Commonwealth of Massachusetts

Executive Office of Technology Services and Security (TSS)

Cybersecurity

Enterprise CISO Council and Risk Heat Mapping Initiative

July 1, 2025 - June 30, 2026

Tony O'Neill, Commonwealth CISO & Chief Risk Officer
(Anthony.Oneill@mass.gov)

EXECUTIVE SUMMARY

As government operations become increasingly dependent on mission-critical digital services, the Commonwealth recognized the need for a unified enterprise approach to identifying, assessing, and prioritizing risk. Historically, agencies managed cybersecurity and operational risk independently, resulting in inconsistent methodologies, limited enterprise visibility, and challenges communicating operational impact to executive leadership.

To address these challenges, the Commonwealth re-oriented and strengthened its Enterprise CISO Council composed of Secretariat-level CISOs, risk and security leaders. The Council created a standardized framework to identify critical business applications and government assets while assessing associated security, technology, and operational risks through enterprise risk heat maps.

Since implementing the strategy, the Commonwealth has achieved enterprise-wide participation across Secretariat organizations, standardized risk terminology and scoring methodologies, completion of agency-level risk heat maps, improved identification of critical business assets and operational dependencies, and greater executive engagement in cybersecurity and operational risk management.

The initiative established a sustainable governance model supporting continuous reassessment of emerging risks and enterprise resilience priorities.

IDEA

What problem did the project address?
The Commonwealth lacked a consistent enterprise approach for identifying and prioritizing cybersecurity, technology, and operational risks across Secretariat and agency business lines. Agencies managed risk independently, making it difficult to align priorities, identify systemic vulnerabilities, and communicate operational impact to executive leadership.

To address this challenge, the Commonwealth established an enterprise CISO Council composed of Secretariat-level CISOs and security leaders. The Council developed a standardized methodology for identifying critical business applications and government assets, then assessing associated threats, vulnerabilities, operational impacts, and mitigation strategies through business-aligned risk heat maps.

Why does it matter?
Government services increasingly depend on mission-critical digital platforms. Disruptions to these systems can directly impact residents' access to essential services, including healthcare, transportation, workforce services, public safety, and constituent support.

This initiative improved:

- Enterprise visibility into risk exposure
- Prioritization of cybersecurity investments
- Cross-agency collaboration and governance
- Executive understanding of business risk
- Operational resilience planning

Without a unified framework, agencies would continue operating with inconsistent methodologies and limited enterprise coordination.

What makes it different?
The initiative shifted cybersecurity governance from a technology-focused exercise to a business-driven operational risk framework. Rather than starting with technical assets alone, agencies identified critical business functions and mapped supporting systems, operational dependencies, threats, and mitigation strategies.

The project also created a sustainable governance model through recurring CISO Council collaboration and standardized enterprise risk practices.

What makes it universal?
All states face increasing cyber threats, distributed agency environments, and resource prioritization challenges. This framework is scalable, governance-focused, and adaptable regardless of agency size or technical maturity.

The initiative aligns with the following national and state priorities:

- Cybersecurity and risk management
- Enterprise governance
- Operational resilience
- Cross-agency collaboration

IMPLEMENTATION

What was the roadmap?
The initiative was implemented over a one-year period through four phases:

1. Establishing the enterprise CISO Council governance structure
2. Developing standardized risk heat map methodologies
3. Conducting agency-level risk identification and assessment workshops
4. Consolidating enterprise findings and establishing ongoing governance processes

Who was involved?
Participants included cross-functional enterprise employees comprised of the following:

- Enterprise CISO and risk leadership
- Secretariat CISOs
- Agency security teams
- Technology operations leaders
- Business and operational stakeholders

Buy-in was achieved through collaborative workshops, executive engagement, and alignment of cybersecurity priorities with operational mission delivery.

How was it implemented?
The project leveraged existing enterprise leadership and agency expertise rather than large technology investments. The focus was on creating a repeatable governance framework supported by:

- Standardized risk assessment templates
- Shared scoring methodologies
- Business application inventories
- Executive reporting mechanisms

The initiative emphasized enterprise consistency while allowing agencies flexibility to reflect unique operational missions.

IMPACT

What did the project make better?
The project transformed how agencies identify, communicate, and prioritize risk across the enterprise.

Before implementation:
- Risk methodologies varied by agency
- Critical business assets were inconsistently identified
- Cybersecurity discussions were primarily technical
- Enterprise visibility into operational risk was limited

After implementation:
- Agencies adopted a common enterprise risk framework
- Mission-critical applications and services were systematically identified
- Risk discussions became business-focused and operationally relevant
- Executive leadership gained improved visibility into enterprise exposure
- Mitigation strategies became more strategic and prioritized

How do you know?

Key outcomes included:

- Enterprise-wide participation across Secretariat organizations
- Completion of agency-level risk heat maps
- Standardized risk terminology and scoring methodologies
- Improved collaboration among CISOs and operational leaders
- Enhanced executive engagement in cybersecurity and operational risk management

The CISO Council's focus on asset identification broadly impacted and scaled the Commonwealth's ability to remediate cybersecurity vulnerabilities. Members of the Council worked directly with the Commonwealth Security Operations Center (SOC) and the Enterprise Risk Management Office (ERM) in partnership to significantly reduce cybersecurity vulnerabilities. In calendar year 2025, the SOC handled over 41,000 security events across the Executive Branch. Over 400,000 vulnerabilities were mitigated, a figure that constitutes a 26% increase over calendar year 2024. In concert with these remediation efforts, the SOC took action to quarantine over 88K e-mail messages before they could be opened.

From a July 2025 baseline we have averaged over 5,000 more mitigated vulnerabilities per month than have been discovered, and our velocity, the ability of the team to mitigate a vulnerability within 30 days from discovery to closeout, has also risen year-over-year, at a rate higher than discovery of new vulnerabilities, indicating we are now resolving more issues than we are finding. Further, the Council worked collaboratively to remediate the number of critical vulnerabilities - a severe flaw in a system's hardware, software, or design that can be easily exploited by malicious actors - by 20%.

By joining together and seizing on the opportunity to force multiply, vulnerability management has now expanded to include the identification and mitigation of operational technology and interconnected device vulnerabilities. Operational technologies represent IP enabled utilities like lights, HVAC, and water that are now connected to networks which provide administrative benefits for our building managers but also could introduce cybersecurity risk. Recognizing that every connected device is an open door, the Commonwealth used this opportunity to execute its strategy to reduce the risk of threat actors walking through those doors.

Testimonial
“The initiative enabled us to connect cybersecurity risks directly to operational business impact, helping executive leadership prioritize investments based on mission delivery and resilience rather than purely technical concerns.”

— Tony O’Neill, Commonwealth CISO & Chief Risk Officer

What now?
The CISO Council and risk heat mapping framework are now part of the Commonwealth’s ongoing enterprise governance strategy. Future efforts include the following:

- Continuous reassessment of critical government assets

- Expansion of operational resilience planning
- Enhanced enterprise reporting and dashboards
- Integration with broader enterprise risk management initiatives

This initiative established a sustainable, scalable governance model that strengthens the Commonwealth's ability to protect critical services and improve operational resilience for the long term.