Adversarial Risk Mapping & Assessment

Technical Guide

Document Type: Standard Technical

Document Version: 1.0

Date: 28/03/2025

Authors: Joas Antonio dos Santos

Table of Contents

Executive Summary

The continued advancement of cyber threats, combined with the increasing complexity of technological environments and the rigor of global regulatory legislation, imposes an urgent need for evolution in offensive security testing methodologies. Although traditional practices such as the Penetration Testing Execution Standard (PTES), NIST SP800-115 and guides such as the OWASP Testing Guide offer valuable guidance, it is observed that most intrusion testing still remains limited to the specific identification of technical vulnerabilities, without establishing a robust connection between the exploitation of flaws and the real impact on the business, critical assets and regulatory compliance.

The ARMA - Adversarial Risk Mapping & Assessment methodology emerges as a structured response to this gap, proposing a technical-operational model that transcends the simple technical checklist and the execution of automated tools. Based on the behavioral simulation of real adversaries, ARMA provides a risk-oriented offensive assessment approach, capable of mapping not only individual failures, but the entire exploitation chain and its consequences on the operational continuity and legal exposure of the organization.

In the context of modern threats, attacks rarely occur through a single isolated vulnerability. The concept of Risk Chain Mapping, central to ARMA, allows us to demonstrate how seemingly trivial failures, when strategically linked, result in scenarios of total compromise of critical assets. The methodology leads the test executor to explore multiple attack surfaces — from web environments, APIs, internal systems, cloud and legacy infrastructures — always guiding their decisions by adversarial reasoning and not just by superficial recognition of vulnerabilities.

One of ARMA's key differentiators is its ability to technically quantify each stage of the offensive process, assigning weights and scores that reflect the technical difficulty, the level of depth achieved, the potential for financial and reputational impact, as well as the regulatory risk generated by the exploitation of each vector. This quantification culminates in the generation of a consolidated risk score, structured to be understood by both technical teams and executives and boards of directors, allowing a holistic view of the organization's exposure.

The methodology's structure provides for direct integration with globally recognized threat and compliance frameworks, such as MITRE ATT&CK for mapping adversarial techniques and tactics, CWE Top 25 for categorizing exploited weaknesses, and key regulatory references such as PCI DSS, LGPD, DORA, and GDPR. Each validated vulnerability and each successful pivot are automatically associated with the violated compliance requirements, providing a final report that goes beyond the simple inventory of flaws and presents a true risk map, with well-defined financial, technical, and legal impacts.

Unlike conventional practices, ARMA does not end with the delivery of a technical report. The methodology establishes a continuous cycle of learning and improvement, where each attack exercise leads to an analysis of the defensive deficiencies identified, the flaws in the detection and response mechanisms, and the opportunities to strengthen the organization's cyber posture. This feedback cycle allows the organization to mature its defense processes

in proportion to the complexity of the simulated attacks, leaving the comfort zone of periodic checks to adopt a mindset of continuous evolution.

The final report generated under the ARMA lens strikes a balance between technical depth and executive insight, offering everything from specific details on the tools used and the vectors explored to impact analyses on business lines, critical assets and supply chains. This feature makes the methodology applicable not only to technical assessments of IT environments, but also to sensitive sectors such as ICS/SCADA, multi-region cloud environments, critical financial operations and strategic infrastructures under specific regulations.

Another relevant factor of ARMA is its adaptability to Purple Teaming scenarios, enabling the execution of offensive operations coordinated with the organization's defense teams. This synergy enables real-time validation of detection, response, and containment mechanisms, promoting the practical strengthening of defensive capabilities and providing insights into response time to complex incidents.

Within the scope of risk management and compliance, the methodology allows for the direct mapping of each vulnerability to specific articles of legal regulations, such as article 46 of the LGPD regarding the protection of personal data, or the technical requirements of PCI DSS 6.5 aimed at validating security in applications. With this, ARMA enables the organization to anticipate compliance violations before they result in sanctions, fines or high-profile public incidents.

The methodology also proves to be highly applicable to the reality of large companies, financial institutions, government entities and critical infrastructure operators, scenarios where the impacts of successful exploration transcend the technological environment and directly reverberate on market value, public confidence and operational stability.

Regarding risk measurement, ARMA proposes a robust quantitative model capable of assigning differentiated scores to each phase of adversarial exploitation, taking into account the technical complexity of the exploitation, the depth of access gained, the potential impact on the business and the degree of exposure to applicable legislation. This approach offers a concrete and more realistic alternative to traditional severity models based solely on CVSS, allowing the organization to understand which attack chains truly pose strategic risks and should be prioritized.

It is important to highlight that ARMA was designed to be scalable and integrable with future cybersecurity technologies and practices, including the use of artificial intelligence for offensive decision-making, integration into DevSecOps pipelines, and adaptation to emerging scenarios such as IoT device security and quantum computing environments. The proposed methodological framework even foresees the possibility of partial automated execution, ensuring scalability for continuous and large-scale operations.

In terms of documentation and delivery, ARMA establishes the format for highly visual executive and technical reports, including risk chain maps, risk score charts and visual representations of compliance mapping. These artifacts not only facilitate technical understanding of the findings but also enable direct consumption by risk committees, boards and regulators, increasing the strategic value of the deliverables.

In short, ARMA positions itself as a natural evolution of traditional pentest methodologies, proposing an offensive model oriented to risk, business and compliance, capable of providing organizations with a clear, quantifiable and actionable view of their real cyber exposure. By adopting this approach, companies not only increase their level of maturity in offensive security, but also strengthen their ability to anticipate complex adverse scenarios, becoming more resilient in the face of the modern threat landscape.

Therefore, ARMA establishes itself as a robust, structured, and risk-oriented offensive methodology capable of filling critical gaps in traditional pentest approaches. By leading the security professional through a realistic adversarial journey, mapping risk chains, quantifying impacts, and directly correlating each exploit to applicable regulatory requirements, the methodology provides a new level of maturity and value for cybersecurity operations.

Its cross-functional applicability, combined with its ability to generate rich, visual and decision-oriented reports, makes ARMA an essential tool not only for technical teams, but also for risk managers, compliance and executives responsible for corporate governance and business continuity.

In a global scenario where the complexity of attacks increases in proportion to legal and regulatory requirements, the adoption of ARMA represents a significant advance in strengthening organizational cyber resilience, aligning offensive security practices with the real market demand for integrated, accurate and actionable risk intelligence.

References and Applicable Documents

This technical document on the ARMA - Adversarial Risk Mapping & Assessment methodology was developed based on the main international standards, cybersecurity frameworks and data protection legislation that govern intrusion testing practices, risk analysis and regulatory compliance. The following are references considered essential for the understanding, application and validation of the proposed methodology.

Among the main technical reference documents, widely recognized guides and standards in the areas of information security, reverse engineering, threat modeling and adversarial simulation stand out. The Penetration Testing Execution Standard (PTES), for example, provides a structured basis for planning and executing penetration tests, covering everything from information gathering to threat modeling and reporting results. In addition, NIST Special Publication 800-115 offers detailed guidelines for conducting technical security assessments, reinforcing the need for auditable processes and consistent methodologies.

