City of Los Angeles

RON GALPERIN
CONTROLLER

August 30, 2017

Honorable Eric Garcetti, Mayor
Honorable Michael Feuer, City Attorney
Honorable Members of the Los Angeles City Council
All Angelenos

Re: Audit of Information Technology Disaster Preparedness, Recovery, and Continuity

When disaster strikes Los Angeles, it is critical that our City be prepared. To preserve lives and taxpayer dollars, our City must maintain access to essential services – many of which rely upon information technology (IT), which plays an indispensable role. Several City departments handle critical IT-related systems, without which the City would not be able to continue its business operations. These systems, if impaired or rendered inaccessible, could threaten the basic protections of life for Angelenos.

Due to the critical role of IT in the City's everyday operations, the Controller's office retained KPMG LLP to assess the City's IT disaster recovery plans for critical systems of City Council-controlled departments. Findings of the audit show that the City needs to embrace a more comprehensive approach to IT-related disaster planning, business continuity, and IT systems recovery. Moreover, it is essential that new investments in IT infrastructure be made in the immediate future.

The Information Technology Agency (ITA), Emergency Management Department (EMD), Los Angeles Police Department (LAPD), Los Angeles Fire Department (LAFD), and Controller operate critical IT systems necessary to protect public safety and keep City services running in the event of a disaster. These essential systems include emergency communications, crime monitoring, payroll, and financial management. Some departments, such as the Controller's office, have initiated efforts to protect essential government functions with remote access systems and backup offsite and/or out of state along with basic cybersecurity testing. While City departments have made progress to prepare us for emergencies, this audit found that there is currently too much fragmentation among their roles. **No one department is responsible for making sure these systems work in the event of a natural or man-made disaster.**

To ensure resident safety and City accountability, **policy makers must create a Steering Committee to achieve greater clarity on the role of EMD as the lead agency for IT disaster recovery planning along with clarifying the responsibilities and needs of the ITA and each City department**.

My audit also found that the City lacks a formal, codified IT business continuity plan and Citywide recovery strategy. Both are imperative to ensuring that critical IT infrastructure, communications, and City business operations can continue during and after a disaster. Both documents also should align with standard industry practices, such as the Department of Homeland Security's Federal Continuity Directive. **I recommend that City policy makers instruct the new Steering Committee to develop and implement a Citywide recovery strategy and IT business continuity plan. This would establish clear procedures to allow our City to properly and expeditiously recover when disaster strikes.**

Most L.A. City IT disaster recovery plans have not been tested in a wide variety of scenarios, nor by a wide variety of staff members. Additionally, few staff members are trained in disaster recovery planning. Departments should undergo more training to develop formal test plans and test cases as part of its recovery strategy, to test the City's critical IT systems during a multitude of scenarios. These scenarios should include, but not be limited to, earthquakes, fires, catastrophic system failure, and cyberattacks. **My audit recommends that all disaster recovery personnel in City departments participate in disaster recovery testing plans and test cases, and those plans should adhere to industry practices.**

Lastly, the City needs to re-think its view of IT systems. Given the fundamental dependence we have on our critical IT systems, **it is essential that we view IT as critical infrastructure, not merely software or computers.** Some City departments are using outdated systems that would not quickly recover in a disaster. In addition, we found that adequate funding has not been provided for necessary infrastructure support and modernization. As a result, the City has not built the necessary resilient IT systems.

Moving forward, appropriate investments in critical IT systems infrastructure must be prioritized. These investments are appropriate for bond financing and should not have to rely on year-by-year budget requests that often fall short of funding IT adequately. **We will have to make substantial investments in a modernized IT infrastructure to ensure that critical systems are protected from major disruption.**

Department heads have notified me that they are willing to more effectively collaborate. However, these departments will need additional direction and support in order to fully implement these recommendations. Therefore, I strongly urge City leaders to support and invest in their efforts. To protect the City's public safety, health and economy tomorrow, we must prepare and become more resilient today.

Key audit findings:

- Los Angeles does not have a formal Citywide IT disaster recovery strategy or a Citywide IT business continuity plan.

- Responsibility for IT business continuity and the corresponding disaster recovery is fragmented and no one City agency is responsible.
- Department-level staff do not participate in planning or testing and lack formal IT disaster recovery training.
- City IT disaster recovery planning and testing does not include an adequate number of disaster scenarios.

Key audit recommendations:

- Establish a Steering Committee to achieve greater clarity on the role of EMD as the lead agency for IT disaster recovery planning along with clarifying the responsibilities and needs of the ITA and each City department.
- Develop and implement a Citywide recovery strategy and IT business continuity plan.
- Require key City disaster recovery personnel to undergo training and participate in disaster recovery testing plans and test cases for a variety of disaster scenarios.
- Ensure core infrastructure components are redundant, back up both data and systems, and facilitate remote access so that IT interruption is avoided or minimized in the event of a disaster.
- Increase funding through the use of bond financing to expedite and upgrade key IT infrastructure.

Respectfully submitted,

Ron

Ron Galperin
CITY CONTROLLER

AUDIT OF INFORMATION TECHNOLOGY DISASTER PREPAREDNESS, RECOVERY, AND CONTINUITY

RON | GALPERIN
Los Angeles City Controller

LACONTROLLER.ORG

TABLE OF CONTENTS

Executive Summary

Introduction

Being prepared for a disaster is critical; the City of Los Angeles (City) must be able to continue to provide services to its businesses and residents in the wake of any natural or man-made disaster. One of the most important areas where preparedness is needed is in the recovery of vital information technology (IT) systems.

The City's Office of the Controller engaged KPMG LLP (KPMG) to conduct a performance audit in accordance with the performance audit standards contained in *Government Auditing Standards,* issued by the Comptroller General of the United States to evaluate the City's activities related to disaster recovery of mission-critical City data and IT applications (Tier 1 applications). *Government Auditing Standards* require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and recommendations based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and recommendations based on our audit objectives. The audit did not include the City's three proprietary departments including the Port of Los Angeles (POLA), Department of Water and Power (DWP) and Los Angeles World Airport (LAWA).

To be effectively prepared for a disaster, organizations must identify what business processes and supporting systems are critical for the continuity of necessary operations. Once the critical processes and supporting systems are identified, organizations must develop, implement, and test business and disaster recovery plans that include how the people, processes, and systems would continue in the event of a disaster. The plans should also address how the organization would return to regular operations including the various phases of the recovery cycle.

Given critical importance of IT systems and associated data to support operations, both the City's Information Technology Agency (ITA) and Operating Departments must have robust and tested disaster recovery plans (DRP)[1] that address a variety of likely disaster scenarios and the critical nature of business processes.

This audit includes an assessment of how Tier 1 applications were identified; an inspection of the associated DRPs for adequacy and recovery capability; and an evaluation of how each of the plans were tested to ensure systems can be recovered within the timelines determined by Operating Departments. Natural and man-made disasters can occur at any time so it is imperative that the City be prepared before, during, and after a disaster.

Within the City, responsibility for business continuity and the corresponding disaster recovery is decentralized, as follows:

- City Operating Departments are responsible for identifying the processes and systems that are critical to their business operations, and work jointly with ITA to:
  - Develop the associated business continuity plans (BCPs)[2]
  - Develop their DRPs including how soon the systems must be available in the event of a disaster
  - Identify and quantify the impacts of the loss of the system (e.g., financial, regulatory, reputation, etc.) and any mitigating measures (e.g. manual processing)

[1] Disaster Recovery Plan (DRP) is an IT-focused plan designed to restore operability of the target systems, applications, or computer facility at an alternate site after an emergency.
[2] Business Continuity Plan (BCP) is the process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business processes can continue to operate.

- ITA is responsible for implementing the DRP for ITA-supported systems and working jointly with City Departments to develop associated DRPs. For applications not managed by ITA, each City Department is responsible for maintaining its own DRP with guidance from ITA as needed.
- The Emergency Management Department (EMD) is responsible for working with the Departments and ITA to facilitate City disaster risk assessments, collect COOP[3] and DRP documents and, based on the policy established by ITA, identifying critical applications. Plans established for critical applications are incorporated in EMD's emergency management plan for the City.

Audit Objectives

The focus of this audit was disaster recovery, and whether Tier 1 applications could be adequately recovered. Accordingly, specific audit objectives included the following:

A: Evaluate whether City Operating Departments, including ITA, have appropriately identified Tier 1 applications.

B: Evaluate the adequacy of the City's DRPs for Tier 1 applications.

C: Evaluate whether ITA adequately tests their DRPs.

D: Compare the City's DRPs to applicable federal, State, or industry leading practices.

E: Determine how well ITA engages with Departments to facilitate the development of viable technology recovery plans and the regular testing of the plans.

Summary of Key Audit Findings

Favorable Conditions Noted:

We noted several efforts underway where the ITA is working to enhance the City's IT disaster recovery capability; specifically:

- Continuing application tiering exercises to reassess the criticality of the City's applications hosted by ITA.
- Reinforcing disaster recovery in Departmental technology plans.
- Developing and implementing a tiered Disaster Recovery (DR) solution.
- Implementing DR features in the current IT Service Management System, which includes application tiering, DR plans, etc.
- Currently using a remote third-party redundancy solution, or "hot site," for some of the tier 1 applications. Also continuing to transition remaining tier 1 applications to a hot site solution.
- Also, in 2016, ITA developed a *Disaster Recovery Policy* that defines the process and provides guidelines to City Departments and ITA to establish and implement the DRPs for mission critical systems.

