# Major US Bank selected IronSphere to monitor real-time security readiness reviews

## The Situation

The bank has tens of mainframe Lpars used for development, text, integrate and production work. Each Lpar is configured to best performance and availability. The bank auditors need to verify thousands of configuration and permission items to ensure the systems are hardened in a way that preserve client and the bank data.

> "IronSphere put a mirror in front of us. We trusted the manual assessments, but discovered they are legging our business requirement's changes"
>
> **Security Team Leader**

## The Problem

In a frequent changing environment, manual assessments are slow, limited, expensive and requires large team of experienced mainframe security professionals, or an external service.

External (and internal) auditors requested reports they could not generate themselves from the systems under their inspection, and needed detailed explanation on the systems components configuration.

Last, but not least, the bank was unable to requite the proper personnel. This is a global issue related not only to the mainframe industry, but globally to security.

Not only that, the bank experience thousands of attacks every day on his front-end servers and requires to ensure that the backend systems, running on IBM mainframes are hardened to prevent unauthorized use. The security auditors got into conclusion that manual, low frequent assessments, are not the answer to the risks the bank is facing.

> "IronSphere allows us to maintain full history and prove our compliance at any time"
>
> **Compliance manager**

> “The role-based internal access control allowed us to share and limit findings with the technical teams and improve remediation process”
>
> **Audit team manager**

## The Requirement

The auditors looked for a fully automated solution to do the work unattended. The tool should be able to perform frequent, policy-based assessments, while implement NIST ISCM (Information Security Continuous Monitoring) methodology. This will allow the bank to define key security controls that on change, will be investigated in real-time without effecting performance and availability.  The bank also required that the auditors will be able to define their own checks, triggers and parameters.

> “The ITGRC functions implemented in IronSphere allows us to exclude and document decisions not to remediate some findings”
>
> **Systems Programming SVP**

## The Solution

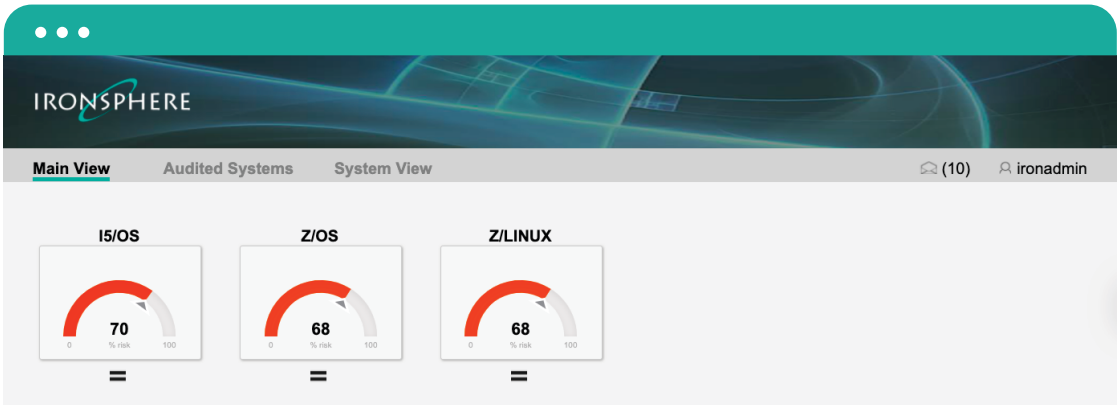
IronSphere is product to perform automatic DISA STIG security readiness reviews that implements NIST ISCM. The product installs on each Lpar and reports to an on-premise server.

After a successful POC, the bank installed IronSphere on 50 Lpars. The first assessment showed that the readiness level is above 50% risk. The auditor team decided to run some checks twice a day, some sensitive security control will be continuously monitored and run on change detection, and others once a week.

The technical teams such as DBAs, Product owners and Systems programming got user accounts allowed them access to a limited, role-based, access to the finding. This ensured that only auditors see the complete security risks and possible attack vectors.

The bank defined a target to reduce the calculated risk score of all agents from above 50% to 10% in a period of six month. To achieve this target, the bank connected IronSphere to the ticketing system using IronSphere REST API. This way, the entire risk life cycle was automated: from detection, to remediation, without a minimum involvement of the auditors.

During a time period of six month, the bank was able to reduce the calculated risk down to ten percents as planned.




IronSphere Inspector is a product of SecuriTeam Software, an Israeli security company.