City and County of San Francisco

Committee on Information Technology

Budget and Performance Subcommittee

03/08/24

Agenda

- Call to Order by Chair
- Roll Call
- General Public Comment
- Department Updates and Announcements
- Approval of Meeting Minutes from March 1, 2024 (Action Item)
- FY 2024 - 2025 & FY 2025 - 2026 Budget Presentations
- Review the remaining schedule for Department presentations (March - April)
- Adjournment

Item Number 3

General Public Comment

Discussion

Item Number 4

Department Updates and Announcements

Discussion

Item Number 5

Approval of Minutes from March 1, 2024

Action item

Item Number 6

FY 2024 - 2025 & FY 2025 - 2026 Budget Presentations

Discussion

Presentation Schedule

- Cloud Infrastructure Implementation (10:10AM - 10:30AM)
- Citywide Data Center Certification Project (10:30AM - 10:50AM)
- Cloud Center of Excellence (10:50AM - 11:10AM)
- Increase City Data Center Resiliency (11:10AM - 11:30AM)
- Rubrik Online Backup Archiving System (11:30AM- 11:50AM)

Office of the Controller – Systems Division

Presentation to COIT Budget & Performance Subcommittee

Cloud Infrastructure Implementation

March 8, 2024

Project Overview

Project Overview

- Problem Statement
  - The current infrastructure for the Controller's enterprise Oracle PeopleSoft systems (SF People & Pay, SF Financials, SF Procurement, and SF Learning) are managed by DT at the DEM Datacenter (production) and the CA State Data Center (non-production). Managing these mission-critical systems from the two locations has been challenging in terms of reliability, performance, and application support.
  - CON Systems and DT are in alignment to transition from the current datacenters to a cloud-base hosting provider, where DT would continue to manage the CON Systems hardware via an Infrastructure as a Service (IaaS) model.

Project Overview

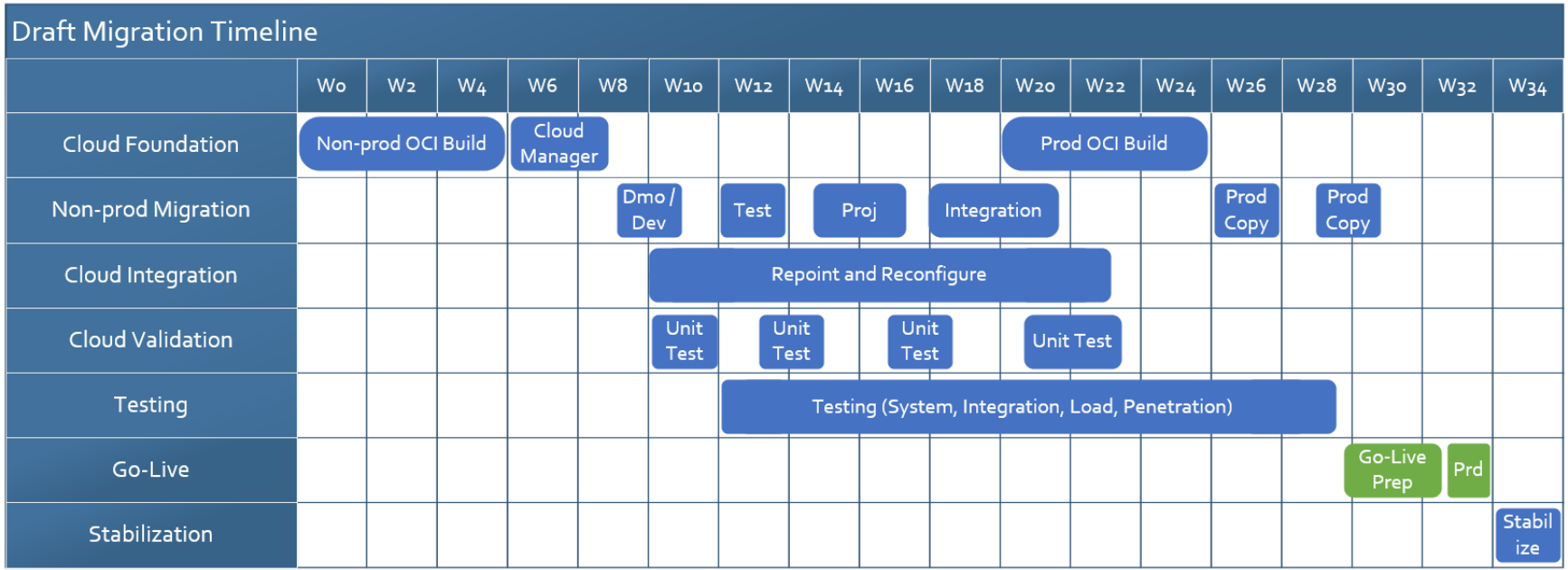
- Project Objective
  - Migrating CON Systems infrastructure to a cloud-base hosting provider will continue to support the City's custom PeopleSoft deployment while improving reliability, scalability, performance, security, and support.

