FORTRA™

Gaining Control of Financial Services Cybersecurity Regulations

Introduction

Organizations in the financial sector are all too aware that their industry continues to be one of the top targets for cyber criminals. Among financial services and insurance organizations, basic web application attacks, miscellaneous errors, and system intrusion represent 77% of breaches.[1] That's why so many cybersecurity compliance regulations have sprung up to ensure systems are kept hardened against attack.

This guide covers the main regulations financial services organizations need to comply with and provides tips to go beyond simple compliance.

Financial Cybersecurity Regulations Organizations Need to Care About

While alignment with compliance mandates doesn't always guarantee perfect system security, meeting compliance requirements does put a set of powerful defenses and a solid foundation in place. And aside from contributing substantially to the digital security of your organization, staying compliant keeps steep audit fines at bay. Achieving and maintaining compliance is a formidable effort considering the sheer number of mandatory regulations organizations must contend with.

We've grouped regulations here by region, but it's important to remember that your organization may need to follow regulatory compliance mandates in other regions. For example, United States companies that offer their goods and services to citizens of the European Union must comply with the EU's General Data Protection Regulation (GDPR).

Global

Payment Card Industry Data Security Standard (PCI DSS)

The payment card industry data security standard (PCI DSS) is one of the world's most ubiquitous banking regulations. It applies to any entity that processes, stores, or transfers payment card data. In addition to helping cardholders' data stay in the right hands, PCI also helps card issuers and banks limit their liability in the event a merchant suffers losses from a breach.

Like many regulations, there are a number of requirements packed into PCI DSS that focus on:

- Building and maintaining a secure network and systems
- Protecting account data
- Maintaining a vulnerability management program
- Implementing strong access control measures
- Regularly monitoring and testing networks
- Maintaining an information security policy

EXPERT TIP

Fortunately, technology can help you to cover multiple PCI DSS requirements at the same time. For example, integrity management tools can help you meet PCI DSS Requirement #2 to "apply secure configurations to all system components" and Requirement #11 to "test security of systems and networks regularly" by monitoring and alerting you to misconfigurations and unexpected changes of networks, servers, firewalls, files, and all other components when they occur.

Society for Worldwide Interbank Financial Telecommunications (SWIFT)

SWIFT provides secure financial messaging standards used by banks to initiate international transactions. The Swift Standards group was established to standardize the electronic messaging used by financial services organizations. They release International Organization for Standardization (ISO) standards that dictate the types of data contained within such messages, such as codes for exchanges and market identification and International Bank Account Numbers (IBAN).

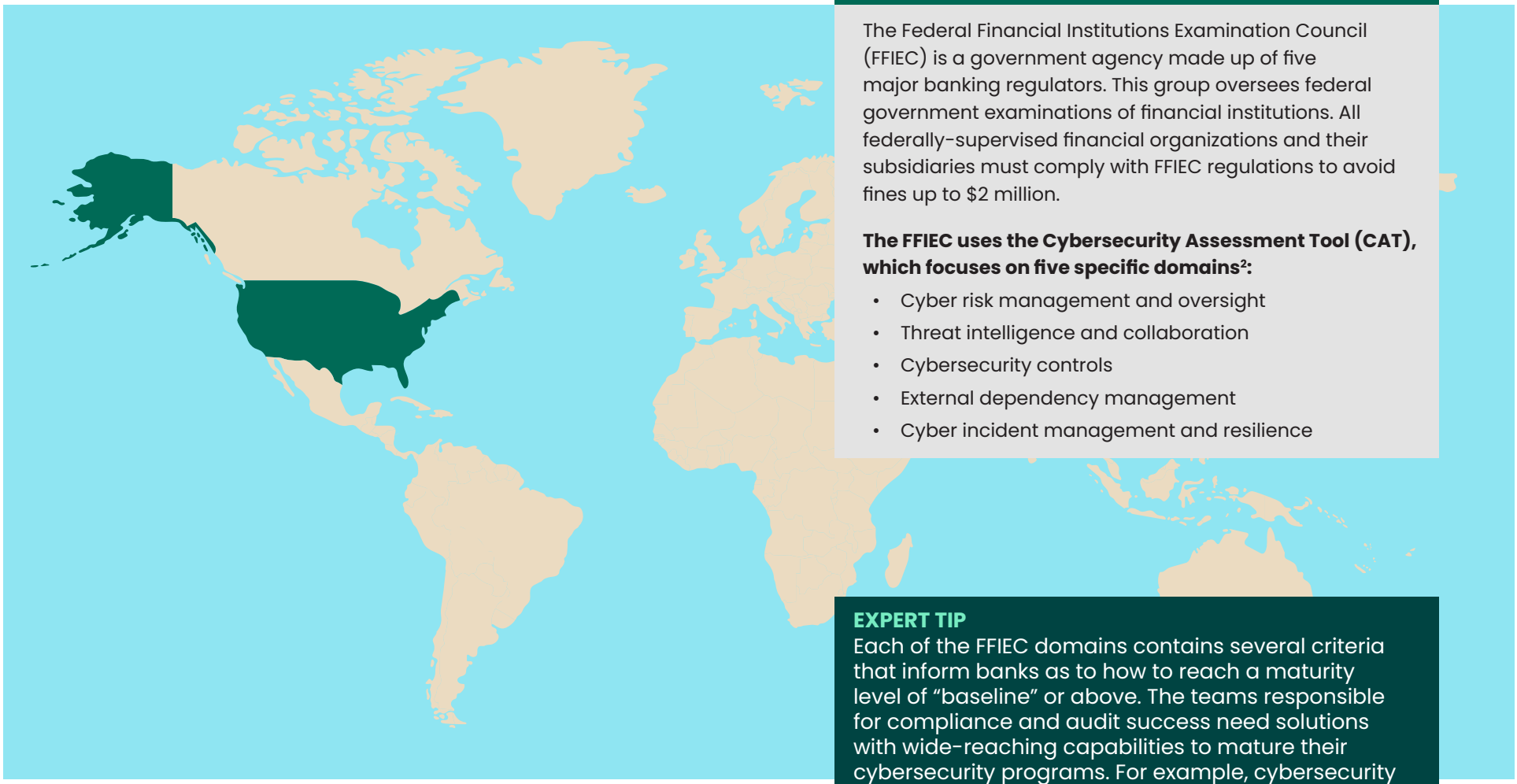
SWIFT data protection policies cover:

