FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

How to Use FFIEC CAT and Digital Guardian to Improve Your Security Posture

Executive Summary

In 2015, the Federal Financial Institutions Examination Council (FFIEC) published the first iteration of the FFIEC Cybersecurity Assessment Tool (CAT). The FFIEC CAT is designed to enable financial institutions to understand the cyber security risks they face based on their size and structure, and assess their preparedness for attacks.

While there is no formal requirement that financial services firms use the FFIEC CAT, many auditors or examiners are now using it as their primary vehicle to assess a firm's cybersecurity posture.

This paper provides an overview of the FFIEC CAT, how to use the CAT to identify areas of risk and levels of cybersecurity maturity, and how Fortra™'s Digital Guardian®'s Data Protection Platform can help reduce risks identified by the CAT, and improve their security maturity.

FFIEC CAT at a Glance

The CAT is structured to help financial institutions identify their biggest areas of risk **[Part One: Inherent Risk Profile]** and then map out their path to cybersecurity maturity **[Part Two: Cybersecurity Maturity]**. Completing the Inherent Risk Profile can give you important visibility into how examiners are likely to view your security risk exposure. Completing Part Two of the FFIEC CAT will enable you to systematically identify missing controls and processes.

Part One - Inherent Risk Profile

A necessary first step is an assessment of the risk an organization faces due to its size and structure alone. A more complex technical environment (more people, devices, applications, service providers, etc.) will have more inherent risk than a less complex environment, simply because there are more things that could go wrong.

The Inherent Risk Profile provides a metric for this complexity, measuring risk based on the volume, type, and complexity of a firm's activities, services, and products. The assessment does not account for any mitigating controls. It is important to note that having a lower inherent risk profile does not necessarily mean that an organization is doing a good job at security. It merely indicates that the firm's technology landscape is less complex than firms with higher inherent risk profiles. The Profile examines five categories; technologies and connection types; delivery channels; online/mobile products and technology services; organizational characteristics; and external threats. Completing the Inherent Risk Profile can give you important visibility into how examiners are likely to view your security risk exposure.

Part Two - Cybersecurity Maturity

Once an organization understands the risk it faces due to its size and complexity, it next assesses its current methods to address risk. The CAT's cybersecurity maturity assessment looks at the organization's security activities, culture, and commitment. Maturity is measured (in increasing maturity) as Baseline, Evolving, Intermediate, Advanced, or Innovative by matching an organization's existing activities to statements in the CAT for each of five domains:

- 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

A maturity level is reached only when all the statements in each maturity level match activities currently in practice at the organization for each domain. Completing Part Two of the FFIEC CAT will enable you to systematically identify missing controls and processes.

The FFIEC Inherent Risk Profile - Framework for Grading Your Risks

Managing risk requires visibility to all sensitive data, analytics to understand the context of how data is used, and controls to enforce data protection policies. These requirements hold true for all types of data. Policies governing use, however, are different for different types of data and different users. A finance director needs access to financial data and may need to share that data with outside auditors. This role does not need access to source code, however. Software engineers need to access source code, but some of that IP may be illegal to provide to a foreign national inside the company. In other words, effective data protection requires visibility to data events, user events, and system events, across endpoints, databases or shares, network traffic, and cloud storage.

Understanding the risk in the existing environment includes visibility to data that may be sought be an adversary such as employee data, financial projections, customer information, and other Intellectual Property (IP). It also includes activities, services, and products that may handle that information. The FFIEC CAT groups these into five categories.

Technologies and Connection Types

Financial institutions have numerous access points and use a variety of connection types, including:

- Virtual private networks
- Wireless networks
- Telnet, File Transfer Protocol
- Local area network that directly connects to other networks or to Internet service providers
- Bring your own device (BYOD)

It makes sense that the more devices and connections with access to data, the greater the risk that unauthorized data movement may go undetected. Organizations should consider whether all types technologies and connection types are required to support business goals, or whether these can be reduced in types and frequency to mitigate risk.

Delivery Channels

Delivery channels cover how users of a system access information. This includes services provided through Automated Teller Machines (ATM), applications for mobile devices, and online internet applications. The greater the number of delivery channels, and the greater the functionality provided through each, the greater the inherent risk.

Online/Mobile Products and Technology Services

This category covers all types of payment services, including in-person payments, debit/credit/prepaid cards, Automated Clearing House, wire transfers, treasury/trust services, and emerging payment technologies like digital wallets. The more payment services and products offered and supported by an organization, the more inherent risk to the organization from misuse. Even more so if the organization provides these technology services to other organizations.