Project 5-Year Financial Forecast

	FY24-25	FY25-26	FY26-27	FY27-28	FY28-29
COIT Allocation	$0				
Other Sources	$1,200,000				
Total Project Funding	$1,200,000				

High-Level Project Plan

8-month implementation



Measuring Project Success

- Key Performance Indicator(s)

No.	Goal
1	Reduce the occurrences of unplanned system outages
2	Improve ability to scale infrastructure up/down as-needed and on demand
3	Improve ability to implement critical security patches more quickly and efficiently
4	Utilize autonomous databases to improve production performance and availability
5	Implement disaster recovery processes that utilize the cloud in the event of disaster
6	Maximize staff productivity to focus on higher level projects

Risk Mitigation Strategies

Project Risk Management Plan

COIT considers a thoughtful list of potential risks and plan to address them to be a strength. For a helpful reference on types of project risk, see this this resource.

Below, please discuss the risks this project might face. What could fail and why? How would you prepare for these risks? Some common risks are pre-populated below, but **feel free to change these** as appropriate for your project.

Potential Risk #1: Budget Overrun and/or Vendor Delays	Your Plan to Prepare for/Mitigate this Risk • This is the Systems Division's highest priority project for FY25. We have been engaged in a very intentional and thorough planning process with our partners for over a year now, and have built in budget and schedule contingencies in case of cost overruns or vendor delays.
Potential Risk #2: Project Scope Creep *(project deliverables expand beyond original plan and exceed available resources)*	Your Plan to Prepare for/Mitigate this Risk • As noted above, we have engaged in a very thorough planning process, including consulting with peer government agencies re: implementation approach and lessons learned, as well as procuring third-party advisory services to perform a detailed review and assessment of our infrastructure needs to validate scope. • We are currently negotiating a milestone-based contract with our implementation partner, including clearly documented process for change orders.
Potential Risk #3: Staffing/Capacity for Implementation, Deployment, Training	Your Plan to Prepare for/Mitigate this Risk • We have dedicated one full-time and one part time project manager to this project and postponed our annual PeopleSoft Update Project 12 months to ensure sufficient staff capacity to support this project. • We have confirmed FY24 and FY25 budget for staff training and are in the process of finalizing topics and schedule.

Change Impact Assessment

Purpose: This template can help you determine the degree and complexity of change your project entails. It also brings focus to who and what is impacted, which can sharpen your plans for communication and training.