- Personal data collection
- Use and disclosure of traffic and message data
- The completion of Security Attestations

EXPERT TIP

Like many of the other major regulations that apply to the financial industry, meeting SWIFT compliance includes keeping detailed reports and audit logs. Security configuration management (SCM) tools can automate the collection of detailed policy data and give you the ability to pull reports from any point in time to demonstrate configuration compliance with standards like SWIFT.

United States



Federal Financial Institutions Examination Council (FFIEC)

The Federal Financial Institutions Examination Council (FFIEC) is a government agency made up of five major banking regulators. This group oversees federal government examinations of financial institutions. All federally-supervised financial organizations and their subsidiaries must comply with FFIEC regulations to avoid fines up to $2 million.

The FFIEC uses the Cybersecurity Assessment Tool (CAT), which focuses on five specific domains[2]:

- Cyber risk management and oversight
- Threat intelligence and collaboration
- Cybersecurity controls
- External dependency management
- Cyber incident management and resilience

EXPERT TIP

Each of the FFIEC domains contains several criteria that inform banks as to how to reach a maturity level of "baseline" or above. The teams responsible for compliance and audit success need solutions with wide-reaching capabilities to mature their cybersecurity programs. For example, cybersecurity controls like configuration and vulnerability management assessed by the FFIEC can be automated—or even managed by your solution provider—in order to streamline proof of compliance.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX), passed by U.S. Congress in 2002, reduces corporate fraud by requiring all publicly held companies to enforce internal controls and procedures for financial reporting. While SOX is not explicit on the required security controls themselves, it refers to the Control Objective for IT (COBIT) framework to give organizations guidance on their IT governance processes. Some of the more challenging requirements of SOX have to do with internal control over financial reporting. Section 302 of SOX—and the Securities and Exchange Commission (SEC) Regulations that were passed to implement it—require companies to enforce internal controls over financial reporting and operations.

Specifically, sections 302(a)(4)(A) and (B) of SOX require a company's chief financial officer and chief executive officer to certify in quarterly and annual reports to the SEC that they:

- Are responsible for establishing and maintaining internal controls
- Have designed such internal controls to ensure that material information about the company and its subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared[3]

EXPERT TIP

To successfully sustain compliance, financial organizations need to implement internal best practices to make sure their IT systems not only achieve a known and trusted state but that they also maintain that state continuously. This helps address the control, evaluation, and disclosure elements of SOX Sections 302, 404, and 409.

Internal Revenue Service (IRS) 1075

The Internal Revenue Service (IRS) 1075 publication applies to any federal, state, county, or local entity that handles federal tax information (FTI). This also includes the contractors of those entities, and its aim is to protect the confidentiality of FTI. The regulation mandates security controls for recordkeeping, data storage and disposal, and computer system security.

