
Information Technology Role in Continuity of Operations (COOP) Planning

John Glenn, MBCI
Certified Business Continuity Planner

COOP then and now

- Continuity Of Operations (COOP) planning initially was concerned only with protecting the computer infrastructure, basically what is known as “Disaster Recovery.”
- COOP evolved into an enterprise process to protect all assets through risk identification and risk avoidance and mitigation functions.
- COOP planning for all Federal agencies is under the direction of the Department of Homeland Security (DHS).
- Protecting and sustaining the computer infrastructure remains a major component of the COOP effort.

COOP is federally mandated

- **COOP is a process mandated by**
 - **Presidential Decision Directives (PDDs)**
 - **Federal Preparedness Circulars (FPCs)**
 - **Executive Orders (EOs)**
 - **Codes of Federal Regulations (CFRs)**

PDDs and FPCs

- **PDDs**

- **PDD 62: Protection Against Unconventional Threats** (Classified)
- **PDD 63: Critical Infrastructure Protection (CIP)**
- **PDD 67: Enduring Constitutional Government and Continuity if Government Operations** (*superseded by NSPD 51*)

- **FPCs**

- **FPC 60: Continuity of the Executive Branch Continuity of the Federal Government at the Headquarters Kevel During National Security Emergencies**
- **FPC 65: Federal Executive Branch Continuity of Operations (COOP)**
- **FPC 67: Acquisition of Alternate Facilities for Continuity Of Operations (COOP)**

EOs, CFRs, other documents

- **EOs**
 - **EO 12148: Federal Emergency Management**
 - **EO 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions**
 - **EO 12656: Assignment of Emergency Preparedness Responsibilities**
- **CFRs**
 - **Title 36 CFR. Part 1236: Management of Vital Records**
 - **Title 41 CFR, Sec. 101.20.103-4: Occupant Emergency Program**
- **Other**
 - **National Security Act of 1947 as amended**
 - **National Security Presidential Directive (NSPD) 51**

EOs, CFRs, other documents

- **EOs**
 - **EO 12148: Federal Emergency Management**
 - **EO 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions**
 - **EO 12656: Assignment of Emergency Preparedness Responsibilities**
- **CFRs**
 - **Title 36 CFR. Part 1236: Management of Vital Records**
 - **Title 41 CFR, Sec. 101.20.103-4: Occupant Emergency Program**
- **Other**
 - **National Security Act of 1947 as amended**
 - **National Security Presidential Directive (NSPD) 51**

DON Critical Infrastructure Protection (CIP)

- **DON CIP* is a comprehensive, Navy-wide initiative to:**
 - **Identify infrastructures, both cyber and physical**
 - **Assess their vulnerability to loss**
 - **Develop a coordinated physical and cyber indications and warning capability against terrorism, natural disaster, or error**
 - **Take necessary action to ensure achievement of objectives during critical infrastructure loss**

* See “Critical Infrastructure Protection for Naval Warfighters” (Cdr Lynne Gaudreau, USN, published Fall 2001 at http://www.chips.navy.mil/archives/01_fall/critical_infrastructure_protecti.htm)

FPC 65 COOP requirements (Slide 1 of 2)

- **FPC-65 describes planning considerations and requirements for COOP plans. FPC-65 requires that all Federal Executive Branch agencies must:**
 - **Be capable of implementing their COOP plans with, and without, warning.**
 - **Be operational not later than 12 hours after activation.**
 - **Be capable of maintaining sustained operations for up to 30 days.**
 - **Include regularly scheduled testing, training, and exercising of personnel, equipment, systems, processes, and procedures used to support the agency during a COOP event.**

FPC 65 COOP requirements (Slide 1 of 2)

- **FPC-65 describes planning considerations and requirements for COOP plans. FPC-65 requires that all Federal Executive Branch agencies must:**
 - **Be capable of implementing their COOP plans with, and without, warning.**
 - **Be operational not later than 12 hours after activation.**
 - **Be capable of maintaining sustained operations for up to 30 days.**
 - **Include regularly scheduled testing, training, and exercising of personnel, equipment, systems, processes, and procedures used to support the agency during a COOP event.**

FPC 65 COOP requirements (Slide 2 of 2)

- **FPC 65 also requires that agencies:**
 - **Provide for a regular risk analysis of current alternate operating facilities.**
 - **Locate alternate facilities in areas where the ability to initiate, maintain, and terminate COOP is optimal.**
 - **Take advantage of existing agency field infrastructures and give consideration to other options, such as telecommuting, work-at-home, and shared facilities.**
 - **Consider the distance of the alternate facility from the primary facility.**
 - **Include development, maintenance, and review of COOP capabilities using a Multi-Year Strategy and Program Management Plan (MYSPMP).**

Source: Emergency Management Institute Course IS-547 *Introduction to Continuity of Operations (COOP)*