The MITRE ATT&CK framework is an indispensable reference for mapping the tactics, techniques, and procedures (TTPs) used by malicious actors in real-world scenarios, and is incorporated into ARMA as a basis for planning offensive actions and aligning with known threat models. Also in the technical sphere, the Common Weakness Enumeration (CWE Top 25) provides a classification of the main software weaknesses exploited by attackers, serving as a guide for identifying and exploiting vulnerabilities during the execution of the methodology.

Regarding regulatory compliance, ARMA establishes a direct correlation with standards and legislation of broad international applicability. The Payment Card Industry Data Security Standard (PCI DSS v4.0) guides the security requirements for environments that process, store or transmit payment card data, and is essential for mapping flaws that represent a risk of financial non-compliance. In turn, privacy legislation such as the General Data Protection Law (LGPD - Brazil), the General Data Protection Regulation (GDPR - Europe) and the Digital Operational Resilience Act (DORA - European Union) support the assessment of regulatory risks and legal exposure arising from the exploited vulnerabilities.

In addition to the normative documents, ARMA recognizes as a reference the set of good practices published by organizations such as the OWASP Foundation, whose Testing Guide v4 is widely used in the validation of web applications and APIs, providing technical parameters for evaluating the security of systems exposed to the internet.

The documents listed below therefore comprise the technical and regulatory framework that underpins the construction of the ARMA methodology:

- **PTES - Penetration Testing Execution Standard**
- **NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment**
- **MITRE ATT&CK Framework**
- **CWE Top 25 Most Dangerous Software Weaknesses**
- **OWASP Web Security Testing Guide (WSTG v4)**
- **PCI DSS v4.0 - Payment Card Industry Data Security Standard**
- **LGPD - General Law on the Protection of Personal Data (Law 13,709/2018 - Brazil)**
- **GDPR - General Data Protection Regulation (Regulation EU 2016/679)**
- **DORA - Digital Operational Resilience Act (EU Regulation 2022/2554)**
- **ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems**

Additionally, the methodology remains open to integration with new emerging regulations and sector-specific standards, ensuring its continuous evolution and adherence to the regulatory challenges of different sectors and jurisdictions.

Introduction

The global cybersecurity landscape has witnessed an exponential growth in the sophistication and frequency of attacks targeting critical infrastructure, financial systems, corporate environments, and sensitive data of citizens and organizations. The constant evolution of attack techniques, driven by advanced threat groups (APTs), cybercriminals, and state actors, demands that organizations adopt a proactive and methodologically sound approach to identifying, mapping, and mitigating cyber risks.

In this context, traditional penetration testing methodologies (pentesting), still largely anchored in linear models and based on the simple verification of technical vulnerabilities, are insufficient to reflect the complexity of modern adversarial scenarios. Most of the tests conducted in the market remain restricted to identifying isolated flaws, without a broad view of the exploitation chain and, mainly, without the proper connection between the technical vectors explored and the effective impact on the business, operational continuity and compliance with current laws and regulations.

Furthermore, the growing adoption of distributed architectures, hybrid environments, cloud services, and the interconnection of legacy systems with modern applications significantly expand the attack surface of organizations, making offensive approaches that disregard the vision of chained risk and strategic impact obsolete. In this context, it is no longer enough for the security professional to identify specific vulnerabilities: it is essential that the offensive assessment process be able to simulate the reasoning and decision-making of a real attacker, going through complex exploitation chains until reaching assets of high strategic value or causing significant operational disruptions.

Another determining factor is the intensification of regulatory requirements related to data privacy, operational resilience and protection of critical infrastructures. Standards such as PCI DSS v4.0, LGPD, GDPR and DORA impose explicit obligations on organizations regarding the identification and treatment of vulnerabilities that may compromise the integrity, confidentiality and availability of data and systems. In this scenario, methodologies limited to the generation of technical reports disconnected from business reality and regulatory risk lose relevance and effectiveness.

Given these demands, there is a need for a methodology that aligns offensive execution with risk logic, strategic impact vision and regulatory compliance. This is where the ARMA - Adversarial Risk Mapping & Assessment proposal comes in: a methodological model that transforms traditional pentesting into an offensive operation oriented towards real adversarial objectives, focusing on demonstrating business impact, the materialization of risks and the violation of regulatory obligations.

The ARMA methodology is designed to guide the tester through a structured flow of offensive actions, from context discovery, through tactical planning and iterative exploit execution, to consolidating findings into a chained risk map and robust impact report. This approach not only increases the technical depth of the assessment, but also ensures that each finding is contextualized against business assets, critical processes, and applicable legal requirements.

Unlike conventional approaches, ARMA incorporates the concept of Risk Chain Mapping, which demonstrates how multiple vulnerabilities, when exploited in a chained manner, can result in scenarios of total infrastructure compromise or severe privacy and compliance violations. Instead of simply reporting technical vulnerabilities, the methodology exposes the potential consequences of their exploitation in a logical and visual flow, providing clear support for decision-making by senior management.

Additionally, the methodology proposes a robust, multidimensional risk scoring model that can assign weights to findings based on technical complexity, depth of access obtained, potential financial and reputational impact, and severity of regulatory exposure. This model provides objective prioritization of vulnerabilities and attack chains, allowing the organization to focus remediation efforts on the points of greatest strategic risk.

Another important differentiator of ARMA is its ability to generate integrated reports, which are not restricted to technical aspects, but offer an executive view, with emphasis on mapping violations of the main applicable regulations and legislation. This feature positions the methodology as a tool not only for information security teams, but also for areas of compliance, legal, governance and corporate risk management.

ARMA was also designed to be compatible with modern Purple Teaming and Continuous Security Validation practices, integrating with DevSecOps workflows and ongoing cyber resilience validation processes. The methodology also provides for the possibility of partial automation of attack cycles and report generation, expanding its applicability in dynamic and large-scale environments.

ARMA’s proposal is not to replace established standards such as PTES or NIST SP 800-115, but rather to evolve the concept of offensive testing, incorporating a holistic and strategic view of cybersecurity into pentesting practices. By adopting this methodology, organizations will have an effective tool to measure their real exposure to advanced attacks, understand the potential impacts on the business, and prioritize investments and corrective actions in line with their risk matrix and the regulatory requirements of their industry.

In addition to technical issues and the increasing complexity of technological environments, the current scenario places additional pressure on organizations to demonstrate due diligence in information security. Global regulations and standards require organizations to not only implement technical controls, but also to demonstrate knowledge of their cyber risks and the concrete actions taken to mitigate them. In this context, simulating real adversaries and modeling risk chains become indispensable elements to ensure a holistic view of the organization's real exposure.

ARMA was created precisely to meet this need: to offer a structured methodology that goes beyond detecting vulnerabilities, promoting a strategic reading of the environment from an adversarial perspective. By adopting this approach, the organization can not only verify flaws, but also understand what a real attacker could do based on those flaws, what exploit chains could be formed, and, above all, what technical, financial and regulatory impacts could be realized.

Risk Chain Mapping proposed by ARMA is a differentiator that allows risk management areas and senior management to clearly visualize the chain of exploitable vulnerabilities and

how each one contributes to increased organizational exposure. This view allows, for example, understanding how a seemingly trivial configuration error in a low-criticality asset can, when chained with other failures, result in the compromise of core business systems or the exposure of sensitive data under regulation.

