, theft, blackmail, sabotage, cyber attacks, and terrorism.
- International events that may affect services (e.g., political instability and economic disruptions).
- Low likelihood and high impact events (e.g., terrorist attacks or pandemic events).

Risk assessment is the process of identifying risks to operations, organizational assets, individuals, and other organizations. Risk assessments incorporate threat and vulnerability

analyses and address the appropriate mitigations. As part of risk assessment processes, information from the ERM can be leveraged, such as business process documentation, critical risks, impacts, and tolerances. Management should use risk assessments to identify, measure, and mitigate risk exposures to critical functions and processes identified by the BIA. Furthermore, the risk assessment process may result in changes to the BIA. For example, management may prioritize business processes based on their importance to strategic goals and safe and sound practices; however, after developing threat models, results may necessitate prompt alteration of initial priorities or recovery plans.

III.B.1 Risk Identification

While management performs risk assessments, the focus of business continuity risk identification is on the resilience of the entity. While the causes of events can vary greatly, many of the effects do not. According to the Federal Emergency Management Agency (FEMA), threats and hazards can be categorized as natural, technological, and adversarial or human-caused.¹⁶ Each of these threats and hazards can be subcategorized, for example as internal (e.g., malicious insider or human error) or external, systemic or non-systemic, deliberate or inadvertent, and with or without warning. Although the characteristics of each hazard and threat (e.g., speed of onset, size of the affected area) may be different, the general tasks for recovering operations are the same. Management should address common operational functions in the business continuity plan (BCP) instead of having unique plans for every type of hazard or threat. Planning for all threats and hazards ensures that, when addressing emergency functions, planners identify common tasks and the personnel responsible for accomplishing the tasks.

Management should evaluate potential risks that are in the entity's geographic area. For example, entities could be located in flood-prone areas, earthquake zones, terrorist targets, or areas affected by tornados or hurricanes. In addition to geographic areas, management should also assess geopolitical risk and the potential for retaliatory cyber attacks. For example, U.S. sanctions against a nation-state could increase the risk of cyber attacks against critical infrastructure(s).

Management should coordinate business continuity risk identification efforts throughout the entity. Individual business units within larger entities should coordinate risk identification activities to identify systemic threats to the overall entity. Management should identify and inventory the entity's internal and external assets, types of threats and hazards, and existing controls as an important part of effective risk identification. Refer to the *IT Handbook's* "Management" booklet for additional information.

Furthermore, management should identify cyber security risks (refer to the *IT Handbook's* "Information Security" booklet for additional information), which should be gathered as part of the risk assessment process. Cyber security can pose risk to customer information as discussed in

¹⁶ Refer to FEMA's [Comprehensive Preparedness Guide \(CPG\) 101 Version 2.0](#). Non-FFIEC agency documents are included for illustrative purposes of common risks and are not supervisory expectations.

the *Interagency Guidelines Establishing Information Security Standards*¹⁷ that implement the Gramm-Leach-Bliley Act (GLBA).

Management should coordinate with external sources to obtain information about hazards and threats. External sources include industry information-sharing groups (e.g., Financial Services Information Sharing and Analysis Center (FS-ISAC)), and local, state, and federal authorities¹⁸ that provide timely and actionable information about hazards and threats. In addition, sharing information about events at an entity may help others identify, evaluate, and mitigate cybersecurity threats and vulnerabilities. Information about hazards and threats should be considered in the BIA, risk assessment, and other BCM processes. Refer to the *IT Handbook*'s "Information Security" booklet for additional information.

One component in the risk identification process is the gathering and assessment of threat intelligence, which National Institute of Standards and Technology (NIST) defines as "information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes." Management should integrate its threat-intelligence process with the BCM function.

Threats are potentially magnified when entities and their third-party service providers are tightly interconnected. An incident affecting one entity or third-party service provider can result in cascading impacts that quickly affect other service providers, institutions, or sectors. The term "supply chain risk" in BCM may be used to represent the risk related to the interconnectivity among the entity and others. A critical failure at a third-party service provider could have large-scale consequences. Management should identify interconnectivity points between the entity and its third-party service providers, as well as between other entities and third-party service providers. Documenting the flow of transactions, such as developing formal process diagrams, may help management identify interdependencies and end-to-end processes.

III.B.2 Likelihood and Impact

Management should evaluate the likelihood and impact of disruptive events. Risks may range from those with a high likelihood of occurrence and low impact, such as brief power interruptions, to those with a low probability of occurrence and high impact, such as pandemics. The most difficult risks to address are those that may have a high impact on the entity but a low probability of occurrence. The Department of Homeland Security's (DHS) *National Infrastructure Protection Plan*¹⁹ provides examples of risk measurement processes and methodologies to help analyze risks.

¹⁷ Refer to the *Interagency Guidelines Establishing Information Security Standards* issued by [12 CFR 364, Appendix B](#) (FDIC); [12 CFR 208, Appendix D-2](#) and [12 CFR 225, Appendix F](#) (FRB); and [12 CFR 30, Appendix B](#) (OCC). Also refer to *Guidelines for Safeguarding Member Information*, [12 CFR 748, Appendix A](#) (NCUA).

¹⁸ Examples include ChicagoFIRST county and state government, the DHS's National Terrorism Advisory System, FEMA, and the World Health Organization.

¹⁹ Refer to DHS's [National Infrastructure Protection Plan](#).

As part of the assessment, management should quantify the impacts and define loss criteria as either quantitative (financial) or qualitative (e.g., impact to customers, reputational impact). The BCM risk assessment should be commensurate with the entity's risk and complexity and should include reasonably foreseeable events. Worst-case scenarios, such as destruction of the facilities and loss of life, should be addressed. State and local authorities may assist management with identifying specific risks or exposures for geographic locations, and special requirements for accessing emergency zones.

Management should also assess whether its third-party service providers consider the likelihood of a disruption based on the geographic location of facilities, their susceptibility to threats (e.g., location in a flood plain), and the proximity to critical infrastructure (e.g., power grids, telecommunications, nuclear power plants, airports, major highways, and railroads).

Management should determine the potential severity of threats and estimate the disruption's impact under various threat scenarios as it assesses the likelihood and impact of a disruption. The results may be scored quantitatively (e.g., based on a numerical ranking) or qualitatively (e.g., high, medium, and low) and then prioritized. Refer to the *IT Handbook's* "Management" booklet for additional information.

Once management identifies scenarios, it should evaluate specific threats to the entity's controls, strategies, and plans. The difference, or the gap, between the risks from likely foreseeable threats and the mitigation provided by current controls, represents the risk exposure. Management should develop strategies to manage risk, which could include risk mitigation, avoidance, acceptance, or risk transfer, based on the entity's risk appetite.

IV Business Continuity Strategies

Action Summary

The board and senior management should develop effective strategies to meet resilience and recovery objectives. Effective oversight generally includes guidelines to achieve defined business continuity objectives.

Examiners should review BCM strategies and determine whether the strategies:

- Address personnel, processes, technology, and facility issues.
- Address critical business risks in the operating environment (e.g., mitigate specific or unique threats, such as cyber threats or loss of critical third-party service providers).
- Outline a combination of backup, replication, and storage methods for data protection.
- Provide for high redundancy levels in the telecommunications infrastructure.
- Detail a consistent change management process throughout the entity.
- Include alternatives for any proprietary systems.
- Include provisions for appropriate international business activities, where applicable.

Business continuity strategies are developed after the BIA and risk assessment process. These strategies should be risk-based and address all foreseeable risks, including non-technology risks (e.g., transaction, liquidity, and reputation risks). Strategies should include allocation of resources to meet resilience and recovery objectives. Strategies should be validated to confirm that they are viable and sufficient for peak work volumes. For example, the increased reliance on and interconnectivity of technology makes it less feasible for many entities to operate manually for an extended period, if at all.

Strategies should include the potential impact to personnel, processes, technology, facilities, and data. Personnel-related strategies may include logistical arrangements to transport or house staff at alternate facilities. In addition, management may establish alternate methods for communicating with employees, customers, and external parties. Process-related strategies may include redundant work sites for business-line operations or manual processes. Technology-related strategies may include fully equipped backup data centers or cloud providers. Backup strategies should include data files, operating systems, and applications and utilities. Facilities-related strategies may include geographic diversity or multiple power sources to reduce single point of failure risk.

Data protection strategies typically include a combination of backup, replication, and storage to achieve different levels of continuity and resilience. For example, it may be appropriate to deploy more automated, scalable solutions, such as data replication to a cloud. Management should develop comprehensive strategies to protect data, such as:

- Integrating operational, continuity, and resilience strategies to protect data based on recovery objectives.
- Designing a process to preserve the integrity and availability of data from threats.
- Monitoring the effectiveness and efficiency of data protection solutions.

Strategies should address critical business risks in the operating environment. Management should consider strategies to mitigate specific or unique threats, such as cyber threats or loss of critical third-party service providers. The specific strategy in response to an event may be different based on the entity's capabilities. Management should determine what alternatives exist for proprietary systems given the significant, unique risks to an entity's business activities. For example, some entities use internally developed assets (e.g., spreadsheets or other tools) that are critical for certain calculations within a business unit, which are often overlooked, including where and how they are stored, during the risk assessment and BIA processes. Furthermore, management should also consider access capabilities for voice and data, mapping technology infrastructure to employee needs, and internal and external capacity (including remote capacity) to determine whether telecommuting strategies are sufficient.

Strategies could include cloud architectures, virtualization, and other technologies. Cloud solutions may provide a cost-effective and high-availability environment. Independent of the strategies selected for architecture and data protection, management should still be responsible for data integrity and overall resilience. Cloud-based disaster recovery services²⁰ may be considered as part of resilience programs. Refer to section [V.C.1, "Data Center Recovery Alternatives,"](#) for additional information.

²⁰ Refer to the FFIEC's statement on [Outsourced Cloud Computing](#).

IV.A Resilience

Action Summary

Management should evaluate whether there are appropriate resources to ensure resilience, including an accessible, off-site repository of software, configuration settings, and related documentation, appropriate backups of data, and off-site infrastructure to operate recovery systems.

Furthermore, management should discuss potential disaster scenarios with the entity's third-party service providers to prepare for an event. Subsequently, management should assess the entity's immediate or short-term space requirements, systems, and personnel capacity to assume or transfer failed operations. Additionally, management should assess critical third-party service providers' susceptibility to simultaneous attacks and verify their resilience capabilities.

Examiners should review the following:

- Appropriateness of resilience practices, including the adequacy of recovery infrastructure and backup processes.
- Integration with disaster recovery services to protect against data destruction.
- Assessment of alternate data communications infrastructure between the entity and critical third-party service providers.
- Evaluation of the entity's susceptibility to multiple threat scenarios in resilience planning, testing, and recovery strategies.
- Designation of emergency personnel, including for critical business process-level employees.

Resilience is “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.”²¹ The business strategy, not technology solutions, should drive resilience. Resilience extends beyond recovery capabilities to incorporate proactive measures for mitigating the risk of a disruptive event in the overall design of operations and processes. Resilience strategies, including maintaining security standards, should extend across the entire business, including outsourced activities. Management should evaluate whether the entity has appropriate resources (e.g., human, financial, time) for resilience. When developing the entity's resilience strategies, management should consider lessons learned from previous events.

²¹ Refer to the Presidential Policy Directive/PPD-21, [Presidential Policy Directive -- Critical Infrastructure Security and Resilience](#) February 12, 2013.

IV.A.1 Physical

Physical resilience is the traditional approach to business continuity and includes IT architecture, infrastructure, facilities, and communications. To avoid the potential for failures after a disruption, management, when possible, should diversify telecommunication lines, establish redundant connections between branches and data centers, create backups, identify multiple power sources, and verify geographic diversity of key entity locations.

IV.A.2 Cyber Resilience

A challenge for cyber resilience is maintaining operations despite ever-changing risks (e.g., malware, data or system destruction and corruption, and communications infrastructure disruption). The sophistication and frequency of cyber attacks increase the potential for disruption and destruction of data and systems. Given the broad and increasing spectrum of cyber threats, resilience measures should be flexible enough to adapt to a diverse range of events. For example, a cyber attack could impact both production and backup facilities simultaneously, potentially rendering both inoperable, whether hosted internally or by a third-party service provider.

In addition, adversaries may initiate a secondary disruption (e.g., the original disruption could be the impact of a hurricane with the secondary disruption being false transactions or accessing sensitive data). Alternatively, adversaries can launch simultaneous attacks (e.g., a distributed denial of service (DDoS) attack combined with a wire transfer compromise). Therefore, management should adhere to established security and privacy policies and processes to comply with applicable regulations, even during disruptive events.

IV.A.3 Data Backup and Replication

Management should maintain data confidentiality, integrity, and availability for all iterations of data, including data backup and replication, not just focused on the production environment. Data backup and re-creation are important to recovering critical business functions in the event of disruptions. Backup files are commonly created electronically and can be mirrored at an off-site location, backed up on removable media, stored temporarily on network servers until rotated off-site, or backed up to a cloud environment. Backups should be readily accessible and adhere to the entity's information security policy.

Management should reassess backup and recovery strategies as the technology and threat environments evolve. For real-time or high-volume systems, it may be appropriate to have advanced duplication and backup methods. These advanced methods, including cloud and mirroring, provide high availability and are detailed in section V.E.1, "Data Center Recovery Alternatives."

Management should maintain an accessible, off-site repository of software, configuration settings, and related documentation. Even standard software configurations can vary from one location to another. Differences could include parameter settings and modifications, security profiles, reporting options, account information, customized software changes, or other options.

Failure to back up software configurations could result in inoperability or could delay recovery. Therefore, a comprehensive backup of critical software is important. Software backups generally consist of the following components:

- Operating systems.
- Applications.
- Utility programs.
- Databases.
- Other critical software identified in the BIA.

Management should establish effective procedures to recover critical networks and systems. Procedures may address the following:

- Backup types (physical or virtual).
- Backup levels (full, incremental, or differential).
- Updates and retention cycle frequencies.
- Software and hardware compatibility reviews.
- Data transmission controls.
- Data repository maintenance.

Refer to the *IT Handbook's* "Operations" booklet for additional information.

Data replication (also referred to as data synchronization or mirroring) is the process of copying data, usually with the objective of maintaining identical data sets in separate locations. Replication is important in any environment for resilience. Furthermore, management should consider integrity controls during replication so that data changes in production, development, and quality assurance environments are applied throughout the network.

Two common data replication processes used for information systems are synchronous and asynchronous. Synchronous replication represents the direct application of the data by applying changes at the same time. In practice, synchronous replication allows data to be transmitted in a continuous stream and minimizes data loss; however, it requires significant communication bandwidth and has limitations on the distance data can be transported due to latency issues. Synchronous replication is typically used for critical business functions where little or no data loss can be tolerated. Conversely, asynchronous replication is the indirect application of data through applying changes to a log before transit. In practice, asynchronous replication allows data to be transmitted in intermittent batches. While asynchronous replication increases the potential for data loss related to the fractions of a second required to transmit the data, this process requires less communication bandwidth and is useful for data transport over longer distances, due to reduced latency issues.

Management should determine the appropriate retention periods for each iteration of data backup. Entities should safeguard against replicating malware and data corruption. This risk is heightened with the use of near real-time data replication systems, as malware can be replicated undetected. Even with diagnostic tools, management could be unaware of an event that causes data integrity issues until well after it happens, as data could appear uncorrupted but later

determined to be inaccurate. Management may determine that the backup of critical data files should be subject to longer retention periods to ensure the ability to recover a backup prior to a corruption event.

Even in situations when the primary and backup facilities are inoperable or corrupted, customers of the entities expect to be able to access their accounts. Entities should develop appropriate cyber resilience processes (e.g., recovery of data and business operations, rebuilding network capabilities and restoring data) that enable restoration of critical services if the institution or its critical service providers fall victim to a destructive cyber attack or similar event. BCM should include the ability to protect offline data backups from destructive malware or other threats that may corrupt production and online backup versions of data. An example of an industry initiative to assist in addressing the resilience of customer account information is Sheltered Harbor.²²

IV.A.4 Personnel

Resilience is dependent upon personnel availability to maintain critical business processes. Personnel could be unavailable or distracted during such events as natural disasters, severe weather events, or pandemics.²³ While any one employee's role may not be designated as mission critical, management should plan for mass absenteeism during an event or disruption. Previous catastrophic events (e.g., Hurricane Katrina²⁴) demonstrate that personnel availability affects timely recovery.

Management should plan for events during which personnel may not be able to access facilities and critical personnel may not be available immediately after the disruption. Public infrastructure and transportation systems may not be operating, and telecommunication systems may be overburdened and unavailable. Therefore, management should consider:

- Staffing and skills needed to operate critical functions related to business continuity.
- Lodging arrangements for displaced employees and their families.
- Basic necessities and services for displaced employees, including water, food, clothing, childcare, transportation, and cash.
- On-site medical support and mobile command centers.
- Secure telecommunication options if employees work from an alternate location.
- Designated emergency personnel, including critical business process-level employees.

²² Sheltered Harbor is a voluntary industry initiative launched in 2015 following a series of cybersecurity simulation exercises between public and private sectors, known as the Hamilton Series. The purpose of the proposed Sheltered Harbor standard is to promote the stability and resiliency of the financial sector and to preserve public confidence in the financial system. The Sheltered Harbor standard proposes a combination of secure data vaulting of critical customer account information with a comprehensive resilience plan to provide customers timely access to their account information and underlying funds during a prolonged systems outage or destructive cyber attack. ([Sheltered Harbor](#)).

²³ Refer to the FFIEC's [FFIEC Highlights Pandemic Preparedness Guidance](#).

²⁴ Refer to the FFIEC's [Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event](#).

IV.A.5 Third-Party Service Providers

Many entities depend on third-party service providers to perform or support critical operations. A disruption in the delivery of those services can have a direct impact on entities' resilience. A critical failure at a widely used third-party service provider could have large-scale consequences. Management should assess critical third-party service providers' susceptibility to multiple event scenarios and verify such third parties' resilience capabilities. An entity's third-party service provider can be a single point of failure if management has not considered alternative providers or other contingency plans. If an alternative third-party service provider is not readily available, management should consider options to continue business operations and reevaluate resilience options periodically as conditions may change. Resilience planning should be closely coordinated with third-party service providers.

Establishing well-defined expectations with third-party service providers is important to business resilience. Contracts and SLAs with third-party service providers should detail roles and responsibilities of each party to promote resilience. Ongoing monitoring of the entity's third-party service providers helps management identify potential weaknesses in the third-party service provider's resilience that could affect the entity's operations.

Management's review of an entity's third-party service provider's BCM program may include independent audit reports or SOC reports. SOC reports can contain valuable information about the third-party service provider's products and processes. If management relies on SOC reports, it should verify whether business continuity activities are audited, including whether the scope and depth of review are sufficient to allow management to evaluate the third-party service provider's control environment.²⁵ Depending on the scope of the audit testing, additional inquiry and activities may be appropriate to understand the resilience of the third-party service provider.

Management should consider the same risks outlined in their entity's own internal BCP(s) in relation to third-party service providers, as well as:

- Capacity of third-party service provider to meet client recovery objectives in the agreements, relative to other clients' needs.
- Ability to participate in recovery testing with third-party service providers and access to testing results.
- Ability to move outsourced processes either in-house or to another third-party service provider.
- Alternative resource options (e.g., personnel and systems) for when primary services cannot be delivered.
- Data confidentiality, integrity, and availability (e.g., transportability and interoperability).

²⁵ SOC 1 reports cover controls at the third-party service provider that affect financial reporting. Business continuity activities are usually reported in unaudited sections of SOC 1 reports because they often do not have a direct correlation to the preparation of the financial statements, unless an event happened during the audit period. SOC 2 reports cover trust services criteria and include activities such as security, confidentiality, availability, privacy, and integrity. Audit firms typically do not opine on the quality of the business continuity activities, because it is difficult to predict what would happen during an actual event. Activities related to business continuity such as replication, plan development, and testing may be included in SOC 2 reports covering availability.

- Financial capacity to continue meeting contractual obligations.
- Services concentrated in a limited number of third-party service providers.

Business continuity-related provisions found in contracts and SLAs may include the following:

- Time parameter(s) for contracted service(s).
- Appropriate baseline metrics describing management's resilience and recovery expectations (e.g., an incident response metric to ensure timely response to events impacting business continuity and resilience).
- Periodic service reviews to ensure up-to-date agreements with all parties involved.

If operations at a third-party service provider cease, the length of time required to convert to an alternate system would, for most applications, exceed a reasonable RTO. To the extent possible, management should establish plans for the resilience of third-party service providers supporting critical operations.

IV.A.6 Telecommunications

Given the critical nature of telecommunications, management should ensure appropriate redundancy levels in the entity's telecommunications infrastructure. The entity's telecommunications infrastructure may contain single points of failure that are outside the control of a single entity. Management should understand the limitations of the entity's third-party telecommunications providers' infrastructure. For example, multiple carriers may rely on the same telecommunications backbone. Key aspects management should consider in establishing telecommunication redundancy include:

- Identifying and mitigating single points of failure across the entity's infrastructure.
- Developing and maintaining a plan to address an outage in the telecommunications lines with the entity's primary third-party service providers.
- Establishing redundant telecommunications links with each of the entity's third-party service providers through a contractual arrangement, which allows either party to switch its connection to an alternate communication path.
- Reviewing the entity's third-party service providers' plans and determining whether critical services can be restored within acceptable time frames.
- Developing guidelines, commensurate with the entity's size, complexity, and risk profile, to diversify connections to mitigate the risk of a telecommunications failure.
- Assessing the communications technology that bridges the transmission distance between the telecommunications service provider and the entity, sometimes referred to as the "last mile," for single points of failure.
- Monitoring relationships with telecommunications providers to manage risks.
- Inquiring about the physical paths used by telecommunications providers and verifying that system redundancies have been properly implemented.

Communication is critical to the financial services sector and other industries. Therefore, management should consider the following services provided by the federal government. These services give participants priority access to telecommunications during a wide-spread event.

- The Telecommunications Service Priority (TSP)²⁶ program.
- Government Emergency Telecommunications Service (GETS).²⁷
- Wireless Priority Service (WPS),²⁸ which is the wireless complement to GETS.

IV.A.7 Power

The financial industry is dependent on power to run its technology infrastructure and to supply basic necessities to personnel and customers. A long-term power outage can negatively impact an entity's resilience. Management should implement measures to provide electricity in the event of a short-term power disruption. Furthermore, management should develop plans to provide electricity in the event of a long-term power disruption. As part of its short-term and long-term plans, management should consider the following:

- Alternate energy sources (e.g., generators, multiple power grids).
- Fuel requirements, both for fuel on-hand and contracts with suppliers for deliveries during events, and any potential impediments to obtaining fuel.
- Load capacity of generators (e.g., length of time, useful life, level of power supplied).
- Continued maintenance of generators.
- Testing of generators.

IV.A.8 Change Management

Management should implement and align a consistent change management process throughout the entity, making sure to include BCM. As changes are made to production systems and business processes during the normal course of business, recovery systems and documentation at alternate locations should similarly be updated to reflect production and primary system changes.

The change management process should allow for expedient implementation of emergency changes during an event, such as changing an access control list to provide rapid access for

²⁶ Refer to the DHS's "[Telecommunications Service Priority](#)" (TSP) webpage. The TSP program provides service vendors a Federal Communications Commission mandate to prioritize requests by identifying those services critical to national security and emergency preparedness. TSP-designated circuits are recovered first in an emergency. Management may contact the entity's primary federal regulator for information on the TSP program and whether the entity qualifies for a TSP designation. If the entity qualifies, management should integrate the TSP program into the entity's BCP.

²⁷ Refer to the DHS's "[Government Emergency Telecommunications Service](#)" (GETS) webpage. GETS provides "priority access and prioritized processing in the local and long distance segments of the landline networks, greatly increasing the probability of call completion." It is intended to be used in an emergency or crisis situation when the landline network is congested and the probability of completing a normal call is reduced. Management may request GETS cards by submitting an application to the entity's primary federal regulator.

²⁸ Refer to the DHS's "[Wireless Priority Service](#)" webpage.

troubleshooting and analysis. Change tickets and corresponding activity should be reviewed for appropriateness once the event has been resolved. Even during events, changes should still be properly authorized, monitored, and documented. Poorly administered emergency changes can result in further disruption. Additionally, the interrelated nature of systems can compound disruptions to previously unaffected systems. After an emergency event, systems documentation should be updated for any changes made. Change management elements are addressed in more detail in the *IT Handbook's* “Development and Acquisition” and “Operations” booklets.

IV.B Communications

Management should consider, plan for, and prepare multiple mechanisms to communicate with others. For example, when traditional voice communications and telecommunications are impaired or inoperable, management may consider alternative communications systems such as text messaging through employer-provided and personal mobile phones, personal email, and instant messaging. Other common solutions include an inbound hotline number, an informational webpage, or a two-way polling phone system. Regardless of the communication device used, appropriate controls to safeguard customer and other sensitive information should be maintained.

BCM should include communication protocols and contact lists to notify stakeholders. Management should consider the content and process for developing such protocols and templates. Communication protocols should incorporate strategic communications and crisis management approaches in concert with public affairs or external communications (e.g., prepared public/press statements, media response plans, managing social media, etc.). Communication protocols provide customers, third-party service providers, and other external groups a means to communicate when normal channels are inoperable. External groups could include the following:

- Regulatory agencies (federal and states).
- Emergency responders.
- Law enforcement.
- Financial sector trade associations.
- Customers, third-party service providers, and other third parties (e.g., counterparties, clearing and settlement partners, payment system operators).
- Information-sharing entities (e.g., FS-ISAC).

V Business Continuity Plan

Action Summary

Management should develop business continuity plan(s) (BCP) with sufficient detail in relation to the entity's size and complexity. The BCP should address key business needs and incorporate inputs from all business units.

Examiners should review the plan for the following:

- Authorities, responsibilities, and relocation strategies.
- Communications protocols, event management, business continuity, and disaster recovery.
- Liquidity concerns before and during an adverse event.²⁹
- Alternatives for payment systems, facilities and infrastructure, data center(s), and branch relocation during a disaster.

As shown in figure 2, a BCP is an important component of BCM. The BCP documents the practices and procedures for continuing business operations during a disruption. The BCP focuses on critical business functions and varies according to the entity's size and complexity. The BCP includes specific elements, such as incident response, disaster recovery, and crisis management. Smaller entities may have a single BCP that includes these elements whereas large, complex entities may have multiple plans supported by subsidiary components for business functions, locations, or departments. Furthermore, the BCP should be a living document, regularly updated so that it remains current with system enhancements and organizational changes.³⁰

A comprehensive plan describes the authorities, responsibilities, procedures, and relocation strategies. Components of the plan should include:

- Roles, responsibilities, and required skills for entity personnel and third-party service providers.
- Solutions to various types of foreseeable disruptions, including those emanating from cyber threats.
- Escalation thresholds.
- Immediate steps to protect personnel and customers and minimize damage.
- Prioritization and procedures to recover functions, services, and processes.
- Critical information protection (e.g., physical, electronic, hybrid, and use of off-site storage).

²⁹ Refer to NIST SP 800-61, [Computer Security Incident Handling Guide](#).

³⁰ Refer to "BCP Strategy Concept," NIST SP 800-34 Rev. 1, [Contingency Planning Guide for Federal Information Systems](#). NOTE: While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

- Logistical arrangements (e.g., housing, transportation, or food) for personnel at the recovery locations.
- Network equipment, connectivity, and communication needs, including entity-owned and personal mobile devices.
- Personnel at alternate sites, including arrangements for those permanently located at the alternate facility.
- Scope and frequency of testing.
- Resumption of a normalized state for business processes.

Representatives from all business units should contribute to BCP development and implementation. The BCP may be developed and maintained internally or outsourced. In either case, the entity's board and senior management should be responsible for the BCP. Management should verify the third-party service provider's qualifications and expertise when outsourcing BCP development. Management should work with the third-party service provider to design executable and viable strategies. Regardless of its development process, the BCP and supporting documentation should be stored so that it is readily accessible by personnel during adverse events.

V.A Event Management

The BCP may define various situations as events, disruptions, or triggers. An event is an occurrence or change in circumstances that may affect operations. An event can be physical, cyber, or a combination of both. A disruption is either an anticipated or unplanned event that causes operations to degrade or fail for an unacceptable length of time (e.g., a minor or extended power outage, an extended unavailable network, or equipment or facility damage or destruction). A trigger is an event that prompts management's response. Predefined threshold escalation triggers are a key element of a BCP, and responses should be designed to mitigate the impact from adverse events.

The BCP should include event management procedures that detail reasonably foreseeable event types and provide thresholds and responses. Procedures should describe how to report an event to management and the situations that warrant notification to those who address events. Management should consider establishing a team(s)³¹ to address events. Individuals managing the event may change depending on the nature of the event and team member availability. While the team should manage the event and communicate with stakeholders, event monitoring is an entity-wide responsibility (e.g., board, senior management, and other personnel).

Responses may include activities, programs, or systems that protect life and property, meet basic human needs, and preserve the entity's operational capability. Examples of event responses include:

- Switching operations to a backup facility after a software upgrade and subsequent rollback fail.

³¹ Depending on the entity's size and complexity, authority to respond to an event may fall to an individual, a team, or multiple teams. The term "team" is used for purposes of this booklet.

- Rerouting personnel to a safer location or authorizing telecommuting when the local area becomes unsafe.
- Authorizing telecommuting when an event causes disruptions to operations.
- Invoking disaster recovery procedures once management has identified a significant cyber attack.
- Activating emergency response procedures once a hurricane threatens the local region.

V.B Continuity and Recovery

Management should establish protocols for operations continuity and system recovery. The BCP may include:

- Addressing customer service requests during downtime.
- Tracking daily transactions.
- Reconciling general ledger accounts.
- Documenting operational tasks.
- Posting entries after system recovery.
- Maintaining backup records to provide customer account information (e.g., account numbers, customer names, addresses, account status, and account balances).
- Documenting steps for system hardware and software recovery and restart.

When appropriate, procedures should address manual steps for critical functions, such as back-office operations, loan operations, and customer support. Business continuity plans and procedures should be clear, concise, and easy to implement in an emergency,³² such as checklists and step-by-step procedures.

Displaced customers may not have access to their normal identification and personal records. The BCP should include alternate identity verification methods, and management should be alert for fraud or other suspicious activities. Procedures should address fraud identification³³ and suspicious activity reporting³⁴ according to protocols and legal requirements.³⁵

During the recovery phase, management should coordinate access and availability of power and telecommunications systems with various entities. Management should coordinate with the police and fire departments and local and state government agencies to facilitate timely, secure resilience strategies. Management may also coordinate with other federal agencies, such as the

³² Refer to NIST SP 800-34 Rev. 1, [Contingency Planning Guide for Federal Information Systems](#). NOTE: While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

³³ Refer to the Financial Crimes Enforcement Network's (FinCEN) FIN-2006-A001, [Guidance to Financial Institutions Regarding Hurricane-Related Benefit Fraud](#).

³⁴ Refer to FinCEN's FIN-2013-G002, [Administrative Difficulties in Submitting Electronic Reports to FinCEN](#).

³⁵ Refer to 31 CFR 1020.220, [Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks](#).

Federal Emergency Management Agency, depending on the disaster severity. Refer to the *IT Handbook's* "Operations" booklet for additional information.

V.C Facilities and Infrastructure

The BCP should identify alternatives for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel. The backup site may mirror the operational functionality of the primary site. Management should consider site relocation for short-, medium-, and long-term scenarios. When selecting a facility, management should plan for scalability because an event may last for an extended period of time. In addition, management should consider the entity's proximity to police, fire, and medical facilities, and the expected response time frames should be factored into recovery strategies. Management should enlist the assistance of state and local agencies to expedite building permits and inspections for temporary facilities. Management should verify that recovery alternatives can accommodate the services and processing capabilities affecting critical operations, including:

- Core processing.
- Check processing and imaging.
- Commercial cash management.
- Payments.
- Mailing, faxing, and printing.
- Customer identification.

V.C.1 Data Center Recovery Alternatives

Data center recovery alternatives vary for infrastructure, configuration, operational state, and data migration. Management should document the reasons (e.g., cost and service level) for choosing an alternative and why it is appropriate based on the entity's risk profile and complexity. The level of intervention required to activate the alternate sites affects both the cost and duration to resume operations. Recovery alternatives may take several forms, such as fully redundant systems at alternate sites, cloud-based recovery solutions (either internally developed or outsourced), another data center, or a third-party service provider. Data center and alternate site development is complex, and management should consider constraints in the analysis and design process. The primary objectives are for data to be available and remotely accessible. Management should maintain appropriate controls, regardless of solution. Alternative recovery site examples may include:

- **Cold site:** A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The facility is ready to receive computer equipment when personnel move from their main computing location to the backup facility. This facility is usually not considered as the primary recovery option within the financial services industry because of the significant time necessary to install and activate the infrastructure. Comprehensive testing cannot occur until the infrastructure is established.
- **Warm site:** An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in

the event of a significant disruption. The systems are not loaded with the software or data required to resume operations and typically require manual intervention for failover and system reboots to resume critical processes. Therefore, end users may experience some disruption.

