BACK

July 2024

City of Palo Alto

Office of City Auditor

Technology Applications Disaster Preparedness Assessment

Contents

Executive Summary

Purpose of the Audit

Baker Tilly US, LLP (Baker Tilly or BT), in its capacity serving as the Office of the City Auditor (OCA) for the City of Palo Alto (the City), conducted an audit of the disaster recovery preparedness based on the approved Task Order 4.19. The objectives of this review were to:

1) Assess the current disaster recovery plan for high priority applications and supporting infrastructure to identify the adequacy of documentation and identify additional documentation requirements.
2) Assess the current disaster recovery capabilities.
3) Develop recommendations to remediate identified capability gaps and to update disaster recovery documentation.

Report Highlights

Finding 1: (Page 8)

Lack of Business Impact Analysis (BIA)

The City has not established a BIA to define critical assets across the City.

Key Recommendations

The City should continue with the planned BIA efforts to gain an understanding of criticalities and RTOs of the assets within the City.

Finding 2: (Page 8)

Lack of Formalized Maintenance Requirements

The City does not have formalized maintenance requirements for resiliency mechanisms.

Key Recommendations

The City should formalize maintenance requirements for resiliency mechanisms through policies and procedures.

Finding 3: (Page 9)

Informal and Inconsistent Backups

The City does not have a formalized Backup Policy to outline backup requirements.

The city does not have a formal process for monitoring and remediating backup failures.

Key Recommendations

The City should formalize backup requirements for key systems through a Backup Policy.

The City should outline backup failure requirements as part of the Backup Policy.

Finding 4: (Page 9)

Lack of Formalized Restoration Testing

The City does not perform system wide or planned restoration testing.

Key Recommendations

The City should establish a process to test the ability to restore data and systems from backups on a periodic basis.

Finding 5:

Unencrypted Backups for Synology Appliance

(Page 10)

The data stored locally within the Synology backup solution is not encrypted.

Key Recommendations

The City should configure the Synology appliance to be encrypted locally.

Finding 6:

(Page 10)

Lack of Detailed Disaster Recovery Plan and Test

The City does not have a detailed Disaster Recovery Plan or formalized process to test disaster recovery processes.

Key Recommendations

The City should continue efforts to implement a detailed Disaster Recovery Plan that outlines actions to be taken to restore operations and recover data in the event of a disaster. The plan should be tested on an annual basis.

Introduction

Objective

The objectives of this review were to:

1) Assess the current disaster recovery plan for high priority applications and supporting infrastructure to identify the adequacy of documentation and identify additional documentation requirements.
2) Assess the current disaster recovery capabilities.
3) Develop recommendations to remediate identified capability gaps and to update disaster recovery documentation.

Background

Information systems are vulnerable to various interruptions ranging from mild (e.g., short-term power outages, accidental equipment damage, equipment failure) to severe (e.g., vandalism, equipment destruction, natural disasters, virus, attackers). A disaster recovery plan along with resiliency mechanisms and backups will allow the City to prepare for disruptions. Without adequate controls and preparation, the effects can lead to catastrophic financial loss in the form of lost revenue, recovery costs, or impact critical membership services, as well as technological consequences, such as losing integral or sensitive data.

Scope

The scope of this assessment was limited to the disaster recovery of high priority applications and supporting infrastructure that is controlled by the City's Information Technology team.

Methodology

To achieve the audit objective #1, the OCA performed the following procedures:

- Conducted interviews with identified IT personnel and key stakeholders to gain an understanding of the operating environment
- Conducted interviews and gathered supporting documentation to determine what the City deemed as high priority applications
- Gathered and analyzed evidence to determine if the City had adequate documentation of the disaster recovery process.

To achieve the audit objective #2, the OCA performed the following procedures:

- Conducted interviews with identified IT personnel and key stakeholders and performed observations of facilities to determine the current disaster recovery capabilities.
- Gathered and analyzed evidence to determine whether the City had adequate technical controls required to recover from a disaster.

To achieve the audit objective #3, the OCA performed the following procedures:

- Compared current state documentation and capabilities to industry best practices to develop recommendations to strengthen the City's disaster preparedness.

Compliance Statement

This audit activity was conducted from September 2023 to November 2023 in accordance with generally accepted government auditing standards, except for the requirement of an external peer review[1]. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Organizational Strengths

During this audit activity, we observed that the City has the following areas of strength as it relates to disaster preparedness:

- Appropriate resiliency mechanisms to ensure that on-premise solutions would be able to run in the event that there was a power outage.
- A documented Continuity of Operations (COOP) plan that outlines how IT would continue to support the rest of the city in the event of a disaster.
- Backups are configured to run on critical systems and retained for a period of time determined to be appropriate by the business.
- Initial criticality rating and recovery time objectives (RTO)'s have been established for services to guide recovery efforts based on business need.

The Office of the City Auditor greatly appreciates the support of the Information Technology Department in conducting this audit activity.

Thank you!

[1] Government auditing standards require an external peer review at least once every three (3) years. The last peer review of the Palo Alto Office of the City Auditor was conducted in 2017. The Palo Alto City Council approved a contract with Baker Tilly U.S, LLP for internal audit services for October 2020 through June 2022 with an extension through June 2025. City Council appointed Kate Murdock, Audit Manager in Baker Tilly's Risk Advisory practice, as City Auditor in May 2024. As a result of transitions in the Audit Office and peer review delays due to the COVID pandemic, an external peer review is targeted for 2025. It should be noted that Baker Tilly's most recent firmwide peer review was completed in October 2021 with a rating of "Pass". The scope of that peer review includes projects completed under government auditing standards. A report on the next firmwide peer review should be available later in 2024

Detailed Analysis

Disaster Recovery Documentation

BT noted that the City maintains a formalized Continuity of Operations (COOP) plan for the Information Technology Department. Per inspection of this plan, BT noted that the plan outlines the roles and responsibilities of personnel involved, the activation of the COOP, the implementation of the COOP, and details various steps that IT personnel would need to perform in order to continue operations. BT noted that the COOP primarily focused on the continuity of IT functions in the event of a disaster or other incident; but did not outline recovery methods, procedures, or processes. Further, BT noted that the City is in the process of reviewing and updating the COOP to ensure alignment with current practices.

BT noted that the City maintains a formalized Disaster Recovery & Business Continuity Process (DR-BCP) and System Back-Up Procedure document. Per inspection, BT noted that the document outlines the backup methodology for the five critical information technology services which include SAP, GIS, internet services, e-mail services, and network services. BT noted that this document outlines the backup requirements, type of information backed up, and frequency of backup. Additionally, BT obtained and inspected the Summary of Data Backup Services document and noted that it outlined the backup services used for the critical applications; however, the document has not been updated to reflect recent changes in the environment.

In the event of a disaster, the Office of Emergency services, through the Emergency Operations Center activation, would manage communication, including internal and external communications. The Office of the CIO may also have direct communication with constituents where required. For external communication, there is a standard template that is used to communicate these instances.

All City employees are deemed disaster employees and receive training upon hire in order to gain an understanding of their roles and responsibilities as it relates to disasters. Further, the IT department is involved in an annual COOP test through various City activities; however, the IT specific COOP is not formally tested on a regular cadence.

While the City has defined processes for backups and continuity, there is no formalized policy or procedure document that outlines requirements and actions to be taken during a disaster. BT further noted that there are plans in place to further strengthen the disaster recovery plan, including performing an analysis to re-classify critical assets; but this project is currently on hold.

Criticality

BT noted that the City has a defined Asset Classification strategy in which assets are categorized within the following tiers:

- Tier 1: Assets which will have direct impact on public safety and or public's well-being.
- Tier 2: Assets which have indirect impact on public safety and or public's well-being.
- Tier 3: Assets which have data confidentiality, legal, and financial impact.
- Tier 4: Assets which have NO direct/indirect impact on public safety/security and does not host any confidential, legal, and financial data.

BT noted that the following IT supported assets have the below designated criticalities:

IT Supported Assets	Tier
GIS	1
Internet Services Network Services E-Mail Services File Services VoIP Telephone	2
SAP	3

BT further noted that Recovery Time Objectives (RTO) have been defined for the critical functions as 72 to 120 hours.

While criticality and RTO have been established across IT assets, the criticality is not rooted in an organizational wide Business Impact Analysis (BIA) which may result in misaligned recovery efforts due to lack of business input.

Resiliency Capabilities

BT noted that the City has deployed various resiliency capabilities across the IT controlled infrastructure. BT noted that UPS devices are deployed across the city and have enough power to maintain services until the generators are turned on. BT noted that there are two generators that are located in the Civic Center Office building that are used to provide power to the IT networking closets and the rest of the building in the event of a power outage. Additionally, there is a fuel contract to ensure that the generator does not run out of fuel in the event of an extended outage. Further, BT noted that there are redundant fiber internet feeds in place to guard the City from an internet outage. Similarly, there are redundant phone systems in place.

Maintenance and testing for UPS and generators occurs on a defined schedule and alerts are actively monitored by either the IT Operations or Maintenance teams. If there are alerts that require changes to the environment, these changes would follow the established change management process and be documented within the ITSM tool.

The resiliency mechanisms listed above would support solutions and services that are hosted on-premises. For SAP, which is hosted in AWS, the City relies upon the vendor to provide resiliency. BT noted that the City is currently working on establishing a recovery site with AWS or Azure to aid in the recovery of on-prem solutions in a long-term disaster.

Backups

BT noted that backups are in place and managed for the critical applications and services throughout the city. BT noted that there are 3 main backup methods:

1. SAP Backups – BT noted differential backups occur daily and full backups occur weekly, with transaction log backups taken every 15 minutes and are managed and monitored by EPI-use. These backups are stored in AWS and retained for 7 years. BT further noted that in the event of a disaster, the City would share responsibility with EPI-use to perform restoration and recovery efforts.
2. Rubrik – BT noted that Rubrik is used to backup on-prem SQL databases, windows volumes, virtual machines, the GIS system, and servers. Backups are taken on a daily, weekly, and yearly basis and are monitored by the IT Operations team. After 45 days, the data backed up using Rubrik is transferred from the local appliance to Azure and retained for 2 years.
3. Synology – BT noted that Synology is utilized to perform backups of the file services. Backups are taken on a daily basis and stored for 360 days in Azure.

For City managed backups, alerts are sent to the IT Operations team on a daily basis for monitoring purposes. Consecutive backup failures that require a change within the system would be documented within the ITSM tool; however, this process is not consistently followed. Further, backup configuration changes would follow the City's established change management processes.

While file or folder level restores occur during the normal course of business, there is currently not a process in place to do failover testing.

Audit Results

Finding 1: Lack of Business Impact Analysis (BIA)

The City has not yet completed a BIA to define the critical assets across the City. Without knowledge from the various departments within the city, disaster recovery efforts including backup configurations and restorations (including Recovery Time Objectives (RTO)) may not be in alignment with the City's needs due to the lack of a BIA.

Recommendation

The City should continue the planned Business Impact Analysis (BIA) efforts to gain a comprehensive understanding of the assets within the environment, including RTOs and criticality ratings associated with those assets and be used to update RTOs and criticality ratings, where necessary.

Management Response

Responsible Department(s): Information Technology + Business Units

Concurrence: Agree

Target Date: Ongoing

Action Plan:

IT and in collaboration with the City's Office of Emergency Services operations will continue to partner with departments to define critical assets and update the disaster recovery plan and IT security risk register as required. This will be an ongoing activity to address upgraded and newly acquired technology solutions as part of the ongoing emergency operations preparation work

Finding 2: Lack of Formalized Maintenance Requirements

The City does not have formalized maintenance requirements for resiliency mechanisms for solutions and services that are hosted on-premises in the means of policies or procedures. Formalization, supports maintenance and resiliency mechanism testing in alignment with expectations. Further, the roles and responsibilities to perform these actions may not be known to employees in the event of turnover.

Recommendation

The City should establish a formal standard operating procedure (SOP) that outlines the requirements and steps to perform maintenance and testing on resiliency mechanisms in alignment with best practice and vendor recommendations. This SOP should outline the roles and responsibilities, as well as any documentation requirements when actions are taken.

Management Response

Responsible Department(s): Information Technology + Facilities

Concurrence: Agree

Target Date: Q2 CY 2025

Action Plan:

IT has initiated a planned Disaster Recovery and Business Continuity project and will include this recommendation as a deliverable.

Finding 3: Informal and Inconsistent Backups	The City has a defined Disaster Recovery & Business Continuity (DR-BCRP) plan, but it does not outline requirements of backups such as schedule, retention, and storage requirements. This may lead to inaccuracies in configurations or misalignment with business need. Additionally, the City monitors backup failures on an ad-hoc basis but does not have a formal process to action consecutive failed backups. Failed backups may result in a loss of data in the event of a disaster
Recommendation	The City should expand the Disaster Recovery & Business Continuity (DR-BCP), System Back-Up Procedure, and/or establish a Backup Policy to formalize the backup requirements including schedule, retention, and storage requirements for critical business functions. This procedure and/or policy should be updated to align with current business practices and include details on any vendor reliance for backups. Additionally, the procedure and/or policy should outline roles and responsibilities related to recovery and backup. Additionally, this procedure and/or policy should outline monitoring requirements and actions to be taken for failed backups based on the City's determined thresholds. Once established, the procedure and/policy should be reviewed on an annual basis to ensure alignment with business needs. Further, formal tracking of corrective action plans should be documented within the ITSM tool, including the root cause of the failure, responsible part, and the actions taken.
Management Response	**Responsible Department(s):** Information Technology **Concurrence:** Agree **Target Date:** Q2 CY 2025 **Action Plan:** As noted in the assessment, the City does maintain system back-ups for the critical applications and services throughout the city though acknowledges this level of detail is not included in the DR-BCRP plan. IT has initiated a planned Disaster Recovery and Business Continuity project and will ensure current processes are documented formally in the updated plan.
Finding 4: Lack of Formalized Restoration Testing	The City performs ad-hoc single file restorations as part of business-as-usual, but does not perform testing on the ability to restore a system or larger data set from backups. This may lead to inability to restore data in the event of a disaster due to issues with restoration processing or misconfigured backups.
Recommendation	The City should establish a formal process to test the ability to restore from backups on a periodic basis. This process should be expanded to a larger set of data or system, rather than ad-hoc file restores. This process should be formally documented, including roles and responsibilities. Further, the results of the test should be documented with any corrective action plans for failures monitored through resolution.
Management Response	**Responsible Department(s):** Information Technology **Concurrence:** Agree **Target Date:** Q2 CY 2025

Action Plan:

A formal process is not documented, however restores for both single files and bare metal restores are performed as required. IT has had a planned Disaster Recovery and Business Continuity project since 2021. We have initiated the project and ensure this recommendation is a deliverable.

Finding 5: Unencrypted Backups for Synology Appliance

One of the City's backup solutions, Synology, is not configured to be encrypted at the local appliance which may lead to loss of data.

Recommendation

The City should configure Synology to encrypt backup data that is stored on the local appliance.

Management Response

Responsible Department(s): Information Technology

Concurrence: Do not Agree

Target Date: Addressed

Action Plan:

There is a local backup (Snapshot) of the S: Drive that is unencrypted by design in order to facilitate file restoration at the user level and is only accessible to authorized IT administrators. For DR backups the data is encrypted in the cloud and not on the appliance. Cloud backups are used for recovery in the case of data loss.

Finding 6: Lack of Detailed Disaster Recovery Plan and Test

The City maintains a formal IT Continuity of Operations Plan (IT COOP) which outlines roles, responsibilities, communications and plan to continue people operations in the event of a disaster; however, this plan does not detail the actions to be taken to restore and recover infrastructure and data in the event of a disaster. Various department COOP's are tested on an annual basis, however, an IT specific disaster recovery test is not performed.

Recommendation

The City should continue efforts to implement a detailed Disaster Recovery Plan. The established plan should include details on roles, responsibilities, communications, and actions to be taken to restore data and recovery infrastructure and systems in the event of a disaster. The plan should be reviewed and approved by leadership on an annual basis. Additionally, the plan should be tested on an annual basis through tabletop exercises or other testing scenarios.

Management Response

Responsible Department(s): Information Technology

Concurrence: Agree

Target Date: Q2 CY 2025

Action Plan:

IT has initiated a planned Disaster Recovery and Business Continuity project and will ensure current processes are documented formally in the updated plan.