In the current context, where data leaks and cyber incidents have become recurrent, the ability to demonstrate knowledge about one's own weaknesses and effectively deal with them becomes a differentiating factor in auditing processes, due diligence and market negotiations, including M&A (Mergers and Acquisitions) processes. In this sense, ARMA allows the organization to increase its cybersecurity maturity, moving from a reactive and specific vision to a strategic, continuous approach oriented towards real risks.

Another crucial point addressed by the methodology is the integration between offensive aspects and regulatory compliance. ARMA maps each validated vulnerability and each successful exploit to specific articles of the main legislation and regulations in the sector. This means that, at the end of a cycle of execution of the methodology, the organization will have not only a technical inventory of vulnerabilities, but a complete report indicating which PCI DSS provisions were violated, which LGPD articles were exposed, and which DORA or GDPR requirements were directly impacted by the exploited weaknesses.

At a time when regulatory sanctions can reach millions in value, and when failure to comply with regulations such as DORA implies a direct risk to the continuity of financial and critical operations, this ability to link technical failures to direct regulatory impacts is one of ARMA's great differentiators. The methodology makes the technical report a strategic document, usable not only by security teams, but also by compliance, legal, auditing and corporate risk management areas.

It is also important to highlight that the proposed model is not restricted to a specific sector. ARMA was designed to operate in any market vertical, whether in highly regulated financial institutions or in industrial and OT environments, where physical risk overlaps digital risk, including telecommunications operators, energy, healthcare, government sectors, or even startups and innovation environments.

The framework’s flexibility allows it to be applied in everything from controlled adversarial simulations, such as Red Team and Purple Team exercises, to broader assessments in Continuous Security Validation processes, integrating with CI/CD tools and DevSecOps pipelines. This enables ARMA to be used both periodically and continuously, allowing organizations to dynamically validate their resilience, always considering the latest threats and constant changes in technological infrastructure.

It is worth noting that ARMA also proposes a risk scoring and prioritization model that is distinct from traditional models based solely on CVSS. While CVSS essentially considers technical aspects, ARMA considers, in addition to the difficulty of exploration, the level of access gained, the relevance of the impacted assets, the potential for financial and reputational damage, and the exposure to the main applicable regulations. This multidimensional scoring model allows for a realistic view of the risk, facilitating the prioritization of corrective actions based not only on the technical aspect, but also on the materiality of the impact.

Another innovative element of the methodology is the provision of learning cycles and continuous improvement. Each ARMA execution must generate not only the mapping of exploited flaws, but also a reflection on the deficiencies of defense mechanisms, the detection and response capacity, and the blind spots of the security architecture. These feedback cycles ensure that the methodology directly contributes to strengthening the defense, transforming each offensive into an opportunity for organizational growth.

Finally, ARMA proposes a structured results delivery standard capable of simultaneously serving technical and executive audiences. The reports produced include technical details of explorations, graphical views of risk chains, scoring and prioritization panels, and regulatory exposure maps, offering a 360° view of the assessment performed. This wealth of information makes the reports generated high-value documents, suitable for use as a basis for strategic security planning, as input for external audits, and even as defense documents in potential legal proceedings or regulatory investigations.

In short, ARMA is a natural and necessary evolution of intrusion testing methodologies, aligning offensive practice with business risk, regulatory compliance and strategic intelligence. By adopting this methodology, the organization takes an important step towards full cybersecurity maturity, gaining real capacity to understand, map and reduce its exposure surface, not only technically, but in an integrated manner with its business objectives and the legal and regulatory obligations to which it is subject.

Methodology Overview (ARMA Phases):

The ARMA Methodology - Adversarial Risk Mapping & Assessment was structured in six interdependent phases, each of which was designed to ensure offensive execution with a focus on real adversariality, strategic impact assessment and precise mapping of organizational risk. These phases allow the intrusion testing cycle to move from being a mere spot check for technical failures to constituting a robust process of threat simulation and risk materialization, with strong adherence to governance, risk and compliance demands.

Each phase of ARMA has clear objectives, well-defined inputs and deliverables that feed into subsequent steps. Each of these phases is detailed below:

Context Discovery

The Context Discovery phase marks the beginning of the offensive operation from an ARMA perspective, distinguishing itself from conventional approaches by its focus on collecting and interpreting the business context, rather than just technically identifying exposed assets. Here, the goal is not merely to map attack surfaces, but to understand the target organization as an operational, regulatory and strategic ecosystem.

This phase involves identifying critical business assets, mapping sensitive data flows, understanding third-party dependencies, and characterizing the legal and regulatory obligations that apply to each business process. This initial analysis allows the pentester to

take on a role that is closer to a real adversary, directing his or her actions not toward the most obvious technical opportunity, but toward targets of greater strategic value.

Within the technical scope, traditional mapping of assets, IP addresses, domains, subdomains, APIs and any exposed communication interfaces is also carried out. However, the analysis goes further, incorporating variables such as user profiles, digital journeys, system interactions and possible pivot points.

At the end of the phase, the offensive team must have a complete mapping of the environment, including prioritized target assets, a data flow map and a list of applicable regulations and legislation, configuring a tactical plan for the subsequent phase.

Adversarial Planning

With the context properly mapped, the methodology moves on to the Adversarial Planning phase, where the offensive strategy to be adopted is established. In this stage, the team acts as a threat agent, making rational decisions about which paths to follow, which techniques to apply and which vectors have the greatest potential to generate a cascade effect on the target environment.

Planning is not limited to choosing tools, but includes defining realistic attack scenarios, simulating everything from the behavior of organized cybercrime groups to advanced persistent threats (APTs) or malicious insiders. MITRE ATT&CK is used as a reference framework for selecting the tactics and techniques that are most appropriate for the target environment and the defined adversary objectives.

Each scenario is described with:

- Adversarial objective;
- Estimated input vectors;
- Expected exploration techniques;
- Possible pivots;
- Expected escalation paths.

This phase also defines the desired impact threshold, that is, how far the simulation can go — whether it be to the point of exposing sensitive data, compromising mission-critical systems or violating a specific regulation.

Adversarial planning is documented, forming the basis of what will be executed in subsequent offensive iterations.

Offensive Iterative Loops

Unlike traditional models, which execute pentests in a linear fashion, ARMA proposes offensive execution through iterative and adaptive cycles. The Offensive Iterative Loops phase is the core of the operation, where each offensive action feeds intelligence for the next cycle, allowing route corrections and exploration of new attack opportunities.

Each iteration consists of:

- Execution of a previously planned technique;
- Validation of results and impacts obtained;
- Reassessment of the scenario;
- Planning the next action based on the findings.

This approach faithfully simulates the behavior of a real adversary, who adjusts his or her strategies based on the environment's response. For example, exploiting a SQL injection attack can reveal credentials that in turn enable a new offensive cycle focused on lateral movement and privilege escalation.

The loop is only completed when the defined impact is reached or the exploitation vectors are exhausted. All adversarial movement is recorded, composing the material that will be used in mapping the risk chain.

This iterative cycle ensures not only greater technical depth, but also the chaining of vulnerabilities, an essential element for the next phase.

Risk Chain Mapping

Risk Chain Mapping is the backbone of ARMA, representing the moment in which offensive actions are logically organized to demonstrate the formation of an exploitation chain. Here, vulnerabilities are not analyzed in isolation, but rather how each technical flaw connects to another, forming a critical path to the asset or final impact.