IT compliance – Meeting customer SLAs

- **Know customer requirements**
 - **Create Business Impact Analysis (BIA)**
 - What applications are used
 - What is each application's criticality
 - Maximum Allowable Downtime or Recovery Time Objective ⁽¹⁾
 - Data Loss Level of Tolerance or Recovery Point Objective ⁽²⁾
 - What are the infrastructure requirements
 - During normal conditions
 - During disaster event conditions
 - Personnel requirements
 - Remote site access
 - What Service Level Agreements (SLAs) are in-place
 - What are customer expectations

(1) Recovery Time Objective (RTO): The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTO's often are used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. Similar Terms: Maximum Allowable Downtime

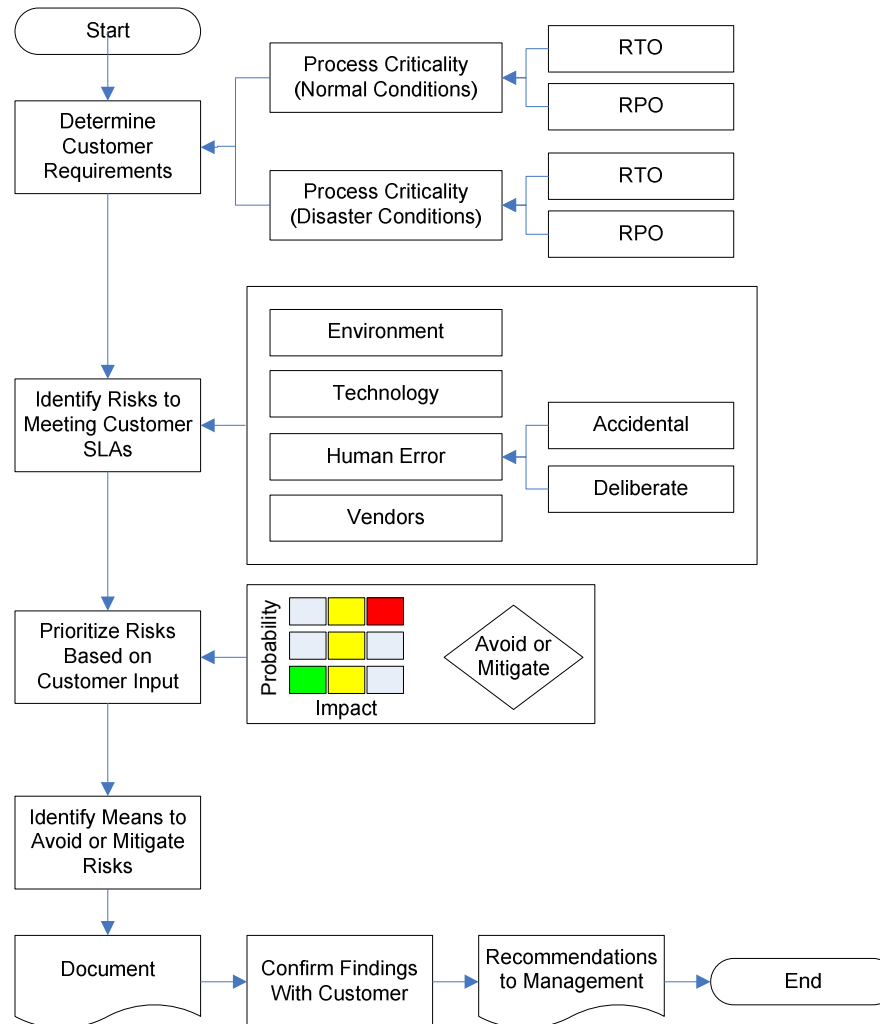
(2) Recovery Point Objective (RPO): The maximum amount of data loss an organization can sustain during an event.

Source for above: *Disaster Recovery Journal Glossary*, <http://www.drj.com/glossary/drjglossary.html>

IT compliance – Reducing risks

- **Identify critical processes**
 - Based on customer input, short and long-range business plans
- **Identify risks to operation**
 - Environment, Human Error, Regulatory, Technology, Vendors, Combination of categories
- **Prioritize (rate) risks and responses**
 - Probability of occurrence (Low/Medium/High)
 - Impact on the organization if risk occurs (Low/Medium/High)
- **Identify means to avoid or mitigate risks**
- **Confirm findings with customer**
- **Recommend avoidance, mitigation measures to command for implementation decision**

IT compliance – BIA overview



IT compliance – Preparing for risks

- **Develop top-down unit response plan**
 - Worse-case scenario – loss of facility
 - Identify critical personnel and their response roles
 - Notification to responders, customers, others
 - Coordination of response with command & support personnel
- **Develop recovery processes and procedures**
 - Create independent documents
 - Follow “KIS(S)” principle
 - Review each document for clarity, completeness
 - Link documents in logical order
 - Identify preceding and following processes & procedures