- **Hot site:** A fully operational off-site data center equipped with hardware and software used in the event of an information system disruption. Hot site development is complex, and management should consider constraints in the analysis and design process.
- **Mirrored data recovery sites:** Two or more separate, active sites that back up one another with each site independently supporting critical business functions. These sites provide almost immediate resumption capacity and are seamless for end users. Physical distance and its related latency present limitations for data centers that use real-time, data mirroring backup technologies. Similar to a hot site, these sites contain all of the equipment and connectivity capabilities; however, they also have a duplicate copy of the data. This method of high availability is commonly referred to as “Active-Active.”
- **Mobile site:** A site that possesses capabilities between what a warm and a cold site offer and has portable structures equipped with computing equipment available to customers or personnel. Completely activating a mobile site depends on how quickly it can be delivered and backups restored.
- **Colocation facility:** A facility that provides space, power, infrastructure, environmental controls, and telecommunications capabilities for multiple non-related tenants. If management relies on a colocation facility to deliver resources, there is a risk that the capacity at the colocation service provider may not be able to support the entity’s operations during a regional or large-scale event.
- **Reciprocal agreement:** An agreement that allows two entities to back up each other. While these agreements may be cost-effective, they are viable only if there is adequate excess capacity at the reciprocal financial institution and both operate on the same version and configuration of core software. Consideration should be given to security and privacy, as sensitive customer information could be exposed to the staff at the reciprocal financial institution. While these arrangements may be acceptable as a short-term solution, management should not rely on them as a long-term recovery solution.
- **Disaster recovery as a service (DRaaS):** A cloud-computing solution for replicating and hosting infrastructure, applications, and data that provides failover and recovery services.

V.C.2 Branch Relocation

An adverse event may lead management to temporarily limit or cease branch operations or temporarily transfer a branch’s operations to alternate locations. An important BCP component is establishing a physical location where personnel and customers can go to conduct business. For financial institutions, approval by the appropriate regulator may be required to close, relocate, or establish additional branch facilities.³⁶

³⁶ Refer to 12 U.S.C. 1831r-1, “[Notice of Branch Closure](#)”; 64 Fed. Reg. 34844, “[Policy Statement of the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision Concerning Branch Closing](#)”; 12 CFR 303, Subpart C, “[Establishment and Relocation of Domestic Branches and Offices](#)” (FDIC); 12 CFR 208.6, “[Establishment and Maintenance of Branches](#)” (FRB); 12 CFR 5.30, “[Establishment, Acquisition, and Relocation of a Branch of a National Bank](#)”

V.D Payment Systems

The BCP should address alternate arrangements if payment systems fail (e.g., automated teller machines (ATM), funds transfers, electronic banking, remote deposit capture, or mobile capabilities). Alternate solutions may include manual procedures for calling in or faxing wire or automated clearing house requests to correspondent financial institutions. In addition, web-based systems or third-party software may be used to perform transactions. Management should verify that redundant electronic payment systems and equipment (e.g., tokens and routers) are included at recovery sites for activation and that documentation is maintained for timely posting of entries when systems are recovered.

The BCP should also address increased cash demands and moving funds through electronic systems, including internet and mobile banking. Management may consider developing procedures for pre-established withdrawal limits based on the financial institution's relationships with customers. In addition, management should prepare for a potential increase in branch traffic when ATMs are unavailable. Pre-established agreements with various cash delivery services within and outside of the local area should also be considered so that ATMs can meet customer demand when service returns.

V.E Liquidity Considerations

The BCP should detail processes to address potential cash and liquidity needs during adverse events. During a disaster, power and communications systems may fail (e.g., inoperable ATMs or debit and credit card systems), requiring cash to fulfill customer and business needs. Arrangements to help meet liquidity needs may include:

- Emergency borrowing access.
- Alternative cash delivery.
- Procedures to secure, deliver, and distribute cash.
- Temporary purchase authority guidelines.
- Expense reimbursement options for personnel.
- Higher-limit credit cards or separate checking accounts, with designated individuals who can sign checks in emergency situations.

V.F Other Components

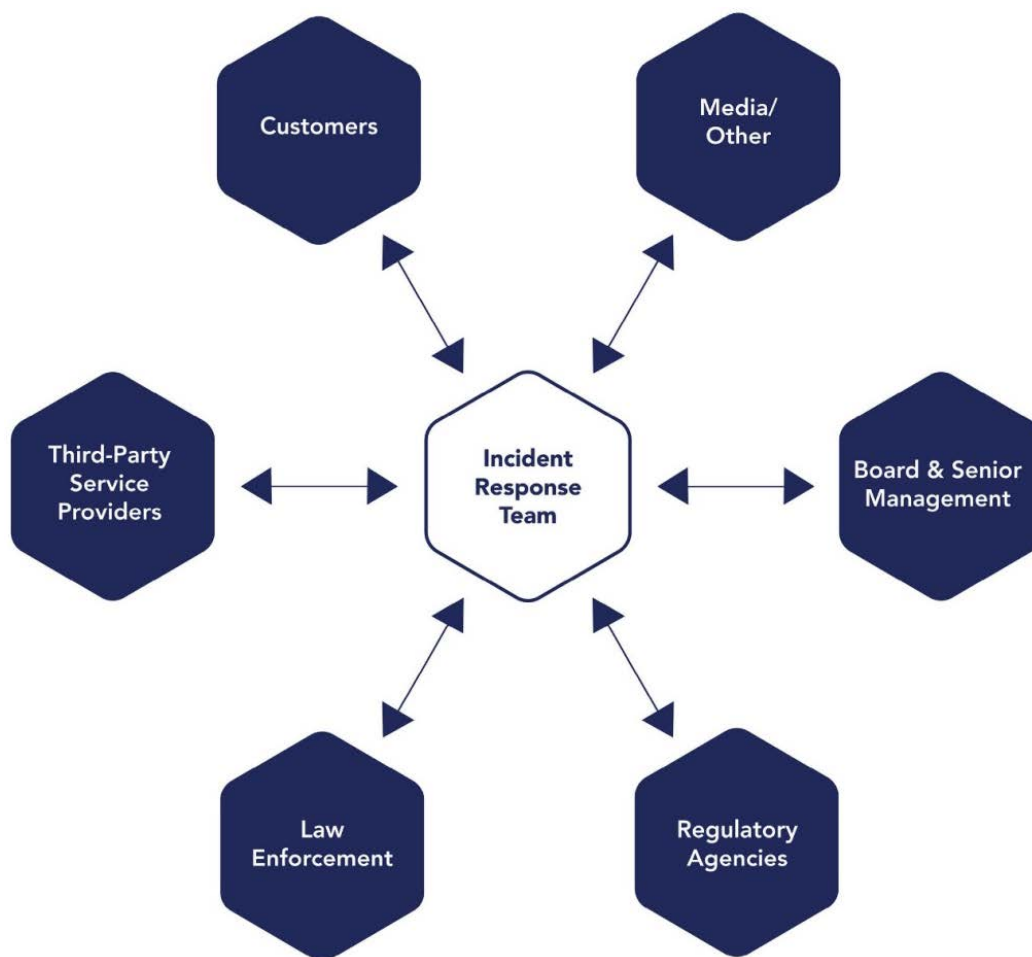
The BCP focuses on sustaining business processes during and after an event. The BCP may incorporate other plans and procedures to minimize a disruption's impact. Components may include incident response, disaster recovery, and crisis or emergency management.

(OCC); and 12 CFR 5.31, "[Establishment, Acquisition, and Relocation of a Branch and Establishment of an Agency Office of a Federal Savings Association](#)" (OCC).

V.F.1 Incident Response

Incident response helps management minimize the disruption of services or loss of information from an adverse event. Incident response priorities include preservation of life, preservation of property, incident stabilization, and communicating with stakeholders (e.g., impacted personnel, third-party service providers, customers, regulators, law enforcement). As shown in figure 4, the incident response team should coordinate communication with the noted stakeholders. Management should align incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security), outsourced services (e.g., contracted incident response obligations), and verify that the procedures are considered during planning and BCP development.

Figure 4: Incident Response Team (Adapted From NIST SP 800-61, Rev. 2)



Management should designate a spokesperson(s) to communicate with the news media. Management should consider various, pre-planned response scenarios approved by the board and senior management. Communication with the news media and via social media may be important for disseminating accurate information. Social media monitoring during an event can help management resolve conflicting messages and proactively respond to issues and concerns.

Management should train personnel to adhere to the plan when approached by the news media or communicating via social media.

Furthermore, management should leverage routine processes (e.g., vulnerability management and network monitoring) to anticipate potential incidents, including cyber incidents, and coordinate incident response planning with any third-party service provider plans. Furthermore, management should consider prearranging third-party forensic and incident response services. Management should periodically update and test the entity's incident response program to verify that it functions as intended, given rapidly changing threats. Refer to the *IT Handbook's* "Information Security" booklet for additional information.

V.F.2 Disaster Recovery

Disaster recovery is the restoring of IT infrastructure, data, and systems. Management should identify key business processes and activities to be maintained while IT systems and applications are unavailable and prioritize the order in which these systems are restored, which should be reflected in the BIA. In addition, management should develop a coordinated strategy for the recovery of data centers, networks, servers, storage, service monitoring, user support, and related software.

Recovery plans should address a broad range of adverse events (e.g., natural disasters, infrastructure failures, technology failures, unavailability of staff, or cyber attacks). Disaster recovery should address guidelines for returning operations back to a normalized state with minimum disruption.

Disaster recovery should also address the following:

- Security controls and protocols, including physical and logical, for implementation and operation of recovery systems.
- Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames.
- Instructions to access critical information repositories and other resources when the primary facility is unavailable.

When developing disaster recovery plans, management should exercise caution when identifying critical and non-critical systems. For example, telephone banking, internet banking, or ATMs may not seem critical when systems are operating normally; however, these systems play a critical role in delivering services to customers during a disruption. Similarly, an email system may not appear critical but may be the primary system available for communication during an adverse event.

V.F.3 Crisis or Emergency Management

Crisis or emergency management³⁷ is the process that allows the recognition of a crisis, activation of a BCP, and management of emergencies. Crisis or emergency management includes the ability to recover from a major event through predefined leadership and communication. Not every event warrants a crisis or emergency management response. Management should consider the impact of a crisis or emergency on the entity's reputation and personnel. For example, management may invoke crisis or emergency response procedures during a natural disaster, cyber attack, or other high-profile event.

The crisis or emergency management portion of the BCP should address coordination with regulatory agencies, local and state officials, law enforcement, and first responders. Scenarios should detail disruptions, and not be confined to a single event, facility, or geographic area. Also, crisis or emergency management plans should address simultaneous disruptions of telecommunications and electronic messaging, including between the entity and third-party service providers.

Management should designate key personnel from applicable departments to act during a crisis or emergency situation, commensurate with the entity's size and complexity. Designated personnel should be authorized to make decisions in a timely manner. Key personnel may include:

- Senior management for leadership.
- Facilities management for safety and physical security.
- Human resources for personnel issues, travel, and relocation.
- Media relations for managing communications.
- Finance and accounting for funds disbursement and financial decisions, including unanticipated expenses.
- Legal and compliance for legal and regulatory concerns.
- IT, including information security, and operations for specific tactical responses.

Communication protocols for a crisis or emergency event should include contact lists and other viable methods to reach personnel and other stakeholders who may be called upon during a crisis. The contact list should be distributed and accessible to key personnel and should be verified and updated regularly. Management should be able to communicate with personnel located in isolated areas or dispersed across multiple locations. Procedures should enable employees to report their status in a centralized manner and obtain current information. Crisis or emergency management communication protocols should include provisions to contact the entity when normal communication channels are inoperable.

Notification systems can be manual or automated. In less complex environments, manual communication techniques, such as call trees, are often used; however, information gathering can

³⁷ The financial services industry uses the terms "crisis management" and "emergency management" interchangeably.

be time consuming, and responses can be unreliable in a crisis. Maintaining contact information can become unwieldy for large entities; therefore, automated solutions may be used.

VI Training

Action Summary

Management should implement a business continuity training program for all stakeholders.

Examiners should review for the following:

- Objectives of business continuity training.
- Alignment of business continuity training with strategies.
- Extent of targeted business continuity training provided to stakeholders, such as personnel, business continuity program staff, and the board.
- Format of the business continuity training program.
- Process for reviewing and updating the business continuity training program.

Management should include training as part of an effective business continuity program to educate stakeholders on resilience, business continuity goals, corporate-wide objectives, policies, and individual personnel roles and responsibilities. The board or senior management delegates a committee or individual to oversee the training program; however, the board should be responsible for the training program's effectiveness. Refer to the *IT Handbook's* "Management" booklet for additional information.

The training program should align with the entity's strategy and use a comprehensive, risk-based, multi-year approach, including interrelated programs (e.g., disaster recovery and third-party risk management). The frequency of exercises should depend on the size and complexity of the entity and the elements of the training program, risks, and testing program iteration, with all elements covered in a timely manner. Management should take inventory of the current skill sets for business continuity and identify and address any gaps. When appropriate, management should establish goals and objectives for supporting the entity's business continuity program as part of the performance management process. Some elements of the training program may include:

- Exercises.
- Current risks.
- Future risks.
- Recent failures.
- New programs/technologies.
- Organizational changes.
- Previous (exercise) lessons learned.

Training generally involves a conceptual understanding of business continuity, including testing methods, test results, and critical business functions. The training program should include conditions for activating the BCP and what to do when key personnel are unavailable. Training should selectively and purposely seek to validate plans and assumptions by testing the interactions of people, processes, and technology risks and vulnerabilities in a consequence-free exercise environment.

Training should be tailored to the target audience, addressing the needs of specific groups. Training participants should include the board, senior management, business process owners, and frontline personnel. For example, training for personnel who manage the business continuity program should be different than training for personnel not directly involved in recovery operations. Training should include significant business continuity concepts, interdependencies, disruption impacts, and operational resilience. When applicable, contractors involved with the business continuity program should also receive appropriate training.

The board should understand the business continuity program, testing initiatives, and key business continuity-related reports. Board training should occur regularly, or more frequently, based on significant changes to business processes, risks, BIA results, or lessons learned from incidents that have impacted the entity. Training methods may involve instructional classes, computer-based training, hands-on experience, lessons learned, and collaborating with other organizations. Role-based training includes cross-training personnel to compensate for significant absenteeism or operational disruptions, which may occur during an event. Training should reflect changes to the business continuity program as they occur.

VII Exercises and Tests

Action Summary

The board and senior management should provide for appropriate exercises and tests to verify that business continuity procedures support business continuity objectives. Exercises and tests should be used to validate one or more aspects of the entity's BCP.

Examiners should review for the following in exercise and testing plans:

- Provisions for exercises and tests occurring at appropriate intervals and when significant changes affect the entity's operating environment.
- Comprehensive program objectives and plans of exercises and tests to validate the ability to restore critical business functions in a timely manner.
- An exercise and test process that provides assurance for the continuity and resilience of critical business functions, without compromising production environments.
- Authorities and control over exercises and tests.
- Exercise and test policies, expectations, and strategies that demonstrate the entity's ability to utilize alternate facilities.
- Exercise and test objectives for resilience, system monitoring, and the recovery of business processes and critical system components.
- Exercise and test scenarios, including exercise and test assumptions, objectives, expectations, and assessment metrics.
- Types of exercises (e.g., full scale, limited scale, or tabletop) and tests.
- Exercises and tests related to interaction with third parties, industry-wide testing, and core and significant firms.
- Documentation of issues identified through exercises and tests, and action plans and target dates for resolution.
- Board expectations for overall business continuity capabilities, including guidelines to achieve defined business continuity objectives.

Exercises and tests³⁸ help ensure that business continuity procedures support business continuity objectives. An exercise is a task or activity involving people and processes that is designed to validate one or more aspects of the BCP or related procedures. There are many different types of exercises, depending on the intended goals and objectives. Exercises may include scenario-driven simulations of BCP elements. For example, exercises may include performing duties in a simulated environment (i.e., functional) or be discussion based (i.e., tabletop).

A test is a type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment. Tests are evaluation tools that use quantifiable metrics to validate the operability of an IT system or system component in an operational environment

³⁸ For purposes of this booklet, the term "exercise" represents both exercises and tests, unless the term "test" is specifically mentioned.

(e.g., what happens as a result of removing power from a system or system component). Tests may focus on backup and recovery options of systems. The degree of testing can vary, from individual system components up to comprehensive tests of all system components that support business operations. Effectively, the distinction between the two is that exercises address people, processes, and systems whereas tests address specific aspects of a system.

