IriusRisk

Digital Modernization: faster and more secure

A guide to scalable threat modeling for banking and financial services organizations

Table Of Contents

Balancing Innovation, Security and Compliance in a Financial Landscape

The number of cyberattacks on banks has almost doubled since before the COVID-19 pandemic,[1] and it is no surprise when it is such a fruitful sector for hackers. In 2023, the global financial system intermediated $140 trillion in assets, generating about $7 trillion in revenue[2].

Add to this the continuation of regulatory compliance, and the finance sector needs to be stringent in its efforts to secure its products and services which are prime targets for attacks, while adhering to new and evolving mandates.

Banks are under pressure from customers to make existing and new services completely digital, and easily accessible to users. These products are also expected much faster. Financial services must continue innovation, while also demonstrating they are conforming to legislation and blocking potential breaches. Combine this with legacy infrastructure that may have less complex security controls in place, and suddenly digital modernization becomes much harder to achieve. Not to mention that emerging competitors with fully online banking solutions — without the legacy systems slowing down innovation — are disrupting the competitive landscape, thus adding another layer of urgency and complexity. So, what steps can be taken to consider GRC requirements, improve overall security, and provide innovative and robust solutions for customers? Let's tackle these one at a time.

A new approach to managing Governance, Risk and Compliance (GRC)

Financial institutions require implementation of robust security measures to safeguard customer data, financial transactions, and operational systems. Certain banking regulations explicitly or implicitly ask them to ensure secure system design and compliance. Basel III/IV are sets of international banking regulations though focused on financial risk, it emphasizes operational risk management, including cyber risks. Others like PCI-DSS explicitly require banks to ensure secure design for handling credit card information, and must also comply with local protection laws (e.g. GDPR, CCPA, PIPEDA, LGDP) that require proactive identification of risks to personal and sensitive information. In many jurisdictions, banks are considered part of critical infrastructure with additional requirements as NIST Cybersecurity Framework (CSF), ISO 27001/27005, European DORA (Digital Operational Resilience Act) and Financial Institutions Examination Council (FFIEC). Keeping up with these evolving regulatory requirements can be complex and resource-intensive.

This is where a Secure by Design technique called Threat Modeling comes in. Threat Modeling as a practice is a structured process which allows users to identify security requirements, recognize security threats and potential design weaknesses. It then gives you the necessary security controls (we call them countermeasures), to mitigate the highest risks. Threat models can demonstrate to auditors how the bank identifies and mitigate risks, ensuring adherence to regulations.

How does this help with adhering to regulation?

IriusRisk Threat Modeling Tool has a built-in security content library, which includes industry standards such as PCI DSS, GDPR, and ISO 27001. When threat modeling the product or services, it is possible to apply the PCI DSS standard for example, to see threats and countermeasures applicable to that compliance need. Allowing financial organizations to focus on those areas first that mitigate the highest levels of risks, and conform to the necessary standards. Including a full audit trail and even a compliance report. These are examples of capabilities that drive your risk management strategy by complying with data protection laws, cybersecurity mandates, and operational resilience standards. This proactive approach minimizes regulatory risk, increases security, and ensures trust in financial systems.

Where is threat modeling mandated?

In the The National Institute of Standards and Technology (NIST) Secure Development Framework (SSDF), it is stated specifically within the guidelines under Control Ref SA-8, Section PW.1.1 - that *'some form of Risk Modeling (including Threat Modeling) must be done to assess the security risk for software and must comply with a variety of standards'.*

The Software Security Framework v1.2 by PCI SSC emphasizes secure coding practices. While not explicitly mentioning threat modeling, it promotes proactive measures to safeguard critical assets and aligns with industry best practices for secure software development.

