imperva

FFIEC Assessment, How Imperva can help

Financial institutions are increasingly dependent on information technology to maintain operations and provide services to customers but the significant rise in the number of cyber attacks targeted at this industry in the last few years has the potential to undermine consumer confidence not only in your organization but also across the wider industry.

In the United States, The Federal Financial Institutions Examination Council (FFIEC), has developed an assessment tool to help financial institutions identify possible risks, assess their current plan, and evaluate it against the risk of a cybersecurity threat. The Cybersecurity Assessment Tool (CAT) also defines the proper controls an organization needs to improve and mitigate the risks and continually improve their overall security posture. It also lays out suggestions for a cybersecurity maturity model, which consists of 5 different domains and maturity levels.

Imperva Sonar Platform can help financial organizations meet needed and planned controls found in both FFIEC and the NIST Framework by offering Data privacy, compliance and security solutions from a single centralized platform. This provides clear visibility of any vulnerabilities or gaps in your security infrastructure and enables better risk management.

Imperva offers a range of security solutions to address the following use cases found in the FFIEC IT Examination Handbook.

II.C Risk Mitigation: Application and Data Analytics

II.C.14 Supply Chain: Runtime Application Protection

11.C.17 Application Security: Edge & Application Protections

11.C.18 Database Security: Multi Cloud and On-prem Database Protections

The Checklist

The easy-to-use checklist below outlines how Imperva application and data security solutions can help you complete a high level FFIEC CAT assessment in each of the 5 cybersecurity domains.

FFIEC Domain	Category	Imperva	My Current Solution
Domain 1 Cyber Risk Management & Oversight	Governance	✔	
	Risk Management	✔	
	Resources	n/a	
	Training & Culture	n/a	
Domain 2 Threat Intelligence & Collaboration	Threat Intelligence	✔	
	Monitoring & Analyzing	✔	
	Information Sharing	✔	
Domain 3 Cybersecurity Controls	Preventative Controls	✔	
	Detective Controls	✔	
	Corrective Controls	✔	
Domain 4 External Dependency Management	Connections	✔	
	Relationship Management	n/a	
Domain 5 Cyber Incident Management & Resilience	Incident Resilience Planning	n/a	
	Detection, Response, Mitigation	✔	
	Escalation & Reporting	✔	

Imperva Domain Key

Application Security

Imperva AppSec Solution	FFIEC Domain Category
Reporting and Analytics	Domain 1: Governance Domain 2: Monitoring & Analyzing Domain 5: Escalation & Reporting
Application Vulnerability Assessment	Domain 1: Risk Management Domain 3: Detective Controls Domain 4: Connections
Application Data Classification	Domain 1: Risk Management Domain 1: Governance
Monitor all external/internal connections	Domain 2: Monitoring & Analyzing Domain 3: Detective Controls
Prevent Unauthorized User Account Access	Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation
Monitor Sensitive Data Access	Domain 1: Risk Management Domain 1: Governance
Prevent Data Exfiltration	Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation
Baseline User Behavior	Domain 2: Threat Intelligence Domain 3: Detective Controls
Detect Anomalous Activity	Domain 3: Detective Controls Domain 5: Detection, Response, Mitigation
Detect Application Attacks	Domain 3: Detective Controls Domain 5: Detection, Response, Mitigation
3rd Party Integrations SIEM, AppScanners, etc	Domain 4: Connections
Prevent DDOS (App, DNS, Infrastructure)	Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation
Protect Serverless Application Code	Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation
Prevent Applications Supply Chain Attacks	Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation
Prevent Client Side Attacks	Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation
Prevent Bad-Bot Activity	Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation
Application User to Data Tracking	Domain 1: Governance Domain 5: Detection, Response, Mitigation Domain 5: Escalation & Reporting
Complete OWASP AppSec Coverage	Domain 1: Risk Management Domain 2: Monitoring & Analyzing Domain 3: Preventative Controls Domain 5: Detection, Response, Mitigation

Imperva Domain Key

Data Security

Imperva DataSec Solution	FFIEC Domain Category
Reporting and Analytics	Domain 1: Governance
DB Vulnerability Assessments	Domain 1: Risk Management
Data Classification	Domain 1: Risk Management Domain 1: Governance
Monitor all external/internal connections	Domain 2: Monitoring & Analyzing
Identify Unauthorized User Privilege Changes	Domain 3: Detective Controls Domain 3: Corrective Actions
Prevent Sensitive Data Access	Domain 3: Preventative Controls Domain 3: Corrective Actions
Prevent Data Exfiltration	Domain 3: Preventative Controls
Baseline User Behavior	Domain 3: Detective Controls
Information Workflow/Orchestration	Domain 2: Information Sharing Domain 3: Corrective Actions Domain 5: Escalation & Reporting
Detect Anomalous Activity	Domain 3: Detective Controls
Detect Insider Threat Events	Domain 3: Detective Controls
Coverage for Any Data Store	Domain 2: Monitoring and Analyzing
Data Access Management/Data Retention	Domain 5: Response (Incident) Domain 1: Governance
3rd Party Integrations	Domain 2: Threat Intelligence Domain 4: Connections