NIST SP800-34, Revision 1 – *Contingency Planning Guide for Federal Information Systems*

MADRA Presentation
February 18, 2010

Table Of Contents

Introduction to NIST SP800-34 – What is It?

- **National Institute of Standards and Technology (NIST)** is responsible for "developing standards and guidelines, including minimum requirements, for providing adequate security for all agency operations and assets"

- NIST has a series of **Special Publications (SP)** that provide federal agencies with standards and guidelines for most aspects of information systems security in their 800 series publications
  - NIST Special Publications can be found at http://csrc.nist.gov/publications/PubsSPs.html

- **NIST SP800-34 – *Contingency Planning Guide for Information Technology (IT)Systems*** was first published in June 2002, and has become the most downloaded document in the series

- NIST SP800-34 "provides instructions, recommendations, and considerations for government IT contingency planning. Contingency Planning refers to interim measures to recover IT services following an emergency or system disruption."
  - While designed for federal systems, NIST SP800-34 has been used as the guideline for contingency planning throughout much of the private sector as well

Changes in NIST SP800-34 Revision 1

- Overall Changes to NIST SP800-34
- Business Impact Analysis
- Training, Testing and Exercise
- ISCP Process Flow Changes
- Technical Considerations
- Appendices
- System Development Life Cycle (SDLC)

Overall Changes to NIST SP800-34

- Revision 1 moves from a technology viewpoint to a system viewpoint, making the scope more inclusive.
- There is a bigger focus on the Information System Contingency Plan (ISCP) as it relates to the differing levels of Federal Information Security Management Act (FISMA) security impact categories.
- Introduces the concept of resiliency and shows how ISCP fits into an organization's resiliency effort.
- Works to more clearly define the different types of plans included in resiliency, continuity and contingency planning.
- Throughout the guide, call out boxes clarify the specific differences and relationships between COOP and ISCP.

Resiliency is a concept that is gaining widespread acceptance in the continuity and contingency planning

- **Department of Homeland Security (DHS)** defines resiliency as the "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions"
- Resiliency is not process, but rather an end-state for organizations.
- Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions.
- An effective resiliency program includes risk management, contingency and continuity planning, and other security and emergency management activities.

The Goal of A Resilient Organization

Continue Mission Essential Functions at All Times During Any Type of Disruption

NIST SP800-34 Revision 1 provides more clarity to the role and function of various contingency and continuity plans

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining business operations while recovering from a significant disruption.	Addresses business processes at a lower or expanded level from COOP mission-essential functions	Functional continuity plan that may be activated with a COOP to sustain non-critical functions.
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's mission- essential functions at an alternate site for up to 30 days; mandated by federal directives.	Addresses the mission- essential functions; facility- based plan; information systems are addressed based only on their support to the mission-essential functions.	Functional continuity plan that may also activate several business unit- level BCPs.
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Pre-incident-based risk management plan that supports COOP plans for organizations with CI/KR assets.

NIST SP800-34 Revision 1 provides more clarity to the role and function of various contingency and continuity plans

Plan	Purpose	Scope	Plan Relationship
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a system cyber attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	System contingency plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	System contingency plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Location-independent plan that focuses on the procedures needed to recovery a system at the current or an alternate location.	System contingency-based plan that may be activated with a DRP or on its own if relocation is not required.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

A new graphic has been developed to better convey the relationships of the different types of plans to the organization

The Business Impact Analysis (BIA) had major revision to more closely tie to other Federal standards and guidelines

- The process for the BIA has been revised to closely tie to FISMA security impact categories and NIST SP800-53 Contingency Planning (CP) controls.
  - The BIA process now takes into consideration that impact levels were determined as part of the security categorization process.
  - FISMA security impact categories are defined in Federal Information Processing Standard (FIPS 199) - http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- The term Maximum Tolerable Downtime (MTD) is defined and discussed in relation to Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- The BIA discussion addresses the differences between BIAs required for systems and those required by Federal Continuity Directives (FCD) -1 and 2 for Continuity of Operations (COOP) Mission Essential Functions (MEF).

NIST SP800-53 – *Recommended Security Controls for Federal Information Systems and Organizations* define 9 CP controls

Control No.	Control Name	Security Controls and Enhancements		
		Low	Medium	High
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercise	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	----	----	----
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2) (3)	CP-10 (2) (3) (4)

NIST SP800-53 Revision 3 (09/14/2009) is the latest version of the standard – the standard can be found at
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

Testing, Training and Exercises Section is also more closely linked to other federal Standards and guidelines

- There is more clarity when defining testing, training and exercises (TT&E)
- References are included for NIST SP800-84 – *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* - http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
- TT&E is also linked to Federal Information Processing Standards (FIPS) Publication 199 security impact categories
  - For **low-impact systems**, a yearly tabletop exercise is sufficient
  - For **moderate-impact systems**, a yearly functional exercise should be conducted
  - For **high-impact systems**, a yearly full-scale functional exercise should be conducted.
- Sample activities are presented to assist in development of effective TT&E programs for systems

