



Regular Meeting

November 17, 2016

**1 Dr. Carlton B. Goodlett Place, City Hall, Room 305
San Francisco, CA 94102**

Agenda

1. Call to Order by Chair
2. Roll Call
3. Approval of Meeting Minutes from September 15, 2016
4. Chair Update
5. CIO Update
6. Department Updates & Announcements
7. Update: FY 2018-22 Information & Communication Technology (ICT) Plan
8. Discussion & Action: City-wide Cybersecurity Policy
9. Discussion & Action: City-wide Password Standard
10. Discussion: Identity & Access Management
11. Public Comment
12. Adjournment

3. Approval of Minutes

Action Item

4. Chair Update

5. CIO Update

Shared Services Update

COIT

November 17, 2016



SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

Shared Services: IT partner of choice, not the IT department of mandate.



- Connectivity



- Digital Service



- Technology-as-a Service



- Tech Talent

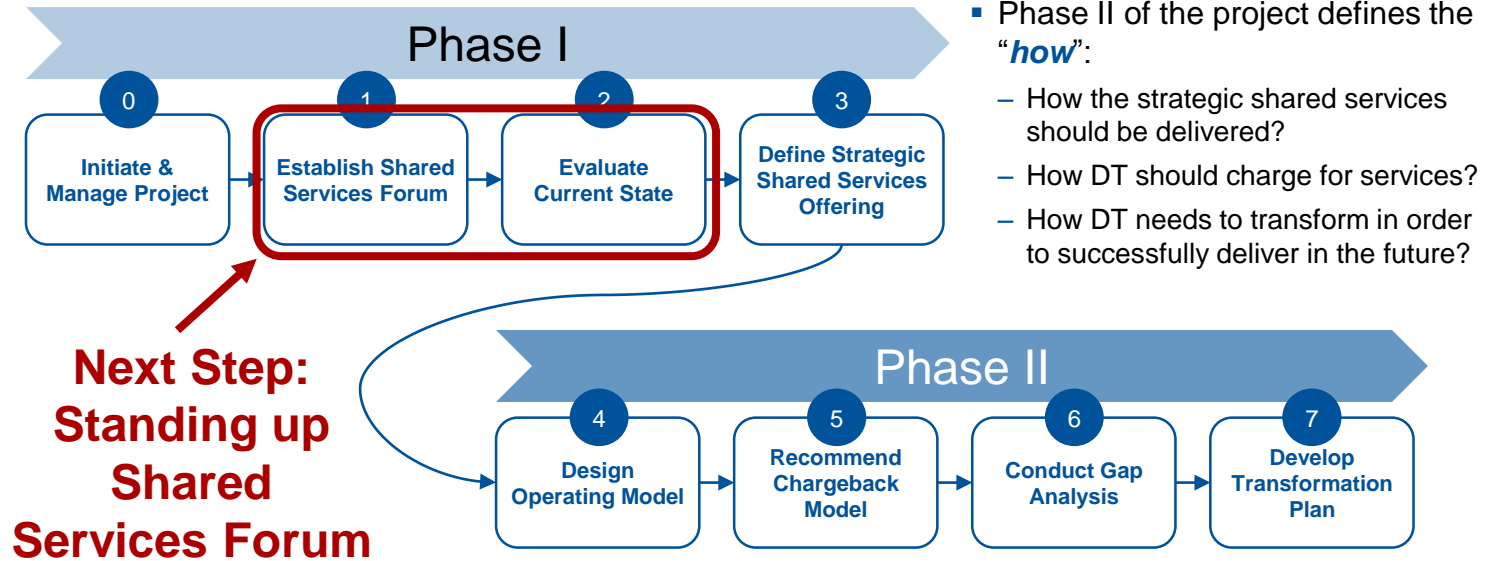


- Cybersecurity

Shared Services is the bedrock of the Department of Technology's strategy. We are focused on developing the right services with the right features at the right cost with the right performance levels according to customer requirements and demands.

Project purpose is to develop a strategy and transformation plan to position DT as a preferred provider of key shared services for city departments.

- Phase I focuses on laying the groundwork for successful collaboration between DT and it's customers; identifying improvement opportunities as well as constraints and barriers to future transformation; and ultimately defining “*what*” services DT should focus on delivering strategically.



- Phase II of the project defines the “*how*”:
 - How the strategic shared services should be delivered?
 - How DT should charge for services?
 - How DT needs to transform in order to successfully deliver in the future?

6. Department Updates & Announcements

7. Update: FY 2018-22 ICT Plan

COIT Staff

FY 18-22 ICT Plan Update

Calendar

MONTH	GOAL	ACTIVITIES
June	Kick-Off Strategy Development	
July-Sept	Diagnose Current	Citywide Survey
October	Identify Ideal State Define Strategies & Tactics	Department Surveys
November/ December	Define Strategies / Recommendations	External Survey Group Sessions Leadership Workshop
January	Review Recommendations/Draft	
February	Final Approval	
March 1	Submit Plan to Mayor and Board of Supervisors	

FY 18-22 ICT Plan Update

Department Technology Plans

- All departments submitted technology plans!
- Opportunity to highlight accomplishments and challenges
- Other key findings to help form the foundation of the ICT Plan

FY 18-22 ICT Plan Update

Department Technology Plans - Accomplishments

- ❖ Goal 1: Support, Maintain, and Secure Critical Infrastructure
 - DPH: Zuckerberg General Hospital Opening (technology infrastructure re-build)
 - DT: Server Virtualization (on-going)
 - DT: Fix the Network (on-going)
 - DEM: Public Safety Radio Replacement Project Implementation
 - LIB: Increased connectivity at branches
 - DHR/DT: Tech Hire Program
 - City CISO
 - Citywide: Disaster Preparedness Response Recovery and Resiliency (DPR3) Policy

FY 18-22 ICT Plan Update

Department Technology Plans - Accomplishments

❖ Goal 2: Increase Efficiency and Effectiveness

- CON: PeopleSoft 9.2 Upgrade (complete)
- PDR: Gideon Upgrades (on-going)
- PUC: Agency wide SharePoint deployment (on-going)
- OCA: eSignatures deployment (on-going)
- CON: Financial Systems Replacement Implementation (on-going)
- FIR: Electronic Pre-hospital Care Report (PCR) Application (complete)
- TTX: Expansion of workflow and process redesign (complete)
- ASR: Property Tax System Readiness Assessment (ongoing)

FY 18-22 ICT Plan Update

Department Technology Plans - Accomplishments

❖ Goal 3: Improve Access and Transparency

- TTX: New Business Registration (complete)
- DHR: Deployed new website (on-going)
- 311: Deployed new website (complete)
- BOS: Assessment Appeals Online Filing System (complete)
- ETH: Electronic Filing Enhancements (on-going)
- HSS: Released first data sets to SF Open Data Portal
- DT: Business Portal Technology Enhancements (on-going)
- Citywide: Digital Services Strategy (complete)

FY 18-22 ICT Plan Update

Department Technology Plans - Initial findings

A few highlights:

Procurement

A majority of respondents said that they had a favorable experience with the Tech Marketplace.

Tech Hiring

Few departments have taken advantage of the program

Disaster Recovery

Majority of departments have identified critical systems; however, less than half have a Continuity of Operations (COOP) plan for these systems

Cyber Security

32 departments rely on the Department of Technology for their cyber security needs.

Connectivity

Continued interest in Voice over IP (VoIP) solution by most departments.

Digital Services

64% have either redesigned their websites in the last 2 years or less.

Shared Services

Cyber security, financial/accounting systems, telephony, and data analytics are reporting identified as top shared services that City would benefit from.

FY 18-22 ICT Plan Update

ICT Plan Metrics

- Re-evaluating current measures
 - Keep what's working
 - Change what's not
 - Better define our objectives
 - Look to what is already being tracked
 - Start small
 - Working groups to develop and bring back to Subcommittee and COIT

8. City-wide Cybersecurity Policy

Discussion and Action Item

Cyber Security Policy

COIT

November 17, 2016



SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

Strategic Alignment: Cybersecurity



• Connectivity



• Digital Service



• Technology-as-a Service



• Tech Talent



• Cybersecurity

The Cybersecurity Policy lays the foundation for the City and County of San Francisco's Cybersecurity Program as a whole and demonstrates executive level support for the program

VISION

- ✓ Provides a Citywide risk based approach to Cybersecurity leading to identification and mitigation of threats.

Changes since last COIT Presentation

- ✓ Revised the language
- ✓ Re-articulated the adopted framework
- ✓ Provided room for other frameworks to be adopted by departments
- ✓ Added COIT and Mayor's Budget Office responsibilities
- ✓ Re-aligned departmental responsibilities

What does it mean for departments?

- ✓ Resource for cybersecurity functions
- ✓ Appoint a cybersecurity officer / Designate a cybersecurity liaison

What does it mean for City staff?

- ✓ Comply with the policy by playing their role in ensuring confidentiality, integrity, and availability of City information resources.

9. City-wide Password Standard

Discussion and Action Item

New Password Standard

COIT

November 17, 2016



SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

Strategic Alignment: Cybersecurity



• Connectivity



• Digital Service



• Technology-as-a Service



• Tech Talent



• Cybersecurity

✓ We will enhance the security of our passwords/passphrases by increasing difficulty for brute force cyber-attacks.

Password Standard

Feature	Minimum Requirements
Password Expiration	Every 90 days
Minimum Length	12 characters
Password Complexity	Enabled, all four categories included (upper case, lower case, numeric, special character)
Minimum Password Age	One day
Password History	Last 7
Account Lockout	After 5 unsuccessful consecutive logon attempts
Lock-Out Duration	10 minutes
Screen saver	Idle after a maximum of 10 minutes, password protected

Password Implementation

- ✓ The new password standard shall be effective on Dec 8, 2016 in order to meet the IAM go live date of Dec 23, 2016.
- ✓ Implementation date for all departments: As soon as practical, but no later than January 31, 2017.

What does this mean for departments?

- ✓ Department AD systems should be modified to meet these requirements.
- ✓ Departments are encourage to implement a higher standard to meet their own individual risk profiles.
- ✓ Departments with legacy systems that cannot comply with this standard should contact the City CISO Joe Voje at joe.voje@sfgov.org.

What does this mean for the users?

- ✓ Passwords will be changed at the next password change cycle between Dec 8, 2016 and March 8, 2017.
- ✓ All users shall use the new password portal located at <https://bifrost.sfgov.org> for all City AD password changes.
- ✓ Avoid using CTRL+ALT+DELETE to change passwords. This causes password mismatch between City AD and IAM platforms.

CONTACTS

Joe Voje: joe.voje@sfgov.org

Jackson Muhirwe: jackson.muhirwe@sfgov.org

Cybersecurity Team: 415-581-3947

10. Project Update: Identity & Access Management

| Identity & Access Management

COIT

November 17, 2016



SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

Strategic Alignment: Cybersecurity



• Connectivity



• Digital Service



• Technology-as-a Service



• Tech Talent



• Cybersecurity

The goal of **Identity & Access Management** is to provide a centralized repository of identities and access control of systems owned and operated by and for the City of San Francisco.

Definitions

An **Identity & Access Management Program** unites multiple initiatives and activities that manage identities, privilege, access, and trust.

IAM enables the right individuals to access the right resources at the right times and for the right reasons.

Why implement an IAM solution?

- ✓ Enhances security of CCSF systems.
- ✓ Enables centralized access to multiple independent systems (eMerge, F\$P).
- ✓ Authentication: The right people logging into the correct service.
- ✓ Privilege: Once people have access, IAM defines the privileges they possess.

What does it mean for departments?

- ✓ By **November 30**, will build a communication package for your department.
- ✓ We will train your Department's Help Desk and they can educate your department. We will be in full support.

What does it mean for employees?

- ✓ Impacts City AD, eMerge, F\$P accounts.
- ✓ Access to enhanced security for authentication.
Introduces multi-factor capability.
- ✓ Self-service password resets upon registration of a non-city email or mobile device and registration of security questions.
- ✓ Will alleviate current state challenges.
- ✓ The Help Desk will remain available for resets!

New Standards

- ✓ We will enhance the security of our passwords/passphrases by increasing difficulty for brute force cyber-attacks.

Next Steps: Technical & Operational

- ✓ Environment Configurations and Updates (Complete by 11/8)
- ✓ Access Authentication and Configuration (Complete by 11/17)
- ✓ IAM Governance Committee Established (Complete by 11/25)
- ✓ Test phase (Complete by 12/15)
- ✓ Deploy IAM (Complete by 12/23)
- ✓ Production Environment Warranty (Complete by 1/30/2017)
- ✓ Establish Disaster Recovery Environment (Complete by 3/1/2017)

Next Steps: Communication

- ✓ Communicate advantages of new system (Complete by 11/18)
- ✓ Pre-Go Live user Training to Departments (Complete by 11/30)
- ✓ Service Desk training video (Complete by 11/30)

IAM Roadmap

- ✓ Multi-factor tool deployment (2017)
- ✓ Privilege Access Management (2018)
- ✓ Develop roadmap for Single Sign-On to 0365 (2018)
- ✓ Explore integration with Social Media Platforms (2018)

11. Public Comment
