CUSTOMER CASE STUDY

How Iceberg helped a large Government Department Digitally Transform and Reduce their Security Assessment & Authorization Time by 75%

Iceberg provided better visibility to leadership, auditability and scalability for the department with the streamlined SA&A process.

BACKGROUND

Since 2011 this Government Agency has been responsible for providing and consolidating information technology services across 42 federal government departments. The mandate is to deliver digital services to Government organizations, to provide modern, secure, and reliable IT services so federal organizations can deliver digital programs and services that meet constituent needs.

Security Assessment & Authorization (SA&A) is terminology for certification and accreditation. It is based on the methodology known as ITSG-33 IT Security Risk Management: A Lifecycle Approach and documented in the Information Technology Security Risk Management Framework. It is the process by which Government departments ensure that only authorized software and hardware are implemented in their information technology (IT) environment in a safe and secure manner AND in accordance with ITSG-33.

THE CHALLENGE

For this department to execute on its mandate of delivering secure and reliable IT services, they needed a better and more efficient way to assess the risks associated with the services they were required to deliver.

They needed to streamline and make more effective the Security Assessment and Authorization (SA&A) process. The current process involved many spreadsheets, documents and information being sent around by email. Reporting was completely inefficient and had senior leaders spending numerous hours per week combing over spreadsheets and data from many sources of info to create dashboards for reporting. This department needed to digitally transform the SA+A process to drive efficiencies, while decreasing the risk to allow the department to increase their threshold of services with the “Authority to Operate” (ATO).

SA&A is an ongoing process that evaluates security practices and controls to determine if these are implemented correctly, operating as intended, and achieving the desired outcome. Security Authorization involves obtaining and maintaining a security risk management decision which explicitly accepts the related residual risk, based on the results of a security assessment. This authorization is referred to as “the Authority to Operate” (ATO).

The challenge was to digitally transform the current process which was highly manual and based in excel spreadsheets, used to assess security controls and potential risks within IT systems and grant authorization to operate these systems in the production environment.

It is to provide an assessment report relying on different multiple data sources to provide a level of confidence that systems and applications individually and collectively:

- Operate within an acceptable level of residual risk to process information and to protect the confidentiality, integrity, availability and value of that information
- Adhere to the Government of Canada (GC), and the department security policies, security requirements, technical standards and operational procedures defined for the department infrastructure as well as those defined for individual systems and applications
- Operate so as not to create vulnerabilities or unintended interdependencies in other systems; and
- Operate, as expected, without introducing new risks to the infrastructure. A specific system must not decrease the availability of other systems nor can the security posture for the set of all systems within the department security zone be decreased because of a specific system.

OUR RECOMMENDED SOLUTION

The department engaged Iceberg Networks to help them design and deliver a more responsive and effective SA&A process that could be delivered and adopted on a much wider scale and ultimately integrate with other departments' SA&As across multiple departments. Iceberg recommended RSA Archer. Using the Archer Assessment & Authorization module, the department could more effectively identify, manage and mitigate issues, including common (inherited) control management, and eliminate bottlenecks and inefficient manual processes including the multitude of spreadsheets. Reporting and authorization artifacts can be automatically updated, providing key stakeholders with accurate, real-time data to enable better-informed strategic decisions and ensure compliance is maintained and effective security measures are proactively enacted.

KEY BENEFITS AND RESULTS

Auditability

- Tracing of record contact; know who's done what and who's approved what for each record
- Ensure more informed decision making with accurate and timely data (no missed updates to data because they were emailed in spreadsheets)
- Expedite approval of records and signature tracking throughout the record lifecycle
- Improve controls tracking across the organization

Scalability

- Streamlined and approved process for ATO's
- Save numerous hours of labor weekly by team members by automatically aggregating data from different reports and data sources in a single repository
- Reduce overall IT and security risk

Visibility to Leadership

- Provided dashboards and reports as to status of where the department is against goals.

ABOUT ICEBERG

Iceberg Networks helps organizations make more confident and effective business decisions. By providing trusted, aggregated, and transparent risk & security intelligence, we plan, deploy, and manage successful programs for Integrated Risk Management (IRM).