# CASE STUDY

## SECURITY PROGRAM REVIEW AND DEVELOPMENT FOR A FINANCIAL INSTITUTION

**HITACHI**
**Inspire the Next**

## QUICK FACTS

**Industry:** Financial Services Industry

**Company Type:** Public Bank

**Location:** 50 Branches in the United States

**Number of Employees:** 500

**Needs & Requirements**:

- Meet regulatory compliance
- Report findings to executive team
- Review security posture following inorganic growth period
- Secure corporate IT assets against vulnerabilities and intrusions
- Develop comprehensive security program

## THE CHALLENGE

The bank had experienced explosive growth due to acquisitions that have changed its security program requirements. The security posture was immature and focused on passing audits as a form of protection against cyber incidents. As many other major banks, it had to comply with a variety of financial regulatory bodies and required external support to determine the technical and security policy posture of the entire organization in relationship to the regulatory oversight.

The bank's Chief Information Officer and Executive Vice President, with full support of the board of directors, desired a comprehensive security program that would go above and beyond what compliance dictates.

## THE SOLUTION

Hitachi Systems Security Inc. recommended a Security Program Review and Development consulting service, including an in-depth assessment and review of the bank's information security architecture to develop security disciplines, strategies, security services, and a comprehensive roadmap to increase the maturity of the bank's security program. As part of this effort, the bank worked closely with the Hitachi Systems Security Inc. team to design an enterprise security architecture that recognizes vulnerabilities associated with the corporate information assets and supports their business operations.

Our Senior Security Consultants recommended using the Sherwood Applied Business Security Architecture (SABSA) methodology as the overarching enterprise security architecture framework. It allows for various cyber security control frameworks and best practices to be integrated and removed as required to meet the banking industry's compliance needs. Examples of regulations and guidelines that were included in this engagement are:

- Gramm-Leach-Bliley Act (GLBA)

- Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook

- FFIEC Cybersecurity Assessment General Observations

- Payment Card Industry (PCI) Data Security Standard

## MAIN BENEFITS

Over the course of this engagement and in preparation for protecting their operations going forward, the bank:

- Gained better control over external and internal audits through the harmonization of compliance regulations.

- Facilitated compliance efforts through the normalization of controls required by multiple laws and regulations.

- Improved the overall security posture with measurable metrics.

- Provided a security architecture when acquiring new banks.

- Achieved consistency and efficiencies across the organization.

- Eased management through a Security Program Review and Development that recognizes vulnerabilities associated with the corporate information assets and supports their business operations.

- Developed a comprehensive measurement of the security program's maturity level.

- Provided an executive-level overview of the security program for review by the bank's board of directors.

## SERVICES PROVIDED

A team of Hitachi Systems Security Inc.'s Senior Cyber Security Experts collaborated on this engagement to:

- Perform a **Risk Assessment** and **Gap Analysis** of the IT environment, assessing the current state of security, and develop a **Security Maturity Level Assessment**.

- Conduct a full **Vulnerability Assessment** of all information security assets within the bank's technical environment.

- Develop a **Security Program Review and Development** using the Sherwood Applied Business Security Architecture (SABSA) model and create an Enterprise Security Program and Architecture Roadmap to institutionalize how IT portfolio and program managers direct investments into the bank's Security Program. This was accomplished by building a clear understanding of the status-quo, organizational capability, and the strategy of the business, IT and security.

- Develop an **Enterprise Security Strategy and Roadmap** to implement the Security Program Review and Development.

- Supported in developing the business case for presenting the Enterprise Security Strategy and Roadmap to the bank's senior management team for approval.