Finally, in the NIST Guidelines on Minimum Standards for Developer Verification of Software, in section 2.1 it says *'We recommend using threat modeling early in order to identify design-level security issues and to focus verification. Threat-modeling methods create an abstraction of the system, profiles of potential attackers, including their goals and methods, and a catalog of potential threats'.*

The Federal Financial Institutions Examination Council (FFIEC) emphasizes the importance of threat modeling within its Information Security Booklet. This guidance underscores threat modeling as a critical activity for financial institutions to identify and quantify risks effectively

- *"Determine whether management uses threat modeling (e.g., development of attack trees) to assist in identifying and quantifying risk and in better understanding the nature, frequency, and sophistication of threats."*

FFIEC explicitly recognizes threat modeling as an essential activity for financial institutions, highlighting its role in strengthening information security and risk management frameworks.

Where can Threat Modeling help with GRC?

ISO/IEC 27001:2022

ISO/IEC 27001 focuses on the establishment, implementation, maintenance, and continual improvement of an Information Security Management System (ISMS). Threat modeling is implied in the following areas:

Clause 6.1.2: Information Security Risk Assessment

Organizations are required to:

- Identify information security risks.
- Assess potential threats, vulnerabilities, and impacts to assets.
- Analyze the likelihood and consequences of security events.

Threat modeling supports identifying and analyzing threats and vulnerabilities affecting information systems.

Annex A: Controls (A.12.6.1, A.18.1.3)

- A.12.6.1: *Technical vulnerability management* mandates identifying and addressing vulnerabilities to prevent exploitation.
- A.18.1.3: Addresses compliance with security-related requirements, which often includes risk and threat identification.

Relevance to Threat Modeling: Helps identify technical vulnerabilities and threats as part of broader risk assessment.

ISO/IEC 27005:2022

ISO/IEC 27005 provides detailed guidance on information security risk management, which strongly aligns with threat modeling practices:

Clause 8: Risk Assessment

- 8.2.2: Risk Identification
  Organizations must identify:
  - Threats to assets.
  - Existing vulnerabilities that can be exploited.
  - Potential impacts on confidentiality, integrity, and availability

The process explicitly requires understanding the interaction of threats, vulnerabilities, and assets, which is the foundation of threat modeling.

- 8.2.3: Risk Analysis

  Analyzing the identified risks includes evaluating the likelihood of threat scenarios and their potential impact

Evaluating “threat scenarios” directly aligns with modeling possible threat paths.

Clause 9: Risk Treatment

- Involves designing controls or mitigations based on the results of the risk assessment.

Threat modeling contributes to identifying which controls best mitigate specific threat scenarios.

Digital Operational Resilience Act (DORA)

1. ICT Risk Management Framework: DORA mandates that financial entities establish a comprehensive framework to manage Information and Communication Technology (ICT) risks. This includes identifying, assessing, and mitigating risks that could compromise the security of network and information systems. Threat modeling directly supports this by systematically identifying potential threats during system design and development.
2. Incident Response and Recovery: DORA emphasizes the importance of having robust incident response and recovery strategies. By engaging in threat modeling, organizations can anticipate possible security incidents and develop effective response plans tailored to specific threat scenarios, thereby enhancing their preparedness and resilience.
3. Third-Party Risk Management: With the increasing reliance on third-party service providers, DORA mandates strict management of third-party risks. Threat modeling extends to evaluating the risks associated with third-party components, ensuring that external services do not introduce unacceptable vulnerabilities.

Balancing security and innovation with legacy infrastructures

Legacy systems often face unique challenges, such as outdated technologies, lack of vendor support, and difficulty integrating with modern solutions.

Financial services are lucrative targets due the level of customer information, and payment data that remain high incentives for hackers. Most financial institutions have older legacy systems and infrastructure that cannot be entirely moved away from, and when integrating this infrastructure with newer technologies, there can be security gaps and design flaws that get overlooked. Leaving crucial pathways open for attackers to exploit.

Malicious Hackers are looking for financial gain, and to cause maximum disruption. If banking and finance companies threat model their entire infrastructure, even third party boundaries, then the whole attack surface is suddenly in view. The threat model will identify areas of sub-par security, and recommend ways to improve and rectify this. In addition, improvements can be made such as containments so that if a successful breach takes place, the level of damage can be isolated, and not result in full access across all systems.

What are the opportunities for ideation and innovation?

