Issue Date: <mm/dd/yyyy>
Revision Date: <dd/mm/yyyy>

Document Purpose

The purpose of this Practices Guide is to provide guidance on the practice of **Contingency Planning** and to describe the practice overview, requirements, best practices, activities, and key terms related to these requirements. In addition, templates relevant to this practice are provided at the end of this guide.

Background

The Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC) is a framework to enhance Information Technology (IT) governance through rigorous application of sound investment and project management principles, and industry best practices. The EPLC provides the context for the governance process and describes interdependencies between its project management, investment management, and capital planning components. The EPLC framework establishes an environment in which HHS IT investments and projects consistently achieve successful outcomes that align with Department and Operating Division goals and objectives.

Practice Overview

Contingency planning can be defined in a number of ways. The National Institute of Standards and Technology (NIST) defines contingency planning as management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergency, system failure, or disaster. The Information Technology Infrastructure Library (ITIL) defines disaster recovery as a series of processes that focus only upon the recovery processes, principally in response to physical disaster, that are contained within business continuity management (BCM). The Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC) defines a contingency/disaster recovery plan as the strategy and organized course of action that is to be taken if things don't go as planned or if there is a loss of use of the established business product or system due to a disaster such as a flood, fire, computer virus, or major failure.

Contingency planning is one component of a much broader emergency preparedness process that includes items such as business practices, operational continuity, and disaster recovery planning. Preparing for such events often involves implementing policies and processes at an organizational level and may require numerous plans to properly prepare for, respond to, recover from, and continue activities if impacted by an event. Project managers must also consider the impacts of disruptions and plan, in alignment with organizational standards and policies, for such events. As one component of a comprehensive risk management approach, contingency planning should identify potential vulnerabilities and threats and then implement approaches to either prevent such incidents from happening or limit their potential impact. HHS defines vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. HHS defines a threat as any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats can generally be grouped into three category types:

- *Natural threats* such as floods, tornadoes, earthquakes, hurricanes, ice storms, etc
- *Technical/man made threats* such as radiological, chemical, biological, mechanical, electrical, etc
- *Intentional acts* such as terrorism, demonstrations, bomb threats, assaults, theft, computer security, etc

Although contingency planning sometimes is thought of as an Operations and Maintenance Phase activity, contingency measures should be identified and integrated at all phases of the project life cycle. NIST Special Publication SP800-34 defines a seven-step contingency planning process to developing and maintaining a viable contingency planning program. These seven progressive steps are designed to be integrated throughout a project's life cycle and help guide stakeholders in the planning, development, implementation, key success factors, and maintenance of contingency plans.

1. *Identify any specific regulatory requirements* related to contingency planning. Develop a formal contingency planning policy statement that provides stakeholders the authority and guidance necessary to develop an effective contingency plan. Obtain executive approval, and publish policies such policies.
2. *Conduct a business impact analysis* (BIA) to identify and prioritize critical systems, business processes, and components. Include impact of events, allowable outage durations, and recovery priorities.
3. *Identify and implement preventive controls and measures* to reduce the effects of disruptions, increase availability, and reduce contingency costs.
4. *Develop recovery strategies* ensuring critical systems, business processes, infrastructure, etc can be recovered quickly and effectively following a disruption. Integrate them into system architecture.
5. *Develop contingency plans* containing detailed guidance and procedures to recover from disruptions.
6. *Plan testing, training, and exercises* to reinforce, validate, and test contingency plans to identify gaps and to prepare recovery personnel for unforeseen events. Document lessons learned and incorporate them into updates to contingency plans.
7. *Maintain contingency plans* as living documents. Update them regularly to reflect changes in any influencing factors.

Contingency plan development is a critical component in the process of developing and implementing a comprehensive emergency preparedness program. In general, as defined by NIST, there are five main components of a project contingency plan:

- Concept of operations
- Notification and activation
- Recovery of operations
- Reconstitution of normal operations
- Supporting information as part of the plan's appendices

For contingency planning to be successful, stakeholders must continuously reexamine areas of operational importance with a focus on things such as business processes, systems, and alternatives analysis; recovery strategies, maintenance, training, and plan execution. These activities occur at both an organization and project level. Information gained is used to develop plans addressing specific areas of importance. Types of contingency plans that should be considered may include:

- *Business Continuity Plan* – part of the Certification and Accreditation process, focuses on sustaining business functions during and after a disruption. May address all key business processes or be developed for a specific business process.
- *Business Recovery Plan* – focuses on restoring business processes after an emergency.
- *Continuity of Operations Plan* – mandated by Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*, focuses on restoring essential functions at an alternate location and performing them for some time before returning to normal operations.
- *Continuity of Support Plan* – required by the Office of Management and Budget (OMB) Circular A-130, Appendix III, focuses on the capability of continuing support and service provided by major applications.
- *Crisis Communications Plan* – focuses on defining structures and methods focused on public outreach including procedures for collecting, screening, formatting, and disseminating information.
- *Cyber Incident Response Plan* – focuses on defining procedures to address cyber attacks.
- *Disaster Recovery Plan* – focuses on defining procedures to recover from catastrophic events that deny access to normal operations for an extended period of time.
- *Occupant Emergency Plan* – focuses on providing response procedures for occupants of a facility in the event of a potential threat to the health and/or safety of personnel, environment, or property.

Contingency plans are developed to facilitate responses to anything that may impact normal operations. These plans should contain information and strategies designed to guide stakeholders in the restoration of normal operations and describe strategies for ensuring the recovery of business products and operations in accordance with defined objectives and timeframes. The actual type(s) of plan(s) created, the information they contain, and the defined response(s) are dependant upon factors such as:

- Risk that a particular type of disruption may occur
- Resource availability to respond to different types of disruptions
- Organizational response capabilities
- Readiness to deal with any type of disruption

For projects, the development of a strong contingency plan must begin early in a project's life with the identification of items such as related organizational and operational policies and procedures, project requirements, and availability requirements of the project's product or service Planning activities should continue throughout the project's life as concepts evolve into designs and solutions are incorporated throughout the product's development, testing, and implementation. For example, NIST identifies that:

- During requirements gathering, identification of very high system availability requirements may dictate that redundancy, real-time monitoring, and fail-over capabilities be built into the project's product.
- During product development it's feasible that redundant communication paths, power management systems, load balancing, data mirroring, and replication may need to be considered.
- During implementation contingency/disaster recovery strategies and procedures must be considered and incorporated into product testing activities.
- During operations and maintenance contingency/disaster recover plans should be maintained and updated to reflect changes in influencing factors. Training programs should be developed and implemented to educate stakeholders on recovery procedures and to keep them abreast of changes.

NIST identifies three high-level phases that should be considered when planning how post disruption/disaster activities should be executed.

1. *Notification/Activation Phase* includes the process of beginning the recovery process through the notification of recovery personnel and stakeholders, performing damage assessments, etc
2. *Recovery Phase* includes the actions performed by the recovery teams to repair and/or restore operations in accordance with defined contingency/disaster recovery plans
3. *Reconstitution Phase* includes actions necessary to restore normal operating conditions

What actions are taken, details of those actions, processes for executing them, and response activities associated with these three phases should be detailed within the appropriate contingency plan(s). It is then the responsibility of the System Owner to ensure that copies of such plans are distributed and details of which are communicated to the appropriate stakeholders which may include, but is not limited to:

- Business Steward
- The Office of the Chief Information Security Officer (OCISO).

Additional information on contingency planning can be found in the NIST Special Publication 800-34, *Contingency Planning Guide for information Technology Systems*. Information on risk management can be found in the NIST Special Publication 800-30, *Risk Management Guide to Information Technology Systems*.

Best Practices

The following best practices are recommended for **Contingency Planning** development:

- **Start Early** – Contingency/disaster recovery planning should begin early in the project's life and continue to evolve/mature as work progresses through the project's life cycle
- **Regulations** – Identify related regulatory requirements such as those outlined in the NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*
- **Plans** – Create as many plans as necessary to ensure the integrity of the organization/project
- **Align** – Align any project contingency/disaster recovery plans with those of the performing organization
- **Anticipate** – Anticipate the worst as well as the best case scenarios and be prepared
- **Update** – Contingency/disaster recovery plans are living documents and should be updated as influencing variables change
- **Educate** – Train stakeholders and staff, and continually reinforce planned responses/procedures
- **Lessons** – Review previously used contingency/disaster recovery plans. Discussions with key personnel involved in these plans may identify specific lessons learned

Practice Activities

- Identify any required regulatory requirements
- Develop a formal contingency planning policy statement
- Obtain executive approval, and publish policies
- Conduct a business impact analysis
- Identify and implement preventive controls and measures

- Develop recovery strategies
- Develop contingency plans
- Plan testing, training, and exercises to reinforce and validate contingency plans
- Continuously test plans to identify and resolve gaps
- Prepare recovery personnel through training and awareness campaigns
- Document lessons learned and incorporate them into updates to contingency plans
- Maintain contingency plans as living document, update them regularly to remain current with changes in influencing factors