Santa Clara Valley Transportation Authority

RSM

Comprehensive IT Risk Assessment

Auditor General Report No. 2018-004

September 5, 2019 Meeting

Fieldwork Completed July 16, 2019

Report Issued August 14, 2019

Table of Contents

Acronym Definitions

Acronym	Definition
DR	Disaster Recovery
EOL	End of Life
EOS	End of Sale
GRC	Governance, Risk Management, and Compliance
LAN	Local Area Network
MFA	Multi-Factor Authentication
OS	Operating System
PMO	Project Management Office
VPN	Virtual Private Network

PROJECT OVERVIEW

Project Overview

Project Goals and Objectives

We performed an assessment of Santa Clara Valley Transportation Authority's (VTA's) information technology operations and governance environment, with a focus on understanding key operations and identifying high risk areas. From this assessment, we sought to understand the long term strategy and organization of the IT department; use of existing business applications; infrastructure that is leveraged to support technology; and overall risks and controls present in the environment. We team collaborated closely with VTA staff to understand objectives and challenges, identify opportunities for improvement and develop actionable recommendations to improve and enhance the IT organization and supporting business processes that seek to improve the overall efficiency and scalability of the environment and mitigate future risk to the business.

The outcome of this assessment is a deliverable, which includes:

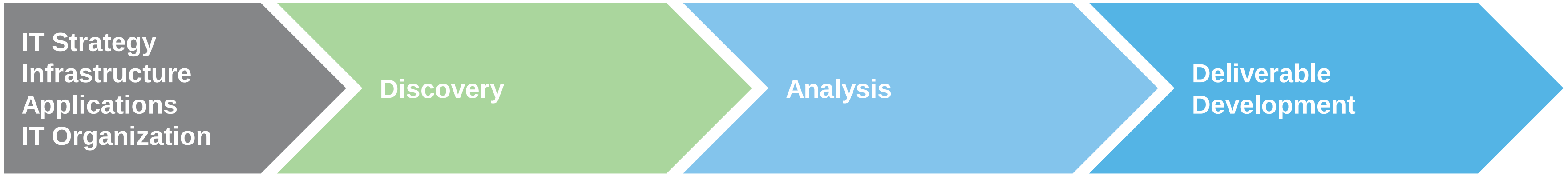
- ✓ **A current state assessment of VTA's overall IT environment, including:**
  - ➢ Strategic vision of the overall organization and IT teams
  - ➢ Overall IT organization and resources
  - ➢ IT governance and budgeting processes
  - ➢ Planned, upcoming, and recently completed projects
- ✓ **An evaluation of the VTA's infrastructure environment, including:**
  - ➢ Comprehensive review of IT infrastructure supporting VTA services
  - ➢ Identity management security and setup
  - ➢ Server administration and security
  - ➢ Endpoint management
- ✓ **A detailed evaluation of VTA's application environment with a focus on the SAP core operating system, including:**
  - ➢ Change management
  - ➢ Logical security
  - ➢ User security administration
  - ➢ Computer operations for core enterprise system, SAP

Key future state requirements were reviewed to inform re-engineering and optimization opportunities identified in this report. Included are recommendations and opportunities to enhance future state operations.

Project Overview

Our Approach

To execute the project, we worked with relevant VTA staff, utilizing our standard assessment approach, while leveraging the knowledge of VTA's team. We reviewed the existing processes and systems in place at VTA through onsite discussions and a review of documents provided by the VTA team. We then critically evaluated these against industry best practices and developed recommendations to improve overall IT operations and reduce business risk.



IT Strategy
Infrastructure
Applications
IT Organization

Discovery

Analysis

Deliverable Development

Discovery Phase	Analysis Phase	Deliverable Development Phase
Scheduled days of on-site meetings with executives and key department leaders to understand organizational objectives and key requirements	**Review and evaluation of current state technology and processes**	**Creation of deliverable with onsite meetings to review deliverable and finalize go forward approach**
• Set overall project objectives and goals and define execution strategy • Conduct interviews and process review meetings with identified participants • Review existing relevant information provided in response to the Document Request List • Review and document existing technology and operations and begin to evaluate how they are supporting operations • Determine requirements for the business to inform any future state recommendations	• Document and validate key current and future state requirements • Analyze and evaluate opportunities for improvement, through organization realignment, process changes, or enhanced controls • Identify high risk areas • Evaluate opportunities to increase use of existing technologies and resources	• Complete assessment deliverable including: ◦ Observations and findings from discovery and analysis ◦ Gaps in existing processes ◦ Assessment of resources ◦ Considerations and recommendations for a future technology operation • Present deliverable and finalize a go forward approach / next steps

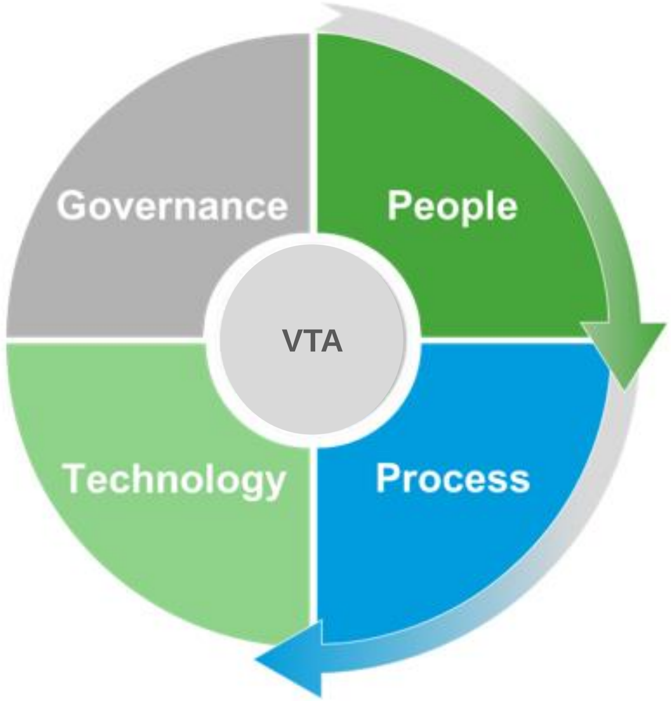
EXECUTIVE SUMMARY

Executive Summary

Business Overview

Santa Clara Valley Transportation Authority (VTA) was created in 1972 and is an independent organization that provides transportation options, such as bus, light rail, and paratransit services, throughout the Santa Clara County. Throughout this assessment our goal was to review and evaluate an IT environment with the following criteria in mind:

- Enable VTA to operate in a sustainable and cost effective way that provides high quality services to the public and strong backend IT support to the business end users
- Understand and mitigate IT system continuity risks to ensure that VTA can continue to operate within the community it serves
- Allow the authority to be flexible and innovative with a supporting and enabling technology environment supporting operations
- Ensure proper controls and tracking across VTA to mitigate risk