Impact Analysis	
Dimension of Change	**Description of the change**
Operational Impact	How will workflows/processes be impacted? • **Improved efficiency in database management processes, freeing up more time for higher value analyses and projects**
Policy & Management Impact	Will the project's implementation require the introduction of a new surveillance technology policy or cybersecurity strategy? Or changes in Management Strategies? (e.g. adjustments to org. chart to reflect new/shifting responsibilities caused by project?) Please discuss. • **No surveillance technology utilized in this project.** • **Improvement in ability to manage cybersecurity risks, but no impacts to cybersecurity policies.** • **No changes in organizational structure, nor management strategies.**
Impact to Specific Roles/Teams, Departments, Residents	Describe the impact the project will have on various employees, teams, other departments, or residents. Please consider whether the new technology could generate frustration or opposition from end users, perhaps due to the need to change methods of conducting business and/or because of a learning curve for mastering the new technology. • **No changes to end user interfaces or applications, but all 35,000+ employees and 5,000+ City suppliers and bidders will experience improved reliability and performance when using the Citywide Systems we support (SF Employee Portal, SF Learning, SF People & Pay, SF Financials, SF Procurement, SF Reports & Analytics, SF Budget, and the SF City Partner site for bidders and suppliers).**

Questions?

Department of Emergency Management

Presentation to COIT Budget & Performance Subcommittee

Citywide Data Center Certification Project

March 2024

Project Overview

- ## Problem Statement

  - The City of San Francisco Citywide Data Center faces issues in infrastructure capacity, operational management, and physical security at the 1011 Turk St facility. Key concerns include non-concurrent maintainability in electrical and mechanical systems, inadequate staffing leading to potential human errors, and a lack of comprehensive security measures, such as outdated access control systems and insufficient surveillance. Urgent actions are required to address these vulnerabilities, enhance operational resilience, and ensure the long-term sustainability and security of the data center.

- ## Project Objective

  - The project aims to fortify the Citywide Data Center at 1011 Turk St by continuing a comprehensive assessment of its infrastructure, management and operations, and security protocols. Objectives include enhancing concurrent maintainability in electrical and mechanical systems, implementing a robust personnel training program, establishing a succession plan, and improving physical security measures. The overarching goal is to optimize operational efficiency, minimize human error, and bolster the data center's long-term resilience against potential vulnerabilities.

Background

- Initial funding received from COIT in FY22-23
  - DEM received $217K to perform an initial/baseline Risk Assessment with Uptime Institute
  - Risk Assessment was performed August 2023 – October 2023
  - Findings/Outcomes provided to DEM, DPW and DRE in early 2024

Basic Capacity

Redundant Components

Concurrently Maintainable

Fault Tolerant

Data Center Risk Assessment Objectives

- **Assess the overall Data Center Topology**
  - Document site Infrastructure Capacity – design, present, and expected
  - Identify potential constraints affecting computer room space, power, and cooling
  - Compare current utilization with industry standard best practices
  - Provide a snapshot of representative computer room management issues
  - Document equipment that has surpassed a reasonable performance life cycle
  - Provide a most likely Tier Classification based on all observations and documentation
  - Identify through a visual inspection lurking vulnerabilities
- **Assess the Management and Operations (M&O) of the Data Center**
  - Staffing and Organization
  - Maintenance
  - Training
  - Planning, Coordination, and Management
  - Operating Conditions
  - Document detailed recommendations to limit human error and improve uptime

Data Center Risk Assessment Objectives, cont.

- **Assess the Physical Security of the Data Center**
  - Staffing and Organization
  - Processes and Procedures
  - Physical Security Elements
  - Electronic Security Systems

Risk Assessment Results- Topology Summary Table

Electrical					Mechanical		
Fuel Systems	Engine Generators	Power Backbone	UPS & Batteries	Critical Power Distribution	Mechanical Plant	Computer Room Cooling	UPS Room Cooling
Basic Capacity	Redundant Capacity Components	Concurrently Maintainable	Concurrently Maintainable	Concurrently Maintainable	Basic Capacity	Basic Capacity	Concurrently Maintainable