Conditions Requiring Attention:

There are eight areas identified that were not consistent with recommended leading practices, and therefore require attention of both ITA and related City Departments:

- A formal business continuity framework has not been adopted and implemented. No City Department or governance committee is ultimately responsible for the development, maintenance or testing of

[3] Continuity of Operations Plan (COOP) – A government equivalent of BCP. Primary focus of COOP is the effort to ensure the continued performance of critical business and government functions during a wide range of potential emergencies.

existing BCPs and DRPs. ***Entity Responsible For Implementation: EMD with the support of City Officials***

- A formal citywide recovery strategy has not been developed since there is no citywide responsibility for business continuity and disaster recovery. ***Entity Responsible For Implementation: EMD with the support of City Officials***
- The process to identify critical Tier 1 applications is relatively informal, and not based on a formal risk assessment and industry leading practices. ***Entity Responsible For Implementation: ITA and Operating Department IT organizations***
- Disaster recovery testing does not adhere to industry leading practices. ITA and user Departments have not developed test plans and processes using recognized testing standards and business continuity frameworks. ***Entity Responsible For Implementation: ITA and Operating Department IT organizations***
- Supporting infrastructure components for Tier 1 applications have not been identified as critical. ITA has not been provided the funding and support required to build the necessary resilient IT infrastructure. ***Entity Responsible For Implementation: ITA***
- The City's mainframe-based Tier 1 applications cannot be recovered within the required Recovery Time Objectives (RTO)[4] in a disaster. The primary critical user, the Police Department, has not been able to replace the existing mainframe applications and ITA has not obtained funding for a disaster recovery capability that will meet required RTOs and Recovery Point Objectives (RPO)[5]. ***Entity Responsible For Implementation: ITA and Operating Department IT organizations***
- The dispatch component of an application that supports Police Department cannot be tested for failover. The Police Department has recognized this shortcoming and is proceeding with a replacement. ***Entity Responsible For Implementation: Police Department***
- Access mechanisms for applications hosted at the City's remote recovery site are incomplete. ITA is responsible for establishing and maintaining the access mechanisms and was in the process of implementing them at the time of our audit. ***Entity Responsible For Implementation: ITA***

Because no one Department has ultimate responsibility for the development, maintenance and testing of existing BCPs and DRPs, this has led to an inconsistent methodology for identifying the critical processes and supporting applications. The identification relies heavily on the historical knowledge of employees of City processes, rather than on formal documented processes that leverage business impact assessments and Business Continuity Risk Assessments. In addition, while it appears that the critical applications have been identified, there is a concern that this process would not be repeatable without the knowledge of certain employees that may soon retire. Further, the lack of a central citywide formal BCM[6] program with adequate resources, staff, and organizational priorities has resulted in business continuity and disaster recovery planning that is not sufficiently comprehensive, and lacks planning for the complete disaster recovery lifecycle and ranges of disaster scenarios. Finally, some ITA customers (City Departments) have chosen to stay on under-utilized platforms which are expensive and cannot currently recover in time to meet established recovery time objectives.

[4] Recovery Time Objective (RTO) – The recovery time objective is the time needed to recover from a disaster or, saying it another way, how long you can afford to be without your systems.

[5] Recovery Point Objective (RPO) – Recovery point objective describes the age of the data you want the ability to restore in the event of a disaster.

[6] Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

Potential Impact

Ineffective disaster recovery capabilities of IT systems can result in failure of processes critical to the City, which in turn could lead to loss of life or serious injury, due to failure or delay of 911 systems to provide timely response by first responders. Additionally, the City could suffer heavy financial loss due to damage from the inability to pay vendors, the inability to collect taxes and revenues in a timely manner, and the incurrence of additional liabilities due to not being able to pay personnel or vendors timely for necessary services and supplies.

What the City should do next

To address these conditions, we recommend:

- Develop a citywide business continuity program with the responsibility for implementing and maintaining a robust business continuity or continuity of government framework such as Disaster Recovery Institute International or International Standards Organization (ISO) IS22031.
- Continue the ITA initiative for a tiered disaster recovery solution.
- Continue to fully implement the features of the IT service management system to enable business continuity and disaster recovery inventory and identification of systems' recovery tier ratings.
- Revise disaster recovery testing and exercise practices to incorporate both the business owner and ITA in the complete exercise lifecycle, beginning with scenario definition and ending with testing the return-to-normal-processing steps.
- Identify all recovery infrastructure dependencies and the tier rating of the systems that rely on those infrastructure components. Develop and test plans to ensure that the components can be recovered to support the dependent systems.
- Pending a permanent recovery solution, identify and implement a short term solution to ensure mainframe-based systems can be recovered to meet established recovery time and recovery point objectives.
- Identify and implement a permanent recovery solution for the City's mainframe-based systems that will enable recovery within the established recovery time and recovery point objectives.
- Expedite the replacement of the component of the LAPD Dispatch System and implement failover testing on a regular basis.
- Expedite implementation of the permanent authentication and authorization mechanisms for all systems at the disaster recovery facility.

Scope and Methodology

The audit was conducted in accordance with the performance audit standards contained in Generally Accepted *Government Auditing Standards (GAGAS),* issued by the Comptroller General of the United States to evaluate the City's activities related to disaster recovery of mission-critical City data and IT applications (Tier 1 applications). *GAGAS* requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and recommendations based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and recommendations based on our audit objectives.

<u>Leading practices were leveraged throughout the audit</u> including Disaster Recovery Institute International (DRII)'s "Professional Practices"; the Business Continuity Institute's "Good Practice Guidelines"; ISO 22301; and the National Fire Protection Association's standard on Business Continuity (NFPA 1600). These are nationally and internationally recognized standards used for business continuity practices throughout the world. These standards provide a common frame of reference and have been validated by leading global organizations ranging from large public to small private companies across several industries (e.g., banking, manufacturing, retail, technology and communications, higher education, and federal, state and local government). Leading practice recommends that assessing the state of readiness of any organization

should not only be based on the DRP (IT-focus), but rather based on three major elements (i.e., BCM, BCP, and DRP). In accordance with these standards and leading practices, we performed the following work:

KPMG interviewed various IT and Department stakeholders to understand their application disaster recovery plans and capabilities. In these interviews, we discussed the methods that were used to determine the tier rating of the application such as financial, regulatory, human safety and public image. We inquired with multiple sources to determine if any formal documentation of these determinations (e.g., business continuity impact assessment and business continuity risk analyses) were available and were informed the determinations were based on personal or historical experience rather than formal analysis.

Additionally, we evaluated recovery-related documentation such as disaster recovery plans and procedures, test procedures, test documentation, system component inventories, and recovery site contracts, to assess their adequacy. During the evaluation of these documents and corresponding inquiry with system and user personnel, we applied the principle of a disaster occurring under the worst possible conditions. These conditions would include occurrence at the most critical time, loss of key personnel, loss of supporting infrastructure, and complete site destruction. Additionally, we performed several tours of data centers/facilities to understand the resiliency and risks to the production and recovery sites.

The focus of this audit was disaster recovery processes, and whether critical IT systems could be recovered. Accordingly, the scope of this audit did **not** include a comprehensive evaluation of the following:

- Business continuity planning program and process
- Business impact assessments
- Business continuity risk assessments
- Business continuity plans such as business process recovery plans
- Detailed business process documentation

Following is a description of some of the steps taken in the performance of this audit.

Interviews, Meetings & Site Visits

We interviewed key:

- ITA staff and management that support major application and infrastructure components within ITA to understand the purpose, infrastructure, and locations of systems.
- Business process owners and staff to understand their reliance on systems and the effects of loss of those systems including the increase in effects the longer the system was unavailable.
- Business process and ITA personnel to understand mitigating or compensating measures that may reduce the effects of system loss.
- Departmental IT support staff for systems that are not supported by ITA (e.g. Fire and Police).

In addition to the above interviews, we also visited the ITA Data Center and the current recovery site for FMS and PaySR.

Systems & Data Analysis

We reviewed ITA policies, system inventories, system architecture documentation, disaster recovery plans, available business continuity materials, disaster recovery test plans and results.

Benchmarking and Literature Review

We reviewed various standards and recommended practices from the National Fire Protection Association, Disaster Recovery Institute International, the International Standards Organization, and the Department of Homeland Security.

Audit fieldwork was primarily conducted from July 2016 through December 2016.

Review of the Report

On April 12, 2017, a draft of this report was provided to ITA, EMD, and LAPD management. We met with ITA, EMD, and LAPD management at exit conferences held between April 24 and May 2, 2017. On May 12, 2017, we provided ITA, EMD, and LAPD management with an updated draft report. On June 29, 2017, we met with ITA to clarify Finding #4. On July 21, 2017, we also met with EMD to clarify Finding #4. We considered their comments as we finalized this report.

