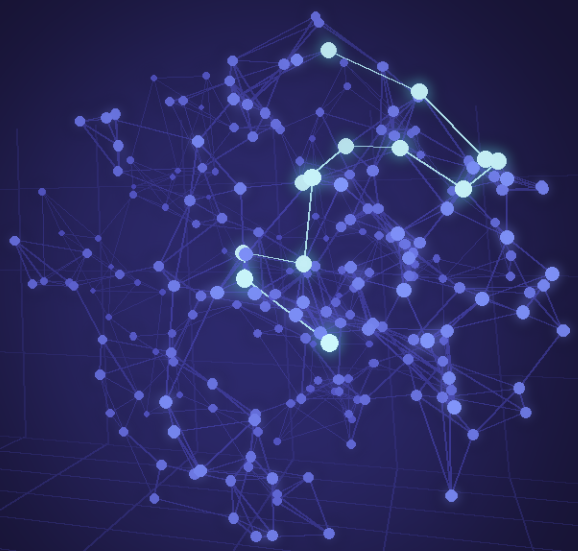
ThreatModeler

WHITEPAPER

A Critical Security Practice

Threat modeling and regulatory compliance.



WHY THIS MATTERS

Introduction

As cyber threats escalate, regulatory compliance has become a baseline requirement for protecting sensitive data and avoiding costly penalties. Building applications, cloud services, and infrastructure secure by design is no longer optional. Threat modeling plays a central role, identifying and mitigating security risk before it is exploited.

This paper looks at how threat modeling supports regulatory and compliance obligations. It separates regulations (laws) from frameworks (guidelines), and shows how ThreatModeler® Nexus™ integrates security into the software development lifecycle and produces compliance reporting as a byproduct of the work, rather than a separate effort.

THE THROUGHLINE

Compliance is an outcome of good design, not a separate task.

When threats, mitigations, and requirements are connected in one system of record, the evidence an auditor asks for is already there.

UNDERSTANDING THE TERMS

Laws vs. Frameworks

Compliance in cybersecurity falls into three areas. Laws and the regulations that implement them carry penalties for non-compliance; voluntary frameworks make meeting them easier. With a solid threat modeling strategy, adopting standards and tracking compliance becomes far more manageable.

1

Laws

Legal requirements set by governments, such as the EU Data Protection Directive and the California Consumer Privacy Act (CCPA). Laws are clarified through regulations that detail how to comply, and non-compliance can carry fines and legal consequences.

2

Regulations

Detailed rules issued by an administrative agency, such as the FTC or the EU Commission, that implement and enforce the law. Well-known examples include HIPAA for healthcare, DORA and PCI DSS for financial services, the EU Cyber Resilience Act (CRA) for products with digital elements, and GDPR for data protection.

3

Standards & Frameworks

Best-practice guidelines organizations adopt voluntarily, such as NIST 800-53 and ISO 27001. Adherence is not always mandated, but it strengthens security posture and simplifies compliance with regulations like GDPR, PCI DSS, and HIPAA.

THE ROLE IT PLAYS

Threat Modeling in Compliance

Threat modeling is a structured way to identify security threats, assess their impact, and define mitigations. It is essential for compliance because it integrates security controls early in the lifecycle, reducing exposure before it reaches production.

PROACTIVE RISK MITIGATION

Finds and addresses design flaws before they can be exploited.

CONTINUOUS INTEGRATION

Embeds security into DevOps and CI/CD rather than bolting it on late.

AUTOMATED COMPLIANCE

Aligns security measures with regulations and frameworks to streamline audits.

COST SAVINGS

Reduces rework by addressing security early in development.

THREAT MODELING IN MAJOR REGULATIONS AND FRAMEWORKS

FRAMEWORK	TYPE	HOW THREAT MODELING SUPPORTS COMPLIANCE
GDPR	Regulation	Identifies risks to personal data and implements the controls that protect it.
PCI DSS	Regulation	Validates security controls in payment-processing applications.
HIPAA	Regulation	Assesses threats to protected health information and confirms required safeguards.
NIST 800-53	Framework	Maps identified security threats to recommended controls.
ISO 27001	Framework	Surfaces risks in the information security management system; used as proof for GDPR, HIPAA, SOX, and DORA.
UNR155 / TARA	Regulation	Supports cybersecurity risk assessment in automotive systems under UNECE vehicle regulations.
DORA	Regulation	Helps financial institutions manage risk and improve operational resilience.
FDA 524B	Regulation	Supports cybersecurity compliance in medical-device manufacturing, enforceable through the FD&C Act.
EU Cyber Resilience Act	Regulation	Supports the secure-by-design and risk-assessment obligations it imposes across the product lifecycle.

Threat modeling is rarely a named line item in regulation. Its value is that it satisfies the underlying secure-by-design and risk-assessment obligations these rules create. The Cyber Resilience Act is a current example: it reaches any product with digital elements sold in the EU, from microprocessors to connected devices to software.

HOW IT WORKS

Automating Threat Modeling for Compliance

ThreatModeler Nexus integrates security into every phase of development, so compliance evidence is generated as the model is built, identified, and mitigated, not reconstructed afterward.

Build a threat model | **Identify threats** | **Apply security controls** | **Generate compliance reports**

A model is built from architecture diagrams, infrastructure-as-code, and cloud environments. The platform draws on a maintained threat library to surface risk, recommends mitigations, and maps threats to regulatory requirements automatically.

WHAT THE REPORTS PROVIDE

- A compliance summary by domain
- A gap analysis of security posture
- Recommendations for remediation
- Audit-ready documentation

Compliance reporting assesses security measures against 180+ frameworks, including PCI DSS, NIST, GDPR, and ISO 27001.

EXAMPLE COMPLIANCE WORKFLOW

1. Select the frameworks relevant to your organization.
2. Generate a compliance report with identified gaps.
3. Implement the recommended mitigations.
4. Validate improvements and maintain continuous compliance.

WHO IT SERVES

Built for Every Role

Secure development is a shared responsibility. ThreatModeler Nexus gives each role the view and the controls that fit how they work.

ROLE	HOW THREATMODELER NEXUS SUPPORTS THEM
Developers	Identify threats and mitigate risk before deployment.
Security Architects	Automate security design reviews and integrate controls.
Compliance Officers	Generate compliance reports and maintain audit readiness.
DevSecOps Teams	Embed security into CI/CD for continuous monitoring.

IN CONCLUSION

Threat modeling is not only a security best practice. It is a compliance enabler.

PROACTIVE SECURITY
Secure applications and infrastructure before issues reach production.

LOWER COST
Reduce security cost by addressing exposure early.

AUTOMATED REPORTING
Generate compliance reports for major regulations automatically.

CONTINUOUS ASSURANCE
Maintain security assurance in fast-paced development cycles.

ThreatModeler

GET STARTED

Make compliance a byproduct of design.

See how ThreatModeler Nexus turns threat modeling into audit-ready evidence across your applications, cloud, and development workflows.

TALK WITH OUR TEAM

threatmodeler.ai

For more information, support, or inquiries:

Email
support@threatmodeler.com

Phone
+1 201 266-0510

Web
threatmodeler.ai