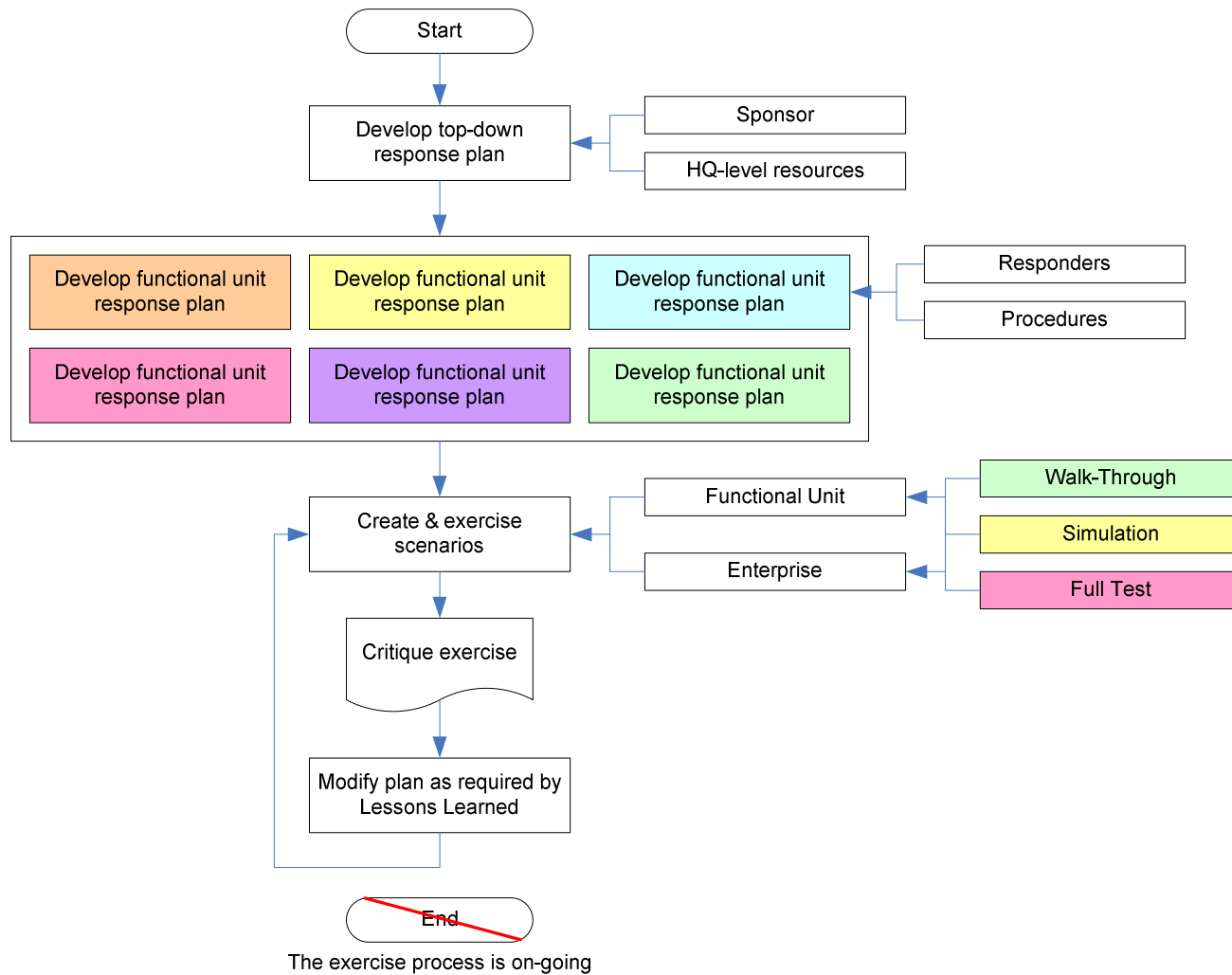
“KIS(S)” = Keep It Simple

IT compliance – Responding to risks

- **Exercise the plans**
 - Start simple with desktop walk-throughs for each process or procedure
 - Increase complexity and inject realism
- **Critique & document each exercise**
 - Identify what worked
 - Identify what can be improved

No exercise is perfect the first time
- **Involve all personnel needed to meet SLAs**
 - Command
 - Support
- **Invite customer to participate**
 - Assures priority agreement
 - Helps customers understand IT response efforts

