THE ARMOR MODEL

A MATURITY MODEL FOR OFFENSIVE SECURITY

www.armormodel.org

Revision 1.0, December 2025

Author(s)
Greg Anderson

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

About This Document

The ARMOR Model was authored by Greg Anderson (The Author). It is intellectual property of The Author and is intended as a vendor-agnostic framework to guide organizations in advancing offensive security maturity.

Terms of Use

Copyright © 2025 Greg Anderson. Published at www.armormodel.org. Licensed under the Creative Commons Attribution–NonCommercial–ShareAlike 4.0 International License (CC BY-NC-SA 4.0).

You may copy, share, and adapt this work for non-commercial purposes with appropriate credit to The Author. Any adaptations must be distributed under the same license. Commercial use, including incorporation into products, training, or services, requires prior written permission.

How to Cite ARMOR

When referencing the ARMOR Model in research, reports, or presentations, please use the following citation format:

> Anderson, Greg. (2025). *The ARMOR Model*. www.armormodel.org.

Disclaimer

The ARMOR Model is provided for informational purposes only. It does not guarantee compliance with regulations or protection against cyber threats. Organizations are responsible for evaluating its applicability and making independent risk management decisions. The Author disclaims any liability for damages or losses resulting from its use.

PREFACE

Over the past several years, I have had conversations with hundreds of CISOs and security leaders across organizations of every size, from small and midsized businesses to global enterprises. What I have learned is that despite their differences in budget, technology, and maturity, they all share a common challenge: most are not strategically using offensive security outcomes to drive tactical, operational, and management decisions.

That is not a criticism, it is the result of how our industry has evolved. For decades, frameworks and compliance programs have conditioned us to think of offensive security as a validation exercise, not a continuous discipline. Penetration testing, in particular, has become our annual report card. Teams work all year to strengthen defenses, prepare playbooks, and implement controls. Then, once per year, a test is performed to see how well they did, vulnerabilities are patched, and attention turns back to operations until the next cycle.

It is an understandable pattern, but it is also a limiting one. Think about athletics: football, baseball, basketball, hockey, any competitive sport. Imagine if every team spent their time exclusively in the gym, focused on strength and conditioning, but never practiced the actual game. They would be strong, well-prepared in theory, and completely untested in execution. When game time arrived, they would lose not because they were incapable, but because they had not practiced under real conditions.

That is exactly what we are doing in cybersecurity. We are building strong networks and endpoints and conditioning our teams through documented procedures, but we are not practicing the game. Our defenses are based on ideal conditions, our playbooks are theoretical, and our incident response processes are largely untested under pressure. We have mastered preparation, but not performance.

That is where The ARMOR Model comes in. ARMOR was created to bridge this gap between compliance and capability, to move organizations from periodic testing toward continuous, adaptive resilience. It is designed to help security leaders understand where they are today and build a clear, practical roadmap for improvement.

ARMOR is not a tool or a product, and it is not owned by any single company or vendor. It is a structured, vendor-agnostic model developed to help organizations use offensive security as a driver of real-world readiness. Each level of the model builds upon the last, transforming testing from a checkbox exercise into a living program that strengthens detection, response, and organizational confidence.

My goal in creating ARMOR is not to replace the frameworks we already rely on, but to help organizations operationalize them. Offensive security should not exist in isolation from governance, risk, and operations. It should inform them. When used effectively, offