EKRAN

7 Best Practices for Banking and Financial Cybersecurity Compliance

www.bakotech.at

Why does compliance matter?

The importance of regulatory compliance, especially for banking and financial organizations, is hard to overestimate.

Financial institutions work closely with highly sensitive data such as personally identifiable information and financial records. And as this data can easily be monetized or used for financial fraud, it's often targeted by cybercriminals.

To ensure secure operations and the proper protection of sensitive data, local and international regulatory bodies establish security compliance requirements for financial institutions. In particular, these requirements can help you outline:

what pain points to pay attention to when building a cybersecurity strategy
what practices and technologies to implement for better data protection.

Compliance regulations explain:

What should be protected

How to protect it

Meeting financial security compliance requirements provides an organization with a number of **essential benefits**, including:

- a clear view of the most critical data and systems
- a better understanding of what cybersecurity tools and practices to use
- greater security for valuable information
- reduced time for cybersecurity incident response.

Not complying with mandatory regulations, in turn, not only deprives financial institutions of these benefits but also **leads to**:

- extensive fines for non-compliance
- financial losses from data leaks, operational disruptions, and lawsuits

- severe reputational damage
- loss of customer trust.

Organizations typically have to comply with more than one set of requirements. There are obligatory and advisory regulations as well as international, federal, and regional laws. By combining the requirements of several laws and standards, financial institutions can build more effective cybersecurity strategies than they can when only following a single set of requirements.
So what IT standards, international regulations, and local laws should financial industry players focus on? In the next section, we overview key mandatory and advisory regulations that banks and other financial institutions should comply with.

Major compliance regulations in the financial industry

Know what requirements you need to meet.

Since financial companies operate with highly sensitive information, it's natural that the financial industry is one of the most strictly regulated. There are three major **international data security standards** that financial institutions should comply with:

Payment Card Industry Data Security Standard (PCI-DSS) — Any organization, institution, merchant, and payment solution provider must comply with PCI DSS. This standard specifies requirements for processing, storing, and transferring payment card data. The key goal of the standard is to reduce cases of credit card fraud and improve cardholder data protections.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 — The ISO/IEC 27001 standard is part of the large ISO/IEC 27000 family of cybersecurity standards. The 27001 standard outlines recommendations and proper procedures for managing security risks, including for managing financial information.

SWIFT Customer Security Programme (CSP) — Any financial organization using SWIFT services must comply with SWIFT SCP requirements. This framework specifies requirements for properly protecting data, managing access, and responding to incidents.

Then come **regulations** that vary from country to country. Some of the most well-known are:

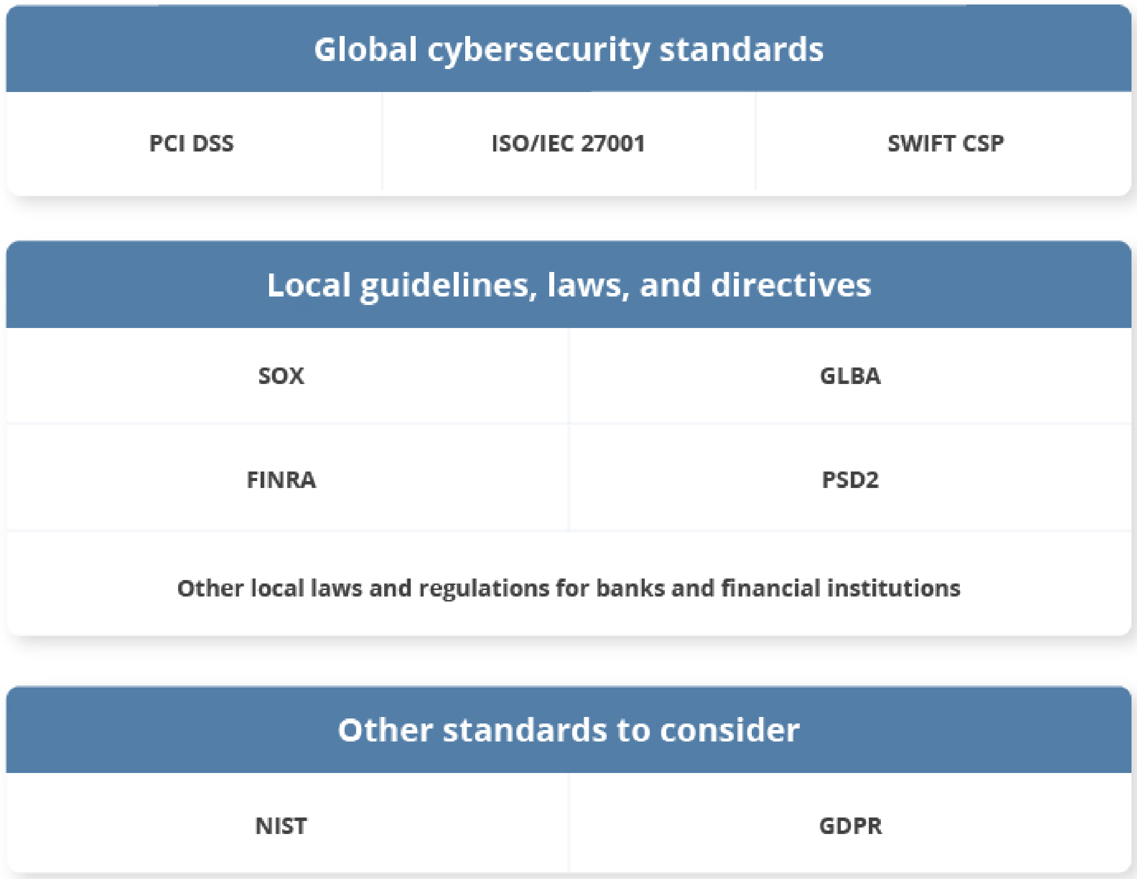
The Sarbanes Oxley Act (SOX) — This act outlines recommended practices that can prevent organizations from processing fraudulent financial transactions. In particular, it specifies what financial records should be stored, for how long, and how they need to be protected. This law is applicable to all public companies registered by the US Securities and Exchange Commission.

The Gramm–Leach–Bliley Act (GLBA) — This US law governs the way financial institutions handle customers' private data. In particular, it requires companies to establish strict data access policies and provide customers with full information on how their data is stored, processed, and secured.

Financial Industry Regulatory Authority (FINRA) — This organization provides guidelines and sets requirements for US broker-dealers. Key FINRA requirements include having written data protection policies for preventing the compromise of consumer data. FINRA also outlines rules for detecting and mitigating cyber threats.

Payment Services Directive (PSD 2) — This EU directive regulates electronic payments within the European Union (EU). It outlines requirements for the way electronic payments are initiated and processed and sets strict rules for the protection of customers' private data.

Major compliance regulations in the financial industry



Global cybersecurity standards		
PCI DSS	ISO/IEC 27001	SWIFT CSP

Local guidelines, laws, and directives	
SOX	GLBA
FINRA	PSD2
Other local laws and regulations for banks and financial institutions	

Other standards to consider	
NIST	GDPR

In addition to industry-specific laws and regulations, there are other requirements that banks and financial institutions should pay special attention to. In particular, guidance from the National Institute of Standards and Technology and the General Data Protection Regulation can be rather helpful for securing sensitive data, ensuring flawless operations, and avoiding expensive fines.

National Institute of Standards and Technology (NIST) — This US government agency provides recommendations for cybersecurity risk management, data protection, threat detection, and incident response. While targeted mostly at federal institutions, NIST recommendations can be effectively followed by any organization that wants to ensure a high level of security for its sensitive assets.

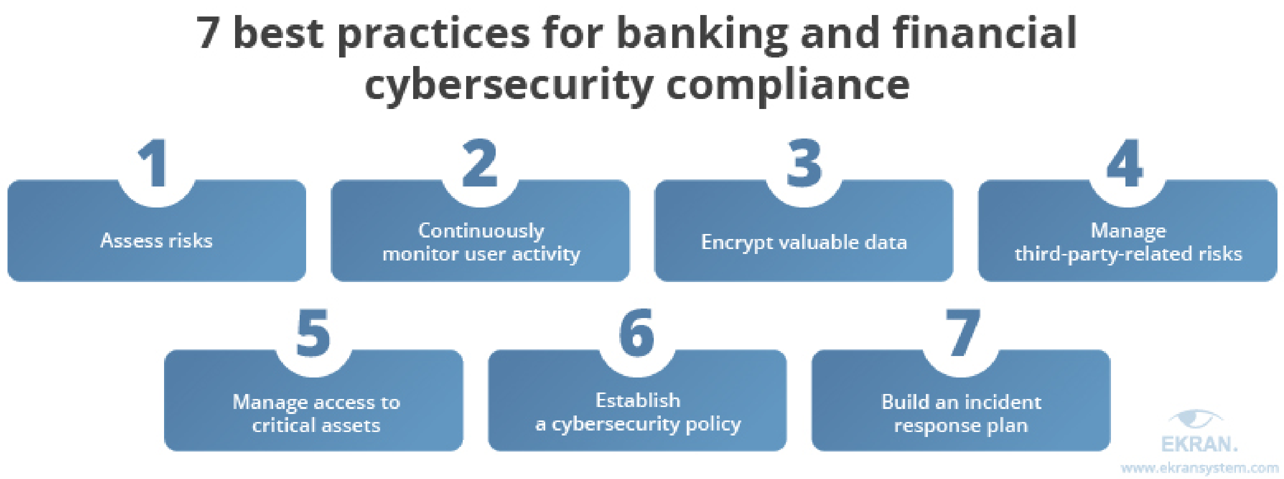
General Data Protection Regulation (GDPR) — This data privacy framework sets rules for collecting, storing, transferring, and processing the personal data of EU residents. Compliance with GDPR requirements is mandatory for any organization that processes the private data of EU citizens, no matter where such an organization is registered and operates.

While having a lot of differences and peculiarities, major data privacy and cybersecurity regulations still have some common ground. In the next section, we outline seven practices that you'll find rather helpful for meeting the requirements of most cybersecurity standards.

7 best practices for cybersecurity compliance

Protecting critical data and systems is a continuous process, not an end state.

It's true that each cybersecurity standard and data protection law imposes different requirements and recommendations. However, meeting them and improving the security of your most critical data and systems becomes much easier when you follow these seven best practices:



7 best practices for banking and financial cybersecurity compliance

1. Assess risks
2. Continuously monitor user activity
3. Encrypt valuable data
4. Manage third-party-related risks
5. Manage access to critical assets
6. Establish a cybersecurity policy
7. Build an incident response plan

EKRAN.
www.ekransystem.com

Let's look closer at each of these practices.

1. Assess risks. Periodic risk assessments give you full visibility into your IT infrastructure. They can help you determine your most valuable assets and detect and prioritize the mitigation of weak spots and vulnerabilities that cybercriminals can use to compromise your corporate network. For instance, businesses in the financial sector often fall victim to insider threats, distributed denial of service and phishing attacks, ransomware, and third- and fourth-party-related risks.

Information gathered during risk assessments can help you analyze and evaluate your current level of protection for critical data as well as outline new vectors for future data security improvements.

2. Continuously monitor user activity. User activity monitoring plays a crucial role in detecting and preventing both insider and outsider threats. It's also the key requirement of many cybersecurity regimes, including PCI DSS and SOX.

By watching and analyzing user actions in your network, you can detect suspicious events and see early signs of an attack in progress. **User and entity behavior analytics (UEBA)** solutions can significantly simplify and speed up this process.

To use your resources wisely, consider applying different amounts of monitoring effort to different groups of users, with privileged users getting the most attention.

3. Encrypt valuable data. Stolen data is only useful when it can be read. Therefore, it's better to encrypt all your sensitive data. Data encryption is either required or recommended by ISO standards, the GDPR, PCI DSS, and other cybersecurity regimes.

To protect your data in full, look for solutions that allow you to encrypt data both in transfer and at rest. This way, you can significantly minimize the risk of a devastating data breach.

4. Manage third-party risks. **Subcontractors** are often granted access to data with different levels of importance. Yet a mistake made by a third party can result in anything from a minor service crash to a major data breach. This is why financial institutions and banks need to closely monitor and carefully manage third parties.

The most efficient ways to manage third-party-related risks include monitoring the activities of third parties, limiting their access to critical data, and requiring subcontractors to comply with the same cybersecurity standards and regulations that you do.

5. Manage access to critical assets. Current cybersecurity trends incorporate approaches based on strict access limitations like the principle of least privilege and the zero trust model. If strict limitations for everyone aren't suitable for you, then at least consider securing your most critical assets by implementing sophisticated **privileged access management (PAM)** solutions and enforcing **multi-factor authentication (MFA).**

Two-factor authentication is a great technology for enhancing the protection of your most critical data and systems. Alongside MFA, you can deploy such solutions as one-time passwords and manual access approvals.

6. Establish a cybersecurity policy. A cybersecurity policy is a summary of all the requirements your organization should meet, all the practices you intend to implement, and the tools that can be used for doing so. Having a written cybersecurity policy in place makes it easier for an organization to establish an effective cybersecurity routine and maintain a certain level of data security in the long term.

For maximum effectiveness, consider implementing a hierarchical cybersecurity policy instead of a centralized one. Also, make sure to periodically revise this policy to keep its requirements and recommendations up to date.

7. Build an incident response plan. Alongside a cybersecurity policy, every financial institution should have a **well-thought-out incident response plan.** This document should outline clear action scenarios for different situations that your organization may find itself in.

In particular, such a plan should specify what can be considered a cybersecurity incident, what the first actions should be in case of a cybersecurity incident, and **what to do to restore lost data** or affected systems. It also should clearly state who to call and notify first and who to turn to if the first contact person is unavailable.

Note that different compliance regulations set different time frames for reporting cybersecurity incidents. Make sure to specify your organization's required response times within your incident response plan.

How to use Ekran System for cybersecurity compliance

While ensuring proper banking security compliance is a tough task, there are solutions that can help you tackle this challenge. Being a full-cycle insider threat management platform, Ekran System provides you with a full set of tools and technologies for deterring, detecting, and disrupting insider threats.

Ekran System makes data protection and cybersecurity compliance in the financial sector easy. In particular, Ekran System enables you to:

- **Granularly manage access to critical data and assets**, thus successfully implementing a zero trust model and adopting the principle of least privilege
- **Continuously monitor and analyze user activity in real time** to know exactly who does what in your system and whether or not their actions seem suspicious
- **Deploy advanced identity verification solutions** to make sure only legitimate users get access to your system
- **Monitor and manage third-party vendors** to improve information security and eliminate subcontractor-related risks
- **Set custom rules for alerts and notifications** to respond to cybersecurity incidents effectively and in a timely manner
- **Generate and export detailed reports** for further forensic investigations and cybersecurity audits
- Meet the requirements of key acts, directives, and standards, including **NIST 800-53, NIST SP 800-171, PCI DSS, SWIFT CSP, SOX, GLBA,** ISO/IEC 27001, and the **GDPR.**

In addition to all that, fast and easy deployment along with an intuitive user interface allow you to spend less time configuring the platform.

Conclusion

The financial sector is one of the most strictly regulated, as banks and financial institutions work closely with customers' private information, social security data, and financial records. Different laws and cybersecurity standards are meant to help financial organizations reduce the risk of cybersecurity incidents and ensure the proper protection of valuable information.

Common cybersecurity requirements for financial service providers include strict access management, continuous user activity monitoring and risk assessment, third-party risk mitigation, data encryption, and incident response implementation.

Ekran System provides financial industry players with all the tools and technologies necessary for ensuring proper protection of the most sensitive data and meeting the requirements of international and local regulations and standards. Try Ekran System free for 30 days to check out all its data protection capabilities for yourself.

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. Geographically the Group operates in 29 countries covering Central, Western and Eastern Europe, the Balkans, the Baltic States, the Caucasus, Central Asia with offices in Prague, Krakow, Riga, Minsk, Vienna, Kyiv, Baku and Nur-Sultan.

To get more information about **Ekran System** solutions, please contact us at **ekran@bakotech.at** or visit **www.bakotech.at**