According to IRS 1075, all organizations and agencies that handle FTI must do the following:

- Specify the types of changes to the information system that are configuration-controlled
- Review proposed configuration-controlled changes to the information system and approve or disapprove them with consideration for security impact analyses
- Document configuration change decisions associated with the information system
- Implement approved configuration-controlled changes to the information system
- Keep records of configuration-controlled changes to the information system for the life of the system.
- Audit activities related to configuration-controlled changes to the information system
- Coordinate and supply oversight for configuration change control activities through a Configuration Control Board that meets when configuration changes happen
- Test, validate, and document changes to the information system before executing the changes on the operational system

EXPERT TIP

The data oriented with planned changes that needs to be collected for IRS 1075 compliance will typically be documented in a system of record like ServiceNow, Cherwell, Jira, or Remedy. Organizations can save time when they use a change monitoring solution that integrates readily with these systems. It's even better if that monitoring solution can be trusted to accurately report unplanned changes as well.

Gramm–Leach–Bliley Act (GLBA)

Organizations in the U.S. that sell financial products or services such as insurance, loans, or investment guidance must comply with the regulations set out in the Gramm–Leach–Bliley Act (GLBA). It requires policies and practices aimed at protecting the confidentiality of customers' nonpublic personal information. Data sharing practices must also be disclosed to the customers themselves.

There are three primary rule areas of the GLBA, each with their own specific guidance on the handling of financial data:

- The Financial Privacy Rule
- Safeguards Rule
- Pretexting Provisions

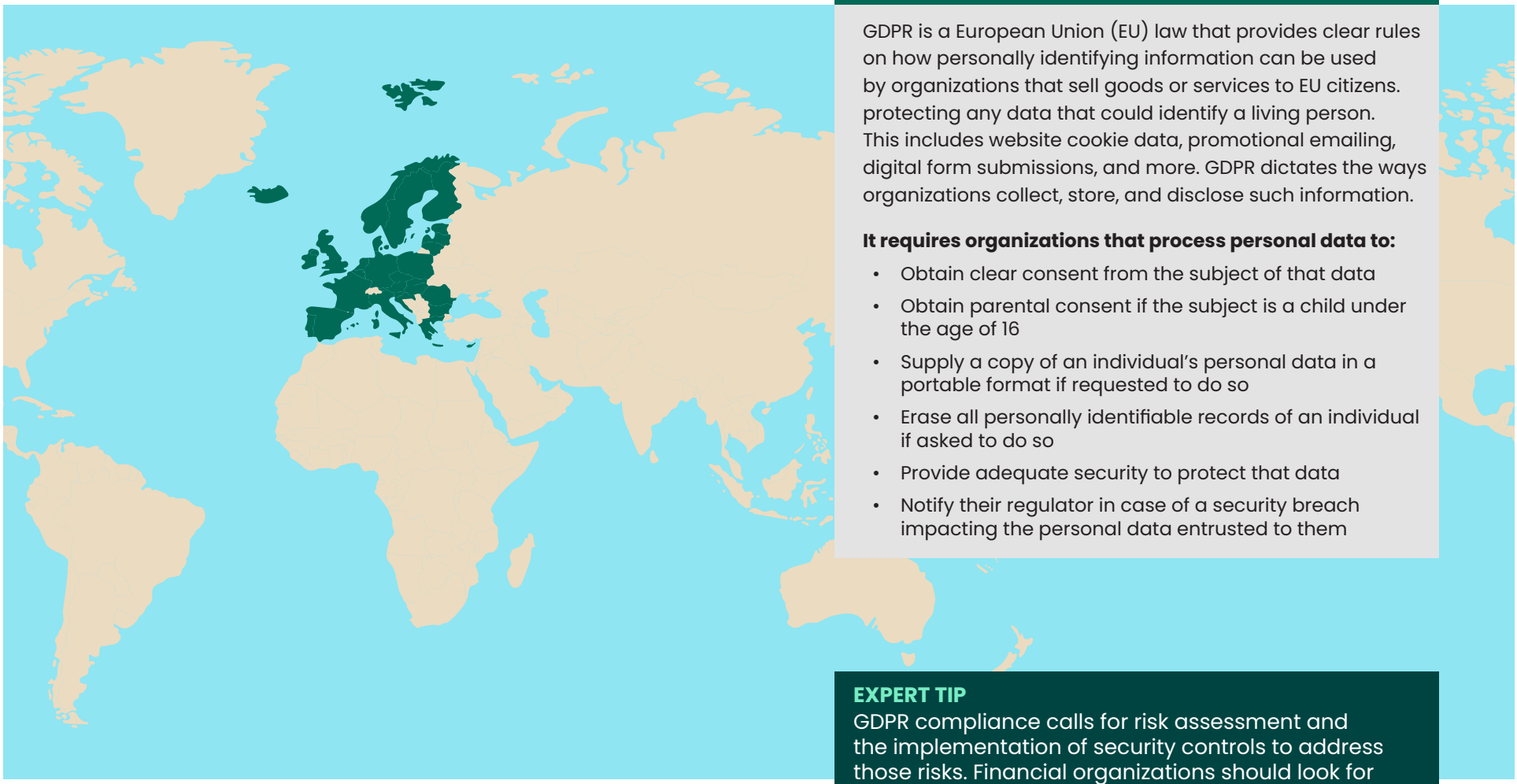
Securities and Exchange Commission (SEC)