Questions to Answer

- What types of connections does my financial institution have?
- Are we managing those connections in light of the rapidly evolving threat and vulnerability landscape?
- Do we need all our connections?Would reducing the types and frequency of connections improve our risk management?
- How do we evaluate evolving cyber threats and vulnerabilities in our risk assessment processes for the technologies we use and the products and services we offer?
- How do our connections, products and services offered, and technologies used collectively affect our financial institution's overall inherent cybersecurity risk?

Organizational Characteristics

Rapidly growing organizations may struggle with controlling data access by employees. Employees could mean well, but put data at risk inadvertently because they don't understand the risk posed by their actions. Mergers and acquisitions add new people and technologies

for sharing information. Smaller companies with fewer IT and security resources may allow employees additional computing privileges. Multiple data centers add complexity – and risk – and a variety of defense technologies.

External Threats

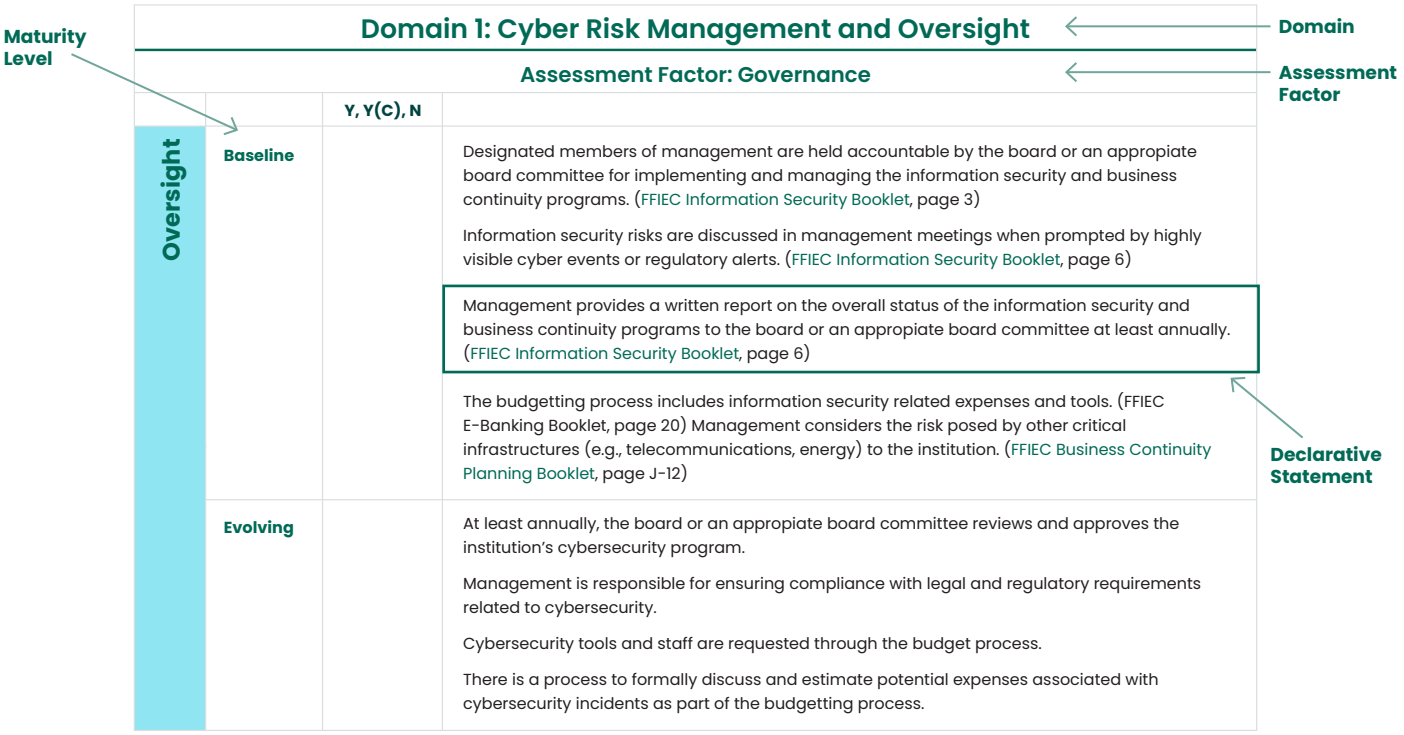
Some organizations will attract more adversaries due to their size or reputation. This category measures the volume and sophistication of the attacks targeting the institution.