High Level Recommendations

- Keep Uptime Institute on consulting contractor for assistance with developing policies, procedures and training frameworks for Data Center Operations
  - Consider an on-going operational expense in DEM-IT Budget
  - Consider a charge model for tenants
- Work with Real Estate (Building Engineering) and Sheriff to evaluate staffing and training
  - Need 24X7X365 On-site Building Engineering for Tiered Status – work to hire/train staff that over next several fiscal years
- Capital Funding Requests
  - Badging System Replacement Project underway – update Turk St. visitor policy in conjunction and add Data Center considerations
  - Critical Power Load project is underway
  - Additional Capital Project Request identified

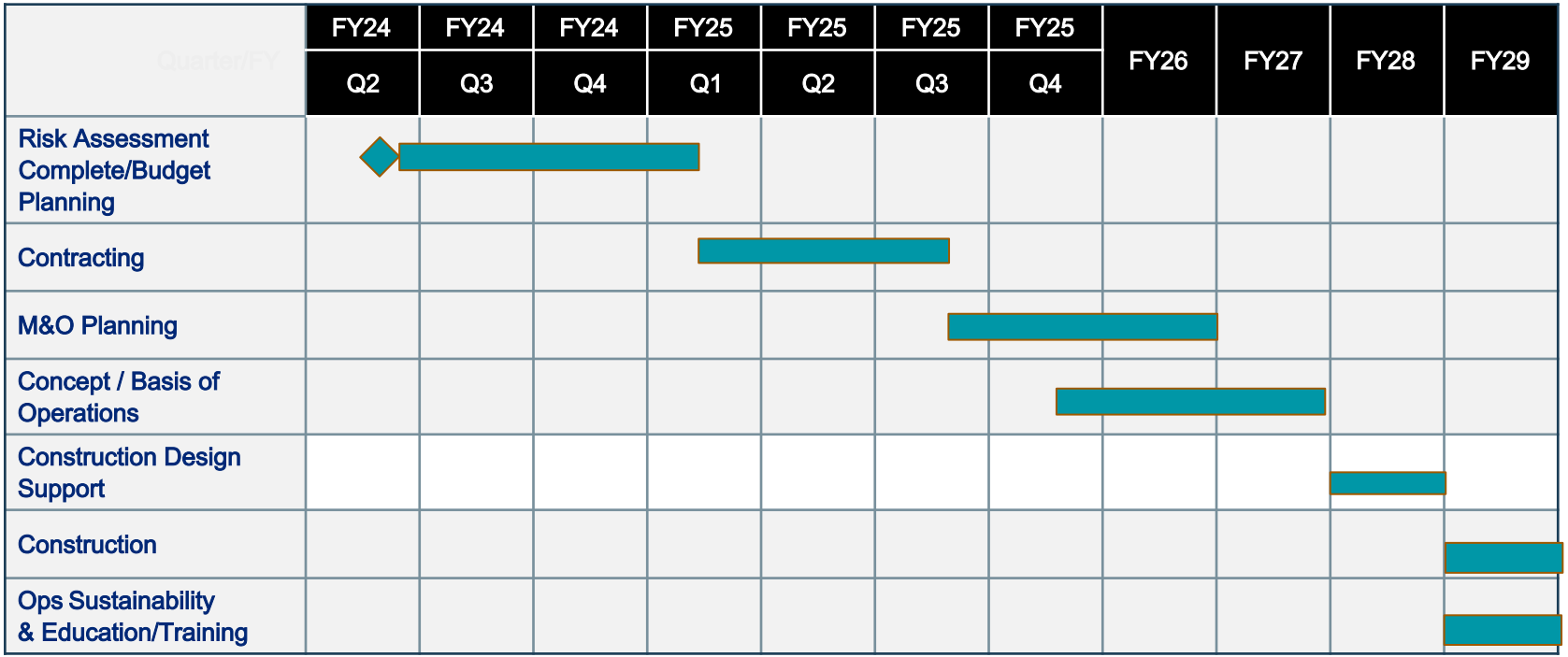
DEM CAPITAL FUNDING REQUEST FY24-25

- 2x New CRAC Units for Data Center Cooling
- Data Center UPS (Eaton) Replacement
- 3x Mechanical Control Center Replacement
- Redesign Data Center Cooling (Chillers/ Indoor Units/ Controllers/ Piping)
- Redesign for Critical Power Load Backup (Generator/ Fuel Day Tanks)
- Redesign of Data Center (1011 Turk St. 1st Floor, room for growth)
- Building Water Intrusion Membrane Redesign & Seismic Review
- Perimeter Swing Gates Retrofit
- Roof Membrane - Protective Pad for Walk Paths
- Fire Alarm Panel

Project 5-Year Financial Forecast

	FY24-25	FY25-26	FY26-27	FY27-28	FY28-29
COIT Allocation	$155,000	$155,000	$155,000	$155,000	$155,000
Other Sources	n/a	n/a	n/a	n/a	n/a
Total Project Funding	$155,000	$155,000	$155,000	$155,000	$155,000

High-Level Project Plan



Measuring Project Success

- Key Performance Indicator(s)
    - Success will be evaluated through comprehensive Key Performance Indicators (KPI) assessing advancements aligned with industry-standard Tier Rating Systems, encompassing decreased non-concurrent maintainability issues, heightened operational resilience, and fortified security measures. The KPI will quantify the percentage reduction in vulnerabilities identified during the initial risk assessment, reflecting the project's effectiveness in mitigating risks and aligning with Tier standards. Achieving a substantial decrease in these vulnerabilities will signify the project's success in enhancing the overall infrastructure, management, and security of the City of San Francisco Data Center. This multifaceted approach ensures a holistic evaluation of success post-launch, aligning with industry best practices and positioning the data center for sustained optimal performance and security.

