

# DefenseStorm Governance Program

Improve efficiency with automated reporting for regulatory requirements

Financial institutions must defend all valuable assets in alignment with a stringent set of regulations while spending time and valuable resources and time proving their compliance.

You need the ability to conduct ongoing cybersecurity compliance monitoring for adherence to your internal policy and process, industry control frameworks and regulatory requirements to bridge the gap between typically siloed teams – like IT, information security and risk. Full understanding of where you stand in your cybersecurity compliance to self-assessment frameworks, like the FFIEC's CAT (Cybersecurity Assessment Tool) allow you to better manage your cyber risk.

GRID Active Governance Program allows financial institutions to monitor the effectiveness of their cyber risk management program. With automated evidence collection processes that prove adherence to regulatory control frameworks like the FDIC's CAT (Cybersecurity Assessment Tool), it simplifies audit and exam preparation. Controls are attached to the information security/cybersecurity program and policies that are important when it comes to managing cyber risk. With a built for banking approach to improve cyber risk management, we give FIs the ability to understand their cyber risk readiness in real time, like they can with any other financial risk.



***23% of respondents have automated less than half of their workflows or have few (or zero) automated work flows.***

## GOVERNANCE PROGRAM

### FEATURES

- Pre-mapped task schedule templates
- Automated evidence collection
- Include self-assessment tools.
- Activities map directly into frameworks and self-assessment directives.
- Automated Reporting

### BENEFITS

- Easily schedule governance program and activities to align with your program cadences.
- Monitor the state and effectiveness of your cyber risk management program and prove adherence to frameworks.
- Simplify audit and exam preparation and access all log data in one integrated platform.
- Schedules can be created for events to improve cybersecurity compliance efficiency.

# DefenseStorm Governance Program

Improve efficiency with automated reporting for regulatory requirements

## Improve Efficiency with Automated Evidence Collection

- Leverage pre-mapped Task Schedule templates to schedule program activities to save time and remain within framework guidelines since activities map automatically and directly into framework and self-assessment directives as evidence.
- Full access to your log data to complete governance and monitoring activities through GRID Active, our integrated data platform to improve your cybersecurity compliance.

## Continuous Monitoring of Control Effectiveness

- Full control to schedule governance and monitoring activities to align with your cybersecurity compliance program cadences.
- Access and leverage your data through GRID Active to conduct monitoring and governance actions and memorialize reviews – all to better demonstrate adherence to your cybersecurity compliance and risk program.

## Demonstrate Adherence to Cybersecurity Compliance Program

- Prove your cyber controls align with regulatory requirements and industry best practices through a curated library of pre-mapped templates shaped from regulatory requirements, industry best-practices, and examiner expectations.

- Guide your program oversight with self-assessment tools for measuring the state of your program.
- The GRID Active integrated data platform systematically collects evidence to support industry and regulatory control frameworks so you can monitor your cybersecurity compliance program against unlimited frameworks.

## Integrated Frameworks

DefenseStorm Governance Program includes multiple frameworks and self-assessments against which you can measure your program. Evidence is collected systematically from activities in GRID Active to support your adherence to industry and regulatory control frameworks. Evidence comes from Threat Surveillance, Fraud Detection, Governance Program, and Risk Assessment to support each individual framework control recommendation or requirement.

## Frameworks integrated into the platform:

- NIST Cyber Security Framework
- CIS Controls
- FFIEC Cyber Assessment Tool
- FFIEC Information Security Exam Procedures
- InTREx Exam Procedures Information Security Exam Assessment (NCUA)
- R-SAT
- FedLine Security and Control Procedures (Advantage and Web)