Risk and Remediation Tracking System

Project Initiated: March 2016
Project Completed: June 2016

Category: Cybersecurity

Nomination Submitted by:
Robert Samson
Chief Information Officer
New York State

Contact:
Giovanna Joseph
ITS Recognition Coordinator
NYS Office of Information Technology Services
Giovanna.joseph@its.ny.gov
518 – 427 - 9750

Risk and Remediation Tracking System
Category: Cybersecurity

EXECUTIVE SUMMARY

The New York State Chief Information Officer and Office of Information Technology Services (ITS) has been charged with improving New York State's decentralized approach to administering IT services across the state enterprise. Over the past several years, ITS has actively been implementing solutions to manage IT systems more efficiently and effectively, and share resources to meet increasing demands and lower statewide operating costs.

One of the top priorities for ITS is managing risk and protecting citizen and critical agency data against cyber-attack. The ITS Enterprise Information Security Office (EISO) is responsible for protecting the State government's cyber security infrastructure and providing Statewide coordination of policies, standards, and programs relating to cyber security, and tracking risks and remediation efforts.

The Risk and Remediation Tracking System evolved out of the need for an efficient and comprehensive strategy to: a) identify high-risk, priority applications; b) establish security baselines and conduct risk assessments; c) collect critical asset inventory information and documentation; d) record and prioritize risks; e) track remediation efforts across the enterprise, and, e) support analytics and reporting requirements.

Using available enterprise technologies to expedite delivery and avoid costs, the team designed an innovative assessment tools, e-forms, centralized repository workflows, a unified control matrix, remediation tracking processes and reporting dashboards to enhance inventory visibility, and support risk assessments, resiliency and disaster recovery capabilities.

The Risk and Remediation Tracking System facilitates efficient and effective security risk assessments through comprehensive risk assessment processes. It supports collection and validation of critical application asset inventory data and documentation needed to support security, resiliency, disaster recovery and other operational objectives. The system also helps analyze identified risks and track remediation efforts.

Prior to this initiative, risk management and remediation efforts were inconsistent and labor-intensive. Critical application information was often unavailable or insufficient to support operational and incident response needs. Now, conducting combined assessment interviews informs and supports all team needs and reduces impact on agency resources.

The system has streamlined processes, consolidated data gathering and automated workflows, reports and dashboard features, which have helped save hundreds of hours of staff time and resources. Overall, the Risk and Remediation Tracking System has resulted in enhanced operational resiliency and improved agency service levels, all while saving money for New York State, benefiting citizens and ITS as a whole.

Risk and Remediation Tracking System
Category: Cybersecurity

CONCEPT

ITS is responsible for maintaining thousands of applications, enterprise core services, and the large and complex technology asset base and underlying critical infrastructure that supports mission-critical State agency and citizen functions.

ITS' EISO Governance, Risk and Compliance (GRC) unit's functions include promulgating State security policy/standards, guiding secure system design, performing security assessments of systems and critical infrastructure, and managing risk remediation efforts.

The development of the **Risk and Remediation Tracking System** arose from the efforts to solve two key problems:

- EISO needed a reliable security assessment process to evaluate business, technical and operational security risks, and enable analysis, reporting and prioritization of enterprise and cluster remediation efforts and investments.

- Multiple ITS units needed access to priority application asset information to support operations, incidents and disaster recovery. Parallel projects were underway to engage clusters and agencies, collect data and documents pertaining to applications. Proceeding in silos would have resulted in duplicate efforts and information storage.

Recognizing the opportunity to streamline data collection and assessment initiatives through consolidated efforts, GRC formed a Collaborative Assessment Team (CAT) comprised of members from EISO, ITS Resiliency, Disaster Recovery, and Rationalization project teams. The team collaboratively developed a comprehensive question set to capture asset data and documentation necessary to support application security risk assessments, operational resiliency and disaster recovery.

Centralizing and standardizing data collection and storage: a) eliminated duplication of effort; b) standardized and centralized data collection; and, c) provided assurance that these various initiatives were looking at the most current documents and data; and leveraged automation to detail, prioritize and report risk remediation actions.

The **Risk and Remediation Tracking System** utilizes enterprise technologies to help expedite delivery and minimize costs:

- Microsoft O365 SharePoint and InfoPath form the system's core, enabling efficient data collection and risk assessment processes, e-forms and automated workflows.
- Microsoft .Net was used to automate summary reports and action plans, and push gathered data into enterprise asset inventory repositories (Enterprise Elements and ITSM Service Now).

Risk and Remediation Tracking System
Category: Cybersecurity

- BMC Atrium Discovery and Dependency Mapping enables hardware, software, configuration, and relationship and dependency details to be efficiently gathered and automatically updated in Enterprise Elements and Service Now ITSM.
- Microsoft O365 Excel and Power BI provide integrated data analytics and business intelligence features that support risk analysis, heat-map views, dashboards and reporting features, to round out this comprehensive and innovative solution.