Department Response & Action Plan

On May 26, 2017, LAPD issued a memo responding to the findings related to LAPD systems, along with their plan of action to address the corresponding recommendations (Recommendations 7.1 and 7.2) directed to LAPD management. (See Appendix III)

On July 25th, 2017 EMD issued a memo responding to the findings and recommendations within the report. EMD generally agreed with the report findings and recommendations, and affirmed that statutory responsibility over citywide disaster recovery planning and coordination resides with EMD. (See Appendix III)

On August 4, 2017 ITA management provided a revised formal response memo and action plan for the recommendations directed toward ITA (Recommendations 2.1, 2.2, 3.1, 3.2, 3.3, 3.4, 4.1, 5.1, 6.1, 6.2, and 8.1). ITA generally agreed with the findings and recommendations, but indicated that the statutory responsibility over citywide disaster recovery planning and coordination lies with EMD (See Recommendation 4.1). We originally directed Recommendation 4.1 toward ITA because, in our opinion, ITA is currently the only City department with the appropriate technical expertise to sufficiently develop and implement citywide disaster recovery plans for Tier 1 systems. ITA management acknowledges that effective development, planning, and testing of citywide IT disaster recovery plans would necessarily involve ITA, and asserted that ITA would continue to participate and provide technical expertise to support the intent of Recommendation 4.1. We also considered ITA's indications related to EMD's responsibility related to implementation of recommendation 4.1 and accordingly requested, and received, an affirmative response to Recommendation 4.1 from EMD. (See Appendix III)

We would like to thank ITA, EMD, LAPD, and the many other participating City department staff and management for their time and cooperation during this audit.

Background

The City has approximately 40 Departments that perform various functions to support operations, such as Treasury and Finance Operations, Fire, Police, Emergency Management, etc. Each Department uses a number of software applications; support for these applications is managed by one or more of the following groups:

1. IT groups within City Operating Departments
2. The City's Information Technology Agency (ITA)
3. Third parties

ITA is the largest IT group in the City and provides data processing, radio, telecommunications, and the network infrastructure that is used by all Departments, including those responsible for public safety. As a matter of public safety and uninterrupted services to citizens of Los Angeles, mission critical applications are necessary during a disaster and require plans and preparations to minimize interruptions that may occur due to natural or man-made disasters and catastrophes.

For this audit, the City defined mission critical applications as "Tier 1" applications, meaning those without which City Operating Departments could not fulfill the City's operating functions during a disaster. The following lists the City's Tier 1 applications, as suggested by ITA:

Note: In most organizations, Tier 0 is the infrastructure layer (e.g., base server, network, authentication/authorization, and security systems such as Intrusion Detection System) that needs to have immediate availability (shorter RTOs than Tier 1). Our audit assumed infrastructure layer is necessary and rated as Tier 0 by the City

Tier 1 system name/description	Business owner	Technical owner
Crime Analysis Application Maintains LAPD's primary repository of data from crime, arrest, and other police reports.	LAPD	ITA
Property Information Application A property tracking system for LAPD's property rooms.	LAPD	ITA
Network Communication Application LAPD's primary crime and arrest report data entry, message switching, and non-mobile facility.	LAPD	ITA
Financial Management System (FMS) Citywide Financial Management System and reporting used by all Council-controlled departments.	Controller	Consultant: CGI (ITA support)
Payroll (PaySR) The City's payroll system, including some Human Resource modules such as Employee Work History.	Controller	Consultant (ITA support)
LAPD Dispatch System Supports LAPD's dispatch process.	LAPD	Motorola (with ITA support)

Tier 1 system name/description	Business owner	Technical owner
LAFD Dispatch System Support LAFD dispatch process.	LAFD	ITA
PSD ShakeCast City implementation of a USGS Earthquake Mapping System will merge shake map files from other ShakeCast users, once sent to the City, for a unified presentation of all ShakeCast user locations and the impact of an earthquake on their facilities.	EMD	USGS (ITA support)
PSD WebEOC A web-enabled crisis information management system used by the City of Los Angeles and neighboring organizations, allows real-time information sharing to help managers make sound decisions quickly.	EMD	ITA

During the audit, we noted that ITA has planned and begun to execute various disaster recovery initiatives. Once fully implemented, these initiatives will remediate some of the findings identified during the audit. These range from short-term quick fixes to long-term robust solutions. Examples include:

1. Application Tiering Exercise: Tiering exercise with City Departments to re-assess City applications, using a quantitative approach.
2. IT Disaster Recovery Policy development: Develop, discuss, and publish citywide IT Disaster Recovery Policy that will include definitions, risk assessment guidelines, and DR planning requirements.
3. Reinforce DR in Department Technology Plans: Under Executive Directive #15, City Departments will be required to submit Technology Plans. ITA will use this as an opportunity to reinforce IT DR planning and gather additional DR data on Department applications.
4. Implementing a tiered DR Solution Approach:
    a. Tier 1 applications: ITA will implement critical applications at a remote redundant hot site.
    b. Tier 2 applications: ITA will promote the use of Cloud Hosting & Data Backup.
    c. Tier 3 applications: ITA will promote offsite data backup and work with City Departments to ensure backup at least weekly and separated from primary infrastructure.
5. Implement DR features in the current IT Service Management System, which include application tiering, DR plans, etc.

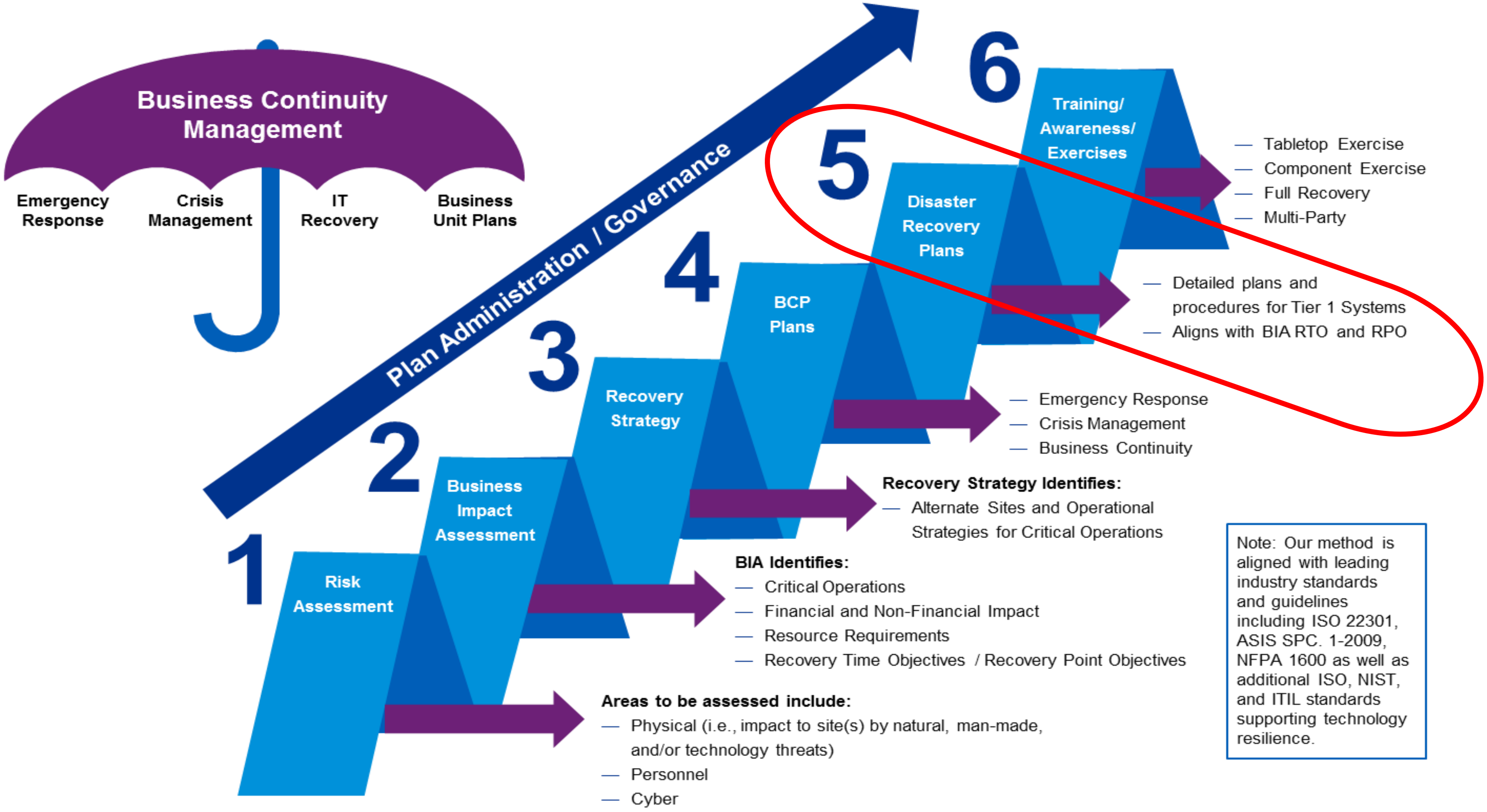
Leading practice recommends that the assessment of the state of readiness of any organization should be based on the following three major elements:

Business Continuity Management (BCM) is a holistic management process that identifies potential impacts which threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value creating activities. This element focuses on management of recovery or continuity in the event of a disaster and also the management of the overall program (i.e., cohesiveness of people, process, and technology) through training, rehearsals, and reviews, to ensure the program stays current and up to date. Essentially, BCM targets the governance piece of the audit. In most organizations, BCM ownership resides on the Executive or City management level.