The big difference in this phase is the ability to visualize and document the cascade effect of smaller vulnerabilities that, in isolation, would not be considered critical, but which, when linked, can lead to a scenario of organizational collapse or serious legal violation.

This phase generates a risk chain diagram as a deliverable, highlighting:

- Entry points;
- Techniques used;
- Pivoting;
- Privilege escalations;

- Impacts achieved;
- Potentially violated regulations.

Risk Chain Mapping is a powerful visual artifact, allowing executives and technical areas to understand, in a graphic and objective way, the adversarial journey and critical risk points.

Impact & Compliance Report

With the risk chain mapped, ARMA moves on to consolidating the results in the Impact & Compliance Report phase. This is not a mere technical report, but a multidimensional document, structured to meet the needs of different audiences within the organization.

The report is divided into three main areas:

1. **Technical**: Details of techniques, tools, successful exploits and proofs of concept.
2. **Business**: Analysis of impacts on critical processes, estimation of financial losses, interruptions and reputational damage.
3. **Regulatory**: Mapping of exploited flaws in relation to regulatory requirements such as PCI DSS, LGPD, GDPR and DORA.

This delivery model allows the same report to be used simultaneously by:

- Technical teams for correction;
- Executives for decision making;
- Legal and compliance as evidence material.

The risk score calculated during the offensive cycle is also presented at this stage, allowing for the prioritization of corrections and investments.

Adversary-Driven Learning

Closing the methodological cycle, ARMA establishes the Adversary-Driven Learning phase, responsible for ensuring that each offensive generates organizational learning and strengthening of the defensive posture.

This step consists of:

- Review of failure points in detection and response;
- Analysis of opportunities for improvement in defensive architecture;

- Definition of corrective and strategic actions.

The goal is to turn each attack into an evolutionary cycle, continually refining security controls and organizational resilience.

Furthermore, learning is used to feed back into ARMA itself, ensuring that future cycles are more effective, exploring new vectors and even more complex adversarial techniques.

Operational Breakdown — Inputs, Outputs, Toolsets and Examples by Phase

1. Context Discovery

Inputs:

- Defined scope (domains, IP ranges, known assets);
- Executive briefing and asset criticality matrix;
- Maps of critical processes and data flows (when provided);
- Applicable compliance requirements.

Outputs:

- Technical inventory of exposed assets (hosts, applications, APIs);
- Identification of high-value assets (HVTs);
- List of possible attack vectors;
- Preliminary mapping of applicable regulatory requirements.

Toolsets:

- OSINT Framework, Recon-ng, Shodan, Censys, SpiderFoot;
- DNS tools (Sublist3r, DNSenum);
- Cloud Asset Discovery (AWS Prowler, ScoutSuite).

Examples:

- Mapping an undocumented API exposed on the subdomain`api.internal.company.com`, allowing for future explorations;
- Identification of legacy server with obsolete operating system.

2. Adversarial Planning

Inputs:

- Technical and critical asset inventory (from the previous phase);
- Frameworks like MITER ATT&CK, CWE Top 25;
- Business objectives and compliance requirements.

Outputs:

- Modeled attack scenarios (e.g., initial access, persistence, lateral movement);
- List of adversarial techniques to employ;
- Definition of rules of engagement and impact thresholds.

Toolsets:

- ATT&CK Navigator, Threat Modeling tools (Microsoft SDL);
- Design adversarial scenarios in Miro, Lucidchart or Threat Dragon.

Examples:

- Definition of a scenario focused on financial data leakage through API injection exploitation;
- Planning SAML Injection exploit for session hijacking.

3. Offensive Iterative Loops

Inputs:

- Modeled adversarial scenarios;
- List of selected techniques.

Outputs:

- Vulnerabilities validated and exploited;
- Collected credentials, tokens and artifacts;
- New vectors discovered for exploration.

Toolsets:

- Burp Suite Pro, SQLmap, Nmap, BloodHound;
- Metasploit Framework, Cobalt Strike, Empire;
- Custom tools for exploits.

Examples:

- SQLi exploitation resulting in the extraction of password hashes;
- Privilege escalation after collecting OAuth token in API.

4. Risk Chain Mapping

Inputs:

- Logs and artifacts of offensive iterations;
- TTPs used and results obtained.

Outputs:

- Visual diagram of the risk chain (Risk Flow);
- Identification of pivots and escalations;
- Prioritization of chained risks.

Toolsets:

- Mindmaps (XMind), Draw.io, Maltego;

- Chart generators (Chart.js, Graphviz).

Examples:

- Mapped chain: Docker API exposure → Container access → Scaling → Financial database compromise;
- Visual mapping of dependencies between vulnerabilities.

5. Impact & Compliance Report

Inputs:

- Complete Risk Chain Mapping;
- Impact matrix and calculated severity.

Outputs:

- Executive and technical report;
- Risk prioritization panel;
- Mapping of compliance violations.

Toolsets:

- PDF generators (LaTeX, Pandoc, html2pdf.js);
- Executive report templates (Word, Markdown).

Examples:

- Report with estimated financial impact of 1.5 million due to exploitation of the X fault;
- SQL Injection mapping directly violating PCI DSS 6.5.1 and LGPD Art.46.

6. Adversary-Driven Learning

Inputs:

- Consolidated final report;

- Record of techniques that bypassed defenses.

Outputs:

- List of recommended defensive improvements;
- Detection and response gaps report;
- Recommendations for new scenarios for the next cycle.

Toolsets:

- SIEM (Splunk, ELK, QRadar);
- Purple Team platforms (MITRE Caldera, Prelude Operator).

Examples:

- Identification of failure in API log monitoring, suggesting WAF integration;
- Recommendation to include CTI (Cyber Threat Intelligence) in future executions.

The ARMA methodological cycle is consolidated as a robust, modular and scalable approach, structuring each phase with clear inputs, tangible deliverables and the support of the best technical tools available on the market. This operational granularity not only guarantees the repeatability and auditability of the process, but also positions the methodology as a reference standard applicable to complex and highly regulated environments.

Each phase contributes directly to the materialization of the methodology's strategic objectives: mapping risk in a chained manner, simulating real adversary behavior, and producing actionable security intelligence for all levels of the organization. ARMA's strength lies in its ability to evolve the classic intrusion test into a true cyber risk assessment exercise, integrating technical, business, and compliance aspects into a single, structured workflow.

With the full cycle — from contextual discovery to organizational learning — ARMA ensures not only the mapping of exploitable weaknesses, but also the continuous strengthening of the defense posture, transforming each execution into a concrete step towards cyber maturity and organizational resilience.

Scoring System Design Quantitative model covering:

The ARMA methodology scoring system represents one of its fundamental pillars, ensuring that each exploration chain is not assessed solely from the perspective of isolated technical

severity, but from a holistic perspective that incorporates financial, regulatory and operational impact variables.

Unlike traditional models such as CVSS, which focus exclusively on the technical severity of vulnerabilities, ARMA's Risk Scoring Model was designed to reflect the real strategic risk faced by the organization, weighing five main dimensions:

Technical Complexity (TC)

Reflects the level of technical skill, knowledge, and resources required to execute the exploit. Trivial attacks are given less weight, while sophisticated exploits—such as multi-exploit chains, CVE chaining, or hardening bypass—are given higher scores.

