PROMONTORY

NIST Cybersecurity Risk Management Services

Cyber risk management has become a crucial component in the safe and sound operation of financial institutions. A growing number of criminals, activists, and nation-states are exploiting weak cybersecurity to pursue illegal activities. Instances of cybercrime, including money laundering, fraud, and information theft, have grown exponentially in recent years, and threaten the overall security and reputational risk of financial institutions.

The recently issued National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is another example of the heightened expectations government agencies and regulators expect institutions supporting our global financial networks to follow in enhancing their cybersecurity risk management frameworks.

A sound cybersecurity framework is good for business. Promontory has the expertise to help financial institutions, small to large, manage their cybersecurity risk.

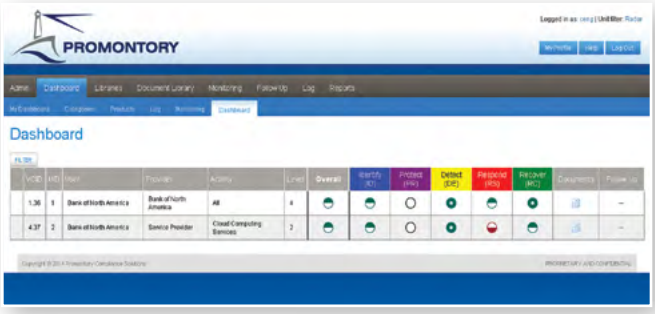
NIST's Framework Core

Framework Risk Management and Validation

Promontory's Web-based risk software allows financial institutions to identify, manage, and report on cybersecurity risk in line with the NIST framework.

Promontory helps financial institutions by:

- Validating and assessing current cybersecurity programs against the framework
- Performing a gap analysis of current cybersecurity programs against the framework and identifying areas of future regulatory concern
- Using the framework review and validation as a pre-evaluation and preparation for upcoming examinations
- Communicating the regulatory impact of the framework to executives and directors, including the board and audit and risk committees

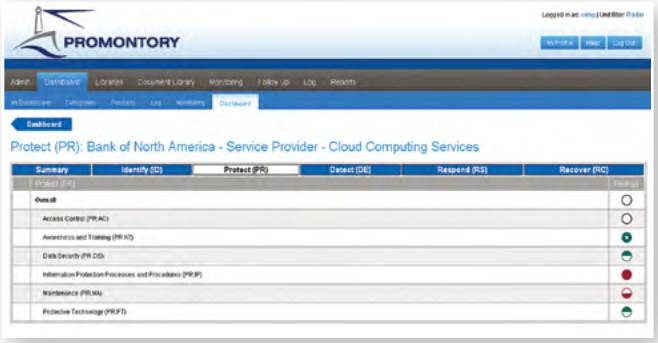


Personalize dashboards to show top risks across an entire enterprise or within a specific business.

Framework Core Assessment

Promontory advises financial institutions how to navigate and assess NIST's five core framework functions:

- Identifying risk
- Protecting against risk
- Detecting cybersecurity events
- Responding to cybersecurity events
- Recovering from cybersecurity events



Users can drill down to view the cybersecurity categories for each function.

Framework Tier Classification

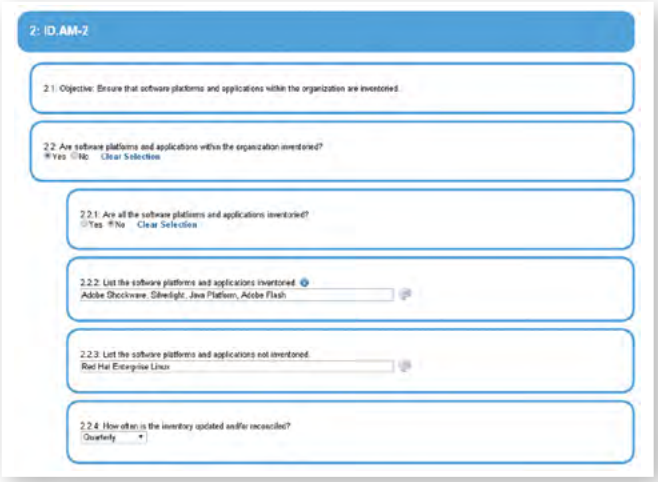
Promontory assists financial institutions to prioritize those framework components in greatest need of enhancement via NIST's Tier Classification Process, using the protocols to determine the appropriate framework tier level:

- Tier 1: Partial
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

Framework Profile

Promontory helps financial institutions to:

- Create a baseline profile of current cybersecurity practices
- Create a target profile to identify areas to improve
- Establish targets to improve the institution's cybersecurity program



Each step in the protocol represents a subcategory in the NIST framework.

About Promontory

Promontory Financial Group helps companies and governments around the world manage complex risks and meet their greatest regulatory challenges with integrity and quality. We are the world's foremost experts in financial risk, regulation, and compliance. Our work makes our clients stronger and the financial system safer for consumers.

Manage and protect your security and reputational risk. Contact us to learn more about our NIST Cybersecurity Risk Management Services:

PROMONTORY

+1 202.384.1200 | compliance@promontory.com

promontory.com