



# Overview of Governance, Risk and Compliance Coverage

---

**ISSUED BY**

Advisor Armor - [www.advisorarmor.com](http://www.advisorarmor.com)



**REPRESENTATIVE**

guidance@advisorarmor.com

(800) 421-7897

---

## Overview

Advisor Armor delivers interpretative guidance, software, and professional services enabling clients to meet information/cybersecurity compliance standards including, but are not limited to, NIST, SEC, DNYFS, FINRA, and NASAA along with state privacy and safe-harbor laws.

# IDENTIFY AND PROTECT

## Risk Assessment

Identify potential business and individual cybersecurity risks, threats, vulnerabilities, and deficiencies.

## Policy and Procedure Development, Attestation, and Enforcement

Establishment and maintenance of comprehensive, customized policies and procedures reflecting the operational handling of critical data and information. Policies are consistent with NIST and other standards and updated regularly. Attestation and automatic enforcement, where possible, included.

## Security Awareness Education and Training

Interactive training modules and assessments to prepare for the latest cybersecurity threats. Customized modules specifically address current issues for regulated professionals and their companies.

Additionally, flash news briefs include weekly security tips, monthly newsletters, and security alerts.

---

## Device Security Testing

Software automatically and continually provides visibility and security status. Customizable monitoring elements include, but are not limited to, non-public information, software updates, encryption, screen timeout, remote login, software and web access.

## Automated Policy Enforcement

Software automatically and continuously enforces policy on all installed endpoints. Full reporting and immediate non-compliance notifications are provided upon failure.

## Phish Testing

Customized phishing attempts delivered randomly to elicit proper user behavior.

## Third-Party Cybersecurity Monitoring

Evaluates and monitors third-party vendor cybersecurity risk. Unlimited vendors included.

# DETECT

## Device Endpoint Monitoring

Software monitors security and access on all installed devices with immediate endpoint security failure notifications provided.

---

## Dark Web/Data Breach Credential Monitoring

Monitoring and alert notification for critical credentials 24/7..

## Network Infrastructure Testing

Penetration Testing and Network Vulnerability scanning. Interpretive Diagnostic Reporting produces the evidence needed for actionable network security improvements.

# RESPOND AND RECOVER

## Incident Response

Includes plan development and testing. Software provides reporting and record keeping. Response plans are developed and included within Policies and Procedures. Advisor Armor also supports the response and recovery efforts that may include containment, investigation, determination, notifications, and many other potentially related actions.

## Regulatory Examination Review

Provides annual cybersecurity examination audits to ensure the proper elements are updated and available on demand.

## Insurance Risk Assessment

Includes a data risk assessment and estimation of potential costs of data security incidents.



## Cyber Liability Insurance

Additional cost. Independently licensed provider.

## Customized Dashboard Experience

Advisor Armor is managed through an Applet or a web-based dashboard. All compliance evidence is stored and available on demand.

