AXONIUS

Axonius Mapping to the FFIEC Cybersecurity Assessment Tool

The Federal Financial Institutions Examination Council (FFIEC) maintains a Cybersecurity Assessment Tool (CAT) to help FFIEC members identify cybersecurity risks within their organizations. The FFIEC CAT follows guidance its members piloted in 2014, as well as FFIEC's Information Technology Examination Handbook and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), along with other industry-accepted leading practices and guidance.

The **FFIEC CAT** is an aid for uncovering institutional cybersecurity risks (internal and external) and mapping financial institutions' maturity and readiness such that it drives continuous cybersecurity awareness and improvement.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

The FFIEC CAT consists of two parts: ***Inherent Risk Profile and Cybersecurity Maturity***. The following material maps the Axonius asset management platform and solution to the five domains included in the Cybersecurity Maturity section.

THEY'RE AS FOLLOWS:

- DOMAIN 1: **CYBER RISK MANAGEMENT AND OVERSIGHT**
- DOMAIN 2: **THREAT INTELLIGENCE AND COLLABORATION**
- DOMAIN 3: **CYBERSECURITY CONTROLS**
- DOMAIN 4: **EXTERNAL DEPENDENCY MANAGEMENT**
- DOMAIN 5: **CYBER INCIDENT MANAGEMENT AND RESILIENCE**

While Axonius can neither determine financial institutions' individual risk profile nor their level of maturity, the solution provides visibility into and mitigations for cyber asset-related risk. Axonius, therefore, ***can be a great aid to any financial institution assessing its compliance with FFIEC CAT***, as well as related industry best practices.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

DOMAIN 1:
CYBER RISK MANAGEMENT AND OVERSIGHT

Cyber risk management and oversight addresses the board of directors' (board's) oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.[1]

ASSESSMENT FACTORS

- **GOVERNANCE** includes oversight, strategies, policies, and IT asset management to implement an effective governance of the cybersecurity program.
- **RISK MANAGEMENT** includes a risk management program, risk assessment process, and audit function to effectively manage risk and assess the effectiveness of key controls.
- **RESOURCES** include staffing, tools, and budgeting processes to ensure the institution's staff or external resources have knowledge and experience commensurate with the institution's risk profile.
- **TRAINING AND CULTURE** includes the employee training and customer awareness programs contributing to an organizational culture that emphasizes the mitigation of cybersecurity threats.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

AXONIUS ALIGNMENT WITH DOMAIN 1

Axonius is a cyber asset management solution that provides comprehensive visibility into all IT assets along with detailed asset-related information, thereby allowing cybersecurity, operations, IT, risk, and management teams to understand and manage the security of all deployed IT infrastructure and associated users.

Further, Axonius provides a way for platform administrators to identify risk areas based on known vulnerabilities, misconfigurations, gaps in security controls and policies, and more. The Enforcement Center in the Axonius platform provides a way for administrators to manage risk and implement controls, either directly via Axonius or through one of the 400+ technology adapters.

[1] All domain descriptions and assessment factors are quoted directly from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

DOMAIN 2:
THREAT INTELLIGENCE AND COLLABORATION

Threat intelligence and collaboration includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties.

ASSESSMENT FACTORS

- **THREAT INTELLIGENCE** refers to the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.
- **MONOTORING AND ANALYZING** refers to how an institution monitors threat sources and what analysis may be performed to identify threats that are specific to the institution or to resolve conflicts in the different threat intelligence streams.
- **INFORMATION SHARING** encompasses establishing relationships with peers and information-sharing forums and how threat information is communicated to those groups as well as internal stakeholders.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

AXONIUS ALIGNMENT WITH DOMAIN 2

The Axonius platform ingests third-party threat intelligence information which customers may use to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.

THIS INFORMATION INCLUDES DATA FROM:

- Shodan
- Censys
- Dell TechDirect
- Common Vulnerabilities and Exposures (CVE) database
- Have I Been Pwned
- Portnox
- Web Servers
- National Vulnerability Database (NVD)

The threat data ingested by/integrated with the Axonius platform can be used to enrich asset data, provide context for external threats, and used by Axonius customers to check whether installed software contains any known vulnerabilities.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

DOMAIN 3:
CYBERSECURITY CONTROLS

Cybersecurity controls are the practices and processes used to protect assets, infrastructure, and information by strengthening the institution's defensive posture through continuous, automated protection and monitoring.