The FFIEC Cyber Security Maturity Model

Once an organization understands the inherent risk in its structure and services, the CAT helps assess an organization's preparedness for attacks. Security is about more than simple perimeter defense, and FFIEC acknowledges this by including five domains in its maturity assessment.

Each domain is comprised of one or more Assessment Factors, which in turn are comprised of one or more components. An example is shown in Figure 4 from the CAT, below:

Figure 4: Cybersecurity Maturity



Maturity levels are determined by Maturity levels are determined by matching an institutions demonstrable practices to a set of "declarative statements" for each Assessment Factor and Component. The metrics applied by FFIEC are strict, and the agency makes tools available to prepare for this assessment. All "Baseline" declarative statements refer back to the FFIEC Information Security Booklet.[1]

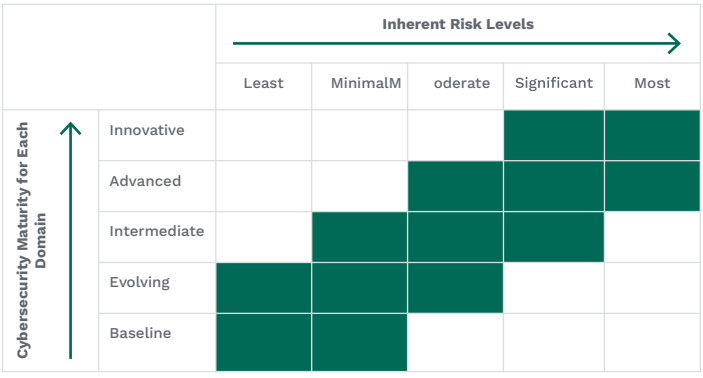
Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

[1]*Source: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx*

Each domain includes two to four Assessment Factors to be scored separately. For each maturity level, one or more "declarative statements" are listed. To achieve a maturity level, an organization must answer "yes" or "yes, with compensating controls" to all the declarative statements for that level, and all previous levels.

The assessment is self-scoring and there is no "passing grade". Instead, it is a tool that institutions can use to identify areas where improvements to security are possible and measure the organization's maturity over time. As show in the graphic from the CAT, as an organization's inherent risk increases, one would expect its maturity to increase as well.

Table 3: Risk/Maturity Relantionship



DG Capabilities for Executing a FFIEC CAT Action Plan

With security resources already stretched thin, meeting the FFIEC targets can be a challenge. While attacks grow in volume and sophistication, pressure increases to protect sensitive information. Since 2003, Digital Guardian has helped financial institutions defend their organizations from internal and external threats.

Product Capabilities

- DG Data Discovery – Find the sensitive assets/data in your organization and view how it is used, including ways that may put data at risk.
- DG Data Classification – Automatically classify structured and unstructured data based on content, context, and user classifications.
- DG Network DLP – Monitor data usage to stop sensitive data from leaving your network.
- DG Endpoint DLP – Enforce company policies on the use of sensitive data on and off your network.
- DG Cloud Data Protection – Stops the loss of data in cloud applications such as Office 365.
- DG Endpoint Detection and Response – Detect, investigate, and mitigate suspicious activities and behaviors at the endpoint.

Service Capabilities

DG Managed Services Offering provides security expertise to deploy, scale, and manage your DLP and EDR defenses.

- Monitor all activity for actions that could put sensitive data at risk
- Incident Response and reporting
- Data analytics to ensure policy enforcement
- Threat hunting across all environments to identify new threats and proactively protect sensitive information

Next, we will look at each domain in the FFIEC CAT maturity model and how Digital Guardian can help.

Domain 1: Cyber Risk Management and Oversight

Questions to Answer

- What is the process for ensuring ongoing and routine discussions by the board and senior management about cyber threats and vulnerabilities to our financial institution?
- How is accountability determined for managing cyber risks across our financial institution? Does this include management's accountability for business decisions that may introduce new cyber risks?
- What is the process for ensuring ongoing employee awareness and effective response to cyber risks?

Domain 1 measures the maturity of activities concerning risk management, program governance, the staffing resources applied to an institutions security program, and how the program is communicated inside and outside the organization. It accounts for executive support including visibility at the Corporate Board level.