Business Continuity Plan (BCP) is the process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business processes can continue to operate. This element is typically owned and maintained by the business processes/Departments.

Disaster Recovery Plan (DRP) is an IT-focused plan designed to restore operability of the target systems, applications, or computer facility at an alternate site after an emergency. A DRP addresses major site disruptions that require site relocation. The DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Typically, DRP involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention. DRP is owned and maintained by the IT department/group within an organization.

The graphic on the following page illustrates BCM Overview and a reference to which aspect of BCM was in scope for this audit. Step 5 (circled in RED) illustrates the primary focus of this audit, which is the technical capabilities of the Tier 1 applications. Limited. In depth consideration of the other BCM steps was beyond the scope of this audit. However, because DRP is part of the more expansive and important BCM process, this audit does include some high-level observations and recommendations related to BCM. In general, aspects of the other BCM steps were evaluated only to determine if the appropriate Tier 1 business systems and applications had been identified



Business Continuity Management

Emergency Response

Crisis Management

IT Recovery

Business Unit Plans

Plan Administration / Governance

1 Risk Assessment

Areas to be assessed include:

- Physical (i.e., impact to site(s) by natural, man-made, and/or technology threats)
- Personnel
- Cyber

2 Business Impact Assessment

BIA Identifies:

- Critical Operations
- Financial and Non-Financial Impact
- Resource Requirements
- Recovery Time Objectives / Recovery Point Objectives

3 Recovery Strategy

Recovery Strategy Identifies:

- Alternate Sites and Operational Strategies for Critical Operations

4 BCP Plans

- Emergency Response
- Crisis Management
- Business Continuity

5 Disaster Recovery Plans

- Detailed plans and procedures for Tier 1 Systems
- Aligns with BIA RTO and RPO

6 Training/ Awareness/ Exercises

- Tabletop Exercise
- Component Exercise
- Full Recovery
- Multi-Party

Note: Our method is aligned with leading industry standards and guidelines including ISO 22301, ASIS SPC. 1-2009, NFPA 1600 as well as additional ISO, NIST, and ITIL standards supporting technology resilience.

Findings & Recommendations

This section presents a summary of the audit results by audit objective, and eight specific audit findings with related recommendations. Overall, based on the testwork performed and comparison to leading practices, the City may be challenged to recover critical applications in the event of a disaster.

Audit Objectives	Conclusions
A: To evaluate whether City Departments, including ITA, have appropriately identified Tier 1 business systems and applications, to ensure inclusion in disaster recovery planning.	While the City has identified Tier 1 Applications, the process to do so was informal and did not consider recommended processes and criteria.
B: To determine the adequacy and comprehensiveness of the City's DRP for a reasonable range of disaster scenarios for the City for Tier 1 applications.	City disaster recovery planning does not include an adequate number of scenarios, nor does it encompass the entire lifecycle of a disaster, from declaration to return to normal processing.
C: To determine whether ITA adequately tests their DRPs to ensure effectiveness when needed.	While ITA performs testing on Tier 1 applications, all mainframe applications cannot be recovered to meet required deadlines. In addition, the City does not test for a scenario that incorporates loss of network connectivity (due to loss of City Hall East); also, the critical component of the Police Dispatch System could not be tested due to risk of health and safety impact to 911 callers. Since all Fire Department 911 calls originate in the Police Dispatch System, this may also impact the Fire Department Dispatch System.
D: To determine how the City DRP compares to applicable federal, State, or industry recommended best practices.	City DRP practices do not include the recommended range of processes, including disaster scenarios, recovery scenarios and recovery lifecycle. In addition, due to lack of robust business continuity practices, DRP practices are not based on quantifiable analyses of risk to the City.
E: To determine how well ITA engages with Departments to facilitate viable Technology Recovery Plans and regular testing of the plan; and how Departments have considered staffs' accessibility to utilize their Tier 1 systems within their respective BCP.	Department-level staff do not participate in planning or testing of ITA-hosted systems, applications and infrastructure.

Finding #1:

A formal Business Continuity framework has not been implemented in accordance with leading practices.

A mature organization has established an enterprise-wide business continuity program using an accepted and standardized framework to ensure robust and consistent business continuity practices across the enterprise. Such a framework would ensure that all Departments correctly address the eight key BCM elements (i.e., program governance, risk assessment, business impact analysis, recovery strategy, program plans, training/awareness, exercise and test, and maintenance). A formal business continuity program should govern the business continuity for the entire City, be supported at the highest level, and should comply with recognized standards including the Department of Homeland Security's Federal Continuity Directive I and DRII Professional Practices*. Recommended activities for an effective citywide BCM program are provided in Appendix II.*

In the course of our audit, we found that there is no formal citywide Business Continuity organization responsible for developing and maintaining the program or associated framework that addresses the eight key BCM elements. The lack of a framework has led to the following conditions:

A. A business continuity risk assessment has not been performed to identify the risks, threats, and vulnerabilities as well as the controls that are currently in place to mitigate the impact of a disaster. An annual business continuity risk assessment should be performed to identify and validate risks, threats and vulnerabilities to the business process and any controls to mitigate the impact in the event of a disaster. Recovery plans and procedures developed without a basis in a current and complete business continuity risk assessment may prevent timely and cost-effective recovery of IT systems and dependent business processes. Such failure may lead to severe impacts in health and human safety, statutory and regulatory compliance, financial cost as well as significant public image impact.

B. A citywide Business Impact Analysis (BIA) has not been performed. A BIA identifies each business process, the effects of interruption over varying periods of time and the resources necessary to maintain and operate the process. Lack of understanding of the business impact may lead to insufficient planning and resource allocation for Business Continuity/Disaster Recovery. Criticality, RTOs, and RPOs as well as process capacity requirements for business functions, applications, and systems may not be properly identified.

C. System or organizational BCP do not exist. With the exception of the Controller's Office, BCP were not available or did not exist. Lack of a robust and tested BCP can prevent or delay the recovery of critical business processes in the event of a disaster. The BCP should be the keystone document for recovery and contain references to all necessary procedures and resource information that may be needed to effect a recovery. Each business process should have a well-defined and detailed recovery plan that addresses a range of recovery scenarios and to reliably allow recovery within established RTOs and RPOs by personnel who may not be familiar with the business process or systems.

D. Current and adequate recovery documentation was not available or did not exist. Lack of current and adequate recovery documentation, including procedures and resources, may prevent responsible staff from having information or resources necessary to recover from a business interruption. If detailed recovery procedures are not available, recovery and restoration actions may not be executed effectively or within the required RTO, RPO, or Recovery Capability Objective (RCO).

E. No citywide business continuity training program exists. Business continuity training should be provided to all staff at the level commensurate with their responsibility. Insufficient training can lead to inadequate knowledge of BCM procedures which could prevent or delay recovery of critical processes and the resources may not be able to fulfil their responsibilities appropriately.

While the City has effectively identified the critical applications, this was not based on any quantifiable or verifiable standard or analysis, but rather on undocumented knowledge of individuals. This lack of a framework may result in fragmented, inconsistent, inefficient and ineffective business continuity efforts that lead to inability to recover from a disaster within appropriate recovery requirements and service levels.

Recommendations

City policymakers should:

1.1 Develop a citywide BCM program that aligns with an industry BCM program framework such as Disaster Recovery Institute International (DRII) or International Standards Organization (ISO) ISO22301. *Recommended activities for a citywide BCM are detailed in Appendix II*. To ensure the BCM program is effectively implemented, policymakers should:

a) Designate a resource with citywide scope, such as the Emergency Management Department, to be responsible for establishing, implementing, and maintaining the BCM program.

b) Establish a Steering Committee with oversight of the program.

c) Document and implement program policies, procedures, and work plan schedules for developing BC plans, exercises, training, and maintenance of the BCM program.

d) Offer annual training and certification to key City BCP/DRP personnel. Personnel with key role in execution and maintenance of BCM, BCP, DRP, crisis management, and emergency response, should be considered for such training and certification. Consider Disaster Recovery Institute International professional certifications (i.e., Associate Business Continuity Professional or Certified Business Continuity Professional). Also, consider annual attendance to BCP/DRP industry-leading conferences (e.g., Annual Disaster Recovery Journal Conference).

Finding # 2:

A formal citywide recovery strategy has not been developed

A citywide recovery strategy should incorporate all applications and processes critical to City functions and be aligned with the Department of Homeland Security's Federal Continuity Directive. Without a formal citywide recovery strategy, the City may identify multiple, inappropriate recovery strategies that result in overly aggressive and expensive recovery capabilities or capabilities that will not meet the required recovery needs of the business process.

Current recovery plans have been developed at *a platform or application level*, and do not include a citywide strategy that includes core supporting, end-to-end, network, communications, and IT infrastructure for all Departments.

The primary reason for this situation is that there is no citywide business continuity framework with sufficient funding, resources, and authorities to develop and maintain a citywide recovery strategy.