Executive Summary

Consolidated Recommendations

Legend

People	Process	Technology

Legend	
$	< $25,000
$$	$25,000 - $100,000
$$$	> $100,000

Ref.	Topic	Recommendation	Details	Benefits	Priority	Est. Cost
1	GEN	**Evaluate Opportunities for Strategic Outsourcing**	• Headcount has not increased at the same rate as the expansion of responsibilities of the IT department. With the current organizational structure, resources are stretched thin and there is an opportunity for strategic outsourcing or additional internal hiring aligned with bargaining requirements. • Services that are either commoditized or can easily be unplugged and moved to a third party (e.g. helpdesk, payroll) should be evaluated.	✓ Allow internal employees to focus on innovation, new projects, and strategic initiatives ✓ Increase accuracy and timeliness with commoditized options ✓ Reduce administrative burden on existing resources	**HIGH**	*TBD*
2	GEN	**Implement employee review program**	• There are no concrete performance metrics for the IT team at VTA and employees are rated on a pass/fail basis. Employee performance ratings and compensation are therefore not tied to goals and employees lack common incentives to perform well in their job functions. • The organization should evaluate options to review employees within existing guidelines, or work to adjust guidelines, in order to resolve this. • Will need to be aligned with collective bargaining cycle	✓ Increase staff engagement and performance ✓ Increase accountability with individual performance reviews ✓ Enhance quality of work completed through incentive based reviews ✓ Align personal career objectives to VTA strategic goals and objectives	**HIGH**	*Internal*
3	INFRA	**Implement a centralized password management system**	• IT is currently storing shared accounts, service accounts and logins in excel spreadsheet on file server. Spreadsheets containing passwords are restricted with read privileges and more sensitive spreadsheets are password protected. • No control of who copies or shares password spreadsheet	✓ Store & organize all your privileged identities in a centralized vault. ✓ Enable password sharing with selective users based on roles or job responsibilities, such as provisioning Windows passwords to Windows admins and database passwords to database admins. ✓ Centrally control and manage access to sensitive resources by provisioning password access to employees and vendors based on the principle of least privilege.	**HIGH**	$
4	RISK	**Upgrade SAP to S/4HANA**	• The current SAP version (ECC 6.0) should be upgraded to S/4HANA in anticipation of the discontinuation of SAP support for older products in 2025 • An upgrade to S/4HANA will also require upgrading supporting infrastructure from Oracle database to HANA	✓ An unsupported version of SAP will no longer receive updates, security or otherwise, leaving the company vulnerable to attacks ✓ Users will see benefits of the improved S/4HANA software, such as user-friendly interface, simplicity, and performance speed	**HIGH**	$$$
5	RISK	**User Access Reviews**	• User access reviews for SAP should be performed on an annual basis. The most recent user access review was completed in November 2017 and the next review is scheduled for November 2020.	✓ Increase VTA's accountability for SAP users by identifying terminated users and dormant accounts ✓ Decrease risks related to inappropriate or excessive access	**MED**	*Internal*

Executive Summary

Consolidated Recommendations

Legend		
People	Process	Technology

Legend	
$	< $25,000
$$	$25,000 - $100,000
$$$	> $100,000

Ref.	Topic	Recommendation	Details	Benefits	Priority	Est. Cost
6	GEN	**Restructure Organization to focus on Innovative Initiatives**	• Currently the CIO is responsible for leading day-to-day IT as well as the Office of Innovation. • The organization should look to break out the Office of Innovation with a new role under the CIO to serve as the Office of Innovation Lead.	✓ Clearly distinguish in tasks and budget allocations between day-to-day IT and innovative new projects in order to ensure priority is placed on each ✓ Measure investment in day-to-day "keeping the lights on" against strategic new initiatives ✓ Improved balance of resources to run and growth IT services vs those transforming the authority	**MED**	$$ - $$$
7	GEN	**Add a Cybersecurity FTE in the Legal Department**	• The organization should consider adding an FTE in the legal department dedicated to cybersecurity to segment policy and process from IT security delivery • Responsibilities include defining policies and procedures and the IT cybersecurity resource would be responsible for execution and delivery.	✓ Improve segregation of duties around security ✓ Enhance the quality of security ✓ Further mitigate risk to the business and responsibility to the IT team in the case of a breach ✓ Improved checks and balances	**MED**	$$ - $$$
8	INFRA	**Implement Multi Factor (MFA)/ Two Factor solutions for On-Prem and Cloud Services**	• MFA solutions such as DUO can be implemented with organizations On-Prem Active Directory Domain, Cloud Services and Pulse Secure VPN • Currently only a select few Admins have MFA enforced in the VTA Office 365 tenant; all accounts with elevated privileges should have MFA enforced.	✓ With the growing threat of external attacks aimed at compromising privileged accounts, Multi-Factor Authentication provides a critical layer of security to significantly reduce the chances of a security breach. ✓ MFA ensures that only authorized users and administrators are able to gain access to mission-critical accounts, computers, and other sensitive resources, even in the event where an attacker gains access to a password.	**MED**	$$
9	INFRA	**Upgrade Firewall Firmware and replace unsupported Firewalls**	• Current production firewalls have firmware over 1 year old. Firmware releases should be reviewed and implemented on a regular basis. • Cisco ASA 5500 series firewalls have been EOL/EOS and should be replaced in any production environment.	✓ New firmware often fixes bugs, contains new features, and protects your organization from security vulnerabilities. ✓ Updated and current firewalls will offer Next-Gen features that are currently unavailable to legacy firewalls	**MED**	$$
10	INFRA / RISK	**Move Disaster Recovery Site Location or leverage Cloud (AWS or Azure)**	• Current DR/Replication site is not geographically separated from production datacenter • Geographic diversity is imperative when it comes to disaster recovery planning. Primary and secondary sites should have enough distance between each other to minimize the potential for a disaster to take down both sites.	✓ Reduced risk from an systemic outage impacting event ✓ Reduce risk of a natural disaster damaging both sites simultaneously ✓ A cloud based Disaster Recovery platform will offer the organization multiple geographically diverse data centers	**MED**	$$$
11	INFRA	**Replace Legacy OS and Hardware**	• Server 2003 is still in production but has been EOL/EOS for 4+ years and should be replaced • Roughly 300 Windows 7 machines still in production and will need to be replaced or upgraded prior to January 2020	✓ Current versions of Microsoft Windows will provide the organization with platforms that benefit from security patches, bug fixes and feature enhancements. ✓ Mitigate security risks to the organization	**MED**	$$

Executive Summary

Consolidated Recommendations

Legend

People	Process	Technology

Legend	
$	< $25,000
$$	$25,000 - $100,000
$$$	> $100,000

Ref.	Topic	Recommendation	Details	Benefits	Priority	Est. Cost
12	INFRA	**Upgrade to Next-Gen Email Security**	• The organization is currently using McAfee Mail Gateway that will soon be deprecated and does not offer any Next-Gen features. • IT is recommended to review the current and potential future needs of organization and compare cloud based solutions to on premise appliance based solutions	✓ A comprehensive multi-layer protection for email communications that offers sandboxing and quarantining of any unknown files, dynamic reputation based blacklisting, advanced content analysis and pattern recognition & strong encryption and DLP for compliance and regulatory requirements	**MED**	$-$$
13	GEN	**Institute an Annual Budget Review Meeting**	• Although the budget is prepared every 2 years, the department should have an annual check in to review spend against budget and make any adjustments that may be needed. • IT systems, platforms and architecture change rapidly	✓ Extend visibility into spend against budget ✓ Increase accuracy of budget and likelihood of remaining within budget at the end of the cycle ✓ Allow for greater flexibility around unexpected expenses or adjustments	**MED**	*Internal*
14	RISK	**Patch Management**	• Currently, SAP patches are applied annually at the time of the support pack upgrade; patches should be applied regularly throughout the course of the year as updates become available	✓ Keep application up-to-date and address known vulnerabilities in a timely manner	**MED**	*Internal*
15	GEN	**Document Steering Committee Notes, Actions, and Decisions in Text Files Formats**	• Agendas are sent ahead of the Technology Steering Committee meetings and notes are recorded for ongoing retention through audio files. It is recommended that action items and key takeaways also be prepared in text format. • Minutes and notes from meetings were not readily available	✓ Ease of access ✓ Allows for key word search functionality for action items or references to specific topics of conversation ✓ More compatible format for sharing and distribution ✓ Improved team understanding of objectives	**LOW**	*Internal*
16	GEN	**Periodically Survey Business End Users to Measure IT Performance Internally**	• Although the IT team has received positive verbal feedback from business end users, the group should look to periodically survey end users to ensure they are meeting expectations. • The IT team should measure their performance against SLAs and previous surveys for continuous improvement.	✓ Allows for formal data tracking ✓ Improves visibility into performance and allows the IT team to adjust based on feedback to better meet the needs of end users ✓ Identify weaknesses and root cause of issues (e.g. headcount, experience/ training, etc.) to understand where IT and the business should focus funds and efforts	**LOW**	$

Executive Summary

Consolidated Recommendations

Legend

People	Process	Technology

Legend	
$	< $25,000
$$	$25,000 - $100,000
$$$	> $100,000

Ref.	Topic	Recommendation	Details	Benefits	Priority	Est. Cost
17	**INFRA**	**Perform Regular Internal/External vulnerability scanning and penetration testing**	• Penetration testing and vulnerability scanning is an organized approach to the testing, identification, analysis and reporting of potential security issues on a network. • An external scan will mimic how hackers on the Internet can attempt to gain access to a network. An internal scan is run from inside the network and can show the path a hacker can take once they have gained access to the network and exactly how much data they could collect.	✓ Based on the information provided, the IT team can take direct action to better protect a network and the information housed within it. ✓ Vulnerability scanning is a non-destructive form of testing that provides immediate feedback on the health and security of a network.	**LOW**	*$-$$*
18	**RISK**	**Segregation of Duties Analysis**	• Although a GRC tool is in use, a third-party SAP segregation of duties analysis should be considered to assess the current rule set	✓ Identify previously undetected SOD conflicts and improve approach to mitigating risks created by SOD conflicts	**LOW**	$
19	**RISK**	**Policy Updates**	• IT policies, such as the System Development, Configuration, and Change Management policy, should be updated annually	✓ Ensure policies are reflective of current practices ✓ Provides regular updates to stakeholders on best practices ✓ Allows for better knowledge transfer and memorialization	**LOW**	*Internal*

ORGANIZATION AND STRATEGY

Organization and Strategy

Scorecard

HEATMAP SCALE

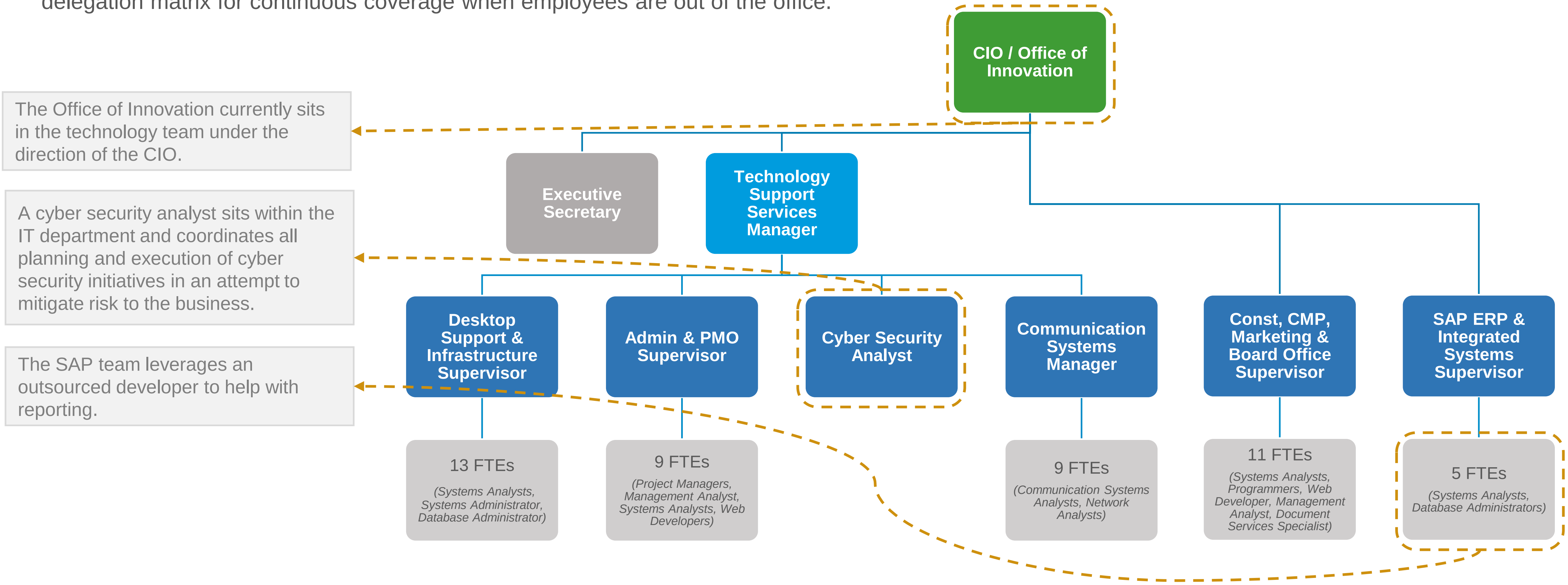
>	0%	Attention !!	🔴	>	55%	Standardized	🔵
>	22%	Attention	🟠	>	66%	Standardized+	🔵
>	33%	Basic	🟡	>	77%	Rationalized	🟢
>	44%	Basic+	⚪	>	88%	Dynamic	🟢

Area	Segment Rating	Area Breakdown	Rating	High-level Observations
Organization	🔵	Number of resources to support operations	🟦	• At the time of this report, there are 54 FTEs in VTA's IT department. • Headcount is not increasing at the same rate as the expansion of IT responsibilities in the Technology Department.
		Organization / structure	🟦	• The IT organization is currently structured into three teams beneath the CIO: Technology Support Services (36), SAP ERP and Integrated Systems (6), and CMP, Marketing, and Board Office (12).
		Education / professional certifications of workforce	🟦	• Resources within the IT department are experienced professionals with long tenure at VTA. • Our team was not able to confirm the number of professional certifications obtained by the IT department.
		Turnover	🟩	• VTA as an organization experiences little turnover with average tenure at approximately 15 years. • The organizations benefit plan is often seen as an incentive that keeps VTA from experiencing attrition.
		Accountability	🟥	• Union contracts currently do not allow performance reviews of employees beyond pass/fail. Without formal reviews, employee production is not tied back to goals or compensation and motivation can decrease.
Budget	🟢	Formal budgeting process	🟩	• There is a formal budgeting process performed every other year that involves all VTA departments. • Budgets are prepared, adjusted, approved, and formally published organization wide.
		Frequency	⬜	• A detailed budget is prepared every two years. • Reforecasts or formal annual check ins are not performed.
		Governance and controls	🟩	• The budget is signed off on by various levels of approval. • An IT steering committee meets regularly to review projects and meeting minutes are recorded.
		IT role and allotment	🟩	• IT is involved in initial preparation of their proposed budget. Although the IT team has asked for additional headcount in the past, this is not always approved.
		Abidance to budget	🟩	• Based on our conversations, it does not appear that the IT team has ever exceeded their budget allotment. • Budget to spend is reviewed on a monthly basis by the IT team.
Strategy	🟢	IT involvement in decision making	🟩	• The technology team has a seat at the table in VTA wide strategy meetings. • Members of the IT team are apart of committees that review and approve capital projects.
		Goal setting	🟩	• The IT team selects projects that align with VTA's overall goals as a business. The IT team then defines their own department goals that align with these projects. Success against goals is not formally measured.
		Project prioritization	🟩	• The technology team personally meets with members of the different business divisions to understand IT project requests. Requests are then reviewed, consolidated, and prioritized before routing for approval and funding.
		Formal feedback of IT	⬜	• Although the IT team has informally heard positive feedback from end users, there is no formal survey or feedback collected.

Organization

Current State Structure

There are approximately 2,335 FTEs beneath the GM/CEO. The Technology and Innovation Division, falling under the Business Services Department, had **54 FTEs** at the time of this report dedicated to IT beneath the CIO. Although formally defined roles are listed below, the organization has a detailed delegation matrix for continuous coverage when employees are out of the office.



The Office of Innovation currently sits in the technology team under the direction of the CIO.

A cyber security analyst sits within the IT department and coordinates all planning and execution of cyber security initiatives in an attempt to mitigate risk to the business.

The SAP team leverages an outsourced developer to help with reporting.

CIO / Office of Innovation

Executive Secretary

Technology Support Services Manager

Desktop Support & Infrastructure Supervisor

13 FTEs

(Systems Analysts, Systems Administrator, Database Administrator)

Admin & PMO Supervisor

9 FTEs

(Project Managers, Management Analyst, Systems Analysts, Web Developers)

Cyber Security Analyst

Communication Systems Manager

9 FTEs

(Communication Systems Analysts, Network Analysts)

Const, CMP, Marketing & Board Office Supervisor

11 FTEs

(Systems Analysts, Programmers, Web Developer, Management Analyst, Document Services Specialist)

SAP ERP & Integrated Systems Supervisor

5 FTEs

(Systems Analysts, Database Administrators)

Organization

Proposed Future State Structure

★ *Proposed New Position*

Based on our observations and analysis, we recommend the following adjustments to VTA's organization structure:

Recommendations

The organization should create a new group beneath the CIO dedicated to the Office of Innovation to drive strategic initiatives. Additional project management roles can fall within this role as needed.