In the Risk Assessment component, a less mature (Baseline) organization would simply focus on identifying "reasonable and foreseeable internal and external threats". An "Evolving" practice would monitor customer information, but also expand beyond this to address all sensitive information. An Advanced company would demonstrate these activities (and others not mentioned here) to add "cyber threat analysis and specific risk exposure as part of the enterprise risk assessment".

How Digital Guardian Can Help

Asset management and risk assessments require more than simply a list of an organization's hardware and software. It also requires information on its most critical asset – data. Security personnel cannot assess risk until they know where sensitive data resides and actions being taken that could put that data at risk.

Digital Guardian provides visibility to sensitive data – and its use – throughout the organization. This includes

endpoints, servers, and cloud services like Box. While the FFIEC "evolving" controls require an updated asset inventory annually, DG provides the ability to know exactly where sensitive data is at any time. DG allows organizations to see, log and control literally any action on a system.

Strategy and Policies are strengthened by monitoring actual use of sensitive data, and Oversight is assured by tamper-proof, evidentiary-grade data event logs. When appropriate, new policies and controls can be applied quickly to mitigate risk. Controls range from logging silently to actively blocking prohibited activity. Other controls warn users of risky behavior, reinforcing security policies and allowing self-correction and ongoing training.

DG also supports Training and Culture through endpoint controls that can provide warnings before blocking actions to provide reminders of policies for sensitive data and allow users to self-correct.

Domain 2: Threat Intelligence and Collaboration

Questions to Answer

- What is the process to gather and analyze threat and vulnerability information from multiple sources?
- How do we leverage this information to improve risk management practices?
- What reports are provided to our board on cyber events and trends?
- Who is accountable for maintaining relationships with law enforcement?

This domain examines the organization's use of internal and external threat information. Since institutions throughout the industry face common threats, the CAT rewards activities that correlate multiple intelligence sources and sharing threat information inside the organization and with peer institutions.

How Digital Guardian Can Help

For customers using DG's EDR as a service, three separate sources of threat information are available: Digital Guardian Customer Intelligence, Virus Total, and FireEye.

With Digital Guardian's Managed Security Program (MSP) offering, security experts manage all aspects of protecting sensitive data, including monitoring, alerting, and incident response. Digital Guardian's Advanced Threat team is continuously diverse, global researching and analyzing campaigns along with targeted attacks to our customer's environments. In the event new, unique, or otherwise novel threats are identified, those risks are mitigated via indicator blacklist feeds or with new rules written by our team of cybersecurity experts. All Digital Guardian MSP customers gain immediate access to these new rules to help protect their sensitive data from the evolving threat landscape.

DG continuously monitors and analyzes all uses of sensitive data, on and off the network. If a user attempts to intentionally or inadvertently misuse data, Endpoint controls include the ability to monitor and log all actions, block actions, warn users of policies for self-correction and prompt them for waivers requests.

Domain 3: Cybersecurity Controls

Questions to Answer

- What is the process for determining and implementing preventive, detective, and corrective controls on our financial institution's network?
- Does the process call for a review and update of controls when our financial institution changes its IT environment?
- What is our financial institution's process for classifying data and determining appropriate controls based on risk?
- What is our process for ensuring that risks identified through our detective controls are remediated?

Cybersecurity Controls covers activities intended to deter and prevent attacks across an organization's infrastructure. Controls include endpoint protection, building more secure software, actions taken to actively identify threats, and ensuring the organization's software and hardware is fully patched.

How Digital Guardian Can Help

DG's Endpoint Detection and Response (EDR) solution works from the same kernel-level agent as DG's DLP solution to detects and blocks advanced threats across the attack lifecycle. Starting from the attack's initial entrance (e.g., phishing) Digital Guardian combines real-time visibility into system, user and data events with the ability to use historical detection to search across the enterprise for any existing infections or attack activity that may have occurred in the past. This provides you the needed context of data movements to enable faster and more accurate determination of the attack, its motivation, and impact.

Advanced threats often introduce and spawn new processes to affected devices. Digital Guardian can detect these malicious applications, block execution or access to protected data, and alert Incident Response in near real time.

DG allows organizations to block unknown executables and ensure that only approved applications are used. This includes legitimate, but undesirable applications such as peer-to-peer networking or chat applications, as well as unknown software that may be malicious. Administrators can enforce the use of specific browsers with controlled settings, including limiting internet access to the company's network proxy or VPN.