The **Risk and Remediation Tracking System** is intuitive, menu-driven and designed for ease of use. The assessment module tools can be used online and offline to facilitate field assessment activities and analysis. Asset information is pushed to central asset repositories, along with auto-generated knowledge articles to aid operational support and incident response.
The resulting process produces a comprehensive asset date set and application security risk profile comprised of three separate risk indices – business, technical and operational risk. Data analytics and business intelligence functionality supports visualization of risk, metrics, and reporting requirements.

Standardized processes and automation reduce the time to affect an application risk assessment by 75%, saving considerable time, avoiding duplication and ensuring consistency. Enterprise solutions and platforms are secured and supported as a core enterprise services platform. A “private” SharePoint site ensures assessment information is secured and access restricted to authorized individuals only.

Remarkably, defining, designing, testing and launching the core system and related workflows took EISO staff just three months to accomplish! Requirements, design and development commenced in March 2016, the system was launched in June 2016, and the cost was $75,000 in staff time.

Risk and Remediation Tracking System
Category: Cybersecurity

SIGNIFICANCE

The **Risk and Remediation Tracking System** is an innovative, integrated system of sound security risk management process building blocks, and readily available enterprise technologies and services. The system is intuitive, menu-driven and designed to assure ease of use across multiple user groups.

Prior to this initiative, risk management and remediation efforts were inconsistent and labor-intensive. Critical application information was routinely unavailable or insufficient to support operational and incident response needs. Multiple teams were engaging cluster and agency application subject matter experts to enhance application asset inventory information.

Now, with the ability to conduct combined assessment interviews to collect asset information, the **Risk and Remediation Tracking System** informs and supports all five teams' needs and reduces burdensome impact on agency and Cluster resources. Identifying and remediating application security risk and enhancing operational support, resiliency and DR capabilities ultimately enhances overall agency service levels.

This system is primarily used by five functional teams within the EISO, Chief Operations Office (COO) and Chief Technology Office (CTO). Moving forward, once priority application risk assessments and asset inventory data collection efforts are completed, access will be expanded to cluster staff for assessments of in-flight applications, remediation planning, tracking and investments. It is projected that between 800-1,000 individuals will ultimately have access and benefit from the information and functionality provided by this system.

The **Risk and Remediation Tracking System's** benefits are far-reaching. First and foremost, New York State agencies and constituents benefit from efficient and effective security risk assessments that help ensure sensitive data is adequately protected and critical systems are readily available. ITS enterprise and cluster teams benefit from a consolidated assessment team and process, as well as efficient use of resources to accomplish risk assessment, asset inventory data collection, analysis and remediation efforts. ITS enterprise and clusters further benefit from a single data gathering process, and analysis insights that help identify risk, prioritize remediation and enhance key operational support capabilities.

IMPACT

Beyond the benefits realized to improving the security of sensitive data and critical systems, the **Risk and Remediation Tracking System** has had many positive impacts on ITS and New York State such as:

- **Improved operations and efficiency:** The consolidated data gathering efforts by conducting combined assessment interviews has resulted in not only more accurate and more complete asset information, but has led to a reduction in burdensome efforts on agency and IT resources by 75% or more. This has also resulted in both hard and soft cost savings for ITS.

- **Cost savings:** In addition to the significant savings achieved through streamlined data gathering efforts, the system also avoids upfront software investment costs by leveraging an innovative combination of available enterprise software, systems and tools to accomplish shared objectives. The core application took three months of EISO staff time to define shared data collection requirements, design assessment methodologies, develop, test and launch.

  The initial cost of procuring and implementing an industry risk and compliance tracking solution ranges $700,000 - 1.2 million. Comparably, in-house costs to date are approximately $75,000 in staff time and resources.

  The tangible return on investment saved hundreds of hours of staff time and resources, and will continue to provide hard and soft cost savings as ITS proceeds to complete application asset inventory and assessment initiatives for approximately 5,400 applications.

- **Significant productivity gains:** Once again, conducting combined assessment interviews has allowed staff to focus their efforts and resources on other important IT functions.

- **Increased security:** Prior to the development of this system, risk management, analysis and remediation efforts were inconsistent and labor-intensive. Critical application information was routinely insufficient to support operational and incident response needs. The combined asset interviews now allow for the collection of more accurate and more complete asset information.

  The resulting analytical data guides risk prioritization and remediation efforts, and security investments. Identifying, quantifying and remediating application security risk enhances the State's security posture, and enhancing operational support, resiliency and DR capabilities improves overall agency service levels.

The **Risk and Remediation Tracking System** is not a "shiny new gadget," and it did not involve major procurements, services, integration efforts or costs. It is a straightforward

and elegant “game-changer” in its effective use of sound security risk management process building blocks, supported by enterprise technologies and services, applied in an innovative and cutting-edge manner. As such, the approach and resulting benefits can be easily and affordably replicated by other organizations to provide the same benefits