Security Design Review

Last updated 12-05-22

The state Office of Cybersecurity (OCS) Security Design Review process provides agencies with a security assessment of their new or updated systems. OCS works with agencies to validate that their security controls and processes are in compliance with the state's IT security policies and standards.

Security design reviews are required when an agency project or initiative requires Office of Chief Information Officer (OCIO) oversight; when an agency project or initiative creates risk to state assets outside the agency; or when required by an agency's IT security program (OCIO IT Security Standard 141.10, Section 1.2.1). Examples of systems that require review include but are not limited to cloud-hosted or internet-available systems.

Intended customers

Agencies required to submit projects for review are those that must comply with the state IT security standard OCIO 141.10. This includes Washington executive branch agencies, and agencies headed by separately elected officials. Legislative and judicial branches, as well as higher education institutions, are exempt from OCIO 141.10 and are not required to utilize the security design review process. The security design review team performs more than 150 reviews a year.

Options available with this service

The security design review process allows agencies to engage with OCS at different stages of planning and development, providing clarity on security-related issues if needed and positioning the project for compliance assessment. An agency can request a workgroup session with WaTech subject matter experts, including at OCS, to discuss compliance and architectural options to solidify approaches prior to formal review. Agencies that don't require a workgroup session can submit a project for review by completing and submitting a security design review checklist.

Helpful information

Service category
Security

Service availability
Business hours

Planned maintenance
Not applicable

Related services
Security design reviews are commonly required prior to the implementation of enterprise services such as single sign-on integration using Active Directory Federation Services or Azure Active Directory and deployments using the Cloud Highway.

How to request service
Submit a request for service through our Customer Portal.

Service owner
Matt Stevens

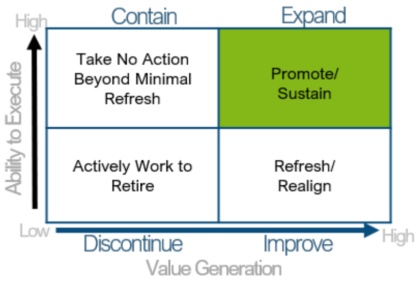
Customer engagement

- WaTech holds a weekly call with agencies' chief information officers and chief information security officers where security topics and services, including security design review process improvements, status updates and future goals and objectives are discussed.
- WaTech meets monthly with state agency security leadership as part of the enterprise security governance process.
- WaTech has established an enterprise security governance workgroup for security design review that meets quarterly.
- Monthly Technology Management Council (TMC) and Business Management Council (BMC) meetings for agency CIOs and IT leaders to inform and sponsor enterprise strategy, policy and investments.
- Regularly scheduled meetings between customers and Business Relationship Managers (BRM) to connect, advise, address concerns and provide solutions.
- Regular outreach to solicit feedback, provide updates and inform agencies on emerging projects, initiatives, and services.

- Requests for new consultations and modifications to existing applications.

Action plan

Current activity



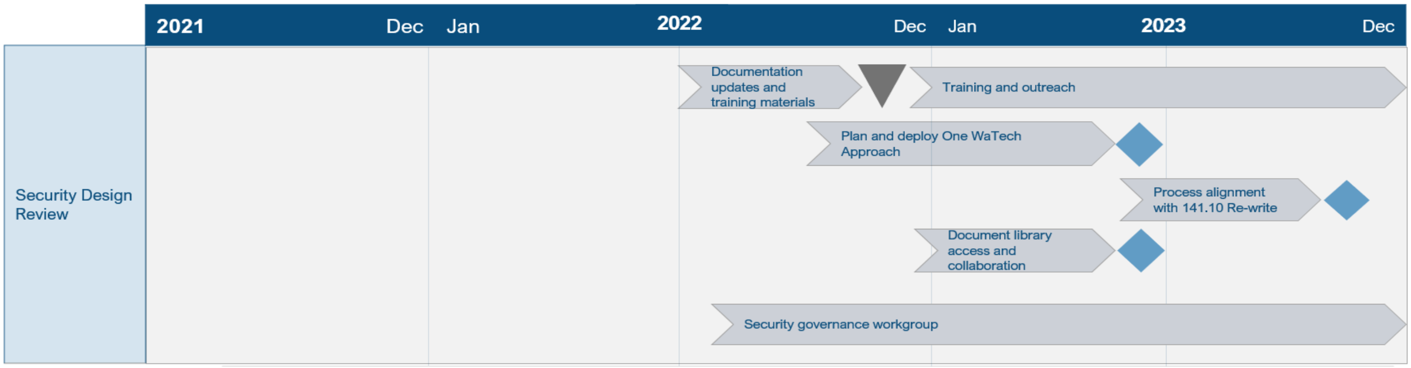
- Assembled a multidisciplinary team to perform an extensive process review of the security design review service. The goals of this effort were to modernize the process, increase efficiency and align security review with the mission and functions of other key WaTech teams to establish a “One WaTech” approach that establishes a holistic design review method linking complementary oversight and consultative activities at WaTech.
- Resulted in the creation of a three-phase improvement plan for security design review that will be implemented over the next 18 months.

One- to two-year goals

- Implement agency access to security design review Teams sites which contain status information, current and historical artifacts and reviews, and provide chat and collaboration features to enhance communication.
- Address the security design review backlog through a combination of process improvements and increased capacity by filling open positions and using contract staff.
- Enhance agency awareness of the design review process and expectations to enable a thorough and timely review.
- Update security design review processes to incorporate changes resulting from the OCIO 141.10 re-write that aligns state security standards with the NIST Cybersecurity Framework.
- Define an SLA which contains key performance indicators and standard review processing timelines to facilitate planning and assessment of security design review process by agencies.

Three- to five-year goals

- Refine security review processes to gain further security benefits and efficiencies as the “One WaTech” approach matures over time.
- Utilize fully online submission and processing of security design reviews.
- Create benefits and positive outcomes via enhanced data visibility and reporting of security review activities to drive data-driven assessments and decisions by WaTech and agencies.



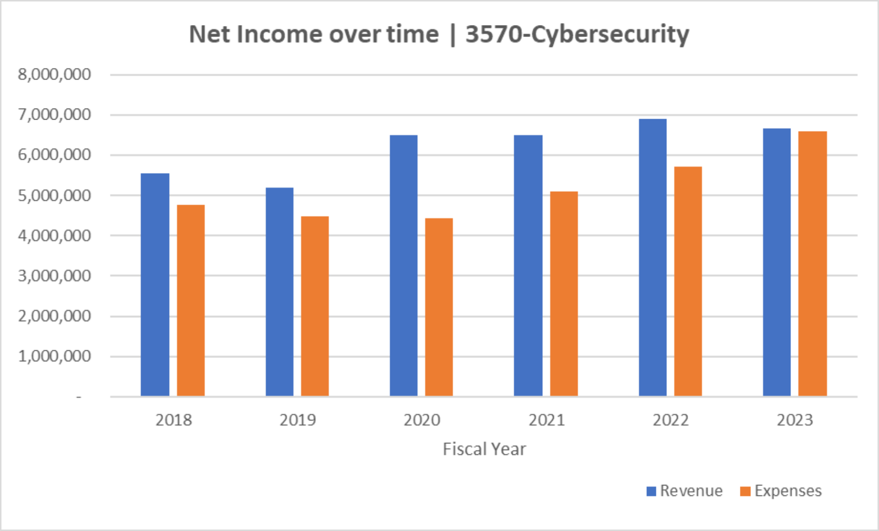
Service review and fully loaded service budget projection

Revenue source

The service is bundled and funded using revenue from the OCS central service model, which was established to ensure consistent funding for cybersecurity policy and technology leadership for state government, as well as to promote cooperation with regional and national governments and corporations. Agencies with 50+ FTEs pay a yearly base fee of

$2,000. The remaining cost is allocated based on the agency's number of budgeted FTEs. OFM maintains the source data for budgeted FTEs.

Net income over time


Net Income over time | 3570-Cybersecurity
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
-
2018
2019
2020
2021
2022
2023
Fiscal Year
■ Revenue
■ Expenses