TREXIN CASE STUDY

STRENGTHENING CYBERSECURITY WHILE GUIDING A BANK'S FRB AUDIT

Trexin assisted an international financial services company in reducing its technology vulnerabilities across its infrastructure and applications during a Federal Reserve Board (FRB) audit.

BUSINESS DRIVER

Wanting to ensure an immediate response to identified risks, our Client's Senior Director of Cybersecurity Engineering asked Trexin to drive the closure of vulnerabilities by collaborating with key Business Unit (BU) and Technology stakeholders to avoid regulatory deficiencies.

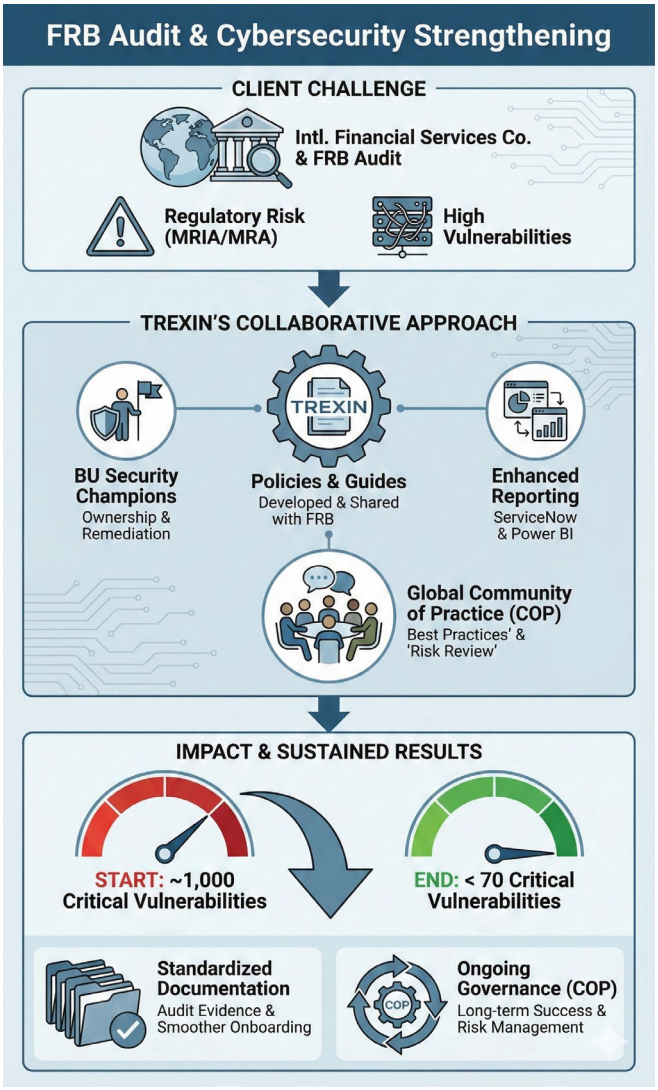
APPROACH

Trexin's highest priority was collaborating with individuals in each BU, enabling the rapid resolution of critical vulnerabilities and helping avoid regulatory actions such as Matter Requiring Immediate Attention (MRIA) or Matter Requiring Attention (MRA) findings. Given the FRB's involvement, Trexin's mission was highly visible and prioritized by the Global CIO.

Trexin designated Security Champions in each BU to take ownership of vulnerability remediation, supported by weekly meetings to track progress, escalate issues, and secure needed resources. Early training gaps led Trexin to develop and refine policies, guides, and procedures, many of which were shared with the FRB. Enhancements to ServiceNow and Power BI improved visibility and leadership reporting, while a global Community of Practice brought together Security Champions, BUs, and Information Security leaders to review risks, share best practices, and ensure long term success.

RESULTS

Trexin assessed and made recommendations to improve our Client team's standard procedures, creating and updating detailed documentation. Clear documentation allowed for smoother onboarding of new team members, standardized practices across the large international organization, and provided evidence of ongoing work to auditors. At the start of the project, our Client had nearly 1,000 open critical vulnerabilities. By the end of Trexin's work, this number had dropped to fewer than 70.



In addition, Trexin recommended and documented best practices, improved reporting and escalation processes, coached our Client's team, and established a Community of Practice (COP) to provide ongoing governance risk assessment and management of system vulnerabilities. Trexin also enhanced reporting and governance, launched the COP, and coached and trained team members through the handover transition to ensure continued success after Trexin's disengagement.

CONTACT US

Financial Services Practice
fs@trexin.com
www.trexin.com

TREXIN
TRUST • EXPERIENCE • INNOVATION