Recommendations

ITA should:

2.1 Continue to focus on its tiered DR solution initiative, but also develop a citywide tiered disaster recovery strategy based upon business impact assessments and risk analyses. This strategy should reflect the City's federated IT model, and be reviewed and revised at least annually.

2.2 Consider incorporating the following elements into its citywide tiered DR initiative:

- **Facilitate a pre-analysis discussion with management regarding "go forward" strategy options with regard to agreed-upon RTOs and RPOs from the BIA and Risk Assessment efforts.**
- **Document procedures on how to map viable process and technology recovery and availability strategies against the requirements, including manual workarounds and recovery metrics mandated by process owners, alternatives, including internal, external, and hybrid solutions, including the implications (pros and cons) of each high-level estimation on the initial implementation costs of the most realistic alternatives, including capital expenditures, revenue loss, ATOD costs, and ongoing maintenance fees.**

Finding #3:

The process used to identify critical Tier 1 systems is relatively informal, and not based on formal risk assessment, and industry leading practices.

Processes and standards for information technology operations should be consistent across the City, including business continuity and disaster recovery processes for identifying and remediating risk to the entity from the full range of event scenarios and required resources. Lack of a single IT governance and operational organization has led to inconsistent processes to define Tier 1 systems and develop and maintain robust and cost-effective business continuity and disaster recovery planning.

The process to identify Tier 1 applications is inconsistent across IT functions within the City and is not based on a formal, defined methodology including business impact assessments. Many IT functions within the City operate independently of ITA and are not governed by citywide standards and governance structure for business continuity.

Recommendations

ITA and Operating Departments should:

3.1 Continue to implement BC and DR features, including disaster recovery plans, in the new IT services system and position it as the authoritative inventory of applications for the City.

3.2 Leverage the new IT services system capabilities to capture DR-specific information (e.g., RTO, RPO, dependencies, etc.) that would be valuable for tracking and maintenance of DRPs.

3.3 Consider expanding the new IT services system capabilities for tracking and maintaining Operating Departments' BCPs.

3.4 Consider using Continuity of Operations Plan (COOP) BIA guidelines, as defined in the National Continuity Policy Implementation Plan and the National Security Presidential Directive 51/Homeland Security Presidential Directive-20.

Finding 4:

Disaster Recovery testing does not adhere to industry practices.

Disaster Recovery testing should include all personnel, events, and scenarios that may be expected in a disaster. This includes both user, facilities, and IT support personnel. Events include the initial recovery at the temporary site, interim moves, and the return to the permanent site. Scenarios include a variety of events such as natural and man-made events that include destruction of the physical processing site, loss of supporting infrastructure including utilities such as water, communications, and electricity, as well as loss of the entire supporting business and IT staff.

Disaster recovery testing did not include users in the complete lifecycle of disaster recovery testing including development of test plans and test cases; nor did testing include the most likely scenarios or the full disaster lifecycle. More specifically:

A. Disaster recovery teams should include all stakeholders, i.e., IT development, IT maintenance and business process users to develop disaster scenarios, recovery processes, test plans, test cases, test data, and test procedures. The IT organization (e.g. ITA or the Departmental IT organization) should validate correct functionality and business users should validate the accurate and complete functionality of the system. *A centralized authority charged with implementing a citywide Business Continuity Management (BCM) program (as recommended in Finding 1) can help ensure participation of all stakeholders in the DR testing process, since the reporting relationships and roles of IT development, IT maintenance, and business process users vary by application and across the City organization.*

   We found that business users are not involved in DR planning or testing, including the development of disaster scenarios and test cases, i.e.

   - Users do not have input into disaster scenarios.
   - Users do not validate the recovered systems’ ability to execute business processes correctly and completely.

B. In case of a major disaster affecting the City, transportation facilities such as air, rail, and highway may not be available to transport recovery material or personnel to recovery or substitute business or IT recovery sites, which may delay or prevent recovery of the business process or supporting applications.

   We noted that current test scenarios do not include loss of associated infrastructure, key personnel or transportation facilities. In the event of a major regional or nationwide event, supporting infrastructure such as telecommunications or key recovery personnel may not be available to effect recovery and efforts may have to rely on substitute personnel. In order for substitute personnel to effect recovery, detailed procedures and resources must be available.

C. The entire lifecycle of a disaster includes at least two transfers: to the recovery site at the time of the disaster, and the return to the permanent production site at the completion of disaster repair and remediation. Additionally, non-proprietary disaster recovery sites typically are intended for short-term use and use is not guaranteed, since they are on a "first-come-first-serve" basis. To ensure continued availability while the effects of the disaster are remediated, systems must move to a long term interim recovery site, prior to returning to the permanent processing site.

   We noted that current tests only evaluate the recovery of the application at the disaster recovery site and do not include transfer from the initial recovery site to long term processing sites and then transfer back to a permanent processing site.

The primary reason for these conditions is because the various groups and personnel responsible lack disaster recovery expertise.

Recommendation

ITA and Operating Departments should:

4.1 Ensure that all members of disaster recovery teams participate in the disaster recovery testing lifecycle, including the development of disaster scenarios, formal test plans, and test cases. These tests cases must validate the complete lifecycle of a disaster from declaration to restoral of normal processing, with success and fail criteria that validate:

- **RTO**
- **RPO**

- **RCO[7]**
- **System functionality**
- **Recovery by substitute personnel**
- **Transition from initial recovery site to interim site**
- **Restoration of normal processing from recovery site(s)**

When designing/developing disaster scenarios consider incorporating results of the Risk Assessment and Business Impact Analysis noted in Recommendation 1.1 (i.e., risks determined as high, risks with no mitigating controls, risks with the greatest impact on life/safety, revenue, and brand/reputation). Also, at the minimum, the following settings should be considered when designing scenarios:

- **IT not available**
- **Key building/facilities not available**
- **No personnel available**
- **No key vendor(s) available**
- **A combination of aforementioned settings is not available**.

Finding #5:

Supporting infrastructure components for Tier 1 systems have not been identified as critical

Key infrastructure components should be highly resilient, fully redundant, and fail-safe, typically with no allowable downtime. Each component should also have its alternate located in a geographically dispersed facility with no common risk factors such as common geography, utility reliance or other site-related risks. In the event of destruction or substantial damage to the facilities, housing key infrastructure components, City systems, other government entities, and the citizens of Los Angeles would not be able to conduct normal business. Emergency services such as Police and Fire would have to rely on backup communications system, which may have limited capacity during a citywide disaster.

Our audit found that supporting infrastructure for applications has not been identified as "critical". Critical systems rely on supporting infrastructure, which must have the same availability as the application. Infrastructure may include items such as servers, network, firewalls, and physical facilities.

The primary reason for the lack of infrastructure resilience has been the prohibitive cost of developing, implementing and maintaining a strongly resilient infrastructure. ITA's current initiative (i.e., Tiered DR System Approach), which includes implementation of hot site redundancy at a remote data center location, promotion of cloud hosting, and offsite data backup, will address this finding.

Recommendations

ITA and other citywide IT organizations should:

5.1 Continue on the path to ensure core infrastructure components are redundant with automated failover and load balancing, so that there is no interruption and only minimal degradation of service in the event of a disaster.

5.2 Develop and document plans and procedures to validate redundancy and resiliency of the components for all identified disaster scenarios.

[7] Recovery Capability Objective (RCO) – The level of processing capacity needed at time of recovery.

Finding #6:

The City's Mainframe-based Tier 1 systems cannot be recovered in the required RTO in a disaster.

The supporting infrastructure for a business process must be recovered in time to meet the business' identified RTO, with necessary data (RPO) and processing capacity (RCO).

The City's mainframe-based applications currently cannot be recovered to meet the identified RTO of eight (8) hours due to the time necessary to transport tapes to the recovery center and to execute recovery. As a result of the failure to meet the established RTO, business processes may also fail.

The current recovery time is approximately 36 hours, plus the time necessary to declare the disaster, recover the tapes, deliver them to the recovery center and prepare them for the recovery. This is estimated to add an additional 12-24 hours to the recovery. In the event of loss of air transport, the 12-24 hour time will extend an additional two to four days.

The primary reason for the lack of mainframe recoverability to meet required RTOs is the prohibitive cost of implementing additional infrastructure for a limited number of applications, which various parties may be considering replacing.

Recommendations

ITA and Operating Departments should consider the following for mainframe supported applications:

6.1 Develop manual interim processes for the period between the continuity event and recovery of the mainframe at the disaster recovery site.

6.2 Evaluate cost, implementation time and expected mainframe life to consider implementing a recovery mainframe at the current recovery site with associated data replication capability to reduce recovery time to meet required RTO. Alternatively, evaluate feasibility of an accelerated program to replace existing applications with more economical systems that have recovery capability designed to meet RTO, RPO, and system capacity requirements.

Finding #7:

A component of the LAPD Dispatch System cannot be tested for failover.

All components of a system should be tested to validate that they can be recovered in the required time (RTO) and to the required state (RPO and RCO). Inability to test recovery procedures increases the risk that planned recovery procedures may not work at the time of a disaster.

