STRATEGIC SECURITY FRAMEWORK

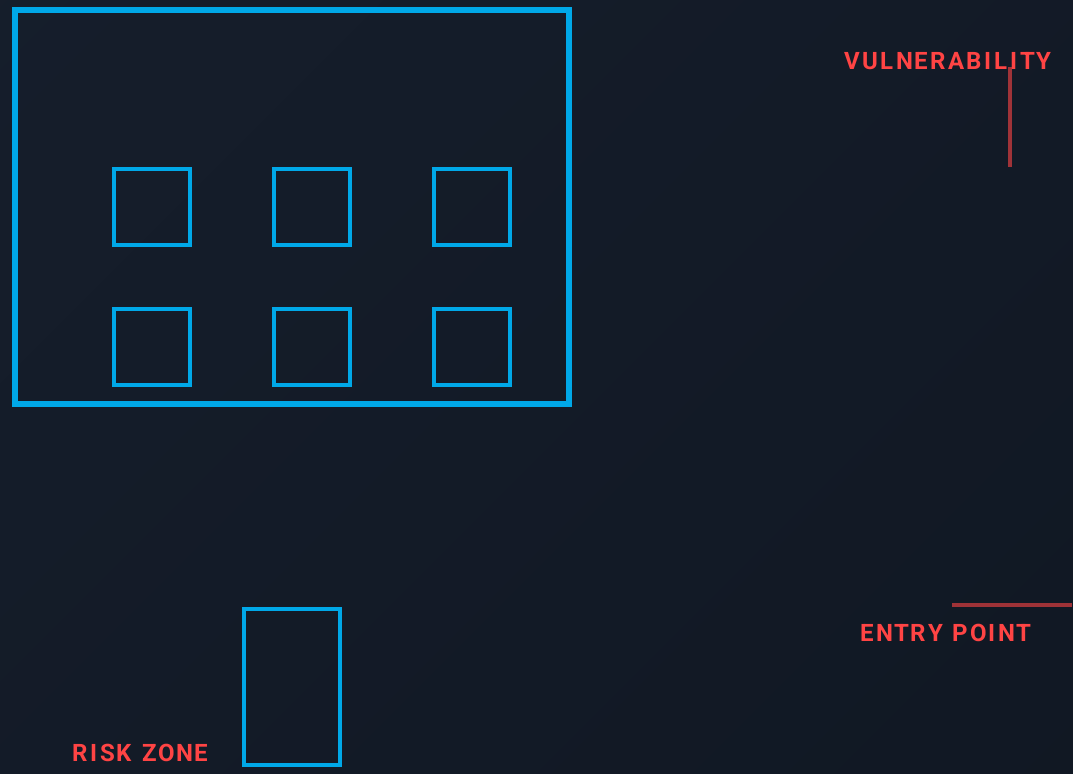
Threat Modeling in GRC

A Strategic Imperative

A BEGINNER'S GUIDE TO THINKING LIKE AN ATTACKER

The Detective and the Blueprint

Imagine a detective examining a building's blueprint, not to admire its design, but to find every possible way a burglar might break in.



CORE CONCEPT

Threat modeling is a proactive approach to identifying and addressing security vulnerabilities by looking at a system from an attacker's perspective.

REACTIVE

Patch when breached

PROACTIVE

Design secure from start

GRC: The Landscape of Risk Management

1 Governance

LEADERSHIP & VISION

Setting the rules, standards, and long-term vision for the organization.

> *"The club's leadership setting membership standards and the long-term vision for the course."*

2 Risk Management

IDENTIFY & PRIORITIZE

Identifying, prioritizing, and managing cybersecurity risks to the business.

> *"The course superintendent monitoring hazards and deciding which to prevent, mitigate, or accept."*

3 Compliance

EXTERNAL REQUIREMENTS

Meeting all external requirements from governing bodies and regulators.

> *"Ensuring the club meets all requirements from authorities like the R&A and local bodies."*

CORE ENGINE OF RISK MANAGEMENT

Threat Modeling's Strategic Role

Threat modeling serves as the **proactive core engine** of the Risk Management pillar. It provides the detailed, data-generating analysis required to translate technical design flaws into **measurable business risks**.

The Four-Question Framework

1

What are we building?

Understand the system, application, or business process in detail. Map out all components and how they connect. Create visual maps such as Data Flow Diagrams (DFDs) to see where data comes from, how it moves, and where it is stored.