VII.A Exercise and Test Program

Management should develop a comprehensive exercise and testing program including objectives, and plans to validate the entity's ability to restore critical business functions. The entity's risk profile should influence the frequency, objectives, and documentation of the overall exercise schedule. The entity's consolidated exercise and test schedule should be reflective of exercise and test objectives and the overall exercise and test universe.³⁹

Management should designate personnel with the authority to control the exercise or test and confirm milestones are met. Business line management should retain ownership and accountability for testing resilience of business operations, including applications and processes (both internal and external). While business line management should be responsible for testing its specific business processes and related interdependencies, managers should coordinate with personnel involved in the enterprise-wide business continuity process and support areas, such as IT and facilities management. Results should be reported to the board and senior management for inclusion in the enterprise-wide business continuity process.

Exercises and tests should occur either at appropriate intervals, when new risks are identified, or when significant changes affect the entity's operating environment. Significant changes can render existing test plans obsolete, so BCP(s) should be retested soon after the change. A comprehensive program allows management to evaluate business interdependencies and improve continuity and resilience.

A key objective for management should be to develop a testing process that validates the effectiveness of the entity's business continuity program, and identifies any deficiencies that may exist. Therefore, the exercise and test program should incorporate the following:

- A policy that includes strategies and expectations for exercise and test planning.
- Roles and responsibilities for implementation.
- Sufficient personnel to perform the exercise or test, provide oversight, and document the results.
- Precautions to safeguard production data, such as performing a backup before performing a test in a test environment, or testing during non-peak hours.
- Provisions for emergency stops (i.e., management's authority to stop an exercise if a real-life event occurs) and concluding exercises and tests.

³⁹ Similar to an audit universe, an entity's exercise and test universe is composed of an inventory of all business processes and system components that are compiled and maintained to identify areas for the exercise and test planning process.

- Verification of continuity and resilience process assumptions and the ability to process a sufficient volume of work during adverse operating conditions.
- Activities commensurate with the importance of the business process, as well as to critical financial markets.
- Result comparison against the BCP to identify gaps between the exercise or test process and recovery guidelines, with revisions incorporated where appropriate.
- Independent review of business continuity program and exercises and tests (internal and external).

VII.B Exercise and Test Policy

The entity's policies should define exercise and testing expectations and strategies. The policies should:

- Identify key roles and responsibilities.
- Establish minimum frequency, scope, and reporting requirements.
- Define documentation expectations that are consistent across business processes.
- Include a process for correcting deficiencies identified during exercises or tests.
- Address testing of communication and connectivity between the entity and third-party service providers.
- Detail participation with critical third-party service providers to confirm that entity personnel understand integration with recovery processes.

VII.C Exercise and Test Strategies

Management should develop exercise and testing strategies that demonstrate the entity's ability to support connectivity, functionality, volume, and capacity using alternate facilities. The strategies should include expectations for individual business lines and use of exercise and testing methodologies and scenarios. Testing strategies should encompass internal and external dependencies, including activities outsourced to domestic and foreign-based third-party service providers. Management should test all aspects of the entity's BCP. Strategies may include:

- A multi-year plan to execute the specific depth and breadth of exercises and tests to identify gaps in the program by using different methodologies and scenarios over time.
- Expectations for testing internal and external recovery dependencies.
- Assumptions, methodologies, and exercises used to develop the test strategies.

Lessons learned from natural disasters and other events show that for critical business functions, testing strategies should include transaction processing and functional testing to assess the recoverability of infrastructure, capacity, and data integrity. Regardless of the recovery strategy used, management should regularly test recovery provisions commensurate with the risk to the entity and, where applicable, the overall financial service sector.

VII.D Exercise and Test Objectives

The exercise and testing objectives should include resilience, system monitoring, and the recovery of business processes and critical system components. Tests can range from recovering a single file to a full-scale failover to another data center. Tests should include physical security, critical systems, multiple departments, and third-party relationships. Exercises should be sufficiently thorough to test dependencies and interrelationships among systems and third-party service providers. As the exercise and test process matures, it should become increasingly complex up to and including full-scale recovery exercises. Exercises and any associated tests should accomplish the following objectives:

- Build confidence that resilience and recovery strategies meet business requirements.
- Demonstrate that critical services can be recovered within agreed upon recovery objectives (RTOs and RPOs), including customer SLAs, and within MTDs.
- Establish that critical services can be restored in the event of an incident at the recovery location.
- Familiarize staff with recovery processes.
- Verify that personnel are adequately trained and knowledgeable of recovery plans and procedures.
- Confirm exercise and test plans remain compatible with the BCP and the entity's infrastructure.
- Identify gaps and deficiencies.

VII.E Exercise and Test Plans

Plans address the objectives and expectations of the exercise or test and outline the scenario and any assumptions or constraints that may exist. Exercises and test plans should include metrics to assess whether objectives are met. Plans should identify roles and responsibilities for participants, support personnel, and observers.⁴⁰ Exercise and test plans should be commensurate with the nature, scale, and complexity of the recovery objectives.

Management should receive and review third-party service provider exercise results, regardless of the entity's extent of participation. Management should consider the scope and results of these exercises in the entity's BCP. Management should evaluate third-party service providers' resilience and ability to recover critical services used by the entity if an event occurs. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for additional information.

Test plans generally include the following:

- Roles and responsibilities for all test participants, including support personnel.
- A consolidated exercise and test schedule that encompasses all objectives.
- A specific description of objectives and methods.
- Identification of decision makers and succession plans.

⁴⁰ For the purposes of this booklet, the term "observers" does not constitute an independent review or audit function.

- Exercise and test locations.
- Exercise and test escalation procedures and the ability to adjust for simulated scenarios.
- Contact information.
- Metrics to measure the success or failure of the exercise or test.

Management should review the exercise and test results, update the BCP where appropriate, and report the results to the board or board-designated committee. Suggestions for improving test scenarios, plans, or scripts provided by test participants should be incorporated into the testing cycle, where appropriate.

VII.F Exercise and Test Scenarios

Management should develop realistic exercise and test scenarios, based on risks, which simulate disruptions in business functions and help management determine the ability to meet both business requirements and customer expectations. The goal should not be to execute “perfect” exercises without issues; instead, it should be to continuously strengthen the business continuity program and validate the BCP(s). Management should identify and document assumptions used in developing each scenario. The scenarios should include threats that could affect third-party service providers and others, such as significant business partners. Exercises and tests should include communication processes with applicable stakeholders. Exercises demonstrate not only the ability to failover to an alternate site but also validate recovery objectives. Management should consider all reasonably foreseeable risks to connectivity and service-level agreements between the entity’s facility(ies), third-party service provider facilities, and with any applicable counterparties (i.e., entities on the other side of a financial transaction) with whom they transact significant or critical business.

Scenarios may include:

- Simultaneous attacks affecting both the entity and a third-party service provider.
- Cyber-related events (e.g., isolated malware attack, DDoS attack, data corruption, or a full-scale data center outage).
- Use of mirrored sites to demonstrate that alternate sites can effectively support customer-specific requirements, work volumes, and site-specific business processes.
- Processing a full day’s work at peak volumes.

To the extent possible, scenarios should include only resources that would be available during an event (e.g., backup files or equipment at the alternate site). Considering data and systems helps management verify the integrity of data backups (including access to encrypted data) and the adequacy of off-site systems and supplies, such as workstations and procedure manuals.

Management should develop exercise and test scripts to guide participants and meet objectives. Each script should document the procedures, which may include:

- Applications, business processes, systems, or facilities reviewed.
- Sequential steps for employees or external parties to perform.

- Procedures to guide manual work-around processes.
- A detailed schedule for completion.
- Methods for participants to record results, quantifiable metrics, and any issues.

VII.G Exercise and Test Methods

Exercises and tests help management validate continuity and resilience of technology components, including systems, networks, applications, and data, that support critical business functions. The type or combination of methods should be determined by the entity's size and complexity and the nature of its business. The DHS offers assistance and examples of testing methods,⁴¹ which are available to all entities and may be helpful when developing exercises and tests. Rigorous exercise methods and increased frequency help provide greater confidence in the continuity and resilience of business functions. While comprehensive exercises involve greater investments of time, resources, and coordination, the benefit is a more accurate assessment of recovery capabilities if a disaster occurs. This assists management in assessing the resilience of systems and responsiveness of the individuals involved in the recovery process. Comprehensive testing of all critical functions and applications allows management to identify potential problems; therefore, management should use one of the more thorough testing methods discussed in this section to verify the BCP's viability.

While names for exercises and tests may be different, or used interchangeably, this booklet lists the most commonly encountered elements in the following subsections.

VII.G.1 Full-Scale Exercise

Full-scale exercises (sometimes called a full interruption or comprehensive exercise) help management validate internal and external interdependencies between critical business functions, information systems, and networks (e.g., for critical functions, exercises should include transaction processing and functional testing). Integrated exercises move beyond comprehensive exercises to include testing with internal and external parties and the supporting systems, processes, and resources. Management should periodically reassess and update exercise and test plans to reflect changes in the business and operating environment.

A full-scale exercise simulates full use of available resources (personnel and systems) prompting a full recovery of business processes. The goal of a full-scale exercise is to determine whether all critical systems can be recovered at the alternate processing site and whether personnel can implement the procedures defined in the BCP. For example, a full-recovery exercise might simulate the complete loss of primary facilities. Features of a full-scale exercise may include the following:

⁴¹ As members of an established sector of critical infrastructure, financial institutions can leverage testing constructs implemented by the DHS. The Homeland Security Exercise and Evaluation Program is the DHS policy and guidance for designing, developing, conducting, and evaluating exercises. The program provides a threat- and performance-based exercise process that includes a mix and range of exercise activities through a series of four reference manuals to establish exercise programs and design, develop, conduct, and evaluate exercises.

- Engaging personnel from all business units to participate and interact with internal and external management response teams.
- Validating the crisis or emergency management process is operating as designed.
- Verifying personnel knowledge and skills.
- Validating management response and decision-making capability.
- Coordinating participants and decision makers.
- Validating communication protocols.
- Conducting activities at alternate locations or facilities.
- Processing data using backup media or alternative methods.
- Completing actual transactional volumes or an illustrative subset.
- Performing recovery exercises over a sufficient length of time to allow issues to unfold as they would in a crisis.

VII.G.2 Limited-Scale Exercise

A limited-scale exercise is a simulation involving applicable resources (personnel and systems) to recover targeted business processes. The goal of a limited-scale exercise is to determine whether targeted systems can be recovered and whether personnel understand their responsibilities as defined in the plan. Features of a limited-scale exercise may include the following:

- Implementing a plan appropriate to the scenario.
- Verifying personnel knowledge and skills.
- Validating management response and decision-making capability.
- Executing on-the-scene coordination and decision-making roles.
- Verifying whether participants can connect to alternate system(s).
- Conducting activities at alternate locations or facilities.
- Testing communication and remote access capability (e.g., switching to alternate equipment or telecommuting).

While limited-scope exercises are important, they often have limited participation (e.g., departmental personnel only) or scope and do not necessarily allow management to gauge interconnectivity and how systems and capacity would support daily activities and workloads.

VII.G.3 Tabletop Exercise

A tabletop exercise (sometimes referred to as a walk-through) is a discussion during which personnel review their BCP-defined roles and discuss their responses during an adverse event simulation. The goal of a tabletop exercise is to determine whether targeted plans and procedures are reasonable, personnel understand their responsibilities, and different departmental or business unit plans are compatible with each other. By themselves, tabletop exercises are likely insufficient to validate recovery capabilities, because they are limited to a discussion-based analysis of policies and procedures.

Features of a tabletop exercise may include the following:

- Engaging operational and support personnel who are responsible for implementing the BCP.
- Practicing and validating specific functional response capabilities.
- Demonstrating knowledge, skills, team interaction, and decision-making capabilities.
- Role playing with simulated responses, critical steps, recognizing difficulties, and resolving problems.
- Clarifying critical plan elements, as well as problems noted during exercises.
- Creating action plans to correct issues.

VII.G.4 Tests

Management uses tests to verify the quantifiable performance and reliability of system resilience. The goal of testing is to determine whether system resilience conforms to the BCP and stated recovery objectives. Test methodologies and frequencies should align with the risk associated with the business function as well as the entity's testing strategies and objectives. Management should clearly define the characteristics of a successful test, which may include the following:

- Validating RPOs, RTOs, and MTDs.
- Demonstrating recoverability at peak volumes.
- Confirming that systems can support critical business processes (e.g., transfer to alternate sites, increased workloads, manual workarounds, and communication).
- Integrating technologies that support critical business activities, including data replication, recovery, and off-site storage.
- Testing backup data to assess integrity and availability.
- Certifying facility controls (e.g., environmental, backup power, and physical security).
- Verifying workspace restoration (e.g., network connectivity and communications).

VII.H Industry Exercises and Resilience

Given the potential for and nature of widespread and systemic disruptive events, public and private sector groups⁴² conduct exercises with their members to verify resilience across the financial industry. These exercises simulate significant regional or industry-wide emergencies, and members are encouraged to use backup sites and test their recovery capabilities. In addition to financial institutions, these coordinated tests often include participation by third-party service providers and government agencies. There are several methods for entities of all sizes to participate, such as through third-party service provider user groups or industry initiatives. For example, industry initiatives include the U.S. Department of the Treasury's Hamilton Series (national and regional series) and the FS-ISAC's Cyber-Attack Against Payment Systems (CAPS). The results of these exercises are usually available to members of industry and regulatory groups, and summaries may be available to the public.

⁴² Public and private groups include the [FS-ISAC](#), [Financial Services Sector Coordinating Council \(FSSCC\)](#), [Financial Systemic Analysis & Resilience Center \(FSARC\)](#), [Financial and Banking Information Infrastructure Committee \(FBIIC\)](#), and some regional coalitions.

Examiners should understand that opportunities to participate in such exercises may be limited. The *Financial Sector Cyber Exercise Template*⁴³ is publicly available from the U.S. Department of the Treasury, and management can use it to help verify the entity's own response capabilities and evaluate how it would respond during similar situations. Additionally, the template and results may be used as resources to validate exercise and testing assumptions and scenarios.

VII.I Third-Party Service Provider Testing

Third-party service providers deliver critical services to many entities and should be included in the enterprise-wide exercise and testing program. The extent of inclusion in the entity's program should be based on the criticality of the third-party service provider and the business function. Management should obtain assurance that third-party service providers are resilient and have adequate infrastructure and personnel to restore critical services consistent with business and contractual requirements. The right to perform or participate in testing with third-party service providers should be included in the contract governing the entity's relationship with the third party.

Management should actively participate in the entity's third-party service providers' testing programs and should verify that testing strategies include likely significant disruptive events. Third-party service providers should be transparent about testing parameters and results because not all clients can participate in every testing activity (e.g., when there is a large client volume) and some exercises and tests may not be relevant to the services provided to a specific customer. Management should request and receive test results and reports, remediation action plans and status reports upon their completion, and related analysis or modeling. Management should track and resolve any issues identified during the exercise in a timely manner, according to the severity of the issues. Any test results that affect the entity should be presented to its board. In most instances, equating one entity's recovery experience with another's does not guarantee similar results; therefore, management should perform its own analysis. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for additional information.

VII.J Testing for Core and Significant Firms

Management at core and significant firms should develop verification strategies and execute exercise and testing activities to validate that the entity implemented sound recovery practices consistent with the entity's role in the industry. Additionally, management should consider the impact of an event at its entity on the entire financial sector. The elements discussed in the *Sound Practices Paper* supplement the agencies' respective policies and other guidance on business continuity planning. Entities not designated as core and significant firms may also consider guidance from the *Sound Practices Paper* as a model for enhancing their testing processes.

Identification of external interdependencies is important given the sector's reliance on core and significant firms. Internal testing activities should include systems that support critical market activities in which these firms are core or significant. Exercise and testing activities should confirm that such critical clearing and settlement activities could be recovered within RTOs.

⁴³ Refer to the U.S. Department of the Treasury's [Financial Sector Cyber Exercise Template](#).

Industry standard time frames are continually adjusted based on available technology, pertinent risks, and industry initiatives. Management should adjust its RTOs to be in line with industry standard time frames. Furthermore, management should design testing activities to demonstrate the ability to perform the following activities if a wide-scale disruption affects the accessibility of key personnel:

- Complete pending material payments and transactions.
- Access funding.
- Manage material open risk positions.
- Make related entries to books and records.
- Validate internal and external communication protocols.
- Ensure connectivity, functionality, and volume capacity.

Management should test with the relevant core firms from their alternate sites and meet testing standards the core firms establish specifically for significant firms and for participants more generally. Management at core and significant firms should perform testing to assess the effectiveness of their recovery strategies. Management is also encouraged, to the extent practical, to participate in pertinent market-wide and cross-market tests⁴⁴ that validate connectivity from alternate sites and include transaction, settlement, and payment processes.

