WaTech
Washington Technology Solutions

Q2 FY23 Strategic Roadmap Dashboard

February 2023

WaTech
Washington Technology Solutions

Table of contents

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: Strategic Roadmap Projects & Initiatives)

- 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
- 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: Q2

Project	October 2022	November 2022	December 2022
Agency Privacy Framework	• Completed draft of Agency Privacy Framework by end of October. Posted online on OPDP website and distributed to privacy community. • Hosted online webinar on Privacy Framework. Webinar posted online and linked in the monthly Privacy Points blog. • Completed curriculum for Privacy training workshop. • Hosted two-day workshop with state agency privacy staff on Oct. 27 and Oct. 28. Agencies that participated included DFW, DRS, LNI, HCA, DOC, HCA, and WaTech.	• Continued to refine Agency Privacy Framework Supplemental Guidance. • Presented and introduced privacy basics and privacy framework to local government community. • Started planning for Privacy Week (Jan. 23-28) activities to further promote privacy framework. • Refined Privacy Framework workshop based on feedback and lessons learned from first workshop. • Promoted workshop with privacy community and at the State Agency Privacy Forum. Second workshop scheduled for March 2 and 3.	• Passed halfway mark with Agency Privacy Framework at 58% complete. • Continued to refine Agency Privacy Framework Supplemental Guidance. • Continued planning for Privacy Week activities to further promote privacy framework. • Hosted Digital Equity panel with Information Professional Management Association (IPMA) on Dec. 6 and Privacy Community of Practice on Dec. 14. • Launched Privacy Threshold Analysis with Security Design Review.
Cybersecurity legislation implementation	• Incident Response Plan: The Legislation also requires OCS to create a model incident response plan for agency adoption.	• Drafted Incident Response Plan.	• Started Incident Response Plan review.
Enterprise Cloud Computing Program (ECC)	• Kicked off work on the Cloud Center of Excellence portal. • Hired a Cloud Architect. • Continued work on Cloud Strategy document. • Started recruitment for Cloud Business Manager and Data Analyst.	• Continued development of the state Cloud Strategy. • Interviewed for Cloud Data Analyst and short-term staff to augment the team until permanent positions can be filled. • Selected Training and Readiness vendor.	• Re-baselined program. Implementation in progress. • Sent Cloud strategy for governance approval. • Progressed on short-term resourcing. • Progressed on permanent hiring for cloud data analyst and cloud vendor specialist.

	• Completed new draft of the Cloud Capability Model (CCM). The CCM describes the types of capabilities desired. • Received vendor quotes for workforce Training and Readiness efforts.		
Enterprise IT Governance	• Continued development of website/SharePoint site for all Boards, Councils and Committees. • Integrated Open Data Advisory Group into Enterprise Governance structure on Oct. 25.	• Continued development of website/SharePoint site for all Boards, Councils and Committees. • Began integrating Cloud Program into Enterprise Governance structure. • Finalized adoption of Technology Management Council (TMC) Charter on Nov. 15. • Onboarded Business Management Council (BMC) Co-chair on Nov. 14.	• Continued development of website/SharePoint site for all Boards, Councils and Committees. • Continued integration of Cloud Program into Enterprise Governance structure. • Held Future of Governance Workshop on Dec. 9 to discuss lessons learned from 2022 and improvements for 2023.
GIS Natural Hazards Mitigation (GeoPortal 2.0)	• Drafted the Legislative report and began internal edits/review. • Completed migration to encrypted storage per Office of Cybersecurity request. • Began setup of hub site to see dataset names. • Completed draft of the organizational change management (OCM) plan for internal review. • Met with MIL and other stakeholders regarding Data Sharing Agreement (DSA) requirements.	• Completed the Legislative report, reviewed both internally and with Office of Financial Management. • Submitted an update checklist to OCS for the design approval. • Set up the draft hub site for stakeholder review. • Completed the OCM Plan and began internal review. • Presented the draft of DSA to stakeholders.	• Completed more than three-quarters of project. • Began development of the readiness checklist. • Corresponded with OCS design review team for approval. • Performed successful Quincy fail-over test. • Completed the OCM plan.

Identity Access Management (IAM)	• Determined initial stakeholder engagement approach and participants. • Identified candidate for Requirements Lead position. • Completed kickoff with the Business Management Council. • Collected initial use case data from the Department of Labor and Industries (LNI), the Department of Revenue (DOR) and the Department of Health (DOH).	• Completed initial research interviews with DOR, DOH, the Employment Security Department (ESD), and the Department of Retirement Systems (DRS). • Hired and onboarded Requirements Lead candidate. • Documented initial stakeholder engagement results. Themes and tiers established. • Refined Guiding Principles. • Completed kickoff with Technology Management Council (TMC).	• Completed remaining initial research interview with LNI. • Completed draft stakeholder engagement summary. • Established targets for requirements workshops. • Completed draft of guiding principles.
Microsoft 365	• Completed 42 authorizations to delete Vault data; 15 remain. • Completed additional pilot migrations confirming expiration date workarounds and scripting automation. • Confirmed Dept. of Corrections (DOC) re-migration will not result in additional vendor cost.	• Completed 48 authorizations to delete Vault data; 9 remain. • Completed additional validation and initiated re-migration for DOC.	• Completed 51 authorizations to delete Vault data; 6 remain. • Began processing DOC vault re-migration.
Oversight Improvement	• Began current-state and future-state discovery. • Completed current-state blueprint validation acceptance.	• Finalizing Phase 1 deliverables. • Completed Phase 1; began close-out report for Phase 1.	• Closed Phase 1. • Began Phase 2 kickoff and work sessions with Slalom (the vendor). • Developed Phase 2 charter. • Began Phase 2 organization change management (OCM) planning. • Developing Phase 2 project schedules.

Resident Portal/AccessWA Transformation	• Held initial kickoff meeting to gather information on Oct. 12. • Began development of charter.	• Updated draft charter with feedback and prepared to send for approval. • Began drafting project plan and scope.	• Completed draft charter for review and approval. • Met with other agencies/states to learn about their portals.
Security Operations Center (SOC) Modernization and Enterprise IT Security Risk Management	**SOC Modernization** • Worked with state agencies to meet OCIO policy requirements and report on the status of efforts and improved risk scores to the Office of Cybersecurity (OCS). • Began Proof-of-Concept (POC) testing of the Intrusion Prevention System (IPS), working with Network Services' lab to determine threshold of effective throughput. **Enterprise IT Security Risk Management** • Continued refinement of the Risk Assessment Standard.	**SOC Modernization** • Reported Risk Scores on a weekly basis and reminded agencies that OCS is obligated by state law to deliver a quarterly report to the state Legislature, and annually to the Governor for agencies that fail to meet policy. • Modeled real traffic for stress testing, adding new traffic sources weekly. Collected test results from the Network Services Division (NSD). **Enterprise IT Security Risk Management** • Completed refining Risk Management Policy by 141.10 workgroup	**SOC Modernization** • Completed 65% of the security technology and process improvement effort. • Continued stress testing and provided results to the SOC and NSD. Timeframe was extended to allow for additional traffic sources to increase stress conditions. **Enterprise IT Security Risk Management** • Continued refinement of the Risk Management Policy.
Security standards and policy	• Completed 16 out of 25 policies/standards.	• Incorporated feedback on the Data Classification and Data Sharing documents. • Continued work on remaining policies.	• Prepared five documents for state CIO and Enterprise Security Governance council review. The Technology Service Board security subcommittee review was planned for January 2023.
Small Agency IT Services	• Continued working with prospective agencies on plans to join service.	• Continued working with prospective agencies on plans to join service.	• Continued working with prospective agencies to join service. Had discussions with Board of Volunteer Firefighters and Reserve Officers (BVFF) and Washington Health Care Facilities Authority (WFCFA).

Teams Telephony migrations	• Continued with Office of Insurance Commissioner (OIC) product familiarization. • Completed product introduction for Amazon Connect, market to select state organizations. • Completed project kickoff for customer billing system.	• Built account for OIC to begin Connect service and manually bill for usage. • Completed terms of service (TOS), Web Page and Operational Support System components, began testing billing system.	• Finished service integration and rolled out product for general consumption. • Began work on Dept. of Licensing application.

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 layered security to mitigate potential threats. This program will update the SOC team's equipment 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
141.10 update. Restructure and update state security polices and standards 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