The Securities and Exchange Commission (SEC) requires public companies, certain company insiders, and broker-dealers to file periodic financial statements and other disclosures. Finance professionals and investors rely on SEC filings to make informed decisions when evaluating whether to invest in a company. Operating under the SEC, the Financial Industry Regulatory Authority (FINRA) regulates individual broker-dealers.

The SEC is also the entity responsible for enforcing the following information security legislation:

- Securities Act of 1933
- Securities Act of 1934
- Investment Advisers Act of 1940
- Dodd-Frank Wall Street Reform Consumer Protection Act of 2010
- The Sarbanes-Oxley Act of 2002
- Jumpstart Our Business Startup (JOBS) Act of 2012

European Union



General Data Protection Regulation (GDPR)

GDPR is a European Union (EU) law that provides clear rules on how personally identifying information can be used by organizations that sell goods or services to EU citizens. protecting any data that could identify a living person. This includes website cookie data, promotional emailing, digital form submissions, and more. GDPR dictates the ways organizations collect, store, and disclose such information.

It requires organizations that process personal data to:

- Obtain clear consent from the subject of that data
- Obtain parental consent if the subject is a child under the age of 16
- Supply a copy of an individual's personal data in a portable format if requested to do so
- Erase all personally identifiable records of an individual if asked to do so
- Provide adequate security to protect that data
- Notify their regulator in case of a security breach impacting the personal data entrusted to them

EXPERT TIP

GDPR compliance calls for risk assessment and the implementation of security controls to address those risks. Financial organizations should look for an automated vulnerability management solution that proactively discovers, profiles, and assesses the vulnerability risks that could be used to compromise systems or data.

United Arab Emirates

UAE Information Assurance (IA) Standard

The United Arab Emirates Telecommunications Regulatory Authority introduced the UAE Information Assurance (IA) Standard to provide requirements for organizations to protect critical data. The regulation insists that in-scope organizations take a lifecycle approach to information assurance. It applies to all UAE government and private entities dealing with personal or private information.

The technical controls mandated by the UAE IA pertain to:

- Asset management
- Physical and environmental security
- Communications
- Operations management
- Access control

How Fortra™ Streamlines Financial Services Compliance

Most financial services organizations are mandated to follow several of these cybersecurity regulations at once—risking data exposure, hefty auditory fines, or negative press if they don't manage to stay in compliance. Because of this complexity, attempts at manual compliance enforcement are too cumbersome and time-consuming for most organizations to even consider.

Another major challenge is that compliance is never a one-time process; enforcing continuous compliance is the only way to ensure that these cybersecurity regulations are doing what they're meant to do and keeping your systems hardened against breaches. That's where picking the right financial services compliance solution comes in.

Fortra's security tools and managed services use tried-and-true security controls to achieve and maintain compliance with multiple standards at once in a streamlined and well-documented manner. With custom policy creation, you can trust that Fortra solutions will keep your organization audit-ready and hardened against cyberattacks year-round.

> The reliability of the FIM product gives us the confidence to fulfill just about any reporting request coming from our stakeholders and auditors, which makes our audits go very smoothly and quickly.
>
> **— IT VICE PRESIDENT, FORTUNE 500 FINANCIAL SERVICES COMPANY**

Sources

1. https://www.verizon.com/business/resources/Tc41/reports/2023-data-breach-investigations-report-dbir.pdf
2. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_All_Documents_Combined.pdf
3. https://www.sarbanes-oxley-101.com/SOX-302.htm

FORTRA™

About Fortra™

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-tw-gd-1023-r2-gm