



Q1 FY23 Strategic Roadmap Dashboard

January 2023

Table of contents

Overview.....	1
Progress Updates: Q1.....	1
Appendix: Strategic Roadmap Projects & Initiatives	6
Agency Privacy Framework.....	6
Cybersecurity legislation implementation	6
Enterprise Cloud Computing Program (ECC).....	7
Enterprise IT Governance.....	7
GIS Natural Hazards Mitigation (GeoPortal 2.0).....	7
Identity Access Management (IAM) Program.....	8
IT Project Oversight Transformation.....	8
Microsoft 365 Exchange Migration.....	9
Resident Portal/AccessWA Transformation	9
Security Operations Center (SOC) Modernization and Enterprise IT Security Risk Management.....	9
Security standards and policy.....	10
Small Agency IT Services.....	10
Teams Telephony migrations	10

Overview

WaTech began its strategic planning in 2019, developing the 2019-2022 Strategic Roadmap and publishing it on Aug. 1, 2019. The Strategic Roadmap is the blueprint that guides the agency's strategic goals and initiatives.

[The 2021-2023 Strategic Roadmap](#) was updated and expanded in late 2021 and takes a more comprehensive view to include all WaTech's external facing initiatives across key domains. Cybersecurity and cloud computing policies, risk and security protection/management, and the expansion, decommissioning and modernization of WaTech services are key drivers.

With the 2021-2023 Strategic Roadmap in place, WaTech will be able to accelerate the state's cloud architecture, modernize and expand services and delivery, and establish stronger security and privacy protections.

This quarterly dashboard provides progress updates on the projects and initiatives identified in the Strategic Roadmap.

Projects & Initiatives ([see Appendix for project descriptions](#))

- Enterprise Cloud Computing Program (ECC)
- Identity Access Management Modernization
- Oversight Improvement
- Enterprise IT Governance
- Resident Portal/AccessWA Transformation
- Security Operations Center (SOC) Modernization and Enterprise IT Security Risk Management
- Cybersecurity legislation implementation
- Security standards and policy
- Agency Privacy Framework
- Microsoft 365
- GIS Natural Hazards Mitigation (GeoPortal 2.0)
- Teams Telephony migrations
- Small Agency IT Service

Progress Updates: Q1

Project	July 2022	August 2022	September 2022
<p>Enterprise Cloud Computing Program (ECC)</p>	<ul style="list-style-type: none"> Identified Cloud Security Architect and signed statement of work (SOW). Scheduled workshops week of Aug. 15. Signed Amazon Web Services (AWS) Control Tower project with Operations. Identified KPIs. Received multiple vendor quotes for Cloud Center of Excellence Portal & Content (CCOE) Portal. 	<ul style="list-style-type: none"> Signed SOW with Planet for Cloud Architect augmentation and onboarded Planet and IBM resources. Completed hold workshops. Began onboarding Microsoft DSE for Azure. Contacted data owners for KPIs for analytic plan. Selected vendor and signed SOW for CCOE Portal-Governance workstream. Received quote for CCOE Portal for Governance workstream planning (Phase 2). 	<ul style="list-style-type: none"> Onboarded CCOE Portal vendor. Completed cloud strategy workshops. Completed draft statewide cloud strategy document. Completed cloud architecture MVP validation.
<p>Identity Access Management (IAM)</p>	<ul style="list-style-type: none"> Modified charter to reflect updated scope and approach. Drafted concept review. Drafted unfinanced request. 	<ul style="list-style-type: none"> Completed updates to Phase 1 schedule and budget. Completed unfinanced request and approval of Phase 1 funding. Completed final draft of Phase 1 charter and submitted to Steering Committee for approval. 	<ul style="list-style-type: none"> Completed refinement of IAM guiding principles. Completed alignment of requirement workshop content and methodology. Completed kickoff with SAW Advisory Group. Completed procurement of organization change management (OCM) vendor. Identified IAM Architect candidate.

