CDC Unified Process

Project Management

Newsletter

Supporting a Common Project Delivery Framework Volume 6 | Issue 12 | December 2012

Contingency Planning

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 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 broader emergency preparedness processes that include business practices, operational continuity, and disaster recovery planning. Preparing for events 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 plans to either prevent such incidents or limit their potential impact. Threats can generally be grouped into three category types:

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

Contingency measures should be identified and integrated at all phases of the project life cycle. NIST defines a seven-step contingency planning process for developing and maintaining a viable contingency planning program.

1. Identify regulatory requirements to develop a contingency plan policy statement that provides stakeholders authority and guidance necessary to develop an effective contingency plan. Obtain executive approval, and publish such policies.
2. Conduct a business impact analysis. 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 disruption effects, increase availability, and reduce contingency costs.
4. Develop recovery strategies for critical systems, business processes, and infrastructure. Integrate them into system architecture.
5. Develop detailed guidance and procedures to recover from disruptions.
6. Plan testing, training, and exercises to reinforce, validate, and test contingency plans and to identify gaps and prepare recovery personnel. Document lessons learned and incorporate them into contingency plan updates.
7. Maintain contingency plans as living documents. Update them regularly to reflect any changes.

In general, as defined by NIST, there are five main components of a project contingency plan:

1. Concept of operations
2. Notification and activation
3. Recovery of operations
4. Reconstitution of normal operations
5. Supporting information as part of the plan's appendices

To be successful, contingency planning stakeholders must continuously reexamine areas of operational importance focusing on systems, business processes and alternatives analysis; recovery strategies, maintenance, training, and plan execution. These activities should occur at both an organization and project level 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 – focuses on restoring essential functions at an alternate location and performing them for some time before returning to normal operations.
- Continuity of Support Plan – focuses on continuing support and service for 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 recovering 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.

For projects, 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 into development, testing, and implementation. For example, NIST identifies that:

- During requirements gathering, identification of 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, power management, and data mirroring may need to be considered.
- During implementation recovery strategies and procedures must be considered and incorporated into product testing activities.
- During operations and maintenance recovery 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.

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

For more information about contingency planning, risk management, the Project Management Community of Practice or the CDC Unified Process please visit the CDC UP website at http://www.cdc.gov/cdcup/. ▮

Project Management Community of Practice

- *December 07, 2012*
  Managing Risk

For more information on the Project Management Community of Practice visit the PMCoP website at http://www2.cdc.gov/cdcup/library/pmcop/ ▮

CDC Unified Process Presentations

The CDC UP offers a short overview presentation to any CDC employee and/or contractor group. Presentations are often performed at your facility, on a day of the week convenient for your group, and typically take place over lunch structured as one hour lunch-and-learn style meeting.

Contact the CDC Unified Process at cdcup@cdc.gov or visit http://www.cdc.gov/cdcup to arrange a short overview presentation for your group. ▮

Contact the CDC Unified Process

The CDC Unified Process Project Management Newsletter is authored by Daniel Vitek, MBA, PMP and published by the Office of Surveillance, Epidemiology, and Laboratory Services.

For questions about the CDC UP, comments regarding this newsletter, suggestions for future newsletter topics, or to subscribe to the CDC UP Project Management Newsletter please contact the CDC UP at cdcup@cdc.gov

http://www.cdc.gov/cdcup/