What cybersecurity framework is right for you?

Pedro J. Pinto

Jun 03, 2024

3 min read

Cybersecurity is vital to any organization that deals with sensitive data, especially financial institutions. Cyberattacks cause significant losses, reputational damage, regulatory fines and legal liabilities for financial institutions.

Therefore, it is essential to have a robust and comprehensive cybersecurity strategy that aligns with the organization's business objectives, risk appetite and regulatory requirements.

One way to achieve this is to adopt a cybersecurity framework that provides a structured and consistent approach to managing cybersecurity risks, implementing best practices and measuring performance. Common benefits of implementing these frameworks include:

- Enhancing the security and resilience of information systems and assets.
- Reducing the likelihood and impact of cyber incidents.
- Establishing a common language and understanding of cybersecurity risks and controls.
- Improving the communication and collaboration among stakeholders, including regulators, auditors, partners and even customers.
- Facilitating the continuous improvement and adaptation of cybersecurity practices.

Common cybersecurity frameworks

Several cybersecurity frameworks are available today, each with its own scope, objectives and methodology. This table lists some details about the most common frameworks used by financial institutions:

Organization	**Framework**	**Benefits**	**Features**
National Institute of Standards and Technology (NIST)	Cybersecurity Framework (CSF)	Provides a common language for understanding, managing and expressing cybersecurity risk.	Consists of five core functi identify, protect, detect, res and recover.
Federal Financial Institutions Examination Council (FFIEC)	Cybersecurity Assessment Tool (CAT)	Helps banks assess their cybersecurity preparedness.	Consists of a series of asse statements to determine ar institution's inherent risk ar cybersecurity maturity.
National Credit Union Administration (NCUA)	Automated Cybersecurity Evaluation Toolbox (ACET)	Helps credit unions assess their cybersecurity preparedness.	

Center for Internet Security (CIS)	Critical Security Controls (CSC)	Provides a prioritized set of actions for improving cybersecurity posture.	Consists of 20 critical secu controls for effective cyber
Financial Services Sector Coordinating Council (FSSCC)	Cybersecurity Profile	Provides a scalable and efficient approach for financial institutions to assess and manage cybersecurity risk.	Consists of diagnostic state determine an institution's cybersecurity risk and matu

Which cybersecurity framework works best for your institution?

Any of these frameworks would do the job, but the question remains: Which one is best for your institution? Here are some considerations to help you choose:

1. Regulators

As regulators are the ones who ultimately have the final say on the adequacy of your institution's cybersecurity preparedness, it is important to understand their expectations. The FFIEC CAT has been the standard used by banks and credit unions. In 2019 the NCUA published an updated assessment tool (ACET) specific to credit unions, though CAT and ACET are very similar.

In 2019, the FFIEC published a press release encouraging institutions to use a standardized approach to assess and improve cybersecurity preparedness and listed several frameworks that could be used for that purpose, signaling that the adoption of other standards, including industry-agnostic ones, was acceptable. In addition to the CAT/ACET, the list included the FSSCC Cybersecurity Profile, the NIST Cybersecurity Framework and the Center for Internet Security (CIS) Controls.

In 2023 the OCC published Bulletin 2023-22: Cybersecurity Supervision Work Program (CSW). They made it clear that institutions could use any framework they chose, but that the new program would more closely align with the NIST CSF.

2. Third-party providers

Another consideration is your third-party providers, especially if they play a more hands-on role in your institution's cybersecurity. In some cases, the provider will help you complete the cybersecurity assessment, so it's worth considering what frameworks they are familiar with so they can better help you or better understand requests you may have for improving certain controls.

3. Leadership

One consideration that sometimes gets overlooked is how the results from assessments can be reported. Depending on the level of comfort your board of directors and leadership team have with more technical information, it might be beneficial to choose a framework that provides the information in a more easily understandable format.

4. Internal teams

Lastly, it is important to consider who in your organization will be responsible for performing information security and cybersecurity assessments. This individual or team needs to be comfortable with the framework and understand its components to make it truly useful to the institution and not just a “checkbox” report to provide to regulators and auditors once a year.

Consider using one of the many risk management platforms available today. These platforms allow you to choose one or more frameworks as the basis for your information security and cybersecurity risk assessments and are automatically updated if the frameworks themselves are updated.

How Wipfli can help

Choosing and implementing a cybersecurity platform is essential to the long-term health and well-being of your financial institution, and our team of dedicated cybersecurity professionals can help put you on the path to long-term peace of mind. From selecting and refining a strategy to measuring performance, we’re with you every step of the way to help keep your data secure and your workflow safe. Learn more about our cybersecurity offerings.