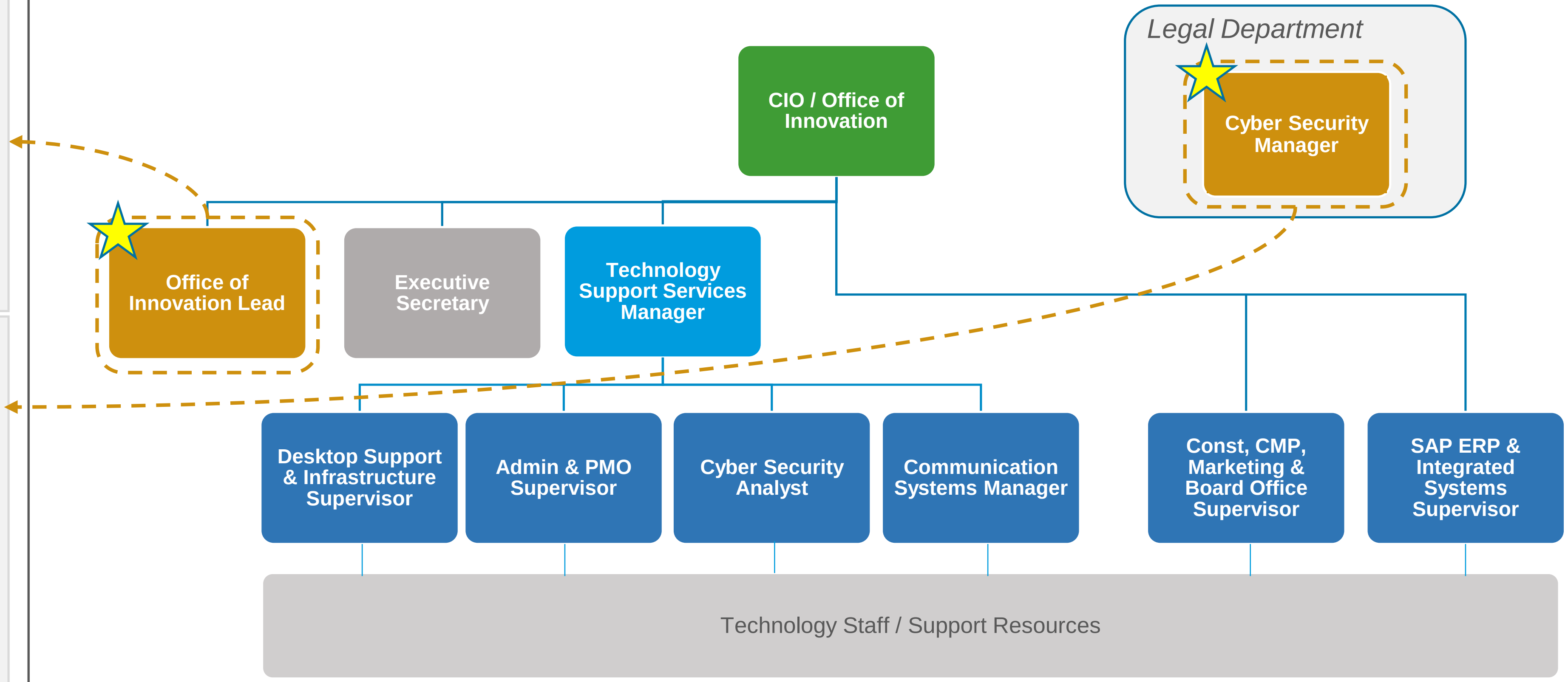
Benefits:

- Clearly distinguish investment in day-to-day "keeping the lights on" against strategic new initiatives
- Improved balance of resources to run and growth IT services vs those transforming the authority

A new cyber security position should be created to sit within the Legal Department and work alongside the cyber security professional in IT. The Legal resource should define policies and processes and monitor, audit, and assess liabilities. The parallel IT role should assist with the delivery / operational aspects of cyber security and executing on the policies and processes defined.

Benefits:

- Improve segregation of duties around security
- Enhance the quality of security
- Further mitigate risk to the business and responsibility to the IT team in the case of a breach



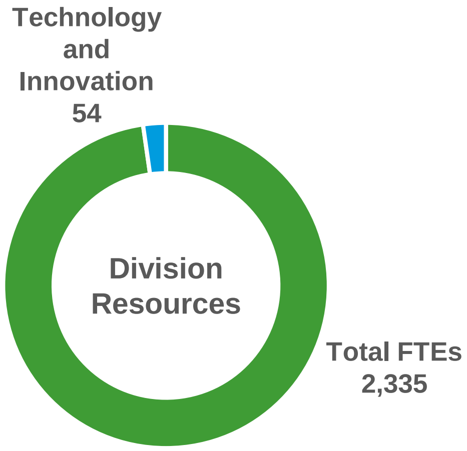
Legal Department
Cyber Security Manager
CIO / Office of Innovation
Office of Innovation Lead
Executive Secretary
Technology Support Services Manager
Desktop Support & Infrastructure Supervisor
Admin & PMO Supervisor
Cyber Security Analyst
Communication Systems Manager
Const, CMP, Marketing & Board Office Supervisor
SAP ERP & Integrated Systems Supervisor
Technology Staff / Support Resources

Organization

Observations and Recommendations

The VTA Technology and Innovation team serves as the main point of contact for all IT related issues, with the various business departments within VTA bringing issues and requests to the IT team. Responsibilities, beyond day to day support of the environment, have been continuously added to the IT team over time. In 2014 an Innovation Group was started to bring new ideas to the forefront of VTA. Since then the team has also taken on the responsibility to manage bus technology, cameras, and safety equipment; track assets; support para transit; and most recently take on logistics and coordination for the new BART program.

The VTA technology team is understaffed due to industry average benchmarks compared to State and Local Government as well as Transportation organizations. The organization does have some complications in their hiring and human resource management due to union collective bargaining agreements and restrictions due to their quasi public status. The overall turnover rate at the organization is low and the average employee tenure at VTA is approximately 15 years.



IT FTEs as a percent of employees	Gartner Benchmark	VTA	Difference
Government - State and Local	4.20%	2.31%	-1.89%
Transportation	3.90%	2.31%	-1.59%

Recommendations

- Headcount has not increased at the same rate as the expansion of responsibilities of the IT department. With the current organizational mix, resources are stretched thin and there is an opportunity for strategic outsourcing or additional internal hiring.
- VTA should evaluate the impact of outsourcing tier one IT helpdesk needs, which will allow employees to focus more on innovation and projects.
- VTA should review current shared service functions and assess opportunities to better leverage third party providers (e.g. payroll).
- There are no concrete performance metrics at VTA. Employees are rated on a pass/fail basis if a job was completed, not on the quality of work performed. Employee performance ratings and compensation are therefore not tied to goals and employees lack common incentives to perform well in their job functions. This can impact staff engagement and increase difficulty in influencing change. The organization should evaluate options to review employees within existing union guidelines, or work to adjust guidelines through further negotiation and discussion.

* *Benchmarks are sourced from the Gartner benchmarking report: IT Key Metrics Data 2018: Midsize Enterprise*

Strategy

Fiscal Year 2018 and 2019 Business Goals

VTA has defined the below goals by business line in its fiscal year 2018 and 2019 strategy*. VTA's Chief Information Officer attends the VTA meetings where overarching business goals are discussed and set for the year. The IT team then uses these goals to prioritize technology projects and set individual department goals that align for the year. Significant changes are made every two years, but goals are reviewed and adjusted annually as needed.

Faster Frequent Reliable Transit

Provide a great transit product that is faster, frequent, and reliable.

- Optimize transit travel times and ensure they are preserved and continually improve.
- Ensure that transit service, especially in core areas, is frequent (every 15 minutes or better).
- Provide customer-focused information systems and preserve and enhance reliable operations through transit-preferential treatments.