<p>Oversight Improvement</p>	<ul style="list-style-type: none"> • Gathered feedback on organizational change management (OCM) position from HR. • Finalized and established Policy Manager position description (PD), recruitment underway. • Approved draft contractor statement of work and sent to procurement. 	<ul style="list-style-type: none"> • Finalized OCM position PD and onboarded OCM consultant. • Completed interviews and offer for Policy Manager candidate. • Completed Risk register with mitigation strategies and status. • Finalized Communication plan. • Signed and onboarded Process Blueprint vendor. 	<ul style="list-style-type: none"> • Onboarded discovery vendor, defined personas, engaged stakeholders in interviews and workshops to identify pain points. • Completed onboarding Policy Manager to the project. • Started discovery process. • Completed website launch. • Created survey and one-pager.
<p>Enterprise IT Governance</p>	<ul style="list-style-type: none"> • Launched Business Management Council (BMC) on June 30. • Completed decision package scoring criteria weighting exercise with BMC. • Approved Enterprise Security Governance (ESG) committee charter. • Began development of website/SharePoint site for all Boards, Councils and Committees. • Completed decision package scoring criteria weighting exercise with Technology Management Council (TMC). 	<ul style="list-style-type: none"> • Reviewed BMC charter for final approval. • Launched Accessibility Committee on August 24. • Decided to resume State Interoperability Executive Committee (SIEC) hybrid meetings. 	<ul style="list-style-type: none"> • Finalized Enterprise Architecture Committee charter. • Began process to integrate Geographic Information Technology (GIT) Committee into Enterprise Governance structure.
<p>Resident Portal/AccessWA Transformation</p>	<p>Project not yet active.</p>	<p>Project not yet active.</p>	<p>Project not yet active.</p>
<p>Security Operations Center (SOC) Modernization and Enterprise IT</p>	<ul style="list-style-type: none"> • Worked with Office of Cybersecurity (OCS) on what to include for this initiative. 	<ul style="list-style-type: none"> • Completed Security Operations Center (SOC) assessment with vendor BlueVoyant. Resolved nearly all issues identified in the assessment. 	<ul style="list-style-type: none"> • Leveraged RCW 43.105.450 to encourage agency accountability for vulnerability remediation.

<p>Security Risk Management</p>	<p>Enterprise IT Security Risk Management</p> <ul style="list-style-type: none"> Selected the NIST Risk Management Framework as the basis for the IT Enterprise IT Risk Management Program and the NIST Risk Assessment Methodology as the basis for the risk assessment procedure. 	<ul style="list-style-type: none"> Deployed managed vulnerability scanning service, staffing in transition. Completed fine-tuning of the Sentinel security incident and event management platform. <p>Enterprise IT Security Risk Management</p> <ul style="list-style-type: none"> Drafted the Risk Management Policy and Risk Assessment Standard for review by the 141.10 working group. 	<ul style="list-style-type: none"> Determined viability of IPS function transfer to Firewalls. <p>Enterprise IT Security Risk Management</p> <ul style="list-style-type: none"> Worked with the 141.10 working group to refine the Risk Management Policy and Risk Assessment Standard for review by the CIO/CISO community.
<p>Cybersecurity legislation implementation</p>	<ul style="list-style-type: none"> Completed development of a catalog of cybersecurity services and functions for WaTech’s Office of Cybersecurity (OCS) to perform and submitted it to the Legislature. 	<ul style="list-style-type: none"> Submitted independent assessment of IT audits report for Office of Financial Management review prior to submission to the Governor’s Office. 	<ul style="list-style-type: none"> Closed out assessment of audit project and report finalized. Worked on building out additional tasks including enterprise incident response plan.
<p>Security standards and policy</p>	<ul style="list-style-type: none"> Progressed on the Office of Chief Information Officer (OCIO) 141.10 revision as of July 11. Completed Identify section. Completed nearly all protect sections. Created content outlines and narratives for each part of the remaining three sections. 	<ul style="list-style-type: none"> Completed the Detect section of the OCIO 141.10 revision and submitted it for agency community review. Created a plan to divide OCIO 141.10 into new policies and standards to include content from the completed Identify and Protect sections. 	<ul style="list-style-type: none"> Completed nearly half of the policies and standards planned for submission to the Technology Services Board (TSB) in early November.
<p>Agency Privacy Framework</p>	<ul style="list-style-type: none"> Completed launch of Privacy Basics for Washington State Employees on July 19, 2022. Conducted Measuring Privacy - Privacy Metrics webinar for all state agencies and local governments on July 21, 2022. 	<ul style="list-style-type: none"> Used NIST Privacy Framework as guide in terms of Framework Functions Identify, Govern, Control, Communicate, Protect. Facilitated in-person Team workshop on NIST Privacy Framework model adoption (Aug. 11, 2022). Created draft based on workshop. 	<ul style="list-style-type: none"> Conducted Artificial Intelligence and Automated Decision-Making Systems Webinar Sept. 29, 2022. Launched Privacy Basics Training for State Employees; completed launch of training in the Department of Enterprise Services (DES) learning