Examples of variation:

- Low TC (1-3): Exploitation via simple SQLi or brute-force;
- Medium TC (4-6): Exploiting logical vulnerability or RCE in custom applications;
- High TC (7-10): Complex chains involving zero-day exploits, sandbox bypasses, or internal pivots.

Formulation: `TC = Assigned Technical Complexity (1 to 10)`

Business Impact (BI)

Calculates the direct or potential impact on the organization's business, considering financial loss, interruption of operations, reputational damage and strategic risks.

Parameters analyzed:

- Low BI (1-3): Exposure of non-sensitive data or data with minimal operational impact;
- Medium BI (4-6): Leakage of strategic information, interruption of non-critical services;
- High BI (7-10): Massive leak of personal data, disruption of core processes, business interruption.

Formulation: `BI = Operational and Financial Impact Scale (1 to 10)`

Compliance Risk (CR)

Measures the risk of regulatory non-compliance, mapping exploits to applicable regulations such as PCI DSS, LGPD, GDPR, HIPAA, DORA. The greater the exposure to regulatory sanctions, the higher the score.

Examples of assignment:

- Low CR (1-3): Exposure with no direct relation to regulations;
- Medium CR (4-6): Possible violation of required technical control;
- High CR (7-10): Direct violation of regulatory privacy or security requirements.

Formulation: `CR = Severity of regulatory exposure (1 to 10)`

Detection/Stealth (DS)

Assesses the degree of evasion of the organization's detection and response mechanisms. The stealthier the attack and the less noticeable it is to the defenses, the greater the weight assigned.

Considerations:

- DS Low (1-3): Activities detected and alerted;
- Medium DS (4-6): Partial or delayed detection;
- DS High (7-10): Fully stealthy, complete EDR/SIEM bypass.

Formulation: `DS = Attack evasion ability (1 to 10)`

Recommended Formula — Weighted Risk Score

The final ARMA Risk Score calculation can follow the weighted formula below, allowing customization by sector or organization:

```
Risk Score = (TC * 0.15) + (DC * 0.25) + (BI * 0.25) + (CR * 0.2) + (DS * 0.15)
```

Justification of Weighings:

- **Technical Complexity (15%)**: Relevant, but does not alone determine risk;
- **Depth of Compromise (25%)**: Reflects the severity of the adversary's advance;
- **Business Impact (25%)**: Prioritization by potential for financial and operational damage;

- **Compliance Risk (20%)**: Reflects the legal exposure, often more impactful than the technical one;
- **Detection/Stealth (15%)**: Importance of understanding whether the attack went unnoticed.

Real Application Example (Case)

Scenario: Initial access via exposed API + SQL Injection + lateral movement → access to financial database and leak of sensitive data.

Metric	Score	Justification
Technical Complex	7	Use of chaining techniques and manual exploration
Depth Commitment	9	Full control of critical system
Business Impact	8	Financial data leak
Compliance Risk	9	Direct violation of LGPD and PCI DSS
Detection/Stealth	6	Some of the activity was not detected

Final Calculation:

```
Risk Score = (7*0.15) + (9*0.25) + (8*0.25) + (9*0.2) + (6*0.15)
Risk Score = 1.05 + 2.25 + 2 + 1.8 + 0.9 = **8.0 (Scale 0 to 10)**
```

Result: Exploration considered CRITICAL, high priority for remediation and immediate reporting to the risk committee.

Customization and Scalability

The ARMA model allows:

6. Weight adjustments according to sector (banking, health, industrial);
7. Integration with dynamic dashboards;
8. Powering GRC and SIEM systems;
9. Use in Red Team/APT success probability calculations.

The scoring model proposed by ARMA elevates the concept of risk measurement in offensive operations, integrating critical variables that go beyond the purely technical view. By weighing complexity, depth of compromise, business impact, regulatory risk and detection capacity, the system provides a multidimensional view of real cyber risk, enabling more assertive prioritization and strategic decision-making.

This scoring mechanism makes the methodology adaptable to different scenarios, sectors and regulatory environments, being able to support from specific assessments to integrations with GRC (Governance, Risk and Compliance) frameworks and SIEM platforms, consolidating itself as a high-value tool for integrated cyber risk management.

With the model validated and applied, the ARMA Risk Score provides the decision maker not only with an understanding of what can be technically exploited, but what really threatens the organization's core business, putting cyber risk into perspective with the strategic and regulatory objectives of the entity being assessed.

Risk Chain Mapping Visualization

Risk Chain Mapping represents the visual and strategic core of the ARMA methodology, being the critical link between technical exploration and the actual materialization of cyber risks for the business. It is the graphic and logical construction of the adversarial journey, highlighting how isolated vulnerabilities connect, form exploration paths and, when linked, result in significant impacts for the organization.

Unlike traditional pentest reports that list vulnerabilities in a descriptive and isolated way, Risk Chain Mapping provides a dynamic, linked and visual view, allowing the technical and executive audience to understand how each flaw contributed to the advancement of the threat agent within the corporate environment.

Objectives of Risk Chain Mapping

The main objective of risk chain mapping is to translate the real path taken by an attacker, demonstrating:

- As an initial input vector enabled subsequent accesses;

- How low severity vulnerabilities, when combined, resulted in high risk scenarios;
- Where there were failures in defensive controls and opportunities for mitigation.

This visualization also allows the identification of breaking points in the chain, where a specific control improvement would prevent the advancement of exploration, functioning as a direct insight for hardening and continuous improvement strategies.

Essential Components of the Risk Chain

Risk Chain Mapping is composed of:

- **Entry Node:**Initial exploitation vector (e.g. exposed API, spear-phishing);
- **Exploit Points:**Vulnerabilities effectively exploited;
- **Pivot Points:**Points where the attacker expands his access or changes the vector;
- **Impacted Assets:**High-value systems or data affected;
- **Compliance Flags:**Visual indication of violated regulatory requirements;
- **Kill Chain Milestones:**Relevant points in the attack chain, mapped according to the ATT&CK or Lockheed Martin Cyber Kill Chain framework.

Visualization Tools and Templates

The ARMA methodology recommends the use of tools capable of generating dynamic and interactive diagrams, such as:

- **Graphviz, Draw.io or Lucidchart:**For flowcharts and hierarchical maps;
- **Maltego or Mind Maps (XMind, Miro):**For exploratory representations and pivots;
- **Chart.js or D3.js:**For dynamic dashboards on integrated platforms.

Each vulnerability is represented as a node in the diagram, connected by arrows that indicate the progression of the attack. Decision points (forks) and privilege escalations are highlighted, allowing you to quickly identify critical paths.

Risk Chain Example (Conceptual Illustration)

Prohibited:`API exposed without authentication (Technical Complexity 4)`
⬇
`Exploitation: SQL Injection → Credential Dump (Depth 6) ⬇ Pivot: Internal Network Access → Scanning → SMB Service Failure (BI 7) ⬇`

`Escalation: Remote Code Execution via Vulnerable Service (LGPD Compliance Art. 46) ⬇ Final Impact:` Access to financial databases and PII → Extreme regulatory and financial risk (Risk Score 8.5)

This visualization connects all the nodes, clearly demonstrating how the impact was built by the sum of the exploits.