Delivering Projects and Programs

Creatively and pragmatically provide a full suite of projects and programs that address the current and evolving multimodal needs of Silicon Valley.

- Create concepts, plans, designs, programs, and policies to optimize current conditions and identify and seize new opportunities.
- Deliver projects and programs on time and within budget, and creatively pursue new construction, operational, and business practices that make VTA more efficient and successful.
- Provide a comprehensive line of services, technical support, funding programs, and mobility solutions to the public and Congestion Management Program Member Agencies.

Transportation System Management

Lead the region in transportation systems management, funding, integration, and innovation.

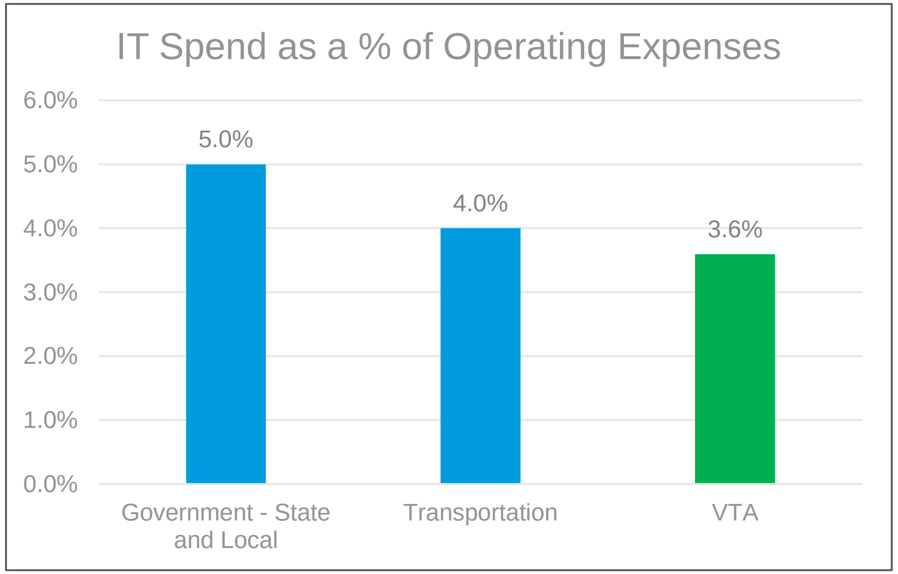
- Address roadway congestion and all modes of transportation system operations by collecting and analyzing data, developing and applying technology, refining current practices, and implementing new planning and management tools.
- Retain and increase the value of existing infrastructure and services, and optimize the utility of new investments and services.
- Improve and expand mobility options by innovatively applying technology, planning, design, construction, operations, and business techniques.

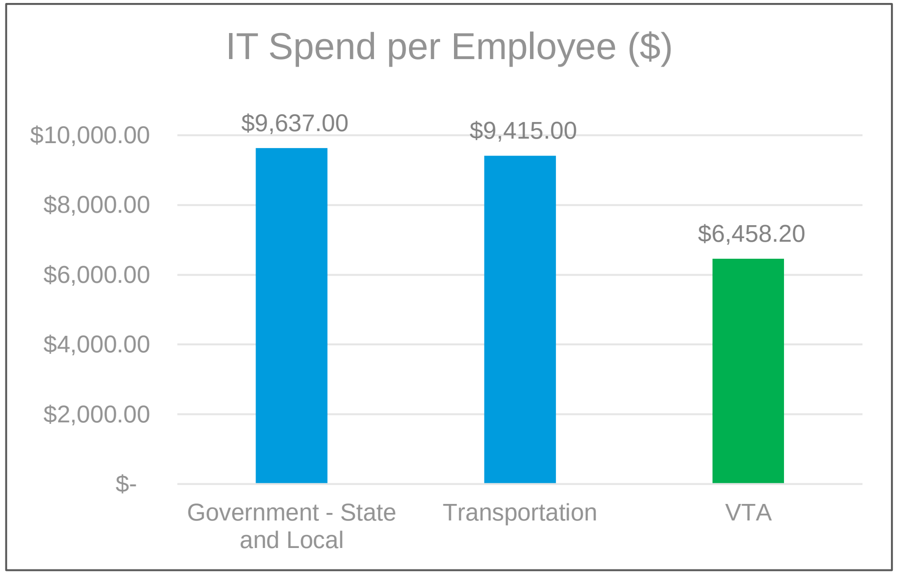
* *Contained within VTA's Adopted Biennial Budget – Fiscal Years 2018 and 2019; pages 16 & 17.*

Strategy

IT Spend v. Benchmark

Technology spend is typically broken up into four categories: day-to-day IT support (or, “keeping the lights on”), maintenance to replace equipment, enhancements to improve existing technology, and innovation for new projects and investments. A formal budgeting process occurs every two years where the budget is discussed and approved. The technology team reviews their spend against the budget on a monthly basis and reallocates funds as needed between different line items but does not overspend the total allocated amount.





Recommendations
• The technology team’s overall allocated funds are approximately 3.6% of VTA’s total operating expenses, which is slightly below industry average benchmarks. VTA should consider increasing overall spend on strategic IT initiatives to allow the technology team to sufficiently support existing operations, including the new BART program, and scale with additional future growth and innovation. • VTA should review its overall budget on an annual basis and make small adjustments as needed.

* *Benchmarks are sourced from the Gartner benchmarking report: IT Key Metrics Data 2018: Midsize Enterprise*

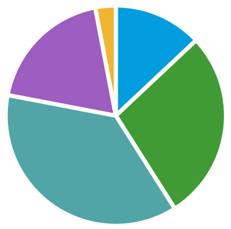
Strategy

IT Spend by Category v. Benchmark

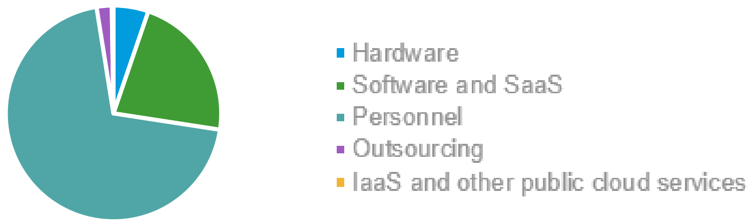
When compared with industry average benchmarks, VTA's spend is heavily skewed toward personnel expenses. This can be explained in part by minimal outsourcing and a limited investment in cloud services.

- Although benchmarks do not define exactly what each organization should be spending, they are an important tool to understand where businesses may be over or underspending in order to identify opportunities to enhance operations.
- There are opportunities to outsource commoditized services, such as tier one IT helpdesk support or payroll, that will allow internal employees to focus on more strategic, value add initiatives.
- A current trend exists in the industry with government agencies being more open to shifting to cloud based technologies which is an opportunity VTA could further take advantage of.

Gartner Benchmarks for Midsize Businesses



VTA 2019 Budget by Category



Category		FY 18 Budget	FY 18 Spend by Category		FY 19 Budget	FY 19 Spend by Category
Hardware	$	871,452	5.8%	$	791,452	5.2%
Software and SaaS	$	3,273,895	21.8%	$	3,343,868	22.2%
Personnel	$	10,317,046	68.6%	$	10,563,965	70.1%
Outsourcing	$	552,140	3.7%	$	343,000	2.3%
IaaS and other public cloud services	$	17,798	0.1%	$	37,605	0.2%
Total	**$**	**15,032,331**	**100%**	**$**	**15,079,890**	**100%**