Examination and supervisory activities may include evaluations of verification strategies and testing plans to assess whether core and significant firms, which are the focus of the *Sound Practices Paper*, have achieved the resilience to protect the financial system from a wide-scale disruption.

VII.K Post-Exercise and Post-Test Actions

Management should document issues identified during exercises and tests and create action plans with target dates for resolving issues. Exercise and test results should be analyzed and compared with the objectives and success criteria in the exercise and test plans, and reported to appropriate levels of management. For those items not remediated, management should document decisions to accept risks identified during the exercises.

Additionally, management should test corrective actions implemented as a result of a failed recovery objective or to address major issues encountered. Management may choose to retest during or before the next regularly scheduled exercise depending on an issue's severity. Business line management should update the BCP based on test results and adjust the BCM process, including the exercise and testing program. Finally, management should submit regular reports to the board on the exercise and testing activities and whether the BCP meets the entity's recovery and resilience objectives.

Exercise and test results may include the following documentation:

⁴⁴ Industry and cross-market tests are often conducted by associations such as the Securities Industry Association, Bond Market Association, and Futures Industry Association. These associations are mentioned for illustrative purposes only; this note is not an endorsement of any of these associations.

- Dates and locations.
- An executive summary comparing objectives and results.
- Material deviations from the plans, including whether intended participation was achieved.
- Problems identified and lessons learned.
- Assignment of responsibility for timely resolution of issues identified.

Management should periodically analyze results and issues to determine whether problems can be traced to a common source, such as inadequate change control procedures. Fixing the root cause of the problem may help resolve many underlying issues.

VIII Maintenance and Improvement

Because risks and technology often change, management should regularly review and update the business continuity program to reflect the current environment. Periodic reviews allow management to align the business continuity processes with business objectives. Management should use this information to prioritize and focus on system and process corrections and enhancements. Triggers that prompt maintenance and improvement of the business continuity program may include the following:

- Changes in enterprise strategies.
- New or reconfigured products, services, or infrastructure.
- Changes in products and services offered by third-party service providers.
- Deficiencies identified in third-party service provider business continuity processes.
- New legislation, regulatory requirements, or resilience practices.
- Results of operational metric analysis (e.g., key risk indications, key performance indicators).
- Early warning indicators that may identify potential continuity events, crises, or incidents (e.g., frequency and severity of storms, increased cyber attacks, or increases in customer service calls).
- Variances between budgeted and actual business continuity expenses.
- Results from exercises and tests, and lessons learned.
- Changes in the threat landscape (e.g., new capabilities, intent of threat actors).
- Recommendations (e.g., from audits, vulnerability assessments, and penetration tests).

To determine the extent of changes to the business continuity program, BCM program personnel should contact business unit managers regularly to assess the nature of any changes to the business, structure, systems, software, hardware, personnel, or facilities. Management at smaller, less complex entities may perform this function informally; however, the maintenance and improvement concepts remain valid for those entities.

The business continuity program should be reviewed for accuracy and completeness at periodic intervals. Likely areas⁴⁵ that should be adjusted within the BCP may include:

⁴⁵ The concept of business continuity program review elements aligns with NIST SP 800-34 Rev. 1, [Contingency Planning Guide for Federal Information Systems](#). While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

- Operational requirements.
- Security requirements.
- Technical procedures.
- Hardware, software, and other equipment.
- Team member contact information.
- Vendor contact information.
- Alternate and off-site facility requirements.
- Vital records.

When updating the business continuity program, management should document, track, and resolve any changes. Management should document, analyze, and review lessons learned from adverse events. Understanding these lessons allows management to prepare for future adverse events. Documented procedures for incorporating lessons learned should include:

- Identifying the failure(s).
- Determining the cause(s).
- Evaluating potential solutions.
- Implementing timely corrective actions as appropriate.
- Recording and reviewing corrective actions taken.

As part of the maintenance and improvement process, management should maintain version control of key business continuity documents and ensure that the latest versions are readily available to appropriate personnel. The level of detail in documentation should be commensurate with the nature of the entity's operations. This information should be accessible during an event and can be maintained by BCM program management and personnel. The BCM documentation should include evidence substantiating periodic updates of the BIA, risk assessment, and BCP(s).

Business continuity document management processes may include the following:

- Roles and responsibilities.
- Document control.
- Version control.
- Storage and disposal.

Management should follow the entity's information security standards for confidential or sensitive information contained within business continuity documentation. Additionally, management should maintain backup copies of relevant business continuity documentation in the event that the primary repository becomes inaccessible.

IX Board Reporting

Action Summary

The board should establish expectations for management's business continuity reporting, regularly monitor business continuity and resilience activities, and provide credible challenges to management.

Examiners should review reports and meeting minutes and conduct discussions with management on the following:

- BIA.
- Risk assessment.
- BCP.
- Resilience.
- Exercise and test results.
- Identified issues.
- Strategy updates.
- Audit results.
- Metrics, including key risk indicators and key performance indicators for BCM and resilience.

As illustrated in figure 1, management should report on the status of business continuity to the board, completing the BCM cycle. Reports should include a written presentation providing the BIA, risk assessment, BCP, exercise and test results, and identified issues. Additionally, reports should include regular strategy updates based on changes in personnel, roles and responsibilities, and business operations. The board should monitor business continuity and resilience activities regularly to verify that they are implemented as envisioned and reviewed periodically or as changes dictate. The board should be updated in a timely manner based on lessons learned. Board minutes should reflect business continuity discussion (including credible challenges) and approvals.

Appendix A: Examination Procedures

Examination Objective

These examination procedures (also known as the work program) are intended to assist examiners in determining the quality and effectiveness of the business continuity process on an enterprise-wide basis or across a particular line of business. Additionally, these procedures assist examiners in evaluating whether business continuity testing demonstrates the entity's ability to meet its business continuity objectives including management's ability to recover, resume, and maintain operations after disruptions, ranging from minor outages to full-scale disasters. Examiners are not limited by the examination procedures presented here and may choose to use only certain components of the work program based on the size, complexity, and nature of the entity's business. Depending on the examination objectives, a line of business can be selected to sample how the entity's continuity planning or testing processes work individually or for a particular business function or process.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider the following:
 - a. Regulatory reports of examination.
 - b. Internal and external audit reports.
 - c. Reports by independent risk management.
 - d. Business continuity tests.
 - e. Regulatory, audit, and business continuity reports on third-party service providers.
2. Review management's response to issues identified during or subsequent to the last examination. Consider the following:
 - a. Adequacy and timing of corrective action.
 - b. Resolution of root causes rather than symptoms.
 - c. Status of uncorrected issues.
 - d. Retesting to validate corrective action.
3. Interview management and review responses to pre-examination information requests to identify changes to technology infrastructure or new products and services that could affect business resilience. Consider the following:
 - a. Products or services delivered to either internal or external users.
 - b. Network topology or diagram, including changes to configuration or components and all internal and external connections.
 - c. Hardware and software inventories.
 - d. Loss, addition, or change in duties of key personnel.
 - e. Third-party service providers and software vendor listings.
 - f. Changes to internal business processes.
 - g. Changes based on industry changes or threat intelligence.

4. Review newly identified threats and vulnerabilities to the continuity of operations. Consider the following:
 - a. Technology and security vulnerabilities.
 - b. Internally identified threats.
 - c. Externally identified threats (e.g., cybersecurity alerts, pandemic alerts, or emergency warnings published by information-sharing organizations and government agencies).

Objective 2: Determine whether the board and senior management promote effective governance of business continuity through defined responsibilities, accountability, and adequate resources to support the program. (II.A, “[Board and Senior Management Responsibilities](#)”)

1. Determine whether business continuity policies and critical business procedures are:
 - a. Up-to-date and reflective of the current business environment.
 - b. Communicated effectively throughout the entity.
 - c. Available during adverse events.
 - d. Securely maintained.
2. Determine whether the board and senior management provide leadership when overseeing business continuity, including:
 - a. Evaluating continuity risk.
 - b. Setting short- and long-term continuity objectives.
 - c. Adopting appropriate policies and procedures.
 - d. Evaluating continuity performance.
 - e. Adjusting programs and operations in response to test results and actual events.
3. Determine whether management strengthens resilience through the following:
 - a. Assessing continuity risk.
 - b. Resilience planning.
 - c. Testing business continuity plans.
 - d. Incorporating lessons learned from testing and events.
 - e. Considering resilience in business functions and the design of existing operations and new products and services.
4. Determine whether board oversight includes the following:
 - a. Assigning business continuity responsibility and accountability.
 - b. Allocating resources to business continuity (e.g., personnel, time, budget, and training).
 - c. Aligning BCM with business strategy and risk appetite.
 - d. Understanding business continuity risks and adopting appropriate policies and plans to manage events.
 - e. Understanding business continuity operating results and performance.

- f. Providing a credible challenge to management responsible for the business continuity process (e.g., the board minutes provide evidence of active discussions).
 - g. Establishing a provision for management intervention if timeliness for corrective action is not met.
5. Determine whether management oversight of business continuity includes the following:
- a. Defining business continuity roles, responsibilities, and succession plans.
 - b. Allocating knowledgeable personnel and sufficient financial resources.
 - c. Validating that personnel understand their business continuity roles.
 - d. Establishing measurable goals against which business continuity performance is assessed.
 - e. Designing and implementing a business continuity exercise strategy.
 - f. Confirming that exercises, tests, and training are comprehensive and consistent with the exercise strategy.
 - g. Resolving weaknesses identified in exercises, tests, and training.
 - h. Meeting regularly to discuss policy changes, testing plans, and training.
 - i. Assessing and updating business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
 - j. Aligning plans between business units across the enterprise.
 - k. Coordinating plans and responses with external entities.

Objective 3: Determine whether the board and senior management engage audit or other independent review functions to review and validate the design and operating effectiveness of the BCM program. (II.B, “[Audit](#)”)

1. Determine whether the board and senior management have engaged audit (or an independent review) to validate the design effectiveness of the business continuity program and whether controls are operating effectively.
2. Determine whether audit reports to the board and provides an assessment of management’s ability to manage and control risks related to continuity and resilience.
3. Determine whether audit leverages SOC reports and other external artifacts from third-party service providers, as appropriate.
4. Determine whether the board or management validates that the auditor is qualified to carry out the review and is independent of the business continuity or related functions.
5. Evaluate the audit coverage of business continuity, whether through a general controls audit, during audits of business lines, or as a stand-alone business continuity audit. Audit coverage should include the following:
 - a. The reasonableness and comprehensiveness of the BIA and business continuity risk assessment(s).
 - b. The reliability, adequacy, and effectiveness of continuity and resilience controls.

- c. The effectiveness of risk mitigation efforts.
- d. Whether test plans achieve their stated objectives based on reasonable assumptions.
- e. Audit monitoring of exercises and tests, reviewing test plans and results, and verifying that any issues are identified and appropriately escalated.
- f. Assessment of the business continuity program effectiveness.

Objective 4: *Determine whether management developed an appropriate and repeatable BIA process that identifies all business functions and prioritizes them in order of criticality, analyzes related interdependencies, and assesses a disruption’s impact. (III.A, “[Business Impact Analysis](#)”)*

1. Determine the process through which management inventories business functions. Management may use the following artifacts to identify the functions:
 - a. Organizational charts.
 - b. Work flows (also called process maps).
 - c. Interview notes.
 - d. Network diagrams/topologies.
 - e. Data flow diagrams.
2. Determine whether management inventoried the critical assets and infrastructure upon which business functions depend, including the identification of single points of failure. Critical assets and infrastructure may include the following:
 - a. People.
 - b. Hardware.
 - c. Software.
 - d. Cash reserves.
 - e. Supporting activities (e.g., technology support, payroll, contracting).
 - f. Supporting software (e.g., email, office productivity suites).
 - g. Network connectivity.
 - h. Communication lines.
 - i. Facilities.
 - j. Utilities.
 - k. Infrastructure and services provided by third-party service providers.
3. Determine whether the interdependency analysis includes the following:
 - a. Internal systems and business functions, including services, production processes, hardware, software, and application programming interfaces, data, and vital records.
 - b. Third-party service providers, key suppliers, and business partners.
 - c. Telecommunications single points of failure.
 - d. Power single points of failure.
4. Review the BIA to determine whether the prioritization of business functions is reasonable. Consider management’s ability to do the following:

- a. Determine the operational and financial impacts of a disruption.
 - b. Aggregate loss impacts and determine a rating scale to indicate impact severity.
 - c. Reconcile BIA and risk assessment results with prioritization and document whether the reconciliation is adequate.
5. Determine whether the BIA produces sufficient information to estimate the following:
 - a. Recovery point objectives (RPO).
 - b. Recovery time objectives (RTO).
 - c. Maximum tolerable downtime (MTD).

Objective 5: Determine whether management conducts a risk assessment sufficient to evaluate the likelihood and impact of potential disruptions and events. (III.B, “[Risk Assessment](#)”)

1. Review risk assessment(s) to determine whether management has identified all reasonably foreseeable hazards and threats to the continuity and resilience of the entity. Examples of risks can include:
 - a. Natural:
 - Flood, earthquake, hurricane, tornado, and other weather events.
 - b. Technological:
 - Technological: Malware, cyberattack, and hardware and software failure.
 - Operational: Critical infrastructure disruption (e.g., transportation and water systems).
 - c. Adversarial or human-caused:
 - Personnel: Strike, pandemic, and malicious insider.
 - Social: Terrorism, vandalism, looting, riots, and protests.
 - d. Combination:
 - Facility: Fire, power outage, and loss of access.
 - Geographic-related: Proximity to railroad or highways used for transport of hazardous materials, proximity to airports, traffic difficulties, and other issues.
 - Third-party: Services concentrated in a limited number of third-party service providers.
2. Determine whether management identifies BCM risks and coordinates risk identification efforts throughout the entity to identify systemic threats.
 - a. Determine whether management identifies and inventories the following:
 - Internal and external assets.
 - Types of threats and hazards.
 - Existing controls.
 - b. Verify that the risk assessment includes the identification of cybersecurity risks and results of information security risk assessments.
 - c. Assess whether management obtains information about hazards and threats from external sources.
 - d. Determine whether management considers threat intelligence in risk identification efforts.

3. Ascertain whether management identifies interconnectivity points between the entity and its third-party service providers, as well as interconnectivity between other entities and their third-party service providers (i.e., supply chain).
4. Determine whether the risk assessment includes the impact and likelihood of potential disruptive events, including worst-case scenarios.
5. Determine whether management identifies and analyzes gaps between the entity's risk exposure and the risk appetite, and documents any controls implemented to mitigate the residual risk.

Objective 6: Determine whether the entity's risk management strategies are designed to achieve resilience. (IV.A, "[Resilience](#)")

1. Verify that management has evaluated strategies and resource needs and allocates appropriate resources to achieve resilience:
 - a. Appropriate personnel and skillsets to carry out the functions.
 - b. Time to identify and implement solutions.
 - c. Budget to accomplish resilience goals and objectives.
2. Determine whether management has implemented physical resilience measures that:
 - a. Establish redundant communications between branches and data centers.
 - b. Identify multiple power sources.
 - c. Geographically diversify key entity locations.
3. Determine whether management has implemented data and cyber resilience measures that:
 - a. Maintain confidentiality, integrity, and availability for backup, replication, and production environments.
 - b. Implement appropriate backups and sufficient documentation and retention periods for each iteration of data backup.
 - c. Periodically reassess backup and recovery strategies as technology and threats change.
 - d. Maintain an accessible, off-site repository of software, configuration settings, and related documentation.
 - e. Establish procedures to recover critical networks and systems, including:
 - Backup types (physical or virtual).
 - Backup levels (full, incremental, or differential).
 - Update and retention cycle frequencies.
 - Software and hardware compatibility reviews.
 - Data transmission controls.
 - Data repository maintenance.
 - f. Protect offline data backups from destructive malware that may corrupt production and online backup versions of data.