Strategic Benefits of Risk Chain Mapping

By consolidating adversarial exploration in a chained manner, Risk Chain Mapping delivers strategic value by enabling:

- **Executive decision-making based on real impact and risk, not just isolated technical severity**;
- Identification of "single points of failure" — assets or controls whose failure allowed the risk to materialize;
- Visual mapping of possible regulatory violations, allowing preventive action with compliance areas;
- Encouraging integration between Red Teams and Blue Teams, facilitating understanding of the attacker's journey;
- Creating a visual timeline of the offense, useful for training and lessons learned.

Integration with Compliance and Business

Each node or step in the chain can and should be enriched with additional data:

- **Impacted asset value**(financial, reputational);
- **Regulation or article of law violated**;
- **Probability of detection at execution time**;
- **Estimated time to complete the step**.

This enrichment makes Risk Chain Mapping a multidimensional tool, which serves not only the technical team, but also as an executive reporting artifact and even as documentary evidence in auditing or regulatory defense processes.

Expected Outputs

At the end of the phase, ARMA delivers:

- Complete risk chain diagram;
- List of chained vulnerabilities and their weights;
- Strategic mitigation points identified;
- Visual report that can be integrated into corporate risk dashboards.

Risk Chain Mapping is thus consolidated as the main visual and strategic differential of the ARMA methodology, materializing the concept that the real risk does not lie in individual failure, but in the way the adversary uses it to achieve its objectives within the business.

Risk Chain Mapping within the ARMA methodology represents the visual and strategic transformation of the offensive exploitation process, offering a logical, chained view of the adversary's journey. By building this graphical representation, the organization stops seeing vulnerabilities as isolated points and starts to understand them as parts of a dynamic risk chain, where the real impact comes from the chaining and continuous exploitation.

This vision allows, in an unprecedented way, to integrate the technical with the strategic, offering leaders a clear understanding of the risk vectors, the most critical assets and the defensive deficiencies that allowed the threat to materialize. By connecting each stage of the exploration with violated regulations, impacted assets and detection failures, Risk Chain Mapping becomes a powerful tool for prioritizing remediation, investment planning and crisis management.

Finally, this phase consolidates ARMA as a cyber offensive methodology oriented towards real risk and business, allowing information security to move beyond the purely technical sphere and act as a strategic instrument for corporate protection and resilience.

Compliance Mapping Model

In the context of the ARMA methodology, the Compliance Mapping Model is one of the most strategic and differential phases, as it establishes a direct connection between the technical vectors explored and the regulatory and legal obligations applicable to the organization being evaluated.

Unlike traditional offensive approaches that are restricted to analyzing vulnerabilities from a technical perspective, ARMA ensures that each exploit, each attack chain and each compromised asset are also evaluated from a regulatory compliance perspective, providing a clear view of the risks of non-compliance, the potential sanctions involved and the legal requirements violated.

Compliance Mapping Objectives

The main objective of this phase is to technically translate the results of adversarial exploration into a regulatory and legal risk map, allowing the final ARMA report to be used not only by technical teams, but also by:

- **Legal Departments**;
- **Compliance and Audit Areas**;
- **Risk Committees**;
- **Senior Management and Board**.

The model provides objective inputs so that the organization understands not only the technical impact of the exploited flaws, but mainly the legal, financial and reputational impact of each simulated incident.

Integration with Global Standards and Regulations

ARMA establishes direct and continuous integration with key security and privacy regulations and standards, such as:

- **PCI DSS v4.0**
- **LGPD (Brazil)**
- **GDPR (Europe)**
- **DORA (Europe)**
- **HIPAA (USA)**
- **ISO/IEC 27001 and 27002**
- **NIST Privacy Framework**
- **Basel III and sectoral financial regulations**

Each of these standards has explicit requirements regarding data protection, system integrity, privacy and operational resilience. When exploring a vulnerability, the ARMA penetration tester already indicates which articles, clauses or regulatory controls have been potentially violated.

How Compliance Mapping Works

The phase develops in three major stages:

a) Exploration Mapping x Regulations

Each validated vulnerability or risk chain is analyzed and mapped into a correlation matrix with the impacted regulatory requirements.

Example:

- **SQL Injection exploited in payment application:**Violates PCI DSS 6.5.1;
- **Exfiltration of personal data:**It constitutes a violation of LGPD Art. 46 and GDPR Art. 32;
- **Financial system commitment:**Potential violation of DORA - Operational Continuity.

b) Calculation of Compliance Risk Score

Each regulatory violation is scored as follows:

- Severity of the standard;
- Probability of sanction;
- Potential financial impact.

This score makes up the Compliance Risk (CR) metric of ARMA's general scoring model.

c) Production of the Visual Compliance Map

The final report contains:

- Pie or bar charts showing % risk per standard;
- Detailed tables crossing each technical failure x violated article;
- Analysis of potential fines and legal implications.

Practical Example of Applied Compliance Mapping

Vulnerability: Exposed API with unprotected endpoint → SQL Injection → Personal data dump. Violated Regulations:

Normative	Article / Control	Description of Violation
LGPD	Art. 46	Failure to protect personal data

GDPR	Art. 32	Insufficient technical and organizational measures
PCI DSS v4.0	Req. 6.5.1	Input validation failure in application
DORA	Operational Continuity	Risk to financial system resilience

Compliance Risk Score calculated:9 (Critical)

Impact: Potential LGPD fine of up to 2% of annual revenue; PCI violation subject to blocking of card operations.

Strategic Benefits of ARMA Compliance Mapping

✅ Real integration between offensive security and corporate governance;

✅ Objective materialization of regulatory risk in each exploration;

✅ Prioritization of fixes based not only on technical severity, but on the potential for financial and regulatory sanctions;

✅ Strengthening the organization's legal defenses in the event of incidents or external audits;

✅ Full transparency for committees and boards on the regulatory risk situation.

Phase Deliverables

At the end of the phase, ARMA delivers:

- **Complete Compliance Matrix (Technical x Normative);**
- **Table of potential regulatory exposures;**
- **Estimate of financial impact per violated rule;**
- **Visual dashboards for executive reporting.**

This ability to generate robust compliance mapping makes ARMA an essential tool not only for cybersecurity, but for the compliance and governance of organizations, especially in regulated markets such as finance, healthcare, telecommunications and energy.

ARMA's Compliance Mapping Model takes the methodology to a new level, integrating cyber offensives into the world of governance, risk and compliance (GRC). By establishing a direct correlation between each technical exploit and the applicable regulatory standards, ARMA allows organizations to clearly and objectively visualize their legal and regulatory weaknesses, going beyond the simple technical dimension.

This approach provides a robust mechanism for legal, compliance and corporate audit areas to act proactively, anticipating legal risks, estimating potential financial sanctions and prioritizing corrections based on regulatory impact.

At the end of this cycle, ARMA transforms the traditional pentest into a strategic regulatory risk management instrument, becoming essential for organizations exposed to regulations such as PCI DSS, LGPD, GDPR, DORA and other sectoral legislation.

Practical Case Study (DVWA Simulation)

In order to demonstrate the practical application of the ARMA methodology, a complete simulation was conducted on the Damn Vulnerable Web Application (DVWA) environment, a platform widely used in the market for training and proof of concept in offensive security.