		<ul style="list-style-type: none"> • Launched Privacy Assessment Survey Aug. 6, 2022. • Conducted Privacy Assessment Survey Walkthrough Aug. 18, 2022. • Conducted State Agency Privacy Forum on Aug. 25, 2022. 	center and published online on OPDP website.
Microsoft 365	<ul style="list-style-type: none"> • Completed operational migration of Mailboxes (with the exception of 14, which were allowed to remain on premises to accommodate application upgrades) . • Completed initial vault migrations for the Department of Social and Health Services (DSHS) - Behavioral Health Administration and Division of Vocational Rehabilitation; Department of Commerce; and Department of Financial Institutions. • Completed Washington State Patrol (WSP) draft migration assessment report. 	<ul style="list-style-type: none"> • Completed initial vault migrations for all remaining agencies. • Continued vault migration cleanup activities for Department of Corrections (DOC), DSHS, and the Department of Children, Youth and Families. • Completed WSP migration assessment. 	<ul style="list-style-type: none"> • Completed agency application upgrades and migration of all remaining mailboxes. • Completed submission of vault deletion forms to all agencies (exception DOC due to re-migration).
GIS Natural Hazards Mitigation (GeoPortal 2.0)	<ul style="list-style-type: none"> • Onboarded Dept. of Natural Resources, Military and Dept. of Health. • Finalized the onboarding documentation. • Began drafting the Organizational Change Management (OCM) plan. • Began work on System Security plan. • Approved funding for Gate operational 3. 	<ul style="list-style-type: none"> • Completed onboarding additional proviso agencies. • Refined Round 3 requirements-drafted requirements. • Commenced review of final draft of Security Design Review (SDR). • Completed draft OCM Plan. 	<ul style="list-style-type: none"> • Reviewed OCM with Steering Committee. • Finalized Round 3 requirements. • Submitted SDR for review. • Continued to test data sharing with onboarded agencies and added additional datasets as requested by Steering Committee.

	<ul style="list-style-type: none"> • Added the support request from GeoPortal 2.0. 		<ul style="list-style-type: none"> • Developed guidance for users of the system to find and use available data.
Teams Telephony migrations	<ul style="list-style-type: none"> • Developed Amazon Connect rate, support contract with SynchroNet, and presentation of Amazon Connect to the Department of Licensing (DOL). 	<ul style="list-style-type: none"> • Conducted Office of Insurance Commissioner proof of concept with Amazon Connect. Conducted customer testing and training on the Amazon Connect product. • Finalized rate, billing process and formally introduced service. • Continued review of Talkdesk product. • Discussed product with other agencies. 	<ul style="list-style-type: none"> • Finalized product introduction plan for Amazon Connect. • Marketed it to state organizations. • Determined Go/No go decision on Talkdesk product.
Small Agency IT Services	<ul style="list-style-type: none"> • Drafted decision package (DP) for adding agencies to Small Agency IT Support. • Added two agencies to Small Agency Support (Energy Facility Site Evaluation Council and Washington State Leadership Board). 	<ul style="list-style-type: none"> • Finalized Decision Package for adding agencies to Small Agency IT Support. • Finalized draft for Decision Package to extend Small Agency IT Support to four additional agencies. • Worked with Office of Public Defense (OPD) on companion DP funds to join Small Agency IT Support. 	<ul style="list-style-type: none"> • Assisted OPD with decision package to join Small Agency IT Services.