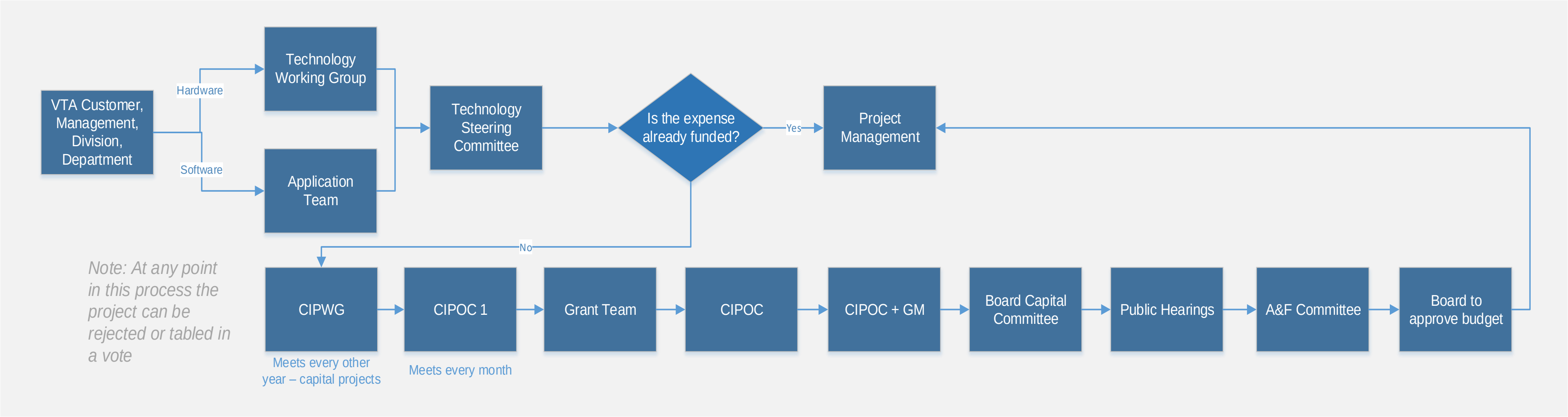
Category	Gartner Spend Benchmark	FY 18 Difference	FY 19 Difference
Hardware	13.0%	-7.2%	-7.8%
Software and SaaS	28.0%	-6.2%	-5.8%
Personnel	37.0%	31.6%	33.1%
Outsourcing	19.0%	-15.3%	-16.7%
IaaS and other public cloud services	3.0%	-2.9%	-2.8%

* *Benchmarks are sourced from the Gartner benchmarking report: IT Key Metrics Data 2018: Midsize Enterprise*

Strategy

IT Spend Governance Process

Every two years the IT team meets with various different business groups to discuss upcoming projects that they want. The IT team then organizes, consolidates and prioritizes these projects based on their business impact and how they align with the overall goals of VTA. Once the capital project list is complete, the IT team then follows the below governance process for project signoff, approval, and eventual funding through VTA's budgeting process. Off cycle projects can be proposed outside of the two year rotation but these tend to be smaller in nature. Approximately $2 million in unidentified capital is added to the budget for projects that may come up that were not planned for. Additionally, an emergency fund is available to use as needed.



VTA Customer, Management, Division, Department

Hardware

Software

Technology Working Group

Application Team

Technology Steering Committee

Is the expense already funded?

Yes

Project Management

No

CIPWG

Meets every other year – capital projects

CIPOC 1

Meets every month

Grant Team

CIPOC

CIPOC + GM

Board Capital Committee

Public Hearings

A&F Committee

Board to approve budget

Note: At any point in this process the project can be rejected or tabled in a vote

Schedule of FY 2018 & FY 2019 Appropriation
Information Sys & Technology Projects

- Emergency IT Infra Replacement
- Integrated Land Use-Transportation Model
- Mobile Network Upgrade
- Office 365 Deployment
- PCI and EMV Compliance Enhancements
- SCADA Control Center and System Replacement
- SCADA Middleware Replacement
- Survey and Data Collection Program
- Virtual Transit Ride Visualization App
- VTA Big Data Analytics Program
- VTA Gigabit Network Project

Recommendations

- The project approval process as stated above is acceptable in order to receive signoff for capital projects.
- Agendas are sent ahead of the Technology Steering Committee meetings and notes are recorded for ongoing retention through audio files. It is recommended that action items and key takeaways also be prepared in text format for easier access, sharing, and reference.
- Capital projects are weighted and scored by the Capital Improvement Ranking Committee however IT projects do not score as well due to the rating system. Operational upgrades, such as an SAP version upgrade, scores lower than projects that directly impact the business, such as the extension of a rail line into a new city. Because of the high impact IT projects have on affecting the back office, these projects should be evaluated and scored differently to better reflect their priority and impact.

Strategy

Technology Future State Vision

VTA’s technology team’s future strategic vision includes the following key initiatives:

Enhance overall business applications and leverage opportunities to shift to cloud based solutions such as SAP S/4 HANA and transitioning to hosted Microsoft Office 365.

Increase mobile capabilities through implementation of FIORI for SAP mobile capabilities and expanding mobile networks on vehicles.

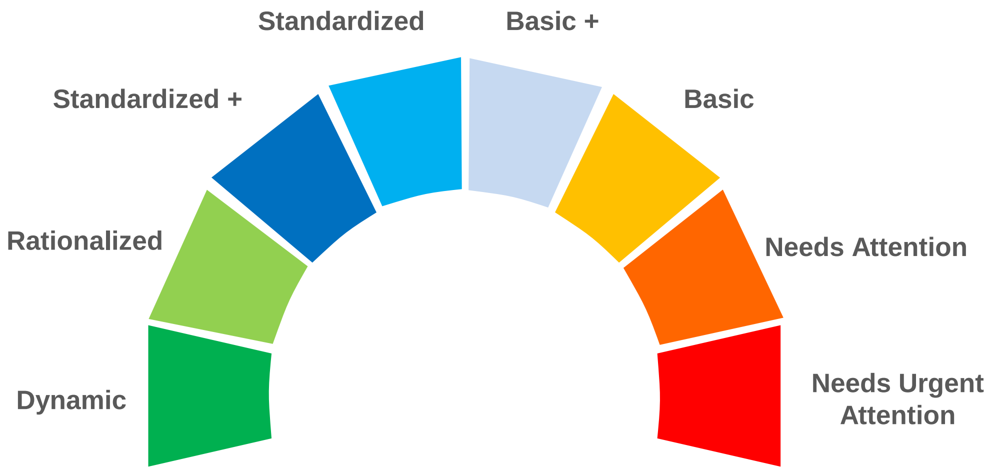
Explore and upgrade to 5G in vehicles to maintain high speed networks.

Upcoming projects will be prioritized by those that align with this strategic vision, as well as VTA’s overall goals.

INFRASTRUCTURE

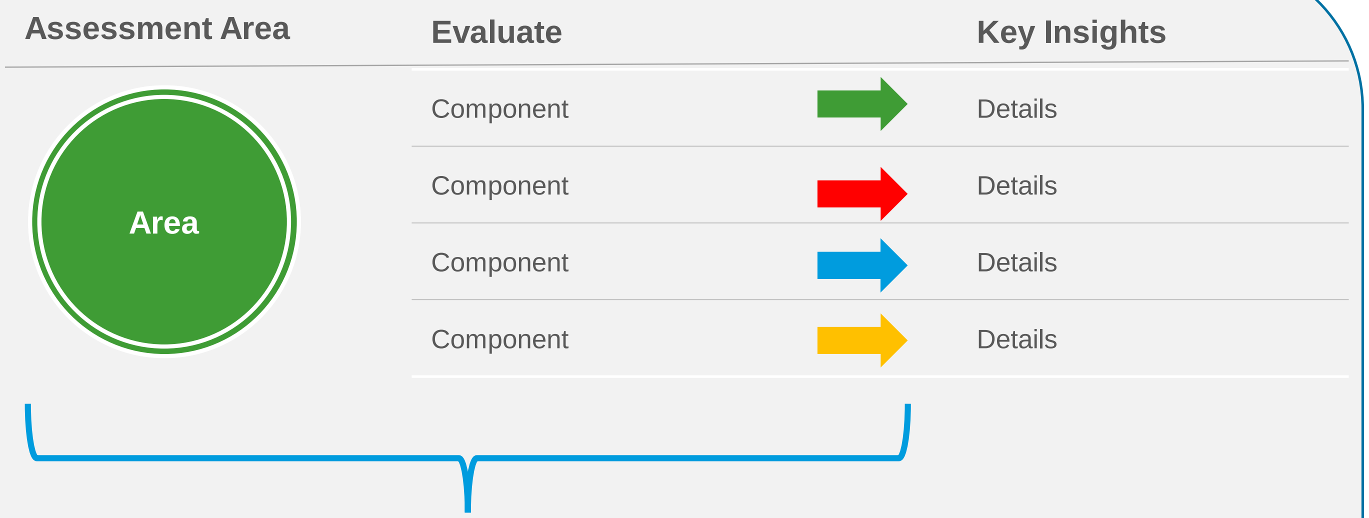
Infrastructure

Detailed Scorecard Breakdown



HEATMAP SCALE

>	0%	Attention !!	🔴
>	22%	Attention	🟠
>	33%	Basic	🟡
>	44%	Basic+	🔵
>	55%	Standardized	🔵
>	66%	Standardized+	🔵
>	77%	Rationalized	🟢
>	88%	Dynamic	🟢



Assessment Area	Evaluate		Key Insights
Area	Component	➡	Details
	Component	➡	Details
	Component	➡	Details
	Component	➡	Details

The following slides leverage the analysis findings and place against the related heatmap color coding for maturity and best practices.