Questions ?

Cloud
Center of Excellence

Cloud Center of Excellence

Problem Statement

Background:

- The City has invested in expanding services to both private and public cloud platforms
  - AWS, Azure, Google Cloud, Oracle Cloud, and on-premise
- There are currently 40+ departments that rely on cloud services to support growing business needs

Problem Statement:

- As cloud adoption continues to grow:
  - Increase in complexity, management overhead, and cost
  - Decrease in optimized usage and security compliance

Cloud Center of Excellence

Project Objective

- Simplify delivery of public clouds
  - Amazon, Microsoft Azure, Google and Oracle
  - Management, tools, platform, integrations that can scale to meet business needs
- Provide advice for cloud to modernize city business systems
  - The City manages over 300+ cloud-based business systems
- Consolidate procurement of cloud services

Cloud Center of Excellence

Performance Measures

Completed FY23/24:

- Simplified onboarding for CCSF departments
- Incorporated Google and Oracle as part of DT service offering
- High-speed connections to cloud service providers (CSP)
- Modernize applications by utilizing cloud native architecture
- Addition of commercial public cloud to CSP portfolio

Planned FY24/25:

- Multi-cloud management platform
- Create a unified cost management platform (FinOps)
- Develop and guide CCSF departments on optimal cloud adoption (cloud smart strategy)
- Negotiate and finalize Enterprise Agreements with Google and Amazon Web Services
- Onboard public safety (CJIS) departments to public cloud

Cloud Center of Excellence

Business Benefit and Impact

The Cloud Center of Excellence has a focus of aiding City departments with cloud adoption by providing services and a governance framework to:

- Streamline multi-cloud management, reducing the need for extensive management while enhancing resilience.
- Optimize cloud spend by analyzing cloud cost trends.
- Strengthen architectural security to manage risk and ensure compliance.
- Enhance performance and efficiency of resource utilization.

Project Risk Management Plan

COIT considers a thoughtful list of potential risks and plan to address them to be a strength.