Domain 4: External Dependency Management

Questions to Answer

- How is our financial institution connecting to third parties and ensuring they are managing their cybersecurity controls?
- What are our third parties' responsibilities during a cyber attack? How are these outlined in incident response plans?

Domain 4 examines controls and mitigations for risk introduced by 3rd parties, including vendors and partners. It looks for controls proving that all 3rd party connections are enumerated and monitored, and that all parties are working together to improve security. The Relationship Management Component covers how an institution monitors the security controls of its partners and service providers. This includes evaluations prior to initiating a relationship and the continued monitoring of those 3rd parties.

How Digital Guardian Can Help

Digital Guardian agents are specially designed to secure data in high-performance environments where thousands of internal and 3rd party end-users access, save, and collaborate with a company's most critical information. Sensitive information required by partners can be automatically encrypted at rest and in transit. Classification of structured and unstructured data is automatic, and controls can enforce encryption at rest or in transit. Copying the data into another format (e.g., a screen shot of sensitive data saved as a .jpeg file) does not bypass DG controls. Any new format of the data "inherits" the original classification.

Digital Guardian monitors and controls all communications channels — including email (SMTP), web (HTTP/HTTPS), File Transfer Protocol (FTP), Secure Sockets Layer (SSL), and applications such as webmail. Digital Guardian detects, alerts, and blocks potential unauthorized or unintentional transmissions of confidential data. Since protection travels with the data, third party access to sensitive data is controlled throughout its lifecycle, and all access is logged.

Case Study

Securing PII Shared with Third Party Vendors

A regional bank needed to protect its sensitive customer data, which was being shared with thirty party vendors for IT management. The firm realized that failure to secure its PII and PCI could result in regulatory penalties, class action lawsuits, or loss of credibility. Digital Guardian's Data Base Record Matching allowed deep inspection into the bank's customer databases and created mathematical hashes of the data. Outgoing traffic to external vendors is now inspected for any matches to regulated data, while also preventing unauthorized data access. Our solution's data protection capabilities protect on and off the network as well as across virtual environments.

Domain 5: Cyber Incident Management and Resilience

Questions to Answer

- In the event of a cyber attack, how will our financial institution respond internally and with customers, third parties, regulators, and law enforcement?
- How are cyber incident scenarios incorporated in our financial institution's business continuity and disaster recovery plans? Have these plans been tested?

Stopping attacks is obviously important, but FFIEC has also prioritized incident response and analysis. When an attack occurs, organizations should have action plans for containing the attack, rerouting critical functions, and post-action analysis. These plans should be practiced on a regular basis, and reviewed as the threat landscape evolves.

How Digital Guardian Can Help

Whether the data is structured or unstructured, Digital Guardian knows where it is and how it is being used. Digital Guardian understands the context of how sensitive data is used, seeing at the system, user, and data level. When data is used according to policy, Digital Guardian is invisible to end users, allowing access and use of data. When policies are violated, or actions are attempted that could put sensitive data at risk, Digital Guardian can apply a wide range of controls, from warnings to hard blocks.

Digital Guardian Endpoint Detection and Response (EDR) provides protection from multiple attack sources using the same agent as Digital Guardian's DLP. Digital Guardian's behavior-based rules automatically detect and block attacks - ransomware, malware, malware-free attacks, and other suspicious data movements. It stops threats even if there are no IOC signatures. Wherever in the kill chain – entrance, lateral movement, installation, command and control, or exfiltrate – Digital Guardian EDR provides the needed context of data movements to enable faster and more accurate determination of the attack, its motivation and impact.

Conclusion

The CAT is a useful tool to help any organization assess and manage risk to their sensitive data, and to guide continuous improvements in an information security program. It is not intended to be a static document; as an organization grows its inherent risk profile will change and new threats develop over time. As new technologies are adopted and new partners are acquired, the risk assessment should be updated and new controls may be warranted.

As always, the most critical first step in assessing risk is identifying sensitive information wherever it resides. To manage that risk, organizations must understand the context of how the data is used and apply controls to allow legitimate use while blocking misuse.

Digital Guardian simplifies the CISO's job by combining DLP, EDR, and UEBA in a single solution to detect, prioritize, respond, and remediate all threats. The granular visibility to all data allows organizations to identify activity that could put data at risk, then build and enforce policies to protect sensitive information. With one agent, security teams have less to manage and monitor. Adding Digital Guardian's Managed Service offering allows scarce security resources to focus more time on high-value tasks and incident response, and less time on managing hardware and software.