TT&E programs and exercise types are defined to address requirements to NIST SP800-53 control CP-4

- NIST SP800-53 Contingency Planning (CP)-4 defines requirements for contingency plan test and exercise.
- A **Tabletop Exercise** is a “Discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing ISCP and individual state of preparedness..”
- A **Functional Exercise** is a “Simulation of a disruption with a system recovery component such as backup tape restoration or server recovery.”
- A **Full-Scale Functional Exercise** is a “Simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternate facility. “

The flow for steps performed during a contingency event have been revised in the ISCP development

- The flow has switched activation and notification steps in the assumption that an ISCP would not be considered for routine downtimes, but would be used for major issues.
  - The original SP800-34 had notification followed by activation – This sometimes created confusion on how to follow a plan's notification procedures without activating the plan itself
- An organization should activate an ISCP to be able to follow the procedures for notifying assessment and recovery teams.
  - The first step after activating an ISCP is to notify the key stakeholders and to start assessing the disruption
- Escalation and notification has been added to convey the need to continually provide updates and escalation problems as necessary for resolution.
  - Procedures have been added to keep upper management informed of the progress of recovery efforts and to escalate the recovery as needed to more specialized or trained personnel

While overall ISCP primary sections have been reduced, several sub sections have been added to Reconstitution and Deactivation

- Reconstitution and Deactivation are now a single primary section
- Reconstitution has been reworked to include data validation and functionality testing, a declaration of the end of recovery efforts, and more details regarding deactivation.
  - Declaration of the end of recovery efforts is a key addition to the process. This step defines the return of the system to operational status, and stops the recovery effort clock, to determine if the RTO and RPO objectives have been met during the incident.
  - More work is required to have the organization ready for the next event
- Deactivation now includes: Notification of the end of recovery and return to operations, cleanup of recovery documentation, returning backup data to offsite storage, performing a baseline data backup, and documenting the event, lessons learned, and updating the ISCP
  - Deactivation of the ISCP after a contingency event and plan activation may take several days, weeks, or months to complete. The intent is to provide defined processes for an organization to ready itself and improve the ISCP

The Technical Considerations section has been updated to better reflect current trends and standards in systems

- Technical Considerations (Section 5) have been simplified to emphasize options for contingency planning for different types of systems, rather than technologies, and with less emphasis in explaining the different types of systems.
  - Section 5 now focus on three system types: Client/server systems, Telecommunications systems, and Mainframe systems
  - The old categories, including desktop computers, servers, web sites, local area networks, wide area networks and distributed systems have been consolidated into the three defined system types
- Older technologies and terminologies (Zip drives, 3.5” floppies, etc.) have been removed and more generic technologies incorporated to reduce obsolescence
- Cloud computing is not included, as the technology is still emerging and not yet stabilized
- Contingency Considerations and Contingency Solutions for each type of system are still included in the Technical Considerations

Appendices to NIST SP800-34 have been expanded and include more ISCP templates

- There are now 3 templates, 1 each for low, medium and high FISMA applications. The templates also provide more instruction and explanation for filling out separate sections.
- The templates also include ISCP appendices appropriate to the system's impact level that can provide complementary information to assist in recovery efforts.
- The sections in the templates have been rearranged to keep the main body of the ISCP focused on the steps required for recovery, with supplemental and supporting information put into ISCP Appendices
- Templates now include suggested ISCP appendices

The ISCP Templates Table of Contents provide a good summary of the contingency plan steps and processes

TABLE OF CONTENTS

The appendices have been sorted to provide the more critical information needed up front, and background and supplemental information toward the back

- The Appendices are suggestions, and a planner may use none, some or all of them

Suggested Appendices
Appendix A – Personnel Contact List
Appendix B – Vendor Contact List
Appendix C – Detailed Recovery Procedures
Appendix D – Alternate Processing Procedures
Appendix E – System Validation Test Plan
Appendix F – Alternate Storage, Site and Telecommunications*
Appendix G – Diagrams (System and Input/Output)
Appendix H - System Inventory
Appendix I – Interconnections Table
Appendix J – Test and Maintenance Schedule
Appendix K – Associated Plans and Procedures
Appendix L – Business Impact Analysis
Appendix M – Document Change Page

* Note that Appendix F is only required for Moderate and High impact system, and is not included in the Low Impact template