The exercise focused not only on exploiting known technical vulnerabilities, but mainly on fully applying ARMA principles, chaining failures, mapping the real risk and assessing the technical, regulatory and business impact, simulating a realistic corporate scenario.

Context Discovery in DVWA

Objectives and Premises:

- Map the DVWA as if it were a productive application of a company;
- Identify sensitive data flows;
- Correlate possible impacts to regulations such as LGPD, PCI DSS and GDPR.

Activities Performed:

- Mapping of the application, functionalities and flows;
- Identification of entry points: forms, uploaders, simulated REST APIs;
- Simulation of critical assets: database, administrative panel, login and file upload functionalities.

Outputs:

- Most critical areas mapped: SQL Injection, File Upload, Command Injection;

- The adversarial objective was defined as accessing and leaking the simulated database.

Adversarial Planning (Threat Modeling)

Exploration Chain Planning:

- Initial access via SQL Injection;
- Credential extraction;
- Lateral movement to the upload module;
- Escalation for remote command execution;
- Complete extraction of the simulated database.

Reference: MITRE ATT&CK ID T1505.003 - Server Software Component: Web Shell expected in final phase.

Rules of Engagement:

- Do not crash the application;
- Prioritize stealth and evasion.

Offensive Iterative Loops Executed

Cycle 1 — SQL Injection (SQLi) Exploitation:

- Tool: SQLMap / Burp Suite Pro
- Result: Access to the user table with password hashes.

Cycle 2 — Credential Stuffing and Lateral Movement:

- Use of the obtained hashes for login;
- Mapping of administrative permissions.

Cycle 3 — Exploring the File Upload module (Web Shell):

- Sending malicious PHP payload;

- Extension validation bypass;
- Remote command execution.

Cycle 4 — Risk Chain Completion:

- Scaling via shell;
- Full database dump.

Resulting Risk Chain Mapping

Chaining Performed:

Exposed Input Field → SQL Injection → Credential Dump → Privilege Escalation → File Upload Exploitation → Remote Shell → Full Database Compromise

Preview: Risk chain built with all pivots and techniques.

Impact: Complete compromise of the application and extraction of sensitive simulated data.

Impact & Compliance Report (Simulation)

Business Impact:

- Leak of simulated data representing PII;
- Simulation of financial impact exceeding 2 million (by extrapolation of LGPD/GDPR fines).

Compliance Mapping:

Vulnerability	Compliance Violated	Detail
SQL Injection	PCI DSS 6.5.1	Input validation failed
File Upload / RCE	LGPD Art. 46 / GDPR Art. 32	Data protection failure
Privilege Escalation	DORA / ISO 27001	Critical environment commitment

Calculated Risk Score (Simulation):

- **Technical Complexity:**7
- **Depth of Compromise:**9
- **Business Impact:**8
- **Compliance Risk:**9
- **Detection/Stealth:**6

Final Risk Score:8.2 (Critical)

Lessons Learned — Adversary Driven Learning

- Identification of gaps in input validation and upload control;
- Monitoring failures: Explorations passed without alerts;
- Recommendation to implement WAF and harden upload permissions.

Conclusion of Practical Simulation

The case study applied at DVWA clearly demonstrated ARMA's potential to transform a technical exercise into a strategic risk analysis. The ability to chain failures, visualize the attacker's journey and produce a report that connects technique, business and compliance validates the methodology as a differentiator compared to the traditional pentest market.

Even in a laboratory environment, ARMA revealed how small vulnerabilities, when ignored or misprioritized, can result in catastrophic scenarios that go beyond the technical realm and put operational continuity and regulatory compliance at real risk.

Recommendations and Use Cases

The ARMA - Adversarial Risk Mapping & Assessment methodology was designed to meet the demands of organizations seeking an advanced offensive approach, oriented towards risk and compliance, overcoming the limitations of traditional pentest models.

Its flexibility allows for cross-cutting application in several critical scenarios, and is recommended as a reference framework for strategic cyber operations, focusing on real business impact and materialization of regulatory risk.

The main usage scenarios and application recommendations are detailed below:

Red Teaming & Adversarial Simulations

ARMA fits natively into Red Teaming operations, where the goal is not just to exploit vulnerabilities, but to simulate the reasoning, behavior and objectives of a real adversary.

Direct Benefits:

- Allows modeling of complex chained attacks;
- Facilitates mapping of impacts on high-value assets;
- Generates visual artifacts that enrich the technical and executive post-mortem;
- Seamlessly integrates Purple Team exercises, feeding back into tested defensive controls.

Recommended Application:

- APT Simulations;
- Insider Threat Scenarios;
- Ransomware Kill Chain Testing;
- Detection and Response Controls (EDR/SIEM) Testing.

ICS/SCADA Environments

In industrial and process control (ICS/SCADA) environments, where technical failure or unavailability can result in physical and catastrophic risks, ARMA offers a secure model for executing offensive simulations.

Main Applications:

- Mapping of risk chains that could lead to operational shutdown;
- Assessment of critical failure points and pivot routes between IT and OT;
- Quantification of financial impact of downtime or sabotage;
- Controlled testing with limited destructive payloads.

ARMA Differential:

Integration of the technical layer with the impact assessment on production lines, reinforcing the link between IT and the factory floor.

Cloud Security Assessments

With the massive adoption of cloud services, ARMA adapts perfectly to AWS, Azure, GCP and multi-cloud scenarios, exploring modern risk vectors such as:

- **Exposing buckets and blobs;**
- **Exploitation of IAM (Identity and Access Management) flaws;**
- **Cross-region pivoting and tenant attacks.**

Recommendations:

- Continuous evaluations of serverless and container architectures;
- Mapping of impacts on SLA and cloud compliance (SOC 2, LGPD, GDPR);
- Cloud permission abuse simulations (e.g. privilege escalation via STS).

Continuous Validation & DevSecOps Pipelines

ARMA's iterative cycle allows it to be directly integrated into DevSecOps workflows, giving organizations the ability to:

- Continuously validate attack surfaces;
- Automate part of the offensive loops;
- Adjust defensive posture based on real risk and not isolated CVE detection.

Application Scenarios:

- Validation of each new feature or critical deployment;
- Continuous monitoring of changes in the exposure surface;
- Resilience testing after updates or architecture changes.

Auditing, Risk and Compliance Alignment

ARMA provides a strategic gain for security audits, risk assessments and compliance mapping, especially for regulated sectors:

- Banking / Finance;
- Telecommunications;

- Health;
- Government;
- Energy.

Main Benefits:

- Materializes the violation of regulations such as PCI DSS, LGPD, DORA, GDPR;
- Provides technical artifacts as proof of actual exposure;
- Supports due diligence in M&A processes or external audits;
- Directly feeds GRC systems.

Final Strategic Considerations on Application

By adopting ARMA, the organization gains real capacity to anticipate strategic risks, moving from a reactive and technical model to offensive management integrated into the business.

The methodology is highly recommended for any organization that:

- Deal with sensitive data or critical infrastructure;
- Be subject to complex regulatory regimes;
- Seek maturity in Cyber Threat Intelligence (CTI);
- Need to justify cybersecurity investments based on real and quantified risks.

The ARMA methodology has established itself as a robust, versatile solution that is suitable for multiple critical scenarios in modern cybersecurity. Its application transcends traditional pentesting, providing real strategic value in Red Teaming operations, industrial environments (ICS/SCADA), cloud, regulatory audits, and continuous security validation processes.