Potential Risk #1: Budget Overrun and/or Vendor Delays	Majority of budget for this project pertains to licensing fees which are predictable. Vendor delays are unlikely as project is ahead of schedule.
Potential Risk #2: Project Scope Creep	A clear project objective has been outlined with strong buy-in from senior management. A project plan has been established to minimize deviation from the objective to prevent scope creep.
Potential Risk #3: Staffing, Resources & Training	The core project team will be supported by team members that can support additional capacity requirements. All team members are cross-trained on the Cloud Center of Excellence initiative.

Project Risk Management Plan, Continued

Consequences of Not Funding	Continued growth of public cloud in an ad-hoc manner without effective governance. Increased wasteful spend, risk of cybersecurity incidents and unsuccessful cloud migrations.
Alternate Plans	The City will be left behind industry maturity and unable to successfully leverage the cloud to further innovation of City technology. Increased on-premises datacenter footprint, staff and capital expenditure. Lack of governance and newly automated processes will delay timelines and lower performance of City technology. Ineffective use of valuable FTE hours.

Project Update

Total Project Cost	Total COIT Funding To Date	Total Other GF Funding	Total NGF Funding	Total NGF + GF Funding	Total Spent	Remaining Balance
$2.44M	$1.37M	-	-	-	$1.18M	$183K

	Status			Comment
Schedule		Begin Date	July 2022	Project ahead of schedule – FY24 deliverables on track for completion within calendar year 2024.
		End Date	July 2026	
		% Complete	60%	
Scope		No notable scope creep to report.		
Budget		Initial year budget in FY22-23 with carry-over of $183k, or 14% due to cost-saving negotiations.		

Cloud Center of Excellence
Funding Request

		FY2024-25	FY2025-26
Total Project Costs	**High**	Carry Over = $183,058 Ask = $1,074,798	$1,257,856
	Low	$700,000	$700,000
Funds requested from COIT		$1,074,799	$1,257,856

Breakdown of Funding Ask:	**FY2024-25**	**FY2025-26**
Multi-Cloud Management Tool	$510,000	$510,000
Multi-Cloud Security Enhancement	$285,000	$285,000
Multi-Cloud Cost Management Enhancement	$10,000	$10,000
Cloud Operations Apps and Integration	$105,000	$105,000
Cloud Disaster Recovery Service (200 VMs)	$115,000	$115,000
Senior IT Engineer- Public Cloud/Professional Services	$232,856	$232,856
Total:	**$1,257,856**	**$1,257,856**

** Existing DT management position and staff will be in the Cloud Center of Excellence and are funded in the operations budget.*

* **Conversion of COIT funding to operational budget in FY26-27 to cover software licensing cost pending MBO approval.**

Increase City Data Center Resiliency

(For the network)

Increase City Data Center Resiliency

Project Objective

- Complete modernizing City Wide Area Network for resiliency:
  - Enable service resiliency - Internet, Domain Name Service (DNS) Authentication
  - Provide resilient network transport enables recoverability of CCSF business applications
- Reduce risk of access interruption to business-critical City services
- Consolidate and reduce support and licensing costs
- Decommission legacy network infrastructure from all 3 data centers and City Wide Area Network (WAN)
- Achieves **High Availability of Network Services**

Increase City Data Center Resiliency

Performance Measures

Completed FY23/24:

- 100% - Aggregation points and Customer Edges upgraded and connected to Network 2.0
- 100% - departmental separation where they all have their own network guarded by firewall
- 100% - Turk Data Center migrated to Network 2.0
- 100% - Rancho Data Center migrated to Network 2.0
- 100% - SFO Data Center migrated to Network 2.0
- 100% - FWAN 1.0 Decommissioned

Planned FY24/25:

- Network Services resiliency testing (DNS/DHCP/Internet..)
- Upgrade Internet Edge routers (>10Gb)
- Increase Internet and WAN capacity, and resiliency between data centers and public cloud
- Continued training for enhanced software defined networking resiliency