Appendix: Strategic Roadmap Projects & Initiatives

Agency Privacy Framework

Description

The Privacy Framework for State Agencies was developed based on the NIST Privacy Framework and other privacy program best practices. It is intended to be a flexible and scalable starting place for agencies of varying size handling personal information of varying sensitivity. Agencies should use this framework to build out more agency-specific resources that form a privacy program skeleton to be expanded and adapted over time. Not all agencies will have all components in place but using this framework can help identify and prioritize risks and opportunities.

Goals/objectives

- Champion Governance & Accountability
 - Strengthen IT Architecture/Security
-

Cybersecurity legislation implementation

Description

Senate Bill 5432, approved by the Legislature in 2021, established WaTech's state Office of Cybersecurity (OCS) as the state's lead organization in combatting cyber threats. The new law also required OCS to do the following:

Catalog of Services. By July 1, 2022, the OCS, in collaboration with state agencies, must develop a catalog of cybersecurity services and functions for the OCS to perform, and submit a report to the Governor and the Legislature. The OCS shall update and publish its catalog of services and performance metrics on a biennial basis. **This was completed on time.**

Report on Data Governance. The OCS, in collaboration with the Office of Privacy and Data Protection (OPDP) and the Office of the Attorney General, shall research existing best practices for data governance and data protection, including model terms for data sharing contracts, and submit a report to the Legislature by Dec. 1, 2021. **This was completed on time.**

Data Sharing Agreements. Before an agency shares or requests category 3 or higher data, a written data sharing agreement that conforms to OCS policies must be in place. This requirement does not limit audit authorities of the State Auditor. **WaTech's OPDP completed data sharing agreement templates and Data Sharing Agreement implementation guidance as resources for state agencies.**

Independent Security Assessment. The OCS must contract for an independent security assessment (assessment) of the statutorily required program audits conducted since July 1, 2015. Minimum assessment requirements are specified such as assessing the context of any audit findings and evaluating the findings relative to industry standards at the time of the audit, evaluating the state's performance in acting upon audit findings, and evaluating policies and standards established by the OCS. **This was completed on time.**

Incident Response Plan: The Legislation also requires OCS to create a model incident response plan for agency adoption, with the OCS as the incident response coordinator for incidents that impact

multiple agencies; impact more than 10,000 citizens; involve a nation state actor; or are likely to be in the public domain. This is underway, but not complete.

Enterprise Cloud Computing Program (ECC)

[Visit the project page.](#)

Description

The Enterprise Cloud Computing Program (ECCP) was created by WaTech to provide leadership, governance, guidance and resources to accelerate the strategic adoption of cloud technologies across Washington state government.

The overall mission of the ECCP is to accelerate efforts to modernize and transform the state information technology services that Washingtonians require by embracing cloud technology. This is an integral part of WaTech's efforts to create a "connected government" where residents and visitors can access state government services more easily and directly, whether it's getting a license, accessing public health resources, or bidding on a government project.

Goals/objectives

- Strengthen IT Architecture/Security
 - Transform Service Delivery
-

Enterprise IT Governance

[Visit the program page.](#)

Description

The Enterprise IT Governance framework brings together the IT and business leadership in the state to shape technology enterprise strategy, policy, standards and investments. The governance groups also drive innovation through the collaboration and sharing of technology solutions to solve business problems and transform agency services.

Goals/objectives

- Champion Governance & Accountability
-

GIS Natural Hazards Mitigation (GeoPortal 2.0)

[Visit the project page.](#)

Description

WaTech was tasked by the Legislature to develop a common data-sharing platform for public organizations in Washington to host and share sensitive natural hazards mitigation geospatial data. This project will provide consistent natural hazards data for use by state, local and higher-education organizations to support state hazard risks and resilience mapping and analysis. The data platform is expected to be available by June 30, 2023.