The aforementioned component of LAPD Dispatch System cannot be tested for failover due to risk to 911 callers. Because of the architecture of this component, the disaster failover process cannot be completely tested due to risk of lost 911 calls during the failover process.

Because of the inability to test the critical LAPD Dispatch System component, both LAPD and LAFD Dispatch System may fail in a disaster, due to untested procedures to activate the DR version, affecting both Police and Fire Department 911 callers.

As a mitigating measure the Police Department has developed and utilized manual processes for use during maintenance and disasters and for the period during conversion from the production system to the disaster recovery system Computer Aided Dispatch component. The LAPD Dispatch System component is currently scheduled to be replaced in 2017 with a fully redundant and load balanced component. All other components of the LAPD Dispatch System are fully redundant and load-balanced, and are regularly tested between the City's dispatch centers.

Recommendations

The Police Department should:

7.1 **Apply sufficient resources and oversight for the replacement of the current** LAPD Dispatch System component **to ensure the successful and timely completion of the migration to the new version.**

7.2 **When replacement is completed, the entire** LAPD Dispatch System**, including** LAPD Dispatch System component**, should be regularly tested for successful failover. In addition, recovery testing scenarios should include staff with the requisite skills, but no** LAPD Dispatch System**-specific experience to execute the recovery.**

Finding #8:

Incomplete Recovery Site Access Mechanisms

Recovered systems must be accessible to users as transparently as possible to reduce the risk to business processes. The recovered systems must be accessible without modifications to individual's workstations or procedures, or modifications to many network components.

Disaster recovery site access and the authentication mechanism, such as Active Directory, are not currently available at the recovery site. Specifically, this means that users must use different login credentials and processes at the recovery site from what is established for the current system. ITA management elected to activate the systems at the current site prior to the implementation of the remote access and authentication capabilities as a cost-saving measure.

The interim access mechanisms require some reconfiguration of the user's network infrastructure. Users and system administrators should be able to access recovery-site systems seamlessly in order to execute standard business processing within established RTO, RPO, and system capacity requirements.

With the interim recovery mechanism, users may not be able to access the systems at the recovery site or may experience delays, thereby preventing or delaying business process recovery.

The primary reason for the lack of current access mechanisms is due to the need to implement a current version of the financial management system before the recovery site was fully implemented. Costs related to purchasing and implementing an interim recovery capability for the short period prior to completion of the recovery site was deemed excessive.

Recommendations

ITA should:

8.1 **Expedite implementation of the permanent authentication and authorization mechanisms for all systems at the disaster recovery facility, with testing and validation of user access mechanisms at the interim recovery site performed at the first opportunity.**

Glossary

Business continuity – Business continuity describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster. Business Continuity Planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.

Business Impact Analysis (BIA) – A business impact analysis is performed to determine the impacts associated with disruptions to specific functions or assets in an organization – these include operating impact, financial impact, and legal or regulatory impact. For example, if billing, receivable, and collections business functions are crippled by inaccessibility of information, cash flow to the business will suffer. Additional risks are that lost customers will never return, the business' credit rating may suffer, and significant costs may be incurred for hiring temporary help. Lost revenues, additional costs to recover, fines and penalties, overtime, application and hardware, lost goodwill, and delayed collection of funds could be the business impact of a disaster.

Continuity of Operations Plan (COOP) – A government equivalent of BCP. Primary focus of COOP is the effort to ensure the continued performance of critical business and government functions during a wide range of potential emergencies. The benefits of COOP planning include the ability to: anticipate events and necessary response actions, improve performance through the identification of agency essential functions that must be supported in an emergency, and improve communication to support essential functions throughout the agency.

Risk analysis – A risk analysis identifies important functions and assets that are critical to an organization's operations, then subsequently establishes the probability of a disruption to those functions and assets. Once the risk is established, objectives and strategies to eliminate avoidable risks and minimize impacts of unavoidable risks can be set. A list of critical business functions and assets should first be compiled and prioritized. Following this, determine the probability of specific threats to business functions and assets. For example, a certain type of failure may occur once in 10 years. From a risk analysis, a set objectives and strategies to prevent, mitigate, and recover from disruptive threats should be developed.

Disaster Recovery Plan (DRP) – The DRP is an IT-focused plan designed to restore operability of the target systems, applications, or computer facility at an alternate site after an emergency. A DRP addresses major site disruptions that require site relocation. The DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Typically, Disaster Recovery Planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.

Bare metal recovery – A bare metal recovery describes the process of restoring a complete system, including system and boot partitions, system settings, applications, and data to their original state at some point prior to a disaster.

Recovery Time Objective (RTO) – The recovery time objective is the time needed to recover from a disaster or, saying it another way, how long you can afford to be without your systems.

Recovery Point Objective (RPO) – Recovery point objective describes the age of the data desired for the ability to restore in the event of a disaster. For example, if the RPO is six hours, systems should be restored back to the state they were in, as of no longer than six hours ago. To achieve this, making backups or other data copies is needed at least every six hours. Any data created or modified inside the recovery point objective will be either lost or must be recreated during a recovery. If the RPO is that no data is lost, synchronous remote copy solutions are the only choice.

Appendices

Appendix I – Audit Action Plan

Appendix II – Recommended Activities for a Citywide BCM Program

Appendix III – Departments’ Formal Response and Action Plan

Appendix I - Audit Action Plan

Finding No.	Page	Finding Description	Recommendation	Page	Entity Responsible for Implementation	Priority
1	12	A formal Business Continuity framework has not been implemented in accordance with leading practices.	City policymakers should: 1.1 Develop a citywide BCM program that aligns with an industry BCM program framework such as Disaster Recovery Institute International (DRII) or International Standards Organization (ISO) ISO22301. Key BCM components that should be considered are: • Designating a resource with citywide scope, such as the Emergency Management Department, to be responsible for establishing, implementing, and maintaining the BCM program. • Establish a Steering Committee with oversight of the program. • Document and implement program policies, procedures, and work plan schedules for developing BC plans, exercises, training, and maintenance of the BCM program. • Offer annual training and certification to key City BCP/DRP personnel. Personnel with key role in execution and maintenance of BCM, BCP, DRP, crisis management, and emergency response, should be considered for such training and certification. Consider Disaster Recovery Institute International professional certifications (i.e., Associate Business Continuity Professional or Certified Business Continuity Professional). Also, consider annual attendance to BCP/DRP industry-leading	13	EMD with the support of City Officials	2

Finding No.	Page	Finding Description	Recommendation	Page	Entity Responsible for Implementation	Priority
			conferences (e.g., Annual Disaster Recovery Journal Conference).			
2	13	A formal citywide recovery strategy has not been developed.	ITA should: 2.1 Continue to focus on its tiered DR solution initiative, but also develop a citywide tiered disaster recovery strategy based upon business impact assessments and risk analyses. This strategy should reflect the City's federated IT model, and be reviewed and revised at least annually. 2.2 Consider incorporating the following elements into its citywide tiered DR initiative: • Facilitate a pre-analysis discussion with management regarding "go forward" strategy options with regard to agreed-upon RTOs and RPOs from the BIA and Risk Assessment efforts. • Document procedures on how to map viable process and technology recovery and availability strategies against the requirements, including manual workarounds and recovery metrics mandated by process owners, alternatives, including internal, external, and hybrid solutions, including the implications (pros and cons) of each high-level estimation on the initial implementation costs of the most realistic alternatives, including capital expenditures, revenue loss, ATOD costs, and ongoing maintenance fees.	14	EMD with the support of City Officials	2

Finding No.	Page	Finding Description	Recommendation	Page	Entity Responsible for Implementation	Priority
3	14	Process to identify critical Tier 1 applications is relatively informal, and not based on formal risk assessment, and industry leading practices.	ITA and Operating Departments should: 3.1 Continue to implement BC and DR features, including disaster recovery plans, in the new IT services system and position it as the authoritative inventory of applications for the City. 3.2 Leverage capabilities to capture DR-specific information (e.g., RTO, RPO, dependencies, etc.) that would be valuable for tracking and maintenance of DRPs. 3.3 Consider expanding capabilities for tracking and maintaining Operating Department BCPs. 3.4 Consider using Continuity of Operations Plan (COOP) BIA guidelines, as defined in the National Continuity Policy Implementation Plan and the National Security Presidential Directive 51/Homeland Security Presidential Directive-20.	14	ITA and Operating Department IT organizations	2
4	15	Disaster Recover Testing does not adhere to industry practices.	ITA and Operating Departments should: 4.1 Ensure that all members of disaster recovery teams participate in the disaster recovery testing lifecycle, including the development of disaster scenarios, formal test plans, and test cases. These tests cases must validate the complete lifecycle of a disaster from declaration to restoral of normal processing, with success and fail criteria that validate: • RTO • RPO • RCO	16	ITA and Operating Department IT organizations.	1