Example: Understanding system architecture and data flows

2

What could go wrong?

Adopt an attacker's mindset and systematically identify potential threats and vulnerabilities. With a clear map of the system, brainstorm the different ways an adversary could compromise security.

Example: Identifying attack paths and exploitation methods

3

What are we doing to defend?

Define specific countermeasures and security controls to prevent or mitigate identified threats. Design defenses to block the attack paths discovered in the previous step.

Example: Implementing encryption, access controls, and monitoring

4

Did we do a good job?

Validate and review the defenses you've put in place to ensure they were implemented correctly and are effective. Confirm that security measures successfully reduce risk to an acceptable level.

Example: Testing controls and validating security measures

Thinking Like an Attacker: STRIDE

A systematic framework to categorize different types of threats

THREAT

S

Spoofing
AUTHENTICITY

Pretending to be someone or something you're not.

> *Example: A scammer sends an email that looks like it's from your bank to steal your password.*

THREAT

T

Tampering
INTEGRITY

Secretly changing data without permission.

> *Example: Modifying a shipping order to redirect a package to a different address.*

THREAT

R

Repudiation
NON-REPUDIABILITY

Denying that you did something, with no way to prove you did.

> *Example: Deleting server logs to hide the tracks of a hacking attempt.*

THREAT

I

Information Disclosure
CONFIDENTIALITY

Exposing information to someone who shouldn't see it.

> *Example: A data breach that leaks customer names, email addresses, and credit card numbers.*

THREAT

D

Denial of Service
AVAILABILITY

Preventing legitimate users from accessing a system or service.

> *Example: Flooding a shopping website with traffic on Black Friday that real customers can't get in.*

THREAT

E

Elevation of Privilege
AUTHORIZATION

Gaining more access or permissions than you're supposed to have.

> *Example: A regular user finding a way to gain administrator-level access and control.*

From Technical Flaw to Business Risk

1

Vulnerability

A weakness or gap in a system.

Example: Unpatched server

2

Threat

A potential negative actor or event.

Example: Cybercriminal

3

Risk

Potential for loss when a threat exploits a vulnerability.

Example: Data breach leading to regulatory fines

THE REAL VALUE OF THREAT MODELING

Translating Technical Issues into Business Risks

Threat modeling analyzes how vulnerabilities could be exploited by threats and documents the potential outcome as a **prioritized business risk** in the official risk register. This ensures resources are focused on mitigating the most significant potential impacts—such as **reputational harm** or **regulatory fines**—not just fixing technical bugs.

Result: A complete, actionable risk register that drives strategic security investment decisions and demonstrates due diligence to auditors and regulators.

Why Threat Modeling Matters: Strategic Value

1

Protecting Revenue & Maximizing ROI

Identifying security flaws in the design phase—before a single line of code is written—avoids exponentially higher costs of fixing them post-launch or post-breach.

- Economic threat modeling reduces security costs
- Maximizes Return on Security Investment (ROSI)
- Protects revenue-generating systems
- CISOs act as chief revenue protection officers

2

Ensuring Compliance & Building Trust

Threat models serve as formal evidence for auditors, providing an unbreakable audit trail that demonstrates due diligence in assessing and mitigating risks.

- Meets stringent regulatory requirements (GDPR, HIPAA, PCI DSS)
- Provides documented evidence of risk assessment
- Builds trust with clients and regulators
- Demonstrates commitment to data protection

3

Creating a Proactive Security Culture

Integrating threat modeling into the development lifecycle fosters "security by design," transforming security from a reactive cost center to a strategic driver of business resilience.

- Encourages security thinking from project start
- Trains developers and architects in security
- Shifts security from cost center to strategic asset
- Builds market success and competitive advantage

The Cornerstone of Mature GRC

Threat modeling is the **essential, proactive practice** that connects technical security activities to the strategic goals of the business.

QUANTIFIABLE DATA

Translates vulnerabilities into measurable business risks

AUDIT TRAIL

Unbreakable evidence of due diligence for compliance

INVESTMENT JUSTIFICATION

Empowers security leaders as revenue protection officers

STRATEGIC IMPERATIVE

Integrate Threat Modeling Into Your Development Lifecycle

Build security in from the start to create a **resilient, market-leading organization** that delivers demonstrable business value.