4. Determine whether management documented and implemented, as appropriate, the following resilience measures for personnel:
 - a. Staffing and skills needed to operate critical functions related to business continuity.
 - b. Lodging arrangements for displaced employees and their families.
 - c. Basic necessities and services for displaced employees, including water, food, clothing, childcare, and transportation.
 - d. On-site medical support and mobile command centers.
 - e. Secure telecommunication options if employees work from an alternate location.
 - f. Designated emergency personnel, including critical business process-level employees (i.e., those necessary to ensure all critical business operations function appropriately).
5. Determine whether management documented and implemented, as appropriate, the following resilience measures for third-party service providers:
 - a. Considered disruptive events that threaten the operational resilience and viability of the entity's third-party service provider.
 - b. Assessed the entity's immediate or short-term space, systems, and personnel capacity to assume or transfer failed operations.
 - c. Assessed critical third-party service providers' susceptibility to multiple event scenarios.
 - d. Reviewed third-party service provider's resilience capabilities, including available test and SOC reports.
 - e. Verified that SLAs with third-party service providers align with the entity's recovery objectives.
 - f. Established plans for the resilience of third-party service providers supporting critical operations.
6. Determine whether management documented and implemented, as appropriate, the following resilience measures for telecommunications:
 - a. Identifying and mitigating single points of failure across the entity's infrastructure.
 - b. Developing and maintaining a plan to address an outage in the telecommunications lines with its primary third-party service providers.
 - c. Establishing redundant telecommunications links with each of the entity's third-party service providers through a contractual arrangement that allows either party to switch its connection to an alternate communication path.
 - d. Reviewing the entity's third-party service providers' plans and determining whether critical services can be restored within time frames acceptable to the entity.
 - e. Developing guidelines, commensurate with the entity's size, complexity, and risk profile, to diversify connections to mitigate the risk of a telecommunications failure.
 - f. Assessing the communications technology that bridges the transmission distance between the telecommunications service provider and the entity for single points of failure.
 - g. Monitoring relationships with telecommunications providers to manage risks.
 - h. Evaluating communications and resilience needs to ensure branch communications.

- i. Inquiring about the physical paths used by telecommunications providers and verifying that system redundancies have been properly implemented.
7. Determine whether management considers the following as part of the entity's power resilience strategies:
 - a. Alternate energy sources (e.g., generators and multiple power grids).
 - b. Fuel requirements, both for fuel on-hand and contracts with suppliers for deliveries during events.
 - c. Continued maintenance of generators.
 - d. Testing of generators.
8. Verify that BCM activities align with the entity's change management process.

Objective 7: Determine whether the entity's BCM includes communication protocols. (IV.B, "[Communications](#)")

1. Determine whether management considers, plans for, and prepares multiple mechanisms to communicate with personnel and other stakeholders while maintaining appropriate controls to safeguard customer information. Other stakeholders could include:
 - a. Regulatory agencies (federal and state).
 - b. Emergency responders.
 - c. Law enforcement.
 - d. Financial sector trade associations.
 - e. Information-sharing entities (e.g., FS-ISAC).

Objective 8: Assess the appropriateness of the entity's enterprise-wide BCP. (V, "[Business Continuity Plan](#)")

1. Verify that management implemented a comprehensive BCP that is reflective of the entity's risk environment. The BCP should outline the following:
 - a. Roles, responsibilities, and required skills for entity personnel and third-party service providers.
 - b. Solutions to various types of foreseeable disruptions, including those emanating from cyber threats.
 - c. Escalation thresholds.
 - d. Immediate steps to protect personnel and customers and minimize damage.
 - e. Prioritization and procedures to recover functions, services, and processes.
 - f. Critical information protection (e.g., physical, electronic, hybrid, and use of off-site storage).
 - g. Logistical arrangements (e.g., housing, transportation, or food) for personnel at the recovery locations.
 - h. Network equipment, connectivity, and communication needs, including entity-owned and personal mobile devices.

- i. Personnel at alternate sites, including arrangements for those permanently located at the alternate facility.
 - j. Scope and frequency of testing.
 - k. Resumption of a normalized state for business processes.
2. If management outsources the BCP's development, verify that management maintains oversight and ownership of the BCP.
 - a. Determine whether management verified the third-party service provider's qualifications and expertise.
 - b. Verify that entity management worked with the third-party service provider to design executable and viable strategies.
 - c. Verify that the plan reflects the entity's current products, business processes, and third-party service providers.
 - d. Determine whether roles and responsibilities reflect the entity's current organizational structure.
3. Determine whether the BCP includes event management procedures that detail reasonably foreseeable event types, and those procedures include threshold metrics and response methods.
 - a. Verify that procedures explain how to report an event to management and the situations that warrant notification.
 - b. Determine whether management (either an individual or team) has implemented procedures to communicate with both internal and external stakeholders.
 - c. Verify that event management processes include event response procedures that are appropriate to the event.
4. Assess management's protocols for operations continuity and system recovery. Verify that procedures are clear, concise, accessible, and can be implemented in an emergency. Verify the BCP includes procedures for the following:
 - a. Manual steps for critical functions, as applicable.
 - b. Alternate identity verification methods.
 - c. Fraud identification and suspicious activity reporting.
 - d. Other procedures as applicable. Examples may include:
 - Addressing customer service requests during downtime.
 - Tracking daily transactions.
 - Reconciling general ledger accounts.
 - Documenting operational tasks.
 - Posting entries after system recovery.
 - Maintaining backup records to provide customer account information (account numbers, customer names, addresses, account status, and account balances).
5. Verify that the BCP lists alternatives for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel.

- a. Verify that the BCP includes site relocation for short-, medium-, and long-term scenarios.
 - b. Determine whether management considers scalability.
 - c. Verify that recovery alternatives can accommodate the services and processing capabilities affecting critical operations, including:
 - Core processing.
 - Check processing and imaging.
 - Commercial cash management.
 - Mailing, faxing, and printing.
 - Customer identification.
 - Data center activities.
6. Verify that the BCP includes procedures for coordination with the first responders and local and state government agencies, when appropriate.
 7. Verify that the BCP includes procedures to establish an alternate physical location(s) where personnel and customers can go to conduct business, if appropriate.
 8. Determine whether the BCP addresses alternate arrangements in the event payment systems fail (e.g., ATMs, funds transfers, electronic banking, remote deposit capture, mobile capabilities).
 - a. Determine whether the BCP addresses processes for retrieving and transmitting transactions when payment systems are disrupted (e.g., manual procedures for calling in or faxing wire or automated clearing house requests to correspondent banks; mitigating strategies for web-based systems; or third-party software used to perform transactions).
 - b. Determine whether management verifies that redundant electronic payment systems and equipment (e.g., tokens and routers) are included at recovery sites for activation and that documentation is maintained for timely posting of entries when systems are recovered.
 - c. Determine whether instant issue cards are utilized and card company security procedures are implemented to limit potential fraud.
 9. Verify that the BCP addresses the entity's cash management requirements. Procedures may include:
 - a. Pre-established cash delivery arrangements.
 - b. Plans for increases in branch traffic when ATMs are unavailable.
 - c. Plans for the entity's operational cash needs.
 - d. Temporary purchase authority guidelines.
 - e. Expense reimbursement options for personnel.
 - f. Higher-limit credit cards or separate checking accounts with designated individuals who can sign checks in emergency situations.
 10. Determine whether management established an incident response process. As part of incident management planning, determine whether management does the following:

- a. Aligns incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security).
 - b. Considers incident response procedures during the development of the business continuity strategy.
 - c. Leverages routine processes (e.g., vulnerability management and network monitoring) to anticipate potential incidents, including cyber incidents.
11. Verify that management developed a coordinated disaster recovery strategy for data centers, networks, servers, storage, service monitoring, user support, and related software. Verify that procedures address the following:
 - a. Security controls and protocols, including physical and logical.
 - b. Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames.
 - c. Instructions to access the repository of critical information when the primary facility is unavailable.
12. Verify whether management designates key personnel from applicable departments to act during a crisis or emergency situation. Key personnel may include:
 - a. Senior management for leadership.
 - b. Facilities management for safety and physical security.
 - c. Human resources for personnel issues and travel.
 - d. Media relations for managing communications.
 - e. Finance and accounting for funds disbursement and financial decisions, including unanticipated expenses.
 - f. Legal and compliance for legal and regulatory concerns.
 - g. IT, including information security, and operations for specific tactical responses.
13. Determine whether management established a crisis or emergency management process. Verify whether the BCP addresses the following:
 - a. Coordination with regulatory agencies, local and state officials, law enforcement, and first responders.
 - b. Disruptions not confined to a single event, facility, or geographic area.
 - c. Simultaneous disruptions of telecommunications and electronic messaging, including between the entity and third-party service providers.
 - d. Crisis or emergency management communication protocols, including the designation of a spokesperson(s) to communicate with the news media, as appropriate.

Objective 9: Determine whether the BCM program includes training and awareness to educate stakeholders about the entity’s continuity objectives and BCM goals. (VI, “[Training](#)”)

1. Verify that the training program aligns with the entity’s BCM strategy. Determine whether management does the following:
 - a. Inventories the current skillsets for BCM and identifies and addresses any training gaps.

- b. Establishes goals and objectives for supporting the BCM program as part of the entity's performance management process.
 - c. Implements a training program to educate stakeholders about the BCM goals and objectives. Elements may include:
 - Exercises.
 - Current risks.
 - Future risks.
 - Recent failures.
 - New programs/technologies.
 - Organizational changes.
 - Previous (exercise) lessons learned.
2. Assess whether management tailors training to the target audience, based on the audience's needs. The target audience could include:
 - a. Board members.
 - b. Senior management.
 - c. Business process owners.
 - d. Frontline personnel.
 - e. Contract personnel, as applicable.
3. Validate that management incorporates significant business continuity concepts, interdependencies, disruption impacts, and operations resilience into the training program.
4. Verify that the BCM training program, including board training, is updated as significant changes occur.

Objective 10: Determine whether the exercise and testing program is sufficient to allow management to assess the entity's ability to meet its continuity objectives. (VII, "[Exercises and Tests](#)")

1. Determine whether management implemented a comprehensive exercise and testing program, objectives, and plans to validate the entity's ability to restore critical business functions.
2. Verify that the program is appropriate for the entity's risk profile. Assess whether the entity's consolidated exercise and test schedule is reflective of exercise and test objectives and the overall exercise and test universe.
3. Determine whether management covers all of the functions in the exercise and test universe according to its established timeframes (e.g., all processes are covered annually or every three years).
4. Determine whether management has designated personnel with the authority to control the exercise or test and confirm exercise and test milestones are met.

5. Verify that business line management retains ownership for testing its specific business processes and coordinates with personnel involved in the enterprise-wide BCM process and support areas.
6. Verify that exercises and tests occur at appropriate intervals, or when significant changes affect the entity's operating environment.
7. Verify that management developed a process that is sufficiently robust to confirm the effectiveness of the entity's business continuity program. Therefore, the exercise program should incorporate the following:
 - a. A policy that includes strategies and expectations for exercise and test planning.
 - b. Roles and responsibilities for implementation.
 - c. Sufficient personnel to perform the exercise or test, provide oversight, and document the results.
 - d. Precautions to safeguard production data, such as performing a backup before performing a test in a test environment, or testing during non-peak hours.
 - e. Provisions for emergency stops and concluding exercises and tests.
 - f. Verification of continuity and resilience process assumptions and the ability to process a sufficient volume of work during adverse operating conditions.
 - g. Activities commensurate with the importance of the business process.
 - h. Entity's processes commensurate with their significance to critical financial markets.
 - i. Comparison of exercise and test results against the BCP to identify gaps between the exercise or test process and recovery guidelines, with revisions incorporated where appropriate.
 - j. Independent review of business continuity program and exercises and tests (internal and external).
8. Determine whether the exercise and test policy is appropriate and includes the following:
 - a. Key roles and responsibilities.
 - b. Minimum frequency, scope, and reporting.
 - c. Documentation expectations.
 - d. Processes for correcting deficiencies identified during exercises or tests.
 - e. Communication and connectivity between the entity and third-party service providers.
 - f. Participation with critical third-party service providers to confirm that entity personnel understand integration with all related recovery processes.
9. Determine whether the exercise and test strategies allow management to demonstrate the entity's ability to support connectivity, functionality, volume, and capacity using alternate facilities. Strategies may include the following:
 - a. Expectations for individual business lines and use of exercise and testing methodologies and scenarios.
 - b. Internal and external dependencies, including activities outsourced to domestic and foreign-based third-party service providers.

- c. Multi-year plan(s) to execute the specific depth and breadth of exercises and tests, which use different methodologies and scenarios over time.
 - d. Expectations for testing internal and external recovery dependencies.
 - e. Assumptions, methodologies, and exercises used to develop the test strategies.
 - f. Transaction processing and functional testing to assess the recoverability of infrastructure, capacity, and data integrity.
10. Verify that exercise and test objectives include resilience, system monitoring, and the recovery of business processes and critical system components.
11. Verify that exercises and associated tests accomplish the following objectives:
 - a. Build confidence that resilience and recovery strategies meet business requirements.
 - b. Demonstrate that critical services can be recovered within agreed upon recovery objectives (RTOs, RPOs, and MTDs) and customer SLAs.
 - c. Establish that critical services can be restored in the event of an incident at the recovery location.
 - d. Familiarize staff with recovery processes.
 - e. Verify that personnel are adequately trained and knowledgeable of recovery plans and procedures.
 - f. Confirm that exercise and test plans remain compatible with the BCP and the entity's infrastructure.
 - g. Identify any gaps between business continuity procedures and objectives.
12. Determine whether management established exercise and test plans, commensurate with the nature, scale, and complexity of the recovery objectives that address the objectives and expectations of the exercise or test and outline the scenario and any assumptions or constraints that may exist. Verify whether exercise and test plans include the following:
 - a. Identification of roles and responsibilities for participants, support personnel, and observers.
 - b. Metrics to assess whether objectives are met.
 - c. A consolidated exercise and test schedule that encompasses all objectives.
 - d. Specific descriptions of objectives and methods.
 - e. Roles and responsibilities for all test participants, including support personnel.
 - f. Identification of decision makers and succession plans.
 - g. Exercise and test locations to be utilized.
 - h. Escalation procedures and the ability to adjust for simulated scenarios.
 - i. Contact information.
13. Determine whether management developed reasonably foreseeable threat scenarios that simulate disruptions in business functions and the ability to meet both business requirements and customer expectations. Management should:
 - a. Identify and document assumptions used in developing each scenario.

- b. Develop scenarios that include threats that could affect third-party service providers, including communication processes with applicable stakeholders.
 - c. Develop exercises that demonstrate not only the ability to failover to an alternate site but also validate recovery objectives.
 - d. Create scenarios that include only the data and systems that would be available for recovery.
- 14. Verify that exercise and test scripts document the procedures for executing the exercise or test, which may include:
 - a. Applications, business processes, systems, or facilities reviewed.
 - b. Sequential steps for employees or external parties to perform.
 - c. Procedures to guide manual work-around processes.
 - d. A detailed schedule for completion.
 - e. Methods for participants to record results, quantifiable metrics, and any issues.
- 15. Assess whether exercise and test methods are commensurate with the size and complexity of the entity and the criticality of the function to the entity. Verify that exercises and tests are designed to do following:
 - a. Validate personnel knowledge and skills, including backup responsibilities.
 - b. Operate and perform duties (e.g., daily, quarterly, annually) from an alternate site.
 - c. Process transactions and assess system functionality.
 - d. Test the viability of both full and incremental backups.
 - e. Test network connectivity and interdependencies, including those with critical third-party service providers.
- 16. If management performs full-scale exercises, verify whether the exercise includes the following, where appropriate:
 - a. Engaging personnel from all business units to participate and interact with internal and external management response teams.
 - b. Validating that the crisis/emergency management process is operating as designed.
 - c. Verifying personnel knowledge and skills.
 - d. Validating management response and decision-making capability.
 - e. Demonstrating coordination among participants and decision makers.
 - f. Validating communication protocols.
 - g. Conducting activities at alternate locations or facilities.
 - h. Processing data using backup media or alternative methods.
 - i. Completing actual transactional volumes or an illustrative subset.
 - j. Performing recovery exercises over a sufficient length of time to allow issues to unfold as they would in a crisis.
- 17. If management performs limited-scale exercises, verify whether the exercise includes the following, where appropriate:

- a. Implementing a plan appropriate to the scenario.
 - b. Verifying personnel knowledge and skills.
 - c. Validating management response and decision-making capability.
 - d. Executing on-the-scene coordination and decision-making roles.
 - e. Verifying whether participants can connect to alternate system(s).
 - f. Conducting activities at alternate locations or facilities.
 - g. Testing communication and remote access capability (e.g., switching to alternate equipment or telecommuting).
18. If management performs tabletop exercises, determine whether targeted plans and procedures are reasonable, personnel understand their responsibilities, and different departmental or business unit plans are compatible with each other. (By themselves, tabletop exercises are likely insufficient to validate recovery capabilities because they are limited to a discussion-based analysis of policies and procedures.) Tabletop exercises may include the following:
- a. Engaging operational and support personnel who are responsible for implementing the BCP.
 - b. Practicing and validating specific functional response capabilities.
 - c. Demonstrating knowledge and skills, as well as team interaction and decision-making capabilities.
 - d. Role playing with simulated responses, evaluating critical steps, recognizing difficulties, and resolving problems.
 - e. Clarifying critical plan elements, as well as problems noted during exercises.
 - f. Creating action plans to correct issues.
19. Verify that management clearly defines the characteristics of a successful test, which may include the following:
- a. Validating RPOs, RTOs, and MTDs.
 - b. Demonstrating recoverability at peak volumes.
 - c. Confirming that systems can support critical business processes (e.g., transfer to alternate sites, increased workloads, manual workarounds, and communication).
 - d. Integrating technologies that support critical business activities, including data replication, recovery, and off-site storage.
 - e. Testing backup data to assess integrity and availability.
 - f. Certifying facility controls (e.g., environmental, backup power, and physical security).
 - g. Verifying workspace restoration (e.g., network connectivity and communications).
 - h. Ensuring that personnel are familiar with and are able to execute their responsibilities.
20. Determine whether the right to perform testing or participate in exercises and tests with third parties is described in the contract governing the entity's relationship with the third-party service provider.
21. Determine whether exercises and tests with third-party service providers are included in the entity's enterprise exercise and test program based on the risk prioritization of the third-party

service provider and the criticality of the services provided to the entity. Assess the following:

- a. The process to rank third-party service providers based on criticality, risk, and testing scope.
 - b. Coordinated exercises and tests that reasonably validate the abilities of both the entity and the third-party service provider to recover, restore, resume, and maintain operations after disruptions consistent with business and contractual requirements.
 - c. Evidence that exercises and tests of critical service providers include reasonably foreseeable significant disruptive events.
 - d. Documentation of the scope, execution, and results of exercises and tests in which the entity is unable to directly participate.
22. Determine whether the entity participates in its critical third-party service providers' exercise and test program(s) at reasonable intervals. Assess the execution of the exercises and tests and whether they included the following:
- a. End-to-end and, when appropriate, full-scale exercises.
 - b. Transaction processing and functional testing.
 - c. Network connectivity and interdependencies to include those with critical fourth parties.
 - d. Bidirectional operations between the entity's and its third-party service provider's primary and alternate locations and systems.
 - e. Supply chain considerations.
23. Determine whether testing scenarios with critical third-party service providers consider the following:
- a. An outage or disruption of the service provider.
 - b. An outage or disruption at the entity.
 - c. Incident response plans.
 - d. Crisis management plans.
 - e. Communication processes with third-party service providers and other stakeholders.
 - f. Cyber events.
 - g. Returning to normal operations.
24. Determine whether the tests validate the core or significant firm's backup arrangements to confirm the following:
- a. Backup sites are able to support typical payment and settlement volumes for an extended period.
 - b. Backup sites are fully independent of the critical infrastructure components that support the primary sites.
 - c. Trained employees are located at the backup sites at the time of disruption.
 - d. Backup site employees are independent of the staff located at the primary site at the time of disruption.

- e. Backup site employees are able to recover clearing and settlement of open transactions within the time frames addressed in the BCM processes and applicable industry standards.
25. Determine whether the exercise and test assumptions are appropriate for core and significant firms and consider the following:
- a. Primary data centers and operations facilities that are completely inoperable without notice.
 - b. Whether personnel at primary sites, who are located at both data centers and operations facilities, are unavailable for an extended period.
 - c. Whether other organizations are also affected, causing effects that have the potential to cascade from one organization across to the entire financial services sector.
 - d. Infrastructure (e.g., power, telecommunications, transportation) that is disrupted.
 - e. Whether data recovery or reconstruction to restart payment and settlement functions can be completed within the time frames defined by the BCM process and applicable industry standards.
 - f. Whether continuity arrangements continue to operate until all pending transactions are closed.
26. Determine whether the core firm's testing strategy includes plans to test the ability of significant firms that clear or settle transactions to recover critical clearing and settlement activities from geographically dispersed backup sites within a reasonable time frame.
27. Determine whether the significant firm has an external exercise and test strategy that addresses key interdependencies, such as exercises and tests with third-party market providers and key customers, and determine the following:
- a. Whether external exercise and test strategies include the significant firm's backup sites to the core firm's backup sites.
 - b. Whether the significant firm participates in industry (e.g., U.S. Department of the Treasury's Hamilton Series and FS-ISAC's CAPS exercises) or cross-market tests sponsored by core firms, markets, or trade associations. Tests should incorporate verifying the connectivity from alternate sites and include transaction, settlement, and payment processes, to the extent practical.
28. Determine whether the exercise and test program is sufficient to demonstrate the entity's ability to meet its continuity objectives and whether the results demonstrate the readiness of personnel to achieve the entity's recovery and resumption objectives. Determine whether management accomplishes the following:
- a. Coordinate the execution of its exercise and test program to fully exercise its business continuity planning process.
 - b. Analyze and compare results against stated objectives.
 - c. Raise issues with appropriate personnel and assign responsibility for resolution.

- d. Escalate issues that cannot be resolved in a timely manner to the appropriate level of management.
 - e. Prioritize and track issues through final resolution.
 - f. Analyze results and issues to determine whether problems can be traced to a common source.
 - g. Document recommendations for future exercise and tests.
29. Verify that corrective actions have been implemented and that retesting occurs in a timely fashion to address deficiencies in meeting the entity's objectives.
30. Verify that test results are used to update the business continuity processes, enhance future testing, and evaluate whether risk mitigation strategies should be adjusted.

Objective 11: *Determine whether management continuously measures the progress and assesses the effectiveness of BCM and uses the information to improve the BCM process.*
(VIII, "[Maintenance and Improvement](#)")

1. Determine whether management reviews and updates the business continuity program to reflect the current environment. Triggers that prompt maintenance and improvement of the BCM may include the following:
 - a. Changes in enterprise strategies.
 - b. New or reconfigured products, services, or infrastructure.
 - c. Changes in products and services offered by third-party service providers.
 - d. Deficiencies identified in third-party service provider BCM processes.
 - e. New legislation, regulatory requirements, or resilience practices.
 - f. Results of operational metric analysis (e.g., key risk indications, key performance indicators).
 - g. Early warning indicators that may identify potential continuity events, crises, or incidents (e.g., frequency and severity of storms, heightened cyber attack activity, or increases in customer service calls).
 - h. Variances between budgeted and actual BCM expenses.
 - i. Results from exercises and tests and lessons learned.
 - j. Changes in the threat landscape (e.g., new capabilities, intent of threat actors).
 - k. Recommendations (e.g., from audits, vulnerability assessments, and penetration tests, including those involving the use of advanced cybersecurity analysis and assessments).
2. Determine whether management has documented, analyzed, and reviewed lessons learned from adverse events. Documented procedures for incorporating lessons learned may include:
 - a. Identifying the failure(s).
 - b. Determining the cause(s).
 - c. Evaluating potential solutions.
 - d. Implementing corrective actions as appropriate.
 - e. Recording and reviewing corrective actions taken.

3. Verify that management documents, tracks, and resolves any changes when updating the BCP and the exercise and testing program(s). Furthermore, verify that management maintains appropriate version control of key BCM documents.
4. Determine whether management maintains backup copies of relevant BCM documentation in the event that the primary repository becomes inaccessible.

Objective 12: Determine whether the board has established expectations for BCM reporting. (IX, “[Board Reporting](#)”)

1. Review board minutes to determine whether management periodically reports to the board on the status of BCM.
 - a. Determine whether reports include a written BCM presentation, including the BIA, risk assessment, BCP, exercise and test results, and identified issues.
 - b. Determine whether management provides the board with regular strategy updates based on changes in personnel, roles and responsibilities, and business operations.
 - c. Verify that management documents the reasons (e.g., cost and service level) for choosing recovery alternatives and why they are appropriate based on the entity’s risk profile and complexity.
 - d. Assess whether the board provides a credible challenge to management, when appropriate.

Objective 13: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge regarding the following:
 - a. Apparent violations of laws and regulations.
 - b. Significant issues warranting inclusion in the report of examination.
 - c. Proposed Uniform Rating System for IT (URSIT) management component rating and the potential impact of the examiner’s conclusions on composite or other URSIT component ratings.
 - d. Potential impact of the examiner’s conclusions on the entity’s risk assessment(s).
2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
3. Document conclusions in a memorandum to the examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and clarifying guidance to future examiners.
4. Organize work papers to show clear support for significant findings by examination objective.

Appendix B: Glossary

The purpose of the glossary is to define technical terms used in the *FFIEC IT Examination Handbook* booklets in the context of supervisory activities for the entities over which FFIEC members have supervisory authority. The FFIEC members strive to align terminology in the glossary with appropriate authoritative standards, including the *NIST Computer Security Resource Center Glossary* (NIST Glossary) as the primary source for cyber-related definitions, as appropriate. FFIEC members employed the following process to select, modify, or develop definitions.

When a NIST definition existed:

- If NIST had a defined term and modifications to the definition were unnecessary, the FFIEC members included the NIST definition in this glossary. When multiple NIST definitions were available for the same term, the FFIEC members selected a definition for supervisory purposes.
- If NIST had a defined term, but the definition needed additional clarity for supervisory purposes to assist with the identification of safety and soundness and enterprise risks related to IT, the FFIEC members included both the NIST definition and the FFIEC-adapted definition. Definitions of this nature are labeled “FFIEC Adapted for Supervisory Purposes” in this glossary’s source column.

When a NIST definition did not exist or the definition was not appropriate for supervisory purposes:

- If NIST did not have a defined term, but there was an appropriate authoritative third-party source (e.g., the International Organization for Standardization (ISO) Glossary), the FFIEC members included that authoritative definition.
- If NIST did not have a defined term and there was not an appropriate authoritative third-party source, the FFIEC members developed a definition for supervisory purposes. Definitions of this nature are labeled “FFIEC Developed for Supervisory Purposes” in this glossary’s source column.

Note: Due to the constantly evolving nature of IT and its associated risks, the FFIEC members may update definitions to maintain alignment with other government agencies and the financial services industry.

Term	Definition	Source
A		
Application programming interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.	NIST Glossary
	Software code that allows two or more programs to communicate with each other.	FFIEC Adapted for Supervisory Purposes

Asynchronous replication	Data is first written to the primary storage area (store) and then copied to the secondary storage area (forward) at predefined intervals, which is useful over smaller bandwidth connections and longer distances where latency could occur.	FFIEC Developed for Supervisory Purposes
B		
Business continuity	The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruption.	ISO 22300:2018(en)
Business continuity management (BCM)	The process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services.	FFIEC Developed for Supervisory Purposes
Business continuity plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.	NIST Glossary
	A comprehensive written plan(s) to maintain or resume business in the event of a disruption.	FFIEC Adapted for Supervisory Purposes
Business impact analysis (BIA)	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.	NIST Glossary
	Management's analysis of an entity's requirements, functions, and interdependencies used to characterize contingency needs and priorities in the event of a disruption.	FFIEC Adapted for Supervisory Purposes
C		
Cold site	A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.	NIST Glossary
Contingency plan	A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.	NIST Glossary
Crisis	Abnormal and unstable situation that threatens the organization's strategic objectives, reputation or viability.	Business Continuity Institute Disaster Recovery Journal Glossary
Crisis management	The process of managing an entity's preparedness, mitigation response, continuity, or recovery in the event of an unexpected significant disruption, incident, or emergency.	FFIEC Developed for Supervisory Purposes
Critical financial markets	Financial markets whose operations are critical to the economy. Critical financial markets provide the means for financial institutions to adjust their cash and securities positions and those of their customers in order to manage liquidity, market, and other risks to their organizations. Critical financial markets also provide support for the provision of a wide range of financial services to businesses and consumers in the United States and support the implementation of monetary policy. Examples of critical financial markets include federal funds, foreign	FFIEC Developed for Supervisory Purposes

	exchange, and commercial paper; U.S. government and agency securities; and corporate debt and equity securities.	
D		
Data	A representation of information as stored or transmitted.	NIST Glossary
	A physical or digital representation of information processed, stored (at rest), or transmitted (in transit).	FFIEC Adapted for Supervisory Purposes
Data center	A facility that houses virtual and/or physical information technology infrastructure(s) (e.g., computer, server, and networking systems and components) designed to store, process, and serve large amounts of data in support of an entity's strategic and business objectives. A data center may be a dedicated facility or an area or room, that contains computer, server and networking systems and components, and may be private or shared (e.g., a co-location facility).	FFIEC Developed for Supervisory Purposes
Data mirroring	The act of copying data from a database at a primary location to a database at a secondary location in or near real time.	FFIEC Developed for Supervisory Purposes
Data replication	The process of copying data, usually with the objective of maintaining identical sets of data in separate locations.	FFIEC Developed for Supervisory Purposes
Data synchronization	The simultaneous comparison and reconciliation of interdependent data files, to ensure that the files contain the same information.	FFIEC Developed for Supervisory Purposes
Database	A repository of information or data, which may or may not be a traditional relational database system.	NIST Glossary
	A repository of information or data organized to be accessed, managed, and updated.	FFIEC Adapted for Supervisory Purposes
Disaster	Situation where widespread human, material, economic, or environmental losses have occurred, which exceeded the ability of the affected organization, community, or society to respond and recover using its own resources.	ISO 22300:2018(en)
Disaster recovery	The process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure, systems, and applications, which are vital to an organization after a disaster or outage. Disaster recovery focuses on the information or technology systems that support business functions, as opposed to business continuity, which involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery is a subset of business continuity.	Business Continuity Institute Disaster Recovery Journal Glossary
Disruption	An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).	NIST Glossary
	An anticipated or unplanned event that causes operations to degrade or fail for an unacceptable length of time	FFIEC Adapted for Supervisory Purposes

E		
Emergency management	See crisis management.	
Emergency response	Actions taken in response to a disaster warning or alert to minimize or contain the eventual negative effects, and those taken to save and preserve lives and provide basic services in the immediate aftermath of a disaster impact, for as long as an emergency situation prevails.	Business Continuity Institute Disaster Recovery Journal Glossary
Event	Occurrence or change of a particular set of circumstances.	NIST Glossary
	An occurrence or change in circumstances that may affect operations. An event can be physical, cyber, or a combination of both	FFIEC Developed for Supervisory Purposes
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.	NIST Glossary
	A task or activity done to practice or test a procedure. There are many different types of exercises, depending on the intended goals and objectives. An exercise may involve performing duties in a simulated environment and can be discussion-based or simulation-based.	FFIEC Adapted for Supervisory Purposes
F		
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.	NIST Glossary
Full-scale exercise	A simulation involving a full use of available resources (e.g., hardware, software, personnel, communications, utilities, and processing from an alternate site) at the same time.	FFIEC Developed for Supervisory Purposes
Functional testing	Testing that verifies that an implementation of some function operates correctly.	NIST Glossary
H		
High availability	A failover feature to ensure availability during device or component interruptions.	NIST Glossary
	Ability of a system to be continuously operational for a desirably long length of time and to maintain a minimum amount of downtime during device or component interruptions. Availability can be measured relative to "100% uptime" or "never failing."	FFIEC Adapted for Supervisory Purposes
Hot site	A fully operational off-site data processing facility equipped with hardware and software, to be used in the event of an information system disruption.	NIST Glossary
I		
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	NIST Glossary