In a more positive outlook, by having a true view of the attack surface and all the intersections of data being passed and various systems integration and communicating with each other, will identify security improvements that can be made. Enhancements to existing systems and innovative ideas to elevate current security practices are possible, visible and easy to track. The threat model can even be theoretical, if a company wants to map out a new product idea and understand the potential vulnerabilities it could have, and how it can interconnect with other platforms. This can be invaluable to encourage ideation and innovation.

Accelerating time to market with secure by design principles

One view of security is that it slows the development and launch process down – particularly using conventional methodologies where the first touchpoint for security is testing just before release. When security issues are inevitably identified, the business often has to make a difficult decision between releasing the software on-time but with known security flaws or delaying the release to correct the security flaws and lose a market opportunity.

With new competitors entering the market with dynamic pricing strategies, bolder and more innovative solutions, the pressure is on to release and update products, and fast. And yet the standard for security cannot slip, or the financial institution or bank may be subject to a data breach. This is where threat modeling can alleviate that pressure, while building in robust security practices from the get go.

When is the right time to introduce threat modeling?

NIST advises that threat modeling should be conducted during the design phase to identify potential security issues before they become costly to address. The NIST has estimated that correcting code once an application is in production can take thirty times the time required for remediation and re-design.

If companies choose to threat model at the design phase, any flaws will be identified right at the beginning. This saves costly and resource-intensive bug fixes, updates and vulnerability management processes. Threat modeling is a proactive layer of security that saves precious time, while elevating your security and risk management processes. Of course a system or architecture can be threat modeled at any point, but it should be viewed as an ongoing activity, and not a one-and-done approach to security. Even if a product doesn't change over a 12-month period, new attack techniques can emerge.

What time saving can be expected from IriusRisk threat modeling?

Up to 90% time saving, as seen in the independent study from Forrester, which found IriusRisk Threat Modeling Tool reduces the average time to threat model from 80 hours down to just 8 hours. The study was based on interviews with finance and software companies. In addition, ClearBank achieved increased time-saving for other crucial activities, the ability to scale, and now has all teams considering security across the SDLC processes. Read more in the ClearBank case study.

Scalability and team adoption, while managing the growing risk landscape

Banking and financial organizations need to ensure any security investments will stand the test of time, and be fully adopted by current teams. As a result, there has been a move towards adopting a start left approach—one that starts earlier on in the development cycle.

The key to scaling this activity across a large portfolio of applications is to move the responsibility for software security from the central security to the engineering teams and to empower those teams with a self-service automated threat modeling solution. This removes the central security team as a bottleneck to the product release process, allowing faster releases that still meet the security and compliance requirements of the organization.

> ***In terms of adoption, having it cloud based gives the ability for anyone to access it, whether their role is a developer, product owner or a risk manager. I think people find the automation part really valuable. We can re-prioritise that time we would usually spend with the team into continuous improvement tasks which helps the business move forward while creating autonomy.***
>
> ClearBank

What about the broadening risk surface that comes with scale and expansion?

Supply chains and overall security is complicated. Managing both legacy infrastructure alongside cloud and digital revolutions is a big job. Efforts need to be scaled, but with scale comes wider risks, and new potential intersections creating vulnerabilities.

> ***IriusRisk allows us to make changes at the design stage. It reduces risk and the financial impact in case of breaches or downtime. In banking, reducing risk is enough of an argument to introduce a new tool.***
>
> Director of Cloud Engineering - Financial industry

Conclusion

Financial institutions are under increasing pressure to protect sensitive data, maintain operational resilience, and comply with a multitude of regulatory requirements. Threat modeling has become an indispensable tool for banks and financial institutions to address these challenges. Not only is threat modeling recognized as a best practice, but it has also become a regulatory necessity, especially in light of stringent standards such as **Basel III/IV, PCI DSS, GDPR**, and frameworks from organizations like **ISO, NIST, DORA**, and the **FFIEC**. These regulations and standards provide a comprehensive approach to managing information security and risk assessment, ensuring that financial institutions can safeguard critical data while maintaining compliance and customer trust.