Finding No.	Page	Finding Description	Recommendation	Page	Entity Responsible for Implementation	Priority
			• System functionality • Recovery by substitute personnel • Transition from initial recovery site to interim site • Restoration of normal processing from recovery site(s) When designing/developing disaster scenarios consider incorporating results of the Risk Assessment and Business Impact Analysis noted in Recommendation 1.1 (i.e., risks determined as high, risks with no mitigating controls, risks with the greatest impact on life/safety, revenue, and brand/reputation). Also, at the minimum, the following settings should be considered when designing scenarios: • IT not available • Key building/facilities not available • No personnel available • No key vendor(s) available • A combination of aforementioned settings is not available			
5	16	Tier 1 applications have been identified, the relevant infrastructure especially the network has not been identified as critical leading to single point of failure.	ITA and other citywide IT organizations should: 5.1 Continue the path to ensure core infrastructure components are redundant with automated failover and load balancing so that there is no interruption and only minimal degradation of service in the event of a disaster. 5.2 Develop and document plans and procedures to validate redundancy and resiliency of the components for all identified disaster scenarios.	17	ITA	1

Finding No.	Page	Finding Description	Recommendation	Page	Entity Responsible for Implementation	Priority
6	17	Current disaster recovery plans for Mainframe based Tier 1 applications do not allow for applications to be available in required timeframe in an event of disaster.	ITA and Operating Departments should: 6.1 Develop manual interim processes for the period between the continuity event and recovery of the mainframe at the disaster recovery site. 6.2 Evaluate cost, implementation time and expected mainframe life to consider implementing a recovery mainframe at the current recovery site with associated data replication capability to reduce recovery time to meet required RTO. Alternatively, evaluate feasibility of an accelerated program to replace existing applications with more economical systems that have recovery capability designed to meet RTO, RPO, and system capacity requirements.	17	ITA and supported Operating Departments.	1
7	18	Due to current design and set up of LAPD Dispatch System (i.e., critical component), it cannot be tested for failover.	The Police Department should: 7.1 Apply sufficient resources and oversight for the replacement of the current component of the LAPD Dispatch System to ensure the successful and timely completion of the migration to the new version. 7.2 When replacement is completed, the entire LAPD Dispatch System, including relevant component, should be regularly tested for successful failover. In addition, recovery testing scenarios should include staff with the requisite skills, but no LAPD Dispatch System-specific experience to execute the recovery.	18	Police Department	1

Finding No.	Page	Finding Description	Recommendation	Page	Entity Responsible for Implementation	Priority
8	18	Incomplete Recovery Site Access Mechanisms	ITA should: 8.1 Expedite implementation of the permanent authentication and authorization mechanisms for all systems at the disaster recovery facility, with testing and validation of user access mechanisms at the interim recovery site performed at the first opportunity.	19	ITA	2

Priority definition:

Priority 1: To be initiated immediately with all required resources to be made available on an as needed basis.

Priority 2: To be initiated upon completion of any priority 1 tasks where there is resource contention from priority 1 projects or any critical projects for non-DR, but no later than 90 days

Appendix II - Recommended Activities for a Citywide Business Continuity Management Program

According to leading practices, activities of a citywide BCM program should include the following:

- Business Impact Assessment of all City Departments and their processes. Once the initial business impact assessment is completed, annual reviews and updates should be completed and validated by the BCM organization.
- A citywide BIA should be performed on an annual basis with resulting RTOs and RPOs, and system capacity requirements should be validated with the business process owner, as well as mitigating controls and capabilities that may extend the RTO. BIA effort should at least include the following elements:
  - Defined business impact categories (financial, reputational, regulatory, health and human safety, etc.) and the impact criteria (minor, moderate, or major impact) and criticality classification of business processes due to an outage or service interruption.
  - Critical dependencies and availability needs: people, property, technology assets, vendor/suppliers, data, and vital records.
  - Critical business processes and cross-entity interdependencies.
  - Potential impacts of system or process outages to key functions.
  - RTO for critical functions and the supporting critical IT systems, networks, and minimal recovery requirements for the individual function.
  - RPO for critical information systems and minimum recovery configurations.
  - Recovery Capability Objective (RCO) for critical information systems.
  - Recovery priorities as determined by RTOs and RPOs.
  - Defined procedures and reporting requirements to perform gap analysis between dependency recovery capabilities and business recovery objectives.
- Establish minimum recovery requirements (e.g. staffing, office space, telecommunications, supplies, etc.) for “At Time of Disaster” (ATOD) operations.
- Perform a Business Continuity Risk Assessment of all City Departments, their processes and supporting infrastructure. While this normally only encompasses IT systems, alternatives to IT processing may be included in order to identify and validate possible recovery strategies. This risk assessment includes both internal and external sources. These risk sources include, but are not limited to:
  - Natural technological or man-made;
  - Industry/business model;
  - Accidental versus intentional;
  - Controllable exposures and risks versus those beyond the entity's control;
  - Events with prior warnings versus those with no prior warnings.
- Implementation and maintenance of business continuity and disaster recovery training program.
  - Raise, enhance and maintain awareness through an ongoing BCM education and information program for all employees and establishing a process for evaluating the effectiveness of the BCM awareness delivery.
  - Communicate to all employees the importance of:
    - Meeting business continuity management objectives
    - Conforming to the business continuity policy
    - Continual improvement
  - Ensure that all employees are aware of their role in the achievement of the organization’s business continuity objectives.

- Development and regular maintenance of robust and tested Departmental Business Continuity/Continuity of Operations plans and corresponding recovery strategies. These plans should accurately reflect required RTOs, RPOs and RCOs in compliance with the Department of Homeland Security's Federal Continuity Directive I and DRII Professional Practices for Business Continuity Practitioners. After each exercise or test, annually review and revise the plans to ensure that they accurately reflect the current business processes, dependencies, resources and recovery procedures. Ensure that plans are sufficiently detailed to enable recovery by personnel who may not normally execute either business or technical tasks.

Appendix III – Department’s Formal Response and Action Plan

FORM GEN. 160 (Rev. 6-80)

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE

Date: August 4, 2017 REF: FAS-128-17-**Revised**

To: Alfred Rodas, Director of Auditing
Office of the City Controller

From: Ted Ross, General Manager
Information Technology Agency

Subject: **INFORMATION TECHNOLOGY AGENCY'S ACTION PLAN FOR THE AUDIT OF THE INFORMATION TECHNOLOGY AGENCY'S INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN**

The Information Technology Agency (ITA) has reviewed the findings in the above audit and prepared the attached Action Plan for the findings for which the Agency is responsible. As noted in the exit conference and discussed with your Office, the Emergency Management Department (EMD) is the entity responsible for designing and developing disaster recovery scenarios, as well as ensuring participation of all relevant parties in these scenarios, and as such, is responsible for addressing finding 4.1. ITA acknowledges the role the department must play and will fully support EMD with this effort.

Should you have any questions, please contact Laura Ito at (213) 978-3322 or via email at laura.ito@lacity.org.

Attachments

ec: Joyce Edson, ITA
Sung Kim, ITA
Paul Alberga, Controller's Office

Finding Description	Section	Recommendation	Action Plan
A formal citywide recovery strategy has not been developed.	2.1	Continue to focus on its tiered DR solution initiative, but also develop a citywide tiered disaster recovery strategy based upon business impact assessments and risk analyses. This strategy should reflect the City's federated IT model, and be reviewed and revised at least annually.	Will leverage "best practice" tiered DR specifics, and apply to City's ServiceNow (SNOW) system. The ability to track will be applied to each app/system as an "asset" within the SNOW inventory, and the SNOW inventory is the Citywide (Federated) Application Portfolio. There will be an annual effort to have dept's review and update, and will tie to ITSM to ensure updates be made as work is done.
	2.2	□ Facilitate a pre-analysis discussion with management regarding “go forward” strategy options with regard to agreed-upon RTOs and RPOs from the BIA and Risk Assessment efforts.	Using the ITPC, will initiate discussions with departments to have them determine and document the recovery time and point of recovery objectives, along with the business impact analysis for all their systems. Rate and rank/tier their apps/systems, and document known risks, as a part of additional enhancements in this area in SNOW.
		□ Document procedures on how to map viable process and technology recovery and availability strategies against the requirements, including manual workarounds and recovery metrics mandated by process owners, alternatives, including internal, external, and hybrid solutions, including the implications (pros and cons) of each high-level estimation on the initial implementation costs of the most realistic alternatives, including capital expenditures, revenue loss, ATOD costs, and ongoing maintenance fees.	Utilizing expanded tiering data from the SNOW App Portfolio and discovery data from infrastructure tools, will be used to determine current risks and diagram recovery and loss mitigation strategies. ITA will work with departments to develop shared recovery alternatives - communication, work site co-location, etc. to mitigate costs.
Process to identify critical Tier 1 applications is relatively informal, and not based on formal risk assessment, and industry leading practices.	3.1	Continue to implement BC and DR features, including disaster recovery plans, in the new IT services system (ServiceNow) and position it as the authoritative inventory of applications for the City.	Efforts are continuing and expanding by centralizing and enhancing Citywide Application Portfolio info to be a current source of BC and DR plans and info, for ITA and departments
	3.2	Leverage ServiceNow capabilities to capture DR-specific information (e.g., RTO, RPO, dependencies, etc.) that would be valuable for tracking and maintenance of DRPs.	Continue to support EMD to encourage departments to better utilize SNOW's knowledge base and app/sys asset inventory as a resource for documenting and maintaining their disaster recovery plans.
	3.3	Consider expanding ServiceNow capabilities for tracking and maintaining Operating Departments’ BCPs	Continue to support EMD to encourage departments to better utilize SNOW's knowledge base and app/sys asset inventory as a resource for documenting and maintaining their disaster recovery plans.