Goals/objectives

- Establish a reusable framework, methods and processes on future state priorities that require data sharing across agencies.
 - Implement a secure common platform for organizations to share natural hazards mitigation data.
 - Identify, categorize and publish standardized data, and establish data management and governance.
-

Identity Access Management (IAM) Program

(Phase 1 - Resident IAM Modernization)

[Visit the project page.](#)

Description

There is a recognized need across the enterprise to modernize the state's Identity Access Management (IAM) capabilities to better manage access to systems and services in a secure and seamless way. The current situation requires users to manage multiple portions of their identity across disparate state systems.

The vision of the IAM program is that Washington residents can access state digital services efficiently with confidence that their information is protected, and privacy is respected. The state reduces risk by verifying all users and authenticating all transactions while increasing digital equity and access to state services.

Goals/objectives

Phase 1 of this program will complete a successful technology Proof of Concept resulting in contracts with technology and service providers necessary to modernize IAM technology and processes for the state of Washington.

IT Project Oversight Transformation

[Visit the project page.](#)

Description

This project aims to transform WaTech's IT Project Oversight program. This transformation seeks to unlock the value, engagement, and expertise of the oversight consultants for agencies to maximize project success and mitigate risks for projects in the state's their IT portfolio.

This will be accomplished by refining the OCIO oversight process to enable scalability, higher value oversight for more complex, higher risk projects, reduced time and cost for lower risk projects and allocation of resources for highest value and maximum efficiency.

Goals/objectives

- Champion Governance & Accountability

- Transform Service Delivery
-

Microsoft 365 Exchange Migration

Description

Migration of all on premises mailboxes and associated enterprise Vault data to Exchange Online.

Goals/objectives

- Complete all remaining mailbox migrations by Sept. 30, 2022.
 - Complete all remaining Vault migrations by March 6, 2023.
-

Resident Portal/AccessWA Transformation

Description

WaTech, in partnership with other agencies and the public, seeks to transform WA.gov into a 'one-stop shop' resident portal which will provide secure and equitable access to government services and benefits to all users. The AccessWashington portal was redesigned, upgraded and rebranded as WA.gov in summer 2022 and will be continually enhanced to offer more content and features until it reaches the ultimate vision of a connected government experience.

Goals/objectives

- Vision for the Resident Portal includes a simple service finder, an authenticated user experience and integration with agency systems while providing an easy-to-use and accessible interface.
 - Focus on services that will help residents of Washington engage with state government.
-

Security Operations Center (SOC) Modernization and Enterprise IT Security Risk Management

Description

The SOC Modernization program will follow industry best practices by applying automated layered security to mitigate potential threats. This program will update the SOC team's processes and skills and ensure continuous education to address the evolution of threats, modifying and adjusting the approach of daily operations.

The Enterprise IT Security Risk Management program will apply industry frameworks to enable agencies to identify IT security risks impacting their missions and to prioritize mitigation strategies. The goal of this program is to allow inter-agency sharing of risk indicators and information in a meaningful way.

Goals/objectives

- Champion Governance & Accountability
 - Strengthen IT Architecture/Security
-

Security standards and policy

Description

Restructure and update state security polices and standards (141.10) to align with industry security program and risk mitigation frameworks. This is underway, but not complete.

Goals/objectives

- Strengthen IT Architecture/Security
-

Small Agency IT Services

[Visit the service page.](#)

Description

The WaTech Small Agency IT Services is a service tailored to small agencies within Washington state who do not have the technical staff to manage and administer technology needs and requirements. Through this model, small agencies can benefit from a centralized service that provides core technical support, equipment and administration. This service is currently available to agencies who pay the Small Agency IT Support Allocation. There are currently 17 agencies included in this program.

Goals/objectives

- Provide cost-effective IT services to all state small agencies in a standard support model that includes a full spectrum of IT skills.
-

Teams Telephony migrations

[Visit the service page.](#)

Description

Teams Telephony Migration involves migrating users off legacy Private Branch Exchanges (PBXs) such as Avaya and Nortel, onto Microsoft Teams Telephone. Although desk sets are available, most deployments consist of softphone technology being deployed to the end user's computer and/or mobile device.

Goals/objectives

- Transform Service Delivery
-