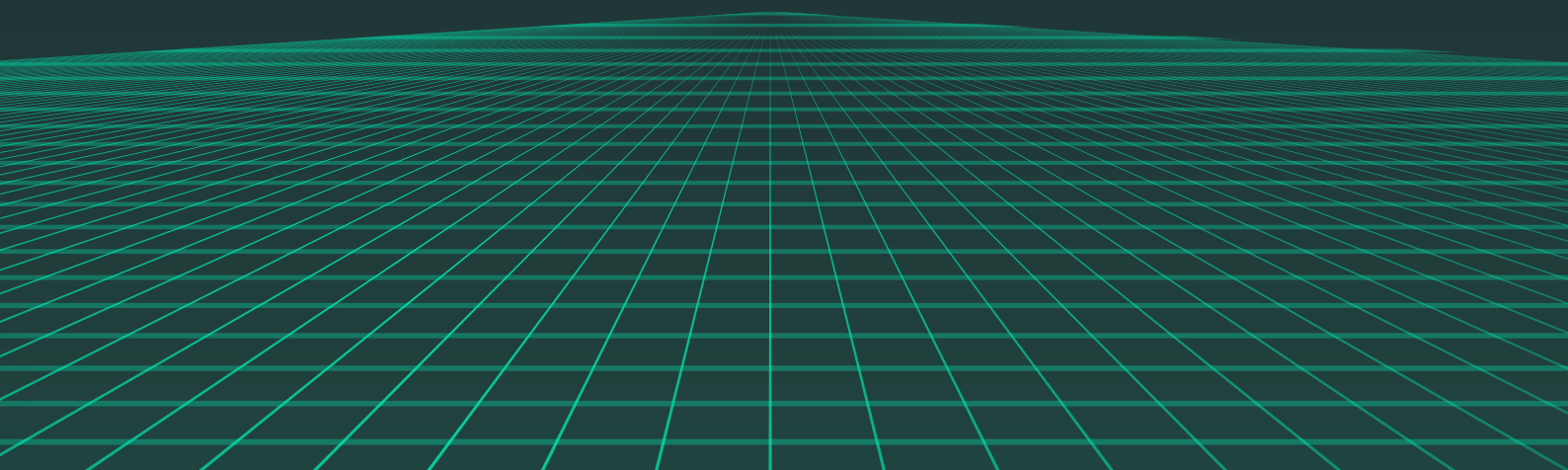
Automate Threat Modeling to fit your existing SDLC

Secure design right from the start

Visit **www.iriusrisk.com**

to book your demo

IriusRisk



References

1. European Insurance and Occupational Pensions Authority, Digital Operational Resilience Act (DORA) (2023) https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
2. Federal Financial Institutions Examination Council (FFIEC), Information Security Handbook (2016) https://www.ffiec.gov/press/pdf/ffiec_it_handbook_information_security_booklet.pdf
3. Forrester, The Total Economic Impact™ Of The IriusRisk Automated Threat Modeling Platform (2023) https://4550632.fs1.hubspotusercontent-na1.net/hubfs/4550632/Forrester%20TEI%20Files/TEI_of_IriusRisk_Automated%20Threat%20Modeling%20Platform.pdf
4. International Monetary Fund (2024), Global Financial Stability Report – The Last Mile: Financial Vulnerabilities and Risks, April
5. International Organization for Standardization, ISO/IEC 27001:2022 https://www.iso.org/standard/27001
6. International Organization for Standardization, ISO/IEC 27005:2022 https://www.iso.org/standard/80585.html
7. McKinsey, Global Banking Annual Review (2024): Attaining escape velocity https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review
8. National Institute of Standards and Technology, Guidelines on Minimum Standards for Developer Verification of Software (2021) https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf
9. National Institute of Standards and Technology, Secure Software Development Framework (SSDF) v1.1 (2021) https://csrc.nist.rip/Projects/ssdf
10. PCI Securirty Standards Council, Software Security Framework v1.2 (2022) https://www.pcisecuritystandards.org/about_us/press_releases/pci-security-standards-council-publishes-version-1-2-of-the-secure-software-standard-and-program/