By aligning offensive simulation, risk assessment and compliance mapping, ARMA enables organizations to visualize, prioritize and mitigate their cyber risks in a practical, visual way that is directly connected to business impacts.

With the ability to integrate with GRC, DevSecOps, SOCs and Purple Team frameworks, ARMA becomes a key element for companies seeking cyber maturity, a holistic view of risk and resilience in the face of modern threats.

Conclusion

The development of the ARMA — Adversarial Risk Mapping & Assessment — methodology represents a significant advance in offensive security practices and cyber risk management. Throughout this document, it has been demonstrated how ARMA transcends the limitations of traditional pentest approaches, introducing a strategic and multidimensional view that allows organizations to understand risk in a chained, quantifiable way and directly correlated to the impact on the business and regulatory compliance.

In the current scenario, where cyber threats evolve in complexity and sophistication, the market demands approaches that not only point out technical failures, but also demonstrate how these failures connect in risk chains capable of compromising operational continuity, exposing sensitive data and generating severe financial and reputational penalties.

ARMA responds to this demand with a structured methodological cycle, composed of phases that lead the offensive professional from the discovery of the organizational context to adversarial learning, going through:

- Threat modeling;
- Iterative execution of explorations;
- Visual mapping of risk chains;
- Integrated technical, business and regulatory reporting.

ARMA's great differentiator lies in its ability to unify technical and executive vision, delivering reports that serve both as continuous improvement artifacts for technology areas and as strategic decision-making instruments for leaders, boards and risk committees.

Furthermore, the proposed multidimensional scoring model allows organizations to move away from generic metrics such as CVSS, offering a much more realistic view of their remediation and investment priorities, based on the actual impact of each risk chain.

From a regulatory perspective, ARMA also stands out by automatically mapping violations of standards such as PCI DSS, LGPD, GDPR, DORA and others, enabling proactive compliance management and preventing technical failures from becoming legal or financial liabilities.

Its transversal applicability — whether in Red Teaming, ICS/SCADA, cloud environments, or compliance audits — reinforces the flexible and scalable nature of the methodology, making it an essential tool for organizations seeking to achieve or maintain a high degree of maturity in cybersecurity and risk management.

Ultimately, ARMA should not be seen simply as an offensive methodology, but as an offensive cyber intelligence framework capable of providing strategic visibility into the attack surface, supporting incident response plans, guiding security investment decisions, and strengthening organizational resilience in the face of modern threats.

Appendices

This section presents the technical support materials, templates and complementary references that support the practical application of the ARMA - Adversarial Risk Mapping & Assessment methodology.

The appendices are intended to facilitate the adoption of the methodology, promote the standardization of deliveries and ensure the reproducibility of processes by different teams and organizations.

Sample Risk Chain Diagram (Visual Risk Chain Model)

Suggested graphical representation to visualize the progression of the attack:

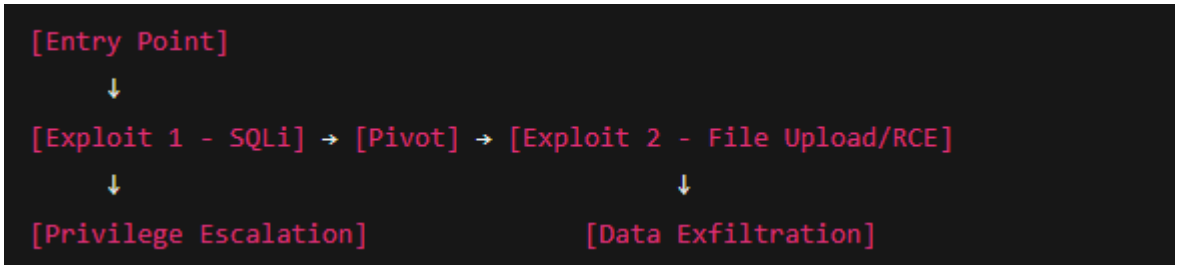

Figure 1 - Attack Progression

Caption:

- Each block represents an exploited vulnerability;
- Lines indicate the sequence and dependence between vectors;
- Pivot points are highlighted as critical moments in the chain.

Example Compliance Mapping Table

Vulnerability	Normative Framework	Article / Control	Description of Violation
SQL Injection	PCI DSS v4.0	6.5.1	Input validation failure
File Upload RCE	LGPD	Art. 46	Data protection failure
Privilege Escalation	GDPR	Art. 32	Lack of technical/organizational controls
Lateral Movement	DORA	Continuity Risk	Operational resilience compromise

Sample Risk Scoring Table

Metric	Score (1-10)	Weight	Weighted Score
Technical Complexity	7	15%	1.05
Depth of Compromise	9	25%	2.25
Business Impact	8	25%	2.00
Compliance Risk	9	20%	1.80
Stealth / Detection	6	15%	0.90
Total Risk Score			**8.0**

Glossary of Terms and Acronyms

Term / Acronym	Description
ARM	Adversarial Risk Mapping & Assessment
A.D	Depth of Compromise
BI	Business Impact
CR	Compliance Risk
TC	Technical Complexity
DS	Detection/Stealth
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge (MITRE)
CVSS	Common Vulnerability Scoring System
ICS/SCADA	Industrial Control Systems / Supervisory Control and Data Acquisition

DORA	Digital Operational Resilience Act

Bibliographic References

NIST SP 800-115— Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology.

MITRE ATT&CK Framework— Adversarial Tactics, Techniques, and Common Knowledge. MITER Corporation. Available at: https://attack.mitre.org

CWE Top 25 Most Dangerous Software Weaknesses— MITER Corporation. Available at: https://cwe.mitre.org/top25/

OWASP Web Security Testing Guide (WSTG)— Open Web Application Security Project (OWASP). Available at: https://owasp.org/www-project-web-security-testing-guide/

PCI DSS v4.0—Payment Card Industry Data Security Standard. PCI Security Standards Council. Available at: https://www.pcisecuritystandards.org

LGPD (General Personal Data Protection Law)— Brazilian General Data Protection Law (Law No. 13,709).

GDPR (General Data Protection Regulation)— European Parliament and Council Regulation (EU) 2016/679.

DORA (Digital Operational Resilience Act)— European Union Regulation on digital operational resilience for the financial sector.

ISO/IEC 27001 & 27002— International Standards for Information Security Management Systems and Controls.

The Diamond Model of Intrusion Analysis— Center for Cyber Intelligence Analysis and Threat Research. Available at: https://apps.dtic.mil/sti/pdfs/ADA586960.pdf

Purple Team Tactics and Exercises— SANS Institute.

Common Vulnerability Scoring System (CVSS) v3.1— Forum of Incident Response and Security Teams (FIRST). Available at: https://www.first.org/cvss

Cloud Security Alliance (CSA) Controls Matrix— Cloud Security Alliance.

NIST Privacy Framework— A Tool for Improving Privacy through Enterprise Risk Management.

Basel Committee on Banking Supervision — Principles for the Sound Management of Operational Risk— Bank for International Settlements (BIS).

With diagrams, compliance matrices, scoring models and a glossary, ARMA provides organizations with practical tools to transform offensive simulation into a strategic risk management and compliance exercise.