Citywide IT focused- Disaster Preparedness, Response, Recovery, and Resilience Policy

Committee on Information Technology (COIT)

The City and County of San Francisco (City) is committed to preparing for natural (e.g., earthquake, Floods) and human caused (e.g., Cyber, Active assault) disasters and any variety of incidents which may adversely impact the City's business operations. A critical element of our preparedness is the resilience of our IT systems, through proper prevention and protection of these systems and their environments, and the capability to quickly recover them when applications, systems, or infrastructure environments fail. The IT-focused Disaster Preparedness, Response, Recovery and Resilience (DPR3) Policy provides clear, consistent, and achievable standards for the City's IT resilience, which apply to all City departments, before, during, and after a disaster. These standards are meant to ensure continued delivery of critical, IT-reliant public services in response to any incident.

PURPOSE AND SCOPE

The DPR3 Policy requires all City departments to develop, test, and maintain departmental IT focused Continuity of Operations plan (IT COOP) also called an IT Contingency Plan for all the Critical IT System/Applications being managed and supported by the city departments to meet the needs of critical system operations in the event of a disruption.

Goals of IT COOP include:

1. Safeguarding and restoring data
2. Safeguarding hardware, software and facilities
3. Resuming critical business processes through high-availability and automate/manual failover recovery strategy

POLICY STATEMENT

The DPR3 Policy requires all departments to:

1. Designate an IT COOP/DR Lead and/or Disaster Preparedness Coordinator (DPC) liaison to coordinate planning and implementation of DPR3 policy requirements
2. Identify and assess the resilience of critical systems
3. Adopt and implement an IT COOP National Institute of Standard and Technology (NIST) framework
4. Review and update the departmental IT COOP annually and Disaster Recovery Plans (DRP) for each critical system bi-annually
5. Exercise the IT COOP at least annually and perform an active Disaster Recovery (DR) test of each critical system bi-annually
6. Department Heads are responsible for ensuring compliance with this policy

COIT Policy Dates

Last Approved: September 15, 2016
Next Review Date: FY 2017-18

IT COOP REQUIREMENTS

1. All City departments must have an IT COOP/DRP and updated annually thereafter
2. Each department must test its IT COOP/DRP at least annually. The specific type, frequency and extent of DR testing will depend upon:
    a. Criticality of system
    b. Complexity of information systems applications, infrastructure, network, and environments
    c. Results of prior testing
3. Each department must train its relevant employees to execute its IT COOP/DRP. Training will consist of:
    a. Awareness of the COOP and its IT COOP/DRP element
    b. DPR3 and departmental policies and procedures
    c. Execution of IT COOP/DRP in response to an incident
    d. Employee roles and responsibilities
4. Departments dependent on Citywide networks and systems under the operation of, or managed by, the Department of Technology (DT) need to establish memoranda of understanding (MOU) and/or service level agreements (SLAs) with DT for DR, to include target recovery times based on the criticality of the system
5. Departments dependent on third-party vendors for IT services need to establish MOU and/or SLAs with these vendors for DR, to include target recovery times, based on the criticality of the vendors' services
6. All new City IT contracts, policies, and procedures must address disaster resiliency and recovery. Existing contracts should be modified upon renewal to address disaster resilience and recovery
7. If a department receives IT services from another department or a third party, the SLAs must be established to address disaster resilience and recovery

ROLES AND RESPONSIBILITIES

COIT

- Provide policy direction to departments
- Provide necessary support to Departments to enable them to develop and complete their IT COOP/DRPs

Department Head

- Designate IT COOP/DR Lead and Disaster Preparedness Coordinator (DPC) liaison staff to coordinate planning and implementation of DPR3, required exercises, and updates to the IT COOP
- Ensure DPR3 compliance
- Responsible to establish MOU with DT, other city department and vendors for their dependent services such as network, system and other support services related to DR SLA and strategy

Department IT COOP/DR Lead and DPC Liaison

- Responsible for development of IT COOP/DRPs and ongoing DR testing and monitoring of DPR3 compliance

- Responsible for departmental business operations to support during/after Natural or Human caused Disaster and compliance and specifying recovery time/point objectives
- Coordinates closely with the IT Leaders for the DRP3 compliance

Department of Technology

- Responsible to support and implement IT COOP/DRPs for Citywide IT infrastructure support, including, but not limited to, the DT managed business network, internet connectivity, telecommunications, email, emergency radio communications and maintaining emergency data sets through department data coordinators as well as assisting departments without internal IT staff with the development of their IT COOP/DRPs

CSA Audits

- CSA Audits will periodically audit departmental IT COOP/DRPs and test results for compliance with DPR3 policy and standards

AUTHORIZATION

SEC. 22A.3. (c) of the City's Administrative Code states, "COIT shall review and approve the recommendations of the City CIO for ICT standards, policies and procedures to enable successful development, operation, maintenance, and support of the City's ICT."

APPENDIX A: TYPES OF CONTINGENCY PLANS

Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. 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.