ASSESSMENT FACTORS

- **PREVENTATIVE CONTROLS** deter and prevent cyberattacks and include infrastructure management, accees management, device and end-point security, and secure coding.
- **DETECTIVE CONTROLS** include threat and vulnerability detection, anomalous activity detection, and event detection, may alert the institution to network and system irregularities that indicate an incident has or may occur.
- **CORRECTIVE CONTROLS** are utilized to resolve system and software vulnerabilities through patch management and remediation of issues identified during vulnerability scans and penetration testing.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

AXONIUS ALIGNMENT WITH DOMAIN 3

As a comprehensive asset management solution, Axonius surfaces security control gaps and missing policies and allows customers to take remediative action.

USING AXONIUS, CUSTOMERS CAN FIND:

- Assets that don't comply with security policies
- Missing endpoint agents
- Malfunctioning agents
- Missing/out-of-date security patches
- Misconfigurations
- Software vulnerabilities
- Hardware vulnerabilities
- Inappropriately open ports
- Known vulnerabilities (as listed by CVE/NVD)
- Risky network interfaces
- Out-of-date agent and OS versions
- Missing vulnerability assessments or scans

In some instances, Axonius customers can use the Enforcement Center to initiate corrective action against vulnerabilities (e.g., isolate a vulnerable device from the network, disable vulnerable users or devices). In other cases, customers may use Axonius to notify asset owners or administrators and allow them to remediate vulnerabilities from a third-party source.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

DOMAIN 4:
EXTERNAL DEPENDENCY MANAGEMENT

External dependency management involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution's technology assets and information.

ASSESSMENT FACTORS

- **CONNECTIONS** incorporate the identification, monotoring, and management of external connections and data flows to third parties.
- **RELATIONSHIP MANAGEMENT** includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the institution's cybersecurity program.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

AXONIUS ALIGNMENT WITH DOMAIN 4

The Axonius platform allows customers to ***identify network interfaces and open ports***, which gives them the ability to make strategic business decisions regarding risks.

Further, Axonius provides a way for customers to measure and monitor their cloud asset compliance. Using the Cloud Asset Compliance Center and the Foundations Benchmark Guidance from AWS, Azure, Google Cloud, and Oracle Cloud, customers can see where controls are in or out of alignment with recommended cloud provider-supplied guidance (as well as company-specific requirements) and adjust accordingly.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

DOMAIN 5:
CYBER INCIDENT MANAGEMENT AND RESILIENCE

Cyber incident management includes establishing, identifying, and analyzing cyber events, prioritizing the institution's containment or mitigation, and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.

ASSESSMENT FACTORS

- **INCIDENT RESILIENCE PLANNING AND STRATEGY** incorporates resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruptions and the destruction or corruption of data.
- **DETECTION, RESPONSE, AND MITIGATION** refers to the steps management takes to identify, prioritize, respond to, and mitigate the effects of internal and external threats and vulnerabilities.
- **ESCALATION AND REPORTING** ensures key stakeholders are informed about the impact of cyber incidents, and regulators, law enforcement, and customers are notified as required.

AXONIUS.COM / Madison Ave. Floor 39 / New York, NY 10017

AXONIUS ALIGNMENT WITH DOMAIN 5

AS AN ASSET MANAGEMENT SOLUTION, AXONIUS IS FOCUSED ON THREE MAIN PRINCIPLES:

- Provide a comprehensive, always up-to-date asset inventory
- Surface security coverage gaps and validate security controls
- Allow asset owners and administrators to take automated action against asset-related vulnerabilities

In alignment with domain 5, Axonius provides rich data and context to allow security, operations, IT, risk, management, and compliance teams to identify, prioritize, respond to, and mitigate asset-related threats and vulnerabilities. The Axonius Enforcement Center allows customers to notify affected and/or responsible parties, as well as send vulnerability and incident data to third-party tools, create an incident in Axonius or send incident tickets to third-party tools, deploy files and run commands, execute endpoint security agent action, manage users and devices via directory services, manage cloud instances, and manage DNS services – all in support of incident handling and business resilience.

In addition, Axonius offers robust reporting features which give customers the ability to dive deep into details or present information at a high level so that security and business decision makers can take appropriate action.

AXONIUS

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with over 300 security and management solutions. Axonius is deployed in minutes, improving cyber hygiene immediately.

330 MADISON AVE., 39TH FLOOR
NEW YORK, NY 10017
INFO@AXONIUS.COM