Increase City Data Center Resiliency
Funding Request

Five-year Costs and GF budget for COIT funding						
		FY2024-25	**FY2025-26**	**FY2026-27**	**FY2027-28**	**FY2028-29**
Total Project Costs	**High**	Carryover - $50,000 Upcoming Need: $224,000 **Funding requested: $174,000**	$204,000	$200,000	$105,000	$0
	Low	Carryover - $50,000 Upcoming Need: $224,000 **Funding requested: $174,000**	$204,000	$200,000	$105,000	$0
Funding requested from COIT		**$174,000**	**$204,000**	**$200,000**	**$105,000**	$0

Breakdown of Funding Ask:	**FY2024-25**	**FY2025-26**
Enhanced software defined networking training	$60,000	$40,000
Public cloud transport resiliency - Connectivity	$164,000	$144,000
Public cloud transport resiliency - Equipment	$0	$20,000
Total:	**$224,000**	**$204,000**

Increase City Data Center Resiliency

Business Benefits and Impact

- One of the three keys to infrastructure resilience:
  - Transport (Increase City Data Center Resiliency)
  - Platform
  - Application
- Reduce chance of long-term network outages
- Provide resiliency for the new City-Wide Area Network and MyApps secured applications
- Increase capacity for City Wide Area Network and Internet
- Cost avoidance:
  - Eliminate old equipment which cause costly wide-spread disruption
  - Lower risk of interruptions to critical City business operations
  - Reduce maintenance and licensing cost (going to one network)
- Primary users & Major Stakeholders: Citywide


Resiliency should not be an afterthought!

JUV Rubrik Online Backup Archiving System

Juvenile Probation Department (JPD)

Verónica Martínez
Deputy Director of Administrative Services
Juvenile Probation Department

Rubrik Online Backup Archiving System

Problem Statement

- ***Background:*** JPD is currently using Altaro to back up the department servers. It is installed on a Windows 10 PC. The on-site backup data is stored on network attached storage (NAS). Offsite backup is stored on pin-secured USB drives with very limited capacity (less than a month worth of data).

- Disadvantages on the existing backup system:
  - There is only one backup server in JPD with no redundancy.
  - Data is stored on limited local and independent data storage (NAS and USB drives).
  - Inability to increase back up capacity without expanding the local storage.
  - Manual procedures for the offsite backup by using portable pin-secured USB drive.
  - Limited system recovery capacity to current infrastructure.

Rubrik Online Backup Archiving System
Project Objective

To implement a more reliable and secure backup system - Rubrik backup and online archiving that offers the following:

- A cluster of Rubrik hosts that will provide high availability and load balancing.
- More flexibility and scalability to recover virtual machines.
- More reliable and secured offsite backup.
- More flexible and configurable options for data retentions.
- Quick recovery minimizes downtime of systems critical for operation of a 24X7 facility.
- A better cyber resiliency solution.

Rubrik Online Backup Archiving System
Funding Request

		FY2024-25	FY2025-26
Total Project Costs	**High**	$180,000	$35,000
	Low	$160,000	$24,000
Funding requested from COIT		**$180,000**	**$0**

Breakdown of Funding	FY2024-25	FY2025-26
Licensing for the equipment	$24,000	$30,000
Equipment (Rubrik R334, 3 nodes)	$140,000	n/a
Professional Services (initial setup and configuration by Rubrik)	$15,000	n/a
Total From COIT:	**$180,000**	**$0**
Total From Capital:	**$0**	**$0**

Rubrik Online Backup Archiving System
Project Timeline

Phase	Tasks	Time Frame
1	Procurement and acquisition of Rubrik system.	1-2 months
2	Inventory existing backup jobs. Plan on the backup job setup, including contents to be backup, scheduling, and local and remote retention period.	2 - 3 weeks
3	Procurement of DT GovCloud service.	3 – 4 weeks
4	Install and configure Rubrik hosts.	2 - 3 weeks
5	Set up connection to cloud service (GovCloud).	2 - 3 weeks
6	Configure backup jobs.	3 - 4 weeks
7	Monitor the backup performance and data size on the local and remote storage. Adjust the settings to meet the needs of the department.	on going