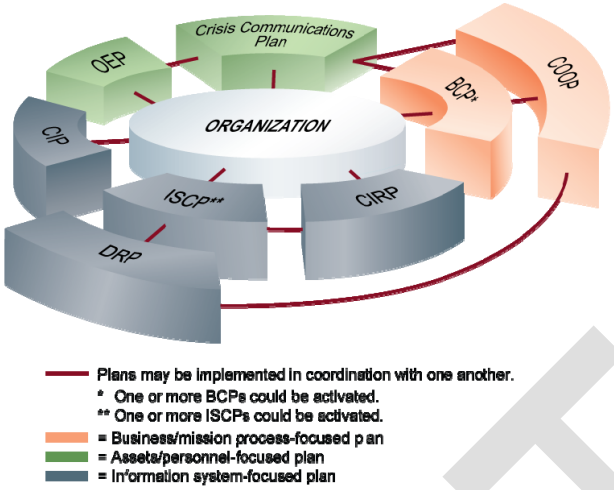
The following briefly describes the type of plans each department is required to conduct in event of a disaster:

- **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
- **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
- **Cyber Incident Response Planning** is a type of plan that normally focuses on detection, response, and recovery to a computer security incident or event

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.
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.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber Incident Response Plan (CIRP)	Provides procedures for mitigating and correcting a cyber-attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system- focused 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.	Information system-focused 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.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system- focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
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 mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Figure shows the interrelationship of each plan as they are implemented to respond to the event as applicable to their respective scopes.


Crisis Communications Plan
OEP
COOP
BCPs
CIP
ORGANIZATION
ISCP**
CIRP
DRP
Plans may be implemented in coordination with one another.
* One or more BCPs could be activated.
** One or more ISCPs could be activated.
= Business/mission process-focused plan
= Assets/personnel-focused plan
= Information system-focused plan

APPENDIX B: IT CONTINUITY OF OPERATIONS AND DISASTER RECOVERY FRAMEWORK

The DPR3 Policy requires all city departments to adopt a Continuity/Contingency of Operations/Disaster Recovery Framework to build contingency plans.

Planning on how to effectively minimize, and recover from, the effects of a service-impacting disaster must be coordinated citywide, as success will rely upon the assistance, resources and expertise of multiple City agencies. Effective recovery is dependent on each City agency following agreed upon procedures and practices for the overall goals of timely response and recovery to be met.

IT 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. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan.

OVERVIEW

Effective contingency planning begins with the development of an organization contingency planning policy and subjection of each information system to a business impact analysis (BIA). This facilitates prioritizing the systems and processes based on impact level and develops priority recovery strategies for minimizing loss.

The guidelines on determining information and information system impact to organizational operations and assets, individuals, other organizations and the nation through a formula that examines three security objectives: confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity** guards against improper information modification or destruction and includes ensuring information non-repudiation and authenticity
- **Availability** ensures timely and reliable access to and use of information. The impact for each security objective is determined to be high, moderate, or low. The highest of the individual security objective impact levels are used to determine the overall information system security impact level. Contingency planning considerations and strategies address the impact level of the availability security objective of information systems Strategies for high-impact information systems should consider high availability and redundancy options in their design. Options may include fully redundant load balanced systems at alternate sites, data mirroring, and offsite database replication. High-availability options are normally expensive to set up, operate, and maintain and should be considered only for those high-impact information systems categorized with a high-availability security objective. Lower-impact information systems may be able to use less

expensive contingency options and tolerate longer downtimes for recovery or restoration of data

STRUCTURE OF IT COOP

Standard elements of a COOP plan include:

- Governance for maintaining each COOP Plan
- Procedures for activating each COOP Plan
- Who is leading each COOP response and who are their proxies
- Cataloging and Prioritizing Mission Essential & Highly Important IT Processes
- Cataloging IT processes which can be suspended until environment is stabilized
- IT and other assets which are required for executing the COOP (e.g. vendors services, backup data, asset costs, etc.)
- Alternate locations for performing recovery and normal tasks (primary and secondary locations)
- Staffing requirements for the initial 120 hours of recovery response
- Intra and inter Department information and service dependencies
- Vendor contact information
- Check list for responding to a major incident
- DR Plan/Runbooks to include step by step procedures to recover critical systems
- Procedures & check list for returning to renovated or new work site
- Staff contact list

STEPS TO DEVELOP AN IT COOP

The process to develop and maintain an effective information system disaster recovery plan are listed below. This process presented is common to all information systems.

The five steps in the process are:

1. Conduct the business impact analysis (BIA);
2. Identify preventive controls;
3. Create/Implement contingency/recovery strategies;
4. Ensure DR plan training, and testing; and
5. Ensure plan maintenance

1. Business Impact Analysis (BIA)

The BIA is a key step in the contingency planning process. The BIA enables the Contingency Planning Coordinator to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. Departments must conduct a BIA. The BIA is a process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster,

accident or emergency. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP.

The BIA is a critical component of a department's Continuity of Operations and Disaster Recovery plan and helps departments:

- Identify Critical IT Resources and dependencies
- Identify Disruption Impacts and Allowable Outage Times; Prioritize uptime requirements, Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Establish recovery strategies, priorities, and requirements for resources and time

2. Identify Preventive Controls

Impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. Preventive controls should be documented in the IT COOP Plan, and personnel associated with the system should be trained on how and when to use the controls. A wide variety of preventive controls are available, depending on system type and configuration. These controls should be maintained in good condition to ensure their effectiveness in an emergency.

3. Develop Recovery Strategies

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

4. Plan Testing, Training and Exercise

Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan.

The following areas should be addressed in a contingency test:

- Validate and update DR Plans/ Runbooks to recover critical system
- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures

5. Plan Maintenance

To be effective, the IT COOP plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required. Generally, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists. Based on the system type and criticality, it may be reasonable to evaluate plan contents and procedures more frequently.