Incident management	The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.	FFIEC Developed for Supervisory Purposes
Incident response	The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.	Business Continuity Institute Disaster Recovery Journal Glossary
Infrastructure	System of facilities, equipment, and services needed for the operation of an organization.	ISO 22300:2018(en)
Integrated exercise	A simulation to test the effectiveness of the continuity plans for a business line or major function that incorporates more than one component or module, including external dependencies.	FFIEC Developed for Supervisory Purposes
Interdependencies	When two or more departments, processes, functions, or third-party providers interact to successfully complete a task, business function, or process.	FFIEC Developed for Supervisory Purposes
L		
Last mile	Communications technology that bridges the transmission distance between the telecommunication service provider and the entity.	FFIEC Developed for Supervisory Purposes
Latency	Time delay in processing voice packets.	NIST Glossary
	Time delay in processing voice and data packets.	FFIEC Adapted for Supervisory Purposes
Limited-scale exercise	A simulation involving applicable resources (personnel and systems) to recover targeted business processes.	FFIEC Developed for Supervisory Purposes
M		
Maximum tolerable downtime (MTD)	The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.	NIST Glossary
	The total amount of time the system owner or authorizing official is willing to accept for a business process disruption, including all impact considerations.	FFIEC Adapted for Supervisory Purposes
N		
Network backbone	The main communication channel of a network that interconnects one or more network segments and provides a path for the exchange of data between devices. A backbone can span any geographic area.	FFIEC Developed for Supervisory Purposes
O		
Operational resilience	The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.	NIST Glossary
	The ability of an entity's personnel, systems, telecommunications networks, activities, or processes to resist, absorb, and recover from or	FFIEC Adapted for Supervisory Purposes

	adapt to an incident that may cause harm, destruction, or loss of ability to perform mission-related functions.	
Outage	The interruption of systems, infrastructure, support services, or essential business functions, which may result in the entity's inability to provide services for some period of time. The amount of time lost from an outage may result in downtime. Conversely, downtime may cause an outage.	FFIEC Developed for Supervisory Purposes
Outsourcing	The practice of contracting through a formal agreement with a third party(ies) to perform services, functions, or support that might otherwise be conducted in-house.	FFIEC Developed for Supervisory Purposes
R		
Reciprocal agreement	An agreement that allows two organizations to back up each other.	NIST Glossary
	An agreement that allows two entities (or two internal business groups) with compatible systems and functionality that allows each one to recover at the other's location.	FFIEC Adapted for Supervisory Purposes
Recovery point objective (RPO)	The point in time to which data must be recovered after an outage.	NIST Glossary
	The point in time to which data used by an activity is restored to enable the resumption of business functions. The RPO is expressed backward in time from the point of disruption and can be specified in increments of time (e.g., minutes, hours, or days).	FFIEC Adapted for Supervisory Purposes
Recovery time objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.	NIST Glossary
Remote access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).	NIST Glossary
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	NIST Glossary
S		
Scenario	A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.	NIST Glossary
Service level agreement	Defines the specific responsibilities of the service provider and sets the customer expectations.	NIST Glossary
	A formal agreement between two parties that records: a common understanding about products or services to be delivered, priorities, responsibilities, guarantees, and warranties between the parties. In addition, the agreement describes the nature, quality, security, availability, scope, and timeliness of delivery and response of the parties, the point(s) of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved, and may include other measurable objectives. The agreement should cover not only expected day-to-day situations, but also unexpected or adverse events, as the need for the service may vary.	FFIEC Adapted for Supervisory Purposes

Supply chain risk management	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.	NIST Glossary
	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to exploit vulnerabilities inserted prior to installation. This is done in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).	FFIEC Adapted for Supervisory Purposes
Synchronous replication	Data is written to both primary and secondary storage areas at the same time to ensure that multiple copies of the data are current and identical. This method is used for critical business functions where latency is unacceptable, and little or no data loss can be tolerated.	FFIEC Developed for Supervisory Purposes
T		
Tabletop exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.	NIST Glossary
	A discussion-based exercise where personnel meet in a classroom setting or in breakout groups to validate a component(s) of the business continuity plan(s) by discussing their roles and responsibilities. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.	FFIEC Adapted for Supervisory Purposes
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an IT plan.	NIST Glossary
	A type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment.	FFIEC Adapted for Supervisory Purposes
Threat intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.	NIST Glossary
Trigger	An event that causes the system to initiate a response. Note: Also known as a triggering event.	NIST Glossary
	An event that prompts a response from management or an automated system. Also known as a triggering event.	FFIEC Adapted for Supervisory Purposes
W		
Warm site	An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.	NIST Glossary

Appendix C: Abbreviations

ATM	automated teller machine
BCM	business continuity management
BCP	business continuity plan
BIA	business impact analysis
CA Letter	Consumer Affairs Letter
CAPS	Cyber-Attack Against Payment Systems
CDC	Centers for Disease Control and Prevention
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DDoS	distributed denial of service
DHS	U.S. Department of Homeland Security
DRaaS	disaster recovery as a service
ERM	enterprise risk management
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIL	Financial Institution Letter
FRB	Board of Governors of the Federal Reserve System
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSARC	Financial Systemic Analysis & Resilience Center
FSSCC	Financial Services Sector Coordinating Council
GETS	Government Emergency Telecommunications Service
IIA	Institute of Internal Auditors
ISO	International Organization for Standards
IT	information technology
<i>IT Handbook</i>	<i>FFIEC Information Technology Examination Handbook</i>
MTD	maximum tolerable downtime
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
ODNI	Office of the Director of National Intelligence
RPO	recovery point objective
RTO	recovery time objective
SLA	service-level agreement
SLC	State Liaison Committee
SOC	systems and organization control
SR Letter	Supervision and Regulation Letter
SSAE	Statement on Standards for Attestation Engagement
TSP	Telecommunications Service Priority
URSIT	Uniform Rating System for Information Technology
USC	United States Code
WPS	Wireless Priority Service Program

Appendix D: References

Laws

- 12 U.S.C. 95(b) / 1463(a) / 3102(b), “Comptroller Authority to Declare a Legal Holiday”
- 12 U.S.C. 1464, “Home Owners’ Loan Act”
- 12 U.S.C. 1831r-1, “Notice of Branch Closure”
- 12 U.S.C. 1861–1867, “Bank Service Company Act”
- 12 U.S.C. 1882, “Bank Protection Act”
- 12 U.S.C. 3352, “Emergency Exceptions for Disaster Areas”
- 15 U.S.C. 6801 and 6805(b), “Gramm–Leach–Bliley Act”
- 18 U.S.C. 1030, “Fraud and Related Activity in Connection With Computers”

Consumer Financial Protection Bureau

Guidance

- CFPB Statement on Supervisory Practices Regarding Financial Institutions and Consumers Affected by a Major Disaster or Emergency (September 2018)
- CFPB Compliance Bulletin and Policy Guidance; 2016-02, Service Providers (October 2016)

Federal Reserve

Regulations

- 12 CFR 208, Appendix D-1, “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 208, Appendix D-2, “Interagency Guidelines Establishing Information Security Standards (State Member Banks)”
- 12 CFR 225, Appendix F, “Interagency Guidelines Establishing Information Security Standards”

Guidance

- SR Letter 20-3 / CA Letter 20-2, “Interagency Statement on Pandemic Planning” (March 2020)
- SR Letter 16-11, “Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than \$50 Billion” (June 2016)
- SR Letter 15-10 / CA Letter 15-8, “Expansion of the Federal Reserve’s Emergency Communications System” (October 2015)
- SR Letter 15-9, “FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors” (July 2, 2015)
- SR Letter 13-19 / CA Letter 13-21, “Guidance on Managing Outsourcing Risk” (December 2013)
- SR Letter 13-16, “End of Microsoft Support for Windows XP Operating System” (October 2013)

- SR Letter 13-6 / CA Letter 13-3, “Supervisory Practices Regarding Banking Organizations and Their Borrowers and Other Customers Affected by a Major Disaster or Emergency” (March 2013)
- SR Letter 12-14, “Revised Guidance on Supervision of Technology Service Providers” (October 2012)
- SR Letter 10-13, “Interagency Supervisory Guidance for Institutions Affected by the Deepwater Horizon Oil Spill” (October 2010)
- SR Letter 06-3, “Interagency Supervisory Guidance for Institutions Affected by Hurricane Katrina” (February 3, 2006)
- SR Letter 05-24, “Interagency Questions and Answers for Financial Institutions in Response to Hurricanes Katrina and Rita” (December 2, 2005)
- SR Letter 05-17, “Katrina Related Marketing Practices Invoking the Name of the Federal Reserve” (September 22, 2005)
- SR Letter 05-16, “Supervisory Practices Regarding Banking Organizations and Consumers Affected by Hurricane Katrina” (September 15, 2005)
- SR Letter 03-9, “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System” (May 28, 2003)

Federal Deposit Insurance Corporation

Regulations

- 12 CFR 304.3(d), “Notification of Performance of Bank Services, Form FDIC 6120/06”
- 12 CFR 364, Appendix A “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 364, Appendix B “Interagency Guidelines Establishing Information Security Standards”
- 12 CFR 364, Supplement A to Appendix B “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”

Guidance

- FIL-25-2020 “Identification of Essential Critical Infrastructure Workers During the COVID-19 Response Efforts” (March 26, 2020)
- FIL-14-2020 “Interagency Statement on Pandemic Planning” (March 6, 2020)
- FIL-19-2019, “Technology Service Provider Contracts” (April 2, 2019)
- FIL-63-2018, “Cybersecurity Preparedness Resource” (October 19, 2018)
- FIL-62-2017, “Major Disaster Examiner Guidance” (December 15, 2017)
- FIL-68-2016, “FFIEC Cybersecurity Assessment Tool: Frequently Asked Questions” (October 18, 2016)
- FIL-43-2016, “Information Technology Risk Examination (InTREx) Program” (June 30, 2016)
- FIL-37-2016, “FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks” (June 7, 2016)
- FIL-55-2015, “Cybersecurity Awareness Resources” (November 23, 2015)
- FIL-28-2015, “Cybersecurity Assessment Tool” (July 2, 2015)

- FIL-13-2015, “FFIEC Joint Statements on Destructive Malware and Compromised Credentials” (March 30, 2015)
- FIL-13-2014, “Technology Outsourcing: Informational Tools for Community Bankers” (April 7, 2014)
- FIL-11-2014, “Distributed Denial of Service (DDoS) Attacks” (April 2, 2014)
- FIL-44-2008, “Third-Party Risk: Guidance for Managing Third-Party Risk” (June 6, 2008)
- FIL-6-2008, “Interagency Statement on Pandemic Planning: Guidance for Minimizing a Pandemic’s Potential Adverse Effects” (February 6, 2008)
- FIL-49-2006, “Lessons Learned from Hurricane Katrina: Preparing Your Institution for a Catastrophic Event” (June 15, 2006)
- FIL-27-2005, “Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice” (April 1, 2005)
- FIL-84-2002, “Financial and Banking Information Infrastructure Committee’s Interim Policy on the Sponsorship of Private Sector Financial Institutions in the GETS Card Program” (August 6, 2002)
- FIL-50-2001, “Bank Technology Bulletin on Outsourcing” (June 4, 2001)

National Credit Union Administration

Regulations

- 12 CFR 748, "Security Program, Report of Suspected Crimes, Suspicious Transactions, Catastrophic Acts and Bank Secrecy Act Compliance"
- 12 CFR 748, Appendix A, “Guidelines for Safeguarding Member Information”
- 12 CFR 749, "Guidelines for Safeguarding Member Information", Records Preservation Program and Appendices – Record Retention Guidelines; Catastrophic Act Preparedness Guidelines"
- 12 CFR 749, Appendix A, “Record Preservation Program and Record Retention”
- 12 CFR 749, Appendix B, “Catastrophic Act Preparedness Guidelines”

Guidance

- NCUA Letter to Credit Unions 20-CU-03, "Identification of Essential Critical Infrastructure Workers" (March 2020)
- NCUA Letter to Credit Unions 20-CU-02, "NCUA Actions Related to COVID-19" (March 2020)
- NCUA Letter to Credit Unions 10-CU-10, "2010 Hurricane Season and Ongoing Disaster, Emergency, and Pandemic Preparedness and Planning" (June 2010)
- NCUA Letter to Credit Unions 09-CU-13, "Hurricane Preparedness and Pandemic Planning" (June 2009)
- NCUA Letter to Credit Unions 08-CU-01, “Guidance on Pandemic” (January 2008)
- NCUA Letter to Credit Unions 07-CU-13, “Evaluating Third-Party Relationships” (December 2007)
- NCUA Letters to Credit Unions (06-CU-11), "Interagency Guidance Lessons Learned by Institutions Affected by Hurricane Katrina" (June 2006)
- NCUA Risk Alert 06-Risk-01, “Disaster Planning and Response” (April 2006)

NCUA Letter to Credit Unions 06-CU-06, “Influenza Pandemic Preparedness” (March 2006)
 NCUA Letter to Credit Unions 02-CU-17, “e-Commerce Guide for Credit Unions”
 (December 2002)
 NCUA Letter to Credit Unions 01-CU-21, “Disaster Recovery and Business Resumption
 Contingency Plans” (December 2001)
 NCUA Letter to Credit Unions 01-CU-20, “Due Diligence Over Third-Party Service
 Providers” (November 2001)

Office of the Comptroller of the Currency

Regulations

12 CFR 5.30, “Establishment, Acquisition, and Relocation of a Branch of a National Bank”
 12 CFR 5.31, “Establishment, Acquisition, and Relocation of a Branch and Establishment of
 an Agency Office of a Federal Savings Association”
 12 CFR 30, Appendix A, “Interagency Guidelines Establishing Standards for Safety and
 Soundness”
 12 CFR 30, Appendix B, “Interagency Guidelines Establishing Information Security
 Standards”
 12 CFR 30, Appendix D, “OCC Guidelines Establishing Heightened Standards for Certain
 Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal
 Branches”
 12 CFR 30, Appendix E, “OCC Guidelines Establishing Standards for Recovery Planning by
 Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured
 Federal Branches”

Guidance

OCC Bulletin 2020-23, “Essential Critical Infrastructure Workers in the Financial Services
 Sector”
 OCC Bulletin 2020-13, “Pandemic Planning: Updated FFIEC Guidance”
 OCC Bulletin 2019-13, “Recovery Planning”
 OCC Bulletin 2019-8, “Loans in Areas Having Special Flood Hazards – Private Flood
 Insurance: Final Rule”
 OCC Bulletin 2018-47, “Recovery Planning Guideline: Final Revised Guidelines”
 OCC Bulletin 2018-14, “Installment Lending: Core Lending Principles for Short-Term,
 Small-Dollar Installment Lending”
 OCC Bulletin 2018-8, “Cyber Insurance: FFIEC Joint Statement on Cyber Insurance and Its
 Potential Role in Risk Management Programs”
 OCC Bulletin 2017-61, “Major Disasters: Interagency Examiner Guidance for Institutions
 Affected by Major Disasters”
 OCC Bulletin 2017-54, “Branches and Relocations: Revised Comptroller’s Licensing
 Manual Booklet”
 OCC Bulletin 2017-35, “Flood Disaster Protection Act: Revised Comptroller’s Handbook
 Booklet”

OCC Bulletin 2017-24, “Branch Closings: Revised Comptroller’s Licensing Manual Booklet”

OCC Bulletin 2017-21, “Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29”

OCC Bulletin 2017-7, “Third-Party Relationships: Supplemental Examination Procedures”

OCC Bulletin 2016-34, “Cybersecurity: Frequently Asked Questions on the FFIEC Cybersecurity Assessment Tool”

OCC Bulletin 2016-30, “Enforceable Guidelines for Recovery Planning: Final Guidelines”

OCC Bulletin 2015-31, “Cybersecurity: FFIEC Cybersecurity Assessment Tool”

OCC Bulletin 2013-29, “Third-Party Relationships: Risk Management Guidance”

OCC Bulletin 2012-28, “Supervisory Guidance on Natural Disasters and Other Emergency Conditions”

OCC Bulletin 2006-26, “Disaster Planning: Hurricane Katrina – Lessons Learned”

OCC Bulletin 2006-12, “Influenza Pandemic Preparedness: Interagency Advisory”

OCC Bulletin 2006-6, “Community Reinvestment Act: Hurricanes Katrina and Rita”

OCC Bulletin 2003-14, “Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System”

OCC Bulletin 2003-13, “Telecommunications Service Priority (TSP) Program: Policy on Sponsorship of TSP for Private Sector Entities”

OCC Bulletin 2002-33, “Government Emergency Telecommunications Service (GETS): FBIIC Policy on Sponsorship of GETS Cards for Private Sector Entities”

OCC Bulletin 2002-16, “Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance”

OCC Bulletin 1998-3, “Technology Risk Management: Guidance for Bankers and Examiners”

Other References

U.S. Department of Health & Human Services, Centers for Disease Control and Prevention, [*Pandemic Influenza*](#) (January 2019)

Communications, Security, Reliability, and Interoperability Council, [*Infrastructure Sharing During Emergencies*](#) (December 2014)

National Infrastructure Protection Plan, [*NIPP 2013: Partnering for Critical Infrastructure and Resilience*](#) (November 2013)

NIST SP 800-34 Rev. 1, [*Contingency Planning Guide for Information Technology Systems*](#) (May 2010)

BITS Financial Services Roundtable, [*BITS Framework for Managing Technology Risk for Service Provider Relationships*](#) (May 2008)

Basel Committee on Banking Supervision, [*The Joint Forum: High-level Principles for Business Continuity*](#) (August 2006)

U.S. Department of Homeland Security, [*Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources*](#) (September 2006)

Department of Health and Human Services, Centers for Disease Control and Prevention [*Business Pandemic Influenza Planning Checklist*](#) (December 2005)

Homeland Security Council [*National Strategy for Pandemic Influenza*](#) (November 2005)

Federal Reserve Bank of New York, [*Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment and Settlement Utilities: Report by the Assuring Telecommunications Continuity Task Force*](#) (September 2004)

The President's National Security Telecommunications Advisory Committee, [*Financial Services Task Report*](#) (April 2004)