COMPLYING WITH THE NYDFS CYBERSECURITY REGULATION

Trexin helped a fast-growing financial services firm assess its IT security and define its improvement roadmap.

BUSINESS DRIVER

Recognizing the "ever-growing threat posed to information and financial systems by nation-states, terrorist organizations, and independent criminal actors", the New York State Department of Financial Services (NYDFS) issued a landmark cybersecurity regulation, 23 NYCRR 500, requiring regulated entities to "assess its specific risk profile and design a program that addresses its risks in a robust fashion". To comply with this new regulation, our Client, a rapidly growing financial services firm, asked Trexin to:

- Perform a thorough IT security assessment based on the Federal Financial Institutions Examinations Council (FFIEC) framework
- Perform an assessment of the current-state of the IT organization and infrastructure more broadly
- Evaluate the skill set of the current staff

APPROACH

Trexin's first step was to conduct an independent assessment of IT infrastructure with respect to people, process, and current IT capabilities within the organization. Once we had established this fundamental understanding, we took a three-phase approach to the IT security assessment itself, starting with the current-state analysis and assessment using the FFIEC framework. In the 2nd Phase we then defined improvement recommendations, working in close cooperation with our Client's leadership. And in the 3rd Phase we developed a prioritized project roadmap outlining costs and timelines for implementing the recommendations defined in Phase 2.

RESULTS

Our Client fully satisfied its regulatory requirement to design, implement, and maintain a cybersecurity program that is relevant to the company and aligned with its technology advances. More importantly, the engagement established a consensus understanding that current processes needed change and new processed needed to be established to fully remediate issues that they were seeing within their organization. This led

CYBERSECURITY PROGRAM *attains* **REGULATORY COMPLIANCE**

to a future-state vision of agreed upon improvements, a set of business cases with cost-benefit analyses, a project roadmap with charters that outlined the scope and goal for each project, and an activated portfolio of projects related to achieving their cybersecurity and business goals.

TREXIN
TRUST • EXPERIENCE • INNOVATION