Rubrik Online Backup Archiving System
Project Risk Management Plan

Consequences of Not Funding:	JPD will not be able to update our outdated backup system to a robust system that can better protect our systems against cyber threats and meet the changing needs of our department in this modern world. JPD will have to continue to rely on and invest in maintaining the infrastructure of an inefficient and outdated backup system.

Item Number 7

Review the remaining schedule for Department presentations (March - April)

Discussion

Budget & Performance Presentation Calendar (10:00AM-12:00PM)

Week of March 22		
	Resource Management & Risk Management & Records Management	
(10:10AM - 10:30AM)	ADM	*Continuation of quality & accessibility funding for migration of City websites to SF.gov
(10:30AM - 10:50AM)	TIS	Disaster Recovery for Critical City Applications
(10:50AM - 11:10AM)	DHR	Disaster Service Worker Management System
(11:10AM - 11:30AM)	POL & DAT	Digital Evidence Management System (DEMS)
(11:30AM-11:50AM)	TTX	*Empty Homes Tax
Week of March 29		
	Major IT Project	
(10:10AM - 10:30AM)	DEM	*Computer Aided Dispatch Replacement Project
(10:30AM - 10:50AM)	ASR	Property Assessment and Tax Systems Replacement
(10:50AM - 11:10AM)	TIS	*VOIP and LAN Modernization
(11:10AM - 11:30AM)	TTX	Business Tax Application
(11:30AM-11:50AM)	POL	NIBRS-Compliant RMS
Week of April 5		
	Customer & Case Management	
(10:10AM - 10:30AM)	ADM	Digital building permit application platform (Phase 1 - PTS/Accela replacement)
(10:30AM - 10:50AM)	ADM	Permitting Database Replacement
(10:50AM - 11:10AM)	DHR	HR Modernization: Electronic Onboarding and e-Personnel Files
(11:10AM - 11:30AM)	SHF	*New Jail Management System
(11:30AM-11:50AM)	DAT	Electronic Subpoena Solution

Budget & Performance Presentation Calendar (10:00AM-12:00PM)

Week of March 1	**Staff Collaborative Tools - Data Analysis / Data Sharing & Business Specific**	
(10:10AM - 10:30AM)	DHR	*Employee Access to their City (Intranet/Employee Portal)
(10:30AM - 10:50AM)	DBI	IVR Enhancement
(10:50AM - 11:10AM)	DBI	Lightweight CRM
(11:10AM - 11:30AM)	TIS	*JUSTIS Program
(11:30AM-11:50AM)	TIS	Generative AI Center of Excellence
Week of March 8		
	Infrastructure: Network & Data Centers	
(10:10AM - 10:30AM)	CON	Cloud Infrastructure Implementation
(10:30AM - 10:50AM)	DEM	Citywide Data Center Certification Project
(10:50AM - 11:10AM)	TIS	*Cloud Center of Excellence
(11:10AM - 11:30AM)	TIS	*Increase City Data Center Resiliency
(11:30AM-11:50AM)	JUV	Rubrik Online Backup Archiving System
Week of March 15		
	Infrastructure: Network/ Data Centers and Risk Management	
(10:10AM - 10:30AM)	DEM	*Radio Project - Financing
(10:30AM - 10:50AM)	AIR	Citizens Broadband Radio Service (CBRS) Private LTE Cellular
(10:50AM - 11:10AM)	AIR	Enterprise Infrastructure Information Management and Integration
(11:10AM - 11:30AM)	AIR	Network Hardware Lifecycle
(11:30AM-11:50AM)	AIR	Dynamic Network Port Security

Adjournment