Finding Description	Section	Recommendation	Action Plan
	3.4	Consider using Continuity of Operations Plan (COOP) BIA guidelines, as defined in the National Continuity Policy Implementation Plan and the National Security Presidential Directive 51/Homeland Security Presidential Directive-20.	ITA will review and work with EMD to incorporate into the City's existing COOP guidelines provided by EMD for annual updates by departments.
Disaster Recover Testing does not adhere to industry practices.	4.1	Ensure that all members of disaster recovery teams participate in the disaster recovery testing lifecycle, including the development of disaster scenarios, formal test plans, and test cases. These tests cases must validate the complete lifecycle of a disaster from declaration to restoral of normal processing, with success and fail criteria that validate: *RTO *RPO *RCO^7 *System functionality *Recovery by substitute personnel *Transition from intial recovery site to interim site *Restoration of normal processing from recovery site(s)	ITA acknowledges that developing and planning an effective disaster scenario would necessarily involve ITA and the buITA acknowledges that developing and planning an effective disaster scenario would necessarily involve ITA and the business owner departments that the systems support. The department will continue to participate and contribute technical expertise to developing a disaster exercise that appropriately tests the infrastructure and system functionality restoration effort. The Operating Departments (business owners) to which this recommendation is also directed must similarly fully participate in the business continuity planning and testing. However, the overall Recommendation 4.1 to "Ensure that all members of disaster recovery teams participate in the disaster recovery testing lifecycle, including the development of disaster scenarios, formal test plans, and test cases", can only be directed to Emergency Management Department (EMD). The Administrative Code specifically defines EMD's duties to include: "Prepare Citywide emergency preparedness plans with the assistance of all other City departments, officers and agencies and assist other departments and agencies desiring to initiate or develop emergency preparedness activities."
		When designing/developing disaster scenarios consider incorporating results of the Risk Assessment and Business Impact Analysis noted in Recommendation 1.1 (i.e., risks determined as high, risks with no mitigating controls, risks with the greatest impact on life/safety, revenue, and brand/reputation). Also, at the minimum, the following settings should be considered when designing scenarios: *IT not available *Key building/facilities not available *No personnel available *No key vendor(s) available *A combination of aforemention settings is not available	See above response.

Finding Description	Section	Recommendation	Action Plan
Tier 1 applications have been identified, the relevant infrastructure especially the network has not been identified as critical leading to single point of failure.	5.1	Continue on the path to ensure core infrastructure components are redundant with automated failover and load balancing, so that there is no interruption and only minimal degradation of service in the event of a disaster.	ITA will continue to explore options via various service vendors in order to provide a feasible solution to provide redundancy and automated failover. Currently, it is not financially feasible for ITA to invest in infrastructure improvement due to the following: 1). solution may only be short term, 2). high CAPex (Capital Expenditure). For these reasons, ITA recommends and will investigate service providers who will provide suitable capabilities via OPex (Operation Expenditure).
Current disaster recovery plans for Mainframe based Tier 1 applications do not allow for applications to be available in required timeframe in an event of disaster.	6.1	Develop manual interim processes for the period between the continuity event and recovery of the mainframe at the disaster recovery site.	ITA will continue to explore options via various service vendors in order to provide a feasible solution to the recommendation as stated. Currently, it is not financially feasible for ITA to invest in infrastructure improvement due to the following: 1). solution may only be short term, 2). high CAPex (Capital Expenditure). For these reasons, ITA recommends and will investigate service providers who will provide suitable capabilities via OPex (Operation Expenditure).
	6.2	Evaluate cost, implementation time and expected mainframe life to consider implementing a recovery mainframe at the current recovery site with associated data replication capability to reduce recovery time to meet required RTO. Alternatively, evaluate feasibility of an accelerated program to replace existing applications with more economical systems that have recovery capability designed to meet RTO, RPO, and system capacity requirements.	ITA has begun to explore options via various service vendors, to remotely host a production mainframe with the added capability of data replication to a redundant alternate site to meet the required RPO and RTO. ITA's target is to be able to achieve an RPO of 8 hours or less and an RTO of less than 36 hours.
Incomplete Recovery Site Access Mechanisms	8.1	Expedite implementation of the permanent authentication and authorization mechanisms for all systems at the disaster recovery facility, with testing and validation of user access mechanisms at the interim recovery site performed at the first opportunity.	ITA is currently investigating the potential usage of VDI (Virtual Desktop Infrastructure) through a cloud vendor to faciliate access to financial applications residing in SwithNap, Las Vegas. If ITA is able to establish contract with a suitable MF service provider, the redundant internet link at Van Nuys can be leveraged to enable, authenticate, and authorize access to remote recovery sites.

FORM GEN. 160 (Rev. 6-80)

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE

CITY of LOS ANGELES
EMERGENCY
MANAGEMENT
DEPARTMENT
"IN OMNIA PARATUS"

Date: July 25, 2017

To: Alfred Rodas, Director of Auditing
Office of the Controller

From: Aram Sahakian, General Manager
Emergency Management Department

Subject: INFORMATION TECHNOLOGY DISASTER RECOVERY AUDIT PROPOSED RESPONSE LANGUAGE

After reviewing the report entitled, "Audit of the Information Technology Agency's (ITA) Information Technology Disaster Recovery Plan", the Emergency Management Department (EMD) agrees with the intent of recommendation #1 to lead the effort to develop a Citywide Business Continuity Management Framework and recommendation #2 to develop a formal Citywide Recovery Strategy (technology recovery).

However, our ability to implement these actions would be dependent on City officials providing EMD with the necessary sponsorship and authority as well as adequate resources. These resources would include one (1) full time Senior Project Coordinator position for EMD and one (1) full time Senior Systems Analyst I position for ITA. These positions would oversee and coordinate the required work. The existing staff resources for both EMD and ITA are inadequate to take on this additional program.

Additionally, with regard to Recommendation 4.1 that was originally addressed to ITA, we are in agreement as indicated by ITA in its response that statutory responsibility for citywide disaster recovery planning and coordination lies with EMD. We acknowledge that this would encompass development of disaster scenarios, formal test plans, and test cases related to Tier I systems. However, it should be recognized that under the City's current organizational structure, City Departments are highly dependent on ITA for addressing the operational support and maintenance needs of Tier I systems.

Accordingly, EMD supports the intent of Recommendation 4.1, but would like to point out that we may need additional resources to fully discharge this responsibility. EMD will also require the cooperation of all City Departments, including ITA, to fully implement this recommendation.

Having said this, to address the several disaster preparedness and testing gaps related to Tier I systems discussed within the report, we plan to work with ITA and other City Departments to assess potential resource needs, and to evaluate strategic options in achieving leading disaster recovery standards. This may include the retention of outside expertise and/or the formation of a cross-sectional City working group that will be led by EMD for the purpose of identifying the most effective and efficient manner to collaborate on addressing/implementing the actions called for in this recommendation.

LOS ANGELES POLICE DEPARTMENT

CHARLIE BECK
Chief of Police

P. O. Box 30158
Los Angeles, Calif. 90030
Telephone: (213) 486-0150
TDD: (877) 275-5273
Ref#: 1.17

ERIC GARCETTI
Mayor

May 26, 2017

Mr. Alfred Rodas
Director of Auditing
Office of the Controller
200 North Main Street, Suite 300
Los Angeles, California 90012

Dear Mr. Rodas:

The Los Angeles Police Department has reviewed the report entitled, "Audit of the Information Technology Agency's Information Technology Disaster Recovery Plan." Please see the enclosed matrix where we have addressed the actions planned or action taken to implement recommendation 7.1 and 7.2. We hope this has sufficiently addressed your request.

If you have any questions, please contact Commander Regina Scott at (213) 486-0770.

Very truly yours,

CHARLIE BECK
Chief of Police

Enclosure

Recommendation	Actions Planned or Action Taken
The Police Department should: 7.1 Apply sufficient resources and oversight for the replacement of the current LAPD Dispatch System component to ensure the successful and timely completion of the migration to the new version.	In March 2016, the Department began the Next Generation Premier One upgrade project. A consultant was engaged contractually to perform the upgrade and replacement of the current LAPD Dispatch Component and mobile platform with an industry leading solution. Sufficient resources and oversight are committed from our consultant and LAPD.
7.2 When replacement is completed, the entire LAPD Dispatch System, including LAPD Dispatch System component, should be regularly tested for successful failover. In addition, recovery testing scenarios should include staff with the requisite skills, but no LAPD Dispatch System-specific experience to execute the recovery.	The police communications systems encompass many technologies such as radio communications, fiber-optics, telephony, dispatch, mobile platforms, AVL, GIS, etc. The planned actions will be to formally establish a service level agreement with the Information Technology Agency to document levels of responsibilities and expectations regarding system currency, support levels, regular testing, and the availability of recovery testing scenarios related to the police system communications infrastructure. LAPD will develop the recommended testing plan and document recovery testing scenarios related to police communications system servers and applications.