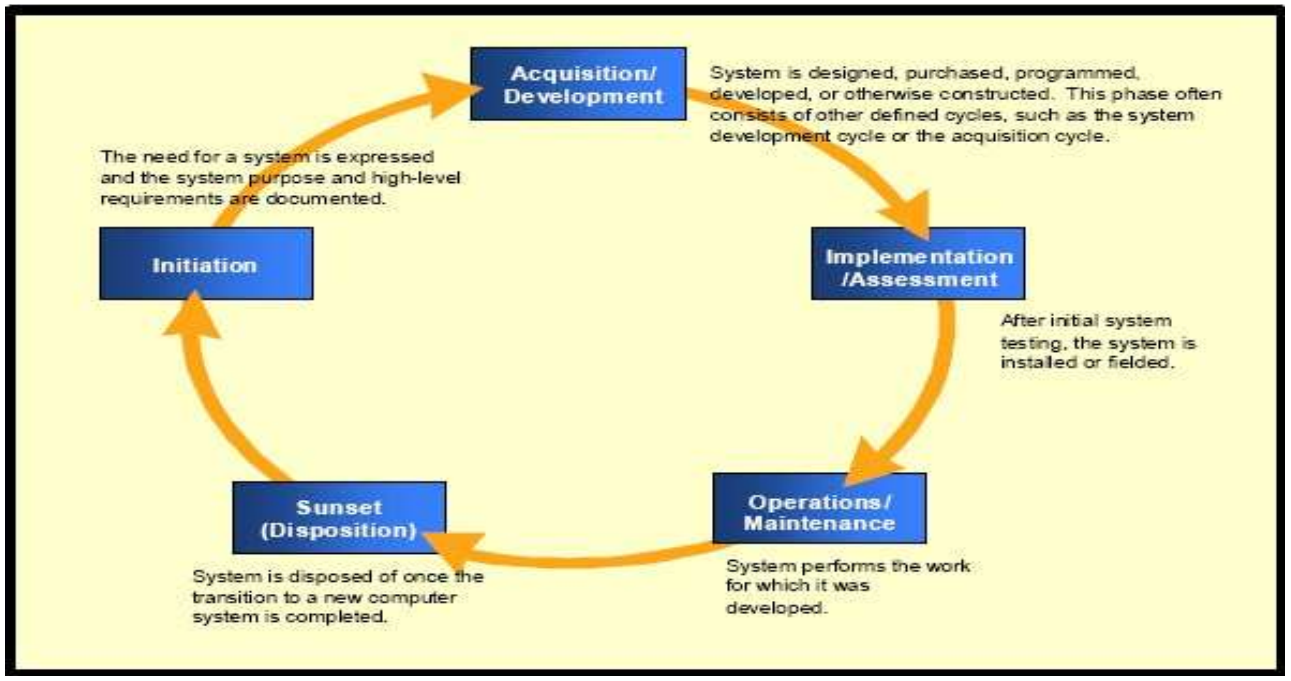
Appendices within NIST SP800-34 have been expanded and changed in Revision 1

- An updated Business Impact Analysis template is provided in Appendix B
- Appendix C is the Frequently Asked Questions section
- Personnel Considerations in Continuity Planning (Appendix D) now includes the use of social networking as part of communications with personnel.
  - Since social networking is an evolving concept, guidance is geared more towards why to use it and what to be aware of rather than what tools to use.

- Appendix E has been added to provide the contingency planning (CP) controls from NIST SP800-53, revision 3

The System Development Lifecycle (SDLC) has been moved from the main body of the guide to Appendix F

- SDLC steps are tied to SP800-53 CP controls and FIPS 199 impact levels to clarify when to get contingency planning included in an SDLC effort.
- Very little in the SDLC has changed, other than tying CP controls into the process. This revision better integrates the three major areas of consideration (contingency planning, SDLC and controls)



Conclusions and Questions

- NIST SP800-34 Revision 1 is the first major update to a contingency planning guideline that is being used by all federal agencies, as well as many state and local agencies
- The guide is also commonly used for contingency plan development within the private sector, and is the most downloaded NIST standard in their library
- Revision 1 focuses more on systems recovery, and incorporates guidance and requirements from NIST SP800-53, FIPS 199, and FCD-1 and 2
- The flow for recovery has been redefined and expanded to provide guidance in all aspects of recovery after a disaster or contingency event.
- New templates have been provided, with more instruction and detail for the contingency planner to better develop effective ISCPs

Questions?

For more information, here is our contact information

- Amy Wohl-Phillips - Associate, Booz Allen Hamilton
  - Address: 8251 Greensboro Drive, McLean, VA 22102
  - Work /Cell Phone: (301) 367-6324
  - Email: wohl_phillips_amy@bah.com
- Dean Gallup – Associate , Booz Allen Hamilton
  - Address: Suite 103 Stafford Commerce Center, 25 Center Street, Stafford, VA 22556
  - Work Phone: (540) 288-5085
  - Cell Phone: (540) 429-2150
  - Email: gallup_dean@bah.com
- David Lynes – Associate, Booz Allen Hamilton
  - Address: 13200 Woodland Park Road, Herndon, VA 20171-3025
  - Work Phone: (703) 984-1430
  - Cell Phone: (703) 217-7183
  - Email: lynes_david@bah.com