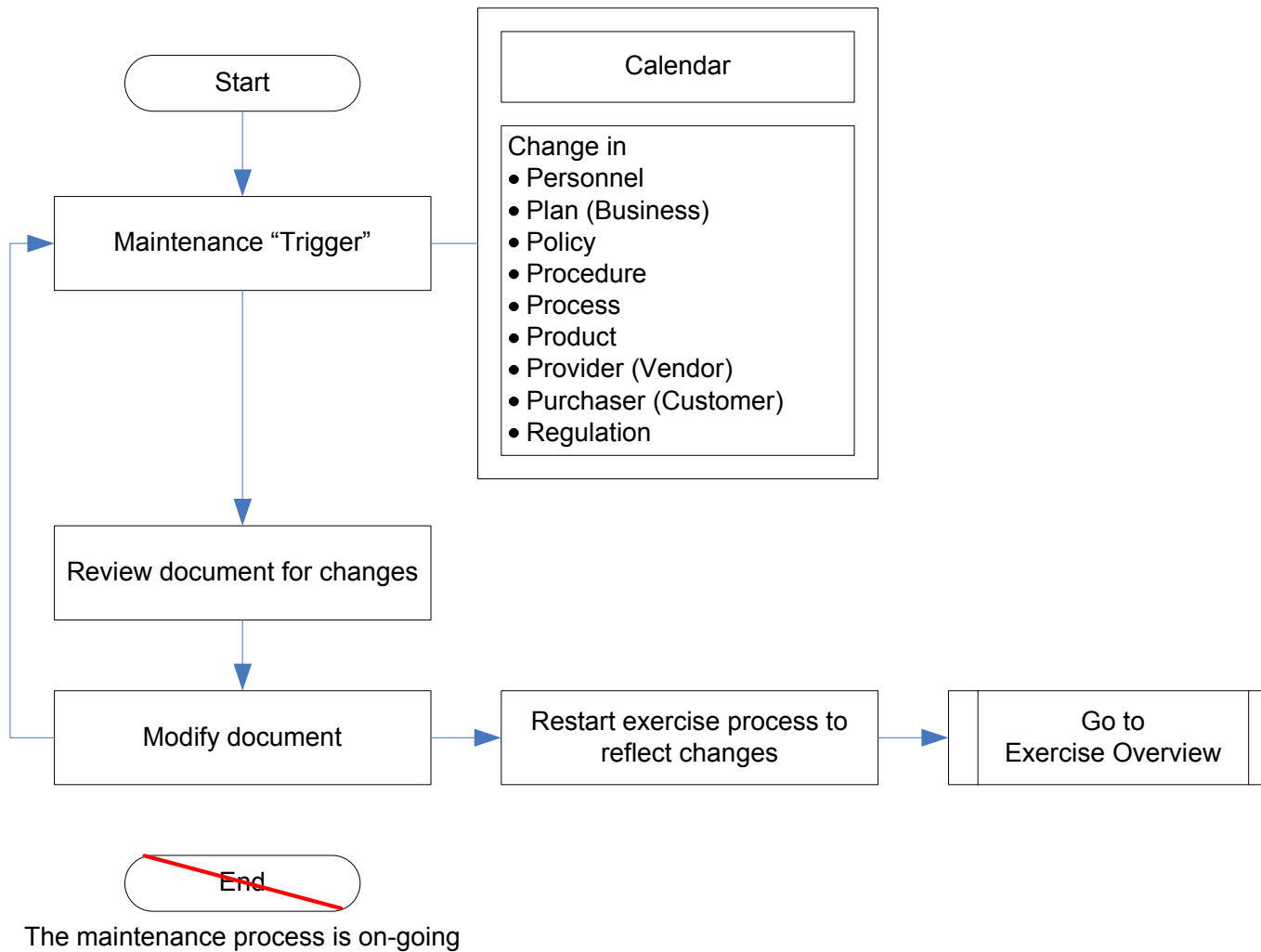
IT compliance – Exercise overview



IT compliance – Plan maintenance

- **At least once-a-year**
 - **Review customer requirements**
 - Any change to business processes which impact IT plan?
 - Any change to customer base which impacts IT plan?
 - Any system adds/moves/deletes which impact IT plan?
 - **Review response plans**
 - Any changes to
 - Personnel
 - IT
 - Command and Support
 - Vendor
 - Processes
 - Procedures
 - Products (hardware, software, infrastructure)
 - **Update and verify documentation**
 - **Exercise modified plan**

IT compliance – Maintenance overview



Special events

- **Special events require individual plans which focus on risks unique to the event**
 - **Data Center relocation risks**
 - **Schedule – too aggressive to be met**
 - **Hardware – lack of, damage-in-transit, failure, incompatibility**
 - **Communications failure between old-new centers**
 - **Latency – too great for user efficiency**
 - **Security – in transit, at new site**
 - **Vendors/Contractors – delayed product delivery, task completion**
 - **Holiday events**
 - **Access to facilities – restricted due to infrastructure closures**
 - **Limited personnel presence**
 - **Physical security issues – crowd environment**