Infrastructure

Overall Area Ratings

HEATMAP SCALE

>	0%	Attention !!	●	>	55%	Standardized	●
>	22%	Attention	●	>	66%	Standardized+	●
>	33%	Basic	●	>	77%	Rationalized	●
>	44%	Basic+	●	>	88%	Dynamic	●

We held meetings with the VTA Infrastructure group to discuss the below topics in detail. VTA's team was rated on a scale of 1 – 5, from poor to well managed, in each of the key areas. From these ratings a weighted average score was calculated, as shown below. A detailed breakdown of key insights and recommendations that fall within each of these areas is included in the following pages of this report.

Network	86.72%	86.5%	Perimeter
		87.1%	LAN
		83.6%	Wireless
		91.4%	VPN
Devices	81.11%	64.2%	Servers
		70.2%	Workstations
		96.4%	Virtualization
		100.0%	Storage
		100.0%	Shared
		100.0%	Printers
		100.0%	Smartphones
		100.0%	Cameras
Identity	68.47%	55.3%	Azure
		78.3%	Active Directory
		57.6%	Devices
		62.7%	Policy
Productivity	72.17%	69.8%	Productivity
		83.5%	File/ECM
		59.2%	Email
		80.0%	Collaboration

Security	75.42%	71.6%	General
		73.3%	Servers
		76.5%	Workstations
		88.5%	Identity
		40.0%	LAN
		63.4%	Perimeter
		80.0%	Messaging
Operations	75.28%	67.4%	Identity
		73.4%	Monitoring
		96.7%	Facilities
		71.1%	Organization
		69.7%	General
BCDR	85.53%	88.7%	Design
		93.5%	Operations
		43.6%	Security
Data	72.61%	75.5%	Controls
		66.7%	Classification
Strategy	92.00%	73.3%	Cloud
		100.0%	Policy

Infrastructure

Key Insights

HEATMAP SCALE

>	0%	Attention !!	🔴	>	55%	Standardized	🔵
>	22%	Attention	🟠	>	66%	Standardized+	🔵
>	33%	Basic	🟡	>	77%	Rationalized	🟢
>	44%	Basic+	⚪	>	88%	Dynamic	🟢

Assessment Area	Evaluate		Key Insights
Network	Perimeter	➡	Redundant and reliable WAN links. Speeds are sufficient for current and future needs Redundant active/active pair of firewalls at Datacenter. However older firewall models in production with aging firmware.
	LAN	➡	Good network reliability with 10Gb backbone and 1Gb uplinks. Some aging equipment but majority is recent and covered under SmartNet. No port security or network gear centralized desired state/configurations.
	Wireless	➡	Guest WiFi is segmented from corporate network and connection resets after 60 minutes, forcing user to portal to accept terms. Cisco Aironet APs with physical controller.
	VPN	➡	Pulse Secure concentrator for client VPN. Site to Site tunnels between locations and buses; approximately 60% using the 1Gb internet connections with remaining tunnels planned to be migrated.
Devices	Servers	➡	Mix of Gen 3 thru 9 HP Servers, some servers out of HP support but 3rd party provides hardware warranty. 6 total blade servers - two generation 2; four generation 1. Mix of server 2003 thru 2016 in production with 2019 in testing. Service accounts and passwords stored in excel spreadsheet.
	Workstations	➡	Roughly 300 Windows 7 Workstations still in production. EOS/EOL January 2020. In place upgrades with new SSDs underway. No encryption of hard drives of laptops or desktops.
	Virtualization	➡	Some VMWare 5.5 still in production, past the General Support End of Life data but is planned to be removed.
Identity	Azure	➡	ADFS connection with Azure. No SSO, Conditional Access Controls or Privileged Identity Management
	Active Directory	➡	AD is clean and accurate. Separate, named domain admin accounts are in place and provided to only those that have a justified need. However no MFA in place for accounts with elevated privileges.
	Devices	➡	Mobile Iron MDM/MAM solution in place. Mobile devices can reach corporate data if connected to VPN. However no enforced encryption or controls with Office 365.
	Policy	➡	ActiveSync only enabled as needed with strong passwords. Good policies on access to organization resources and device management. No enforced MFA/2FA

Infrastructure

Key Insights, continued

HEATMAP SCALE

>	0%	Attention !!	🔴	>	55%	Standardized	🔵
>	22%	Attention	🟠	>	66%	Standardized+	🔵
>	33%	Basic	🟡	>	77%	Rationalized	🟢
>	44%	Basic+	⚪	>	88%	Dynamic	🟢

Assessment Area	Evaluate		Key Insights
Productivity	Productivity	🟦 ➡	A mix of Office 2003 - 2016 with majority on 2013 through volume licensing. When user is migrated to 365 their version is upgraded.
	File & Print	🟩 ➡	Good on prem file structure. Built by division and then department. DFSR leveraged. All users have home folders. Netwrix auditor in use. No cleanup of archival data unless employee separates.
	Email	🟦 ➡	Hybrid Exchange 2013 and Office 365 in production. McAfee Mail Gateway in production but will soon be deprecated. No DMARC or DKIM. Webmail publicly accessible.
	Collaboration	🟩 ➡	Slack is in use by roughly 10 people. No use of Office 365s built in collaboration tools such as Teams or Skype for Business.
Security	General	🟦 ➡	Good physical access controls. Security Policy exists in practice in documented. Password are stored in excel spreadsheet. Defined security team is one person. Bi-annual phishing assessment.
	Servers	🟦 ➡	Production servers patched every month, 3rd Saturday of the month. Security and critical only unless specifically needed optional or SPs. Microsoft SCT not leveraged.
	Workstations	🟦 ➡	SCCM used for workstations, monthly or quarterly. Security and critical only. Windows Security Baselines used in new images. McAfee endpoint security on workstations.
	Identity	🟩 ➡	Least privilege model in use and justification and authorization needed for elevated privileges. No NextGen or Advanced Threat Detection in place currently.
	LAN	🟨 ➡	No internal vulnerability scanning is done by organization. No security assessments targeting LAN have been performed.
	Perimeter	🟦 ➡	Good firewall ruleset. Logrythm SIEM in use. No perimeter penetration testing or vulnerability scanning done by organization. McAfee web filter appliance in place.
	Messaging	🟩 ➡	Office 365 Advanced Threat Detection used in cloud and McAfee Mail Gateway used on premise.

Infrastructure

Key Insights, continued

HEATMAP SCALE

>	0%	Attention !!	🔴	>	55%	Standardized	🔵
>	22%	Attention	🟠	>	66%	Standardized+	🔵
>	33%	Basic	🟡	>	77%	Rationalized	🟢
>	44%	Basic+	⚪	>	88%	Dynamic	🟢

Assessment Area	Evaluate		Key Insights
Operations	Identity	🔵	Account provisioning and de-provisioning process in place and documented but need to be updated to include Crow Canyon and Office 365. No Identity and Access Management systems
	Monitoring	🔵	HP One View, PRTG and VMWare vRealize in use to monitor network and systems. Backup monitoring is done by email to distro group. Good outage process and communications.
	Facilities	🟢	Facilities offers IT good power, environmental and fire suppression. Power is backed up by generator and is tested regularly.
	Organization	🔵	IT Steering Committee in place. Cyber Security team consists of only one member but will pull in resources from appropriate team as needed.
	General	🔵	Current IT doc repository is file share but moving to Crow Canyon for SOPs and KBs. Org policy is to have IT team track time in tickets. End users primarily use self service portal to create tickets.
BCDR	Design	🟢	Veritas NetBackup for both Virtual and Physical workloads. Replication site is in the same geographic area and will not provide continuity in the event of a major disaster.
	Operations	🟢	No cloud based backups. Frequent failover testing with SAP to secondary location. If SAP fails at primary location there is automatic failover to replication site.
	Security	🟡	Backups run on MGMT network separate from LAN. Offsite tape backups picked up and stored with Iron Mountain. However these offsite backups are not encrypted.
Data	Controls	🔵	Control over data in cloud for users migrated to Office 365, however no control of data with the approximately 185 users remaining in Dropbox. Remaining users to be migrated to OneDrive.
	Classifications	🔵	Data mapping and classification; have a good idea of where data (tribal knowledge) but not documented formally. Plan to use Netwrix Auditor for Data Discovery & Classification in future.

Infrastructure

Key Insights, continued

HEATMAP SCALE

>	0%	Attention !!	🔴	>	55%	Standardized	🔵
>	22%	Attention	🟠	>	66%	Standardized+	🔵
>	33%	Basic	🟡	>	77%	Rationalized	🟢
>	44%	Basic+	⚪	>	88%	Dynamic	🟢

Assessment Area	Evaluate	Key Insights
Strategy	Cloud	A defined and documented cloud strategy is currently in the discovery and testing phase. Cloud services used today have published usage policies. Processes that could be digitized in the future are under further review.
	Policy	IT and Acceptable use policies are given to new hires and are signed during onboarding process. Licensing is fully compliant and checked thru self audits. SLAs for critical systems are documented.

SAP RISK ASSESSMENT

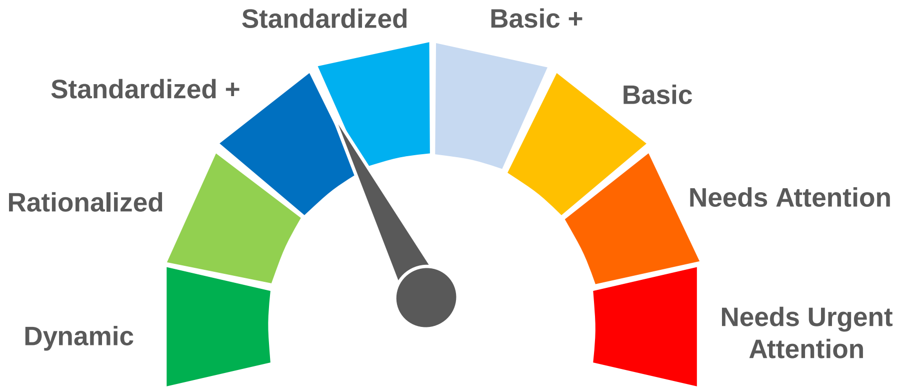
SAP Risk Assessment

IT Risk & Security Scorecard

HEATMAP SCALE

>	0%	Attention !!	●	>	55%	Standardized	●
>	22%	Attention	●	>	66%	Standardized+	●
>	33%	Basic	●	>	77%	Rationalized	●
>	44%	Basic+	●	>	88%	Dynamic	●

Overall, IT controls related to the SAP application are designed and implemented effectively however certain improvements could help to better prevent and detect risks from being exploited.



Domain	Rating	Scope Area	Rating	Comments
Logical Security	●	IT Policies and Procedures	●	• Policies and procedures exist for logical access controls • Strong passwords that meet best practice standards are required in SAP • Administrative access in SAP is restricted to authorized personnel • Access to sensitive transactions in SAP is appropriately restricted to authorized personnel • Logging of sensitive activities, especially those performed by Firefighter roles, is in place and monitored
		Passwords	●	
		Privileged Access	●	
		Logging/Monitoring	●	
Security Administration	●	Access Provisioning	●	• Access provisioning controls are designed and implemented effectively; SAP access requests are formally documented and approved based on a defied approver matrix • Access deprovisioning controls are designed and implemented effectively; an automated process is in place to disable SAP access • User access reviews are performed by personnel knowledgeable of SAP access requirements based on job function, but reviews should be done more regularly • Creation of custom roles in SAP is controlled • Formal SOD analysis should be performed to complement the use of a GRC tool
		Access Deprovisioning	●	
		User Access Reviews	●	
		Customized Access	●	

Recommendations

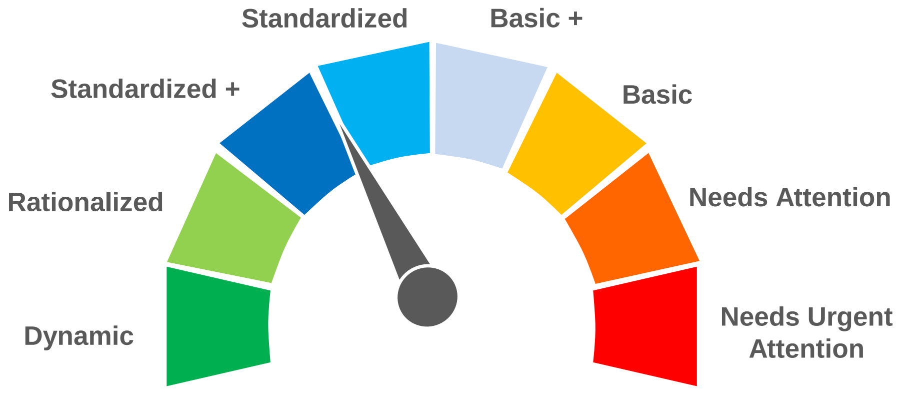
- The last SAP user access review was performed in June 2017 and the next review is scheduled for November 2020. Given the nature and size of VTA's SAP environment, user access reviews should be performed at least annually to sufficiently address risks related to terminated users retaining application access and users maintaining excess access within the application.
- A third-party analysis of SAP segregation of duties should be performed to validate the current rule set.

SAP Risk Assessment

IT Risk & Security Scorecard

HEATMAP SCALE

>	0%	Attention !!	●	>	55%	Standardized	●
>	22%	Attention	●	>	66%	Standardized+	●
>	33%	Basic	●	>	77%	Rationalized	●
>	44%	Basic+	●	>	88%	Dynamic	●



Domain	Rating	Scope Area	Rating	Comments
Change Management	●	IT Policies and Procedures	●	• Policies and procedures exist for change management but are not maintained as well as they could be • The approach to patch management should be revised to enforce more frequent patching • System development and change management process and procedures are well-defined and require formal requests, authorizations, testing, and go-live approvals for changes
		Authorization/Approvals	●	
		Testing	●	
		Change Management SOD	●	
Computer Operations	●	Backups	●	• Data backups are monitored for errors and a process is in place to identify and implement resolutions to issues • A backup data center and disaster recovery site is in place, but its close proximity to the production data center limits its usefulness in the event of a disaster • Critical system interfaces are monitored for errors and a process is in place to identify and implement resolutions to issues
		System Interfaces and Integrations	●	

Recommendations

- The early-stage upgrade to SAP to S/4HANA should be prioritized and considered a high importance strategic project for the organization. This is a large investment that will take considerable effort from a time, resources, and cost standpoint. Approvals for future phase budget allocations should be approved timely and should consider all necessary hardware and network adjacencies to as to provide for a successful and sustainable implementation.
- Additionally, as the S/4HANA upgrade project is already underway; given the long-term timeline and significant scope of the project, it should be regularly reevaluated for progress and resource requirements.
- The System Development, Configuration, and Change Management policy was last updated in September 2017. Policies should be updated annually to ensure they are reflective of current practices.
- SAP patches should be applied throughout the year as they become available to keep the application updated and address known vulnerabilities.
- An alternate solution for a backup data center should be identified due to the close proximity of the current site.

RSM US LLP
100 W. San Fernando Street, Suite 460
San Jose, CA 95113
408.5724450

www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.