InfoSight®
www.infosightinc.com

RISK ASSESSMENTS FOR FINANCIAL INSTITUTIONS

305-828-1003 info@infosightinc.com

Overview

Financial Institutions are required as part of FFIEC, GLBA, FDIC, and NCUA regulations and guidelines to perform risk assessments of various information systems with various frequencies. Your financial institution knows that Federal and State examiners are tasked with reviewing and auditing the financial institution's management of risk, and risk assessments, when they perform an examination under FDIC and NCUA guidelines.

The Challenge

Financial institutions face many challenges when it comes to completing all of the required types of risk assessments. It is common for staff at small to mid-size institutions to wear many hats, leaving the staff tasked with performing these risk assessments without the time, knowledge, or capabilities to perform them and meet the required elements of these risk assessments. In addition, your institution may be looking to streamline or enhance the process, but doesn't know where to start.

InfoSight®
www.infosightinc.com

RISK ASSESSMENTS FOR FINANCIAL INSTITUTIONS

How We Solve It

Infosight has experienced staff members with decades of Banking and Credit Union experience. Our financial institution experts understand the risks that your Financial Institution faces as well as what Examiners are looking for in your Risk Management Program. We have developed risk management practices, assessments, and programs at many financial institutions that have met and exceeded examiners requirements. InfoSight can do the same for you with our advisory risk services.

Our team can complete these information system risk assessments for you;

- GLBA Risk Assessment
- Information Technology Risk Assessment
- Information Systems Risk Assessment
- Information Security Risk Assessment
- Online Banking Risk Assessment
- Mobile Banking Risk Assessment
- And many more

Other Assesments

Vulnerability & Penetration Testing

Consists of a multi-disciplinary, multi-faceted review of the organization's systems which identifies vulnerabilities outside and inside the network and attempts to exploit any vulnerabilities in the same way a malicious actor would.

Red Team/ Blue Team Testing

Designed to test an organization's readiness to detect, withstand and respond to a targeted attack. The red team's goal is to find and exploit any identifiable weaknesses in the organization's security as the blue team works to defend the organization by finding and patching vulnerabilities and responding to successful breaches.

Web & Mobile Security & API

Involves the security testing of web, mobile and software application interfaces to identify privilege escalation, authorization creep, and security controls bypass. It includes a detailed report outlining discovered vulnerabilities and remediation steps.

The Outcome

With InfoSight's information systems risk assessments, you can be assured that your management team and Board of Director's are informed of any and all risks. This allows the management team and Board to make informed risk based decisions that meet your financial institution's cyber risk appetite.

After testing is complete, Digital reports are delivered via our proprietary **Mitigator Vulnerability and Threat Management Platform.** Reports can be exported in multiple formats and printed.

MITIGATOR™
VULNERABILITY & THREAT MANAGER