# Cybersecurity Risk Assessment

The Cybersecurity Risk Assessment service targets the need for a consistent, repeatable assessment methodology. Organizations use cybersecurity risk assessments to identify, estimate and prioritize risk resulting from the operation and use of information assets. The purpose of cybersecurity risk assessments is to inform decision-makers and support risk responses by identifying the potential impact of a threat exploiting an information system. The assessment opens with a definition of its scope and collection of organizational and information systems information. It ends with the submission of a report of risks prioritized by impact, and mitigation recommendations.

The risk insights provided by this service enables users to:

- Inform their mission strategy.
- Prioritize security investments and resources.
- Ensure their security programs address organizational risks.
- Align with state security standards.

Performance Metrics:

- Number of risks identified per agency.
- Number of risks that became issues.
- Number of risks that became issues more than once.
- Time to remediate risks.
- Percentage of risks mitigated.

## Intended customers

This service is intended for state agencies lacking the resources or expertise to perform a cybersecurity risk assessment. There are currently 188 agencies that will benefit from the risk assessments the Policy and Program Management team will perform. The Office of Cybersecurity will use findings from the assessment to manage statewide risks.

## Customer engagement

- The Office of Cybersecurity (OCS) will provide cybersecurity assessment guidance and supporting tools to all agencies. It will engage agencies through the Cybersecurity Risk Management program to validate the assessment of cybersecurity risks and the associated treatment plans.
- OCS will hold workshops to familiarize agencies with the cybersecurity risk assessment and management methodologies.
- Monthly Technology Management Council (TMC), Business Management Council (BMC) and Enterprise Security Governance (ESG) 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.
- Weekly group calls for state CIOs and CISOs to provide updates on important and immediate issues and actions.
- 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.

## Helpful information

### Service category

Security

### Service availability

24/7/365

### Planned maintenance

Performed as required during non-peak hours.

### Related services

The security risk assessment service leverages information from the vulnerability assessment service, threat information from the Security Operations Center and insights from MS-ISAC/CISA national security advisories. Other inputs include:

- Security Design Review reports conveying system-level risks of applications used by agencies.
- Nationwide Cybersecurity Review reports describing agency control inventories.
- Application and infrastructure Inventories.

### How to request service

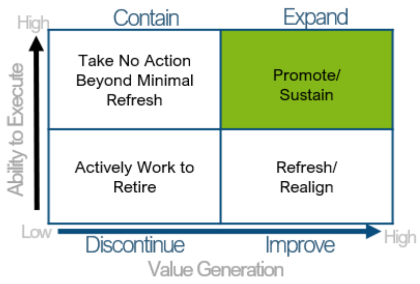
Submit a request for service through our Customer Portal.

### Service owner

Stevens Fox

# Action plan

## Current activity



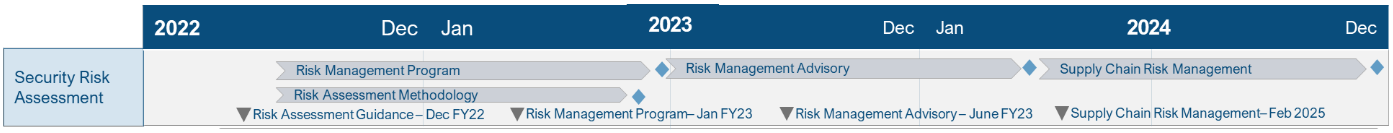
- OCS will develop the cybersecurity security risk assessment program based on the NIST SP 800-30 Guide for Conducting Risk Assessments.
- Promotion of the service will occur via the Cybersecurity Risk Management Workgroup and recorded educational sessions.
- OCS will launch a pilot of the risk assessment service by the end of Q1 2023.
- Review of pilot assessment artifacts will inform finalization of the risk assessment service.

## One- to two-year goals

- Build a statewide cybersecurity risk management program to consolidate risk information into a dashboard focused on state-wide risks.
- Ensure that agencies use a risk register to track agency-level risks and risk treatment plans.
- Implement a Governance, Risk, and Compliance tool which will provide agency and state-level risk reporting, tracking of compliance with information security requirements, and facilitate an agency's risk management program.
- Identify cybersecurity risk metrics for reporting via a statewide risk management dashboard.
- Build consultative cybersecurity risk management advisory practice that will advise agencies on risk treatment options based on an analysis of their risk posture.
- Provide opportunities for shared learning on risk management across the State.

## Three- to five-year goals

- Integrate Cybersecurity and Enterprise Risk Management to enable the management of supply chain risks.
- Ensure that agencies monitor Key Risk Indicators in order to take action on potential risks before they come issues.
- Share Key Risk Indicators between agencies with a common mission, aka Communities of Practice.
- Ensure that agencies use risk management as a basis for strategic decision making.

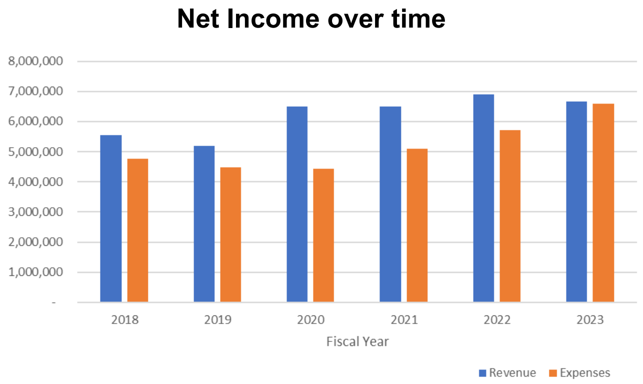

2022
Dec
Jan
2023
Dec
Jan
2024
Dec
Security Risk Assessment
Risk Management Program
Risk Management Advisory
Supply Chain Risk Management
Risk Assessment Methodology
Risk Assessment Guidance – Dec FY22
Risk Management Program– Jan FY23
Risk Management Advisory – June FY23
Supply Chain Risk Management– Feb 2025

# Service review and fully loaded service budget projection

## Revenue source

The service is bundled and funded using revenue from the Office of Cybersecurity (OCS) central service model.

The OCS central service model was established to ensure consistent funding for cybersecurity policy and technology leadership for state government, as well as to promote cooperation and coordination between regional and national governments and corporations.


Net Income over time
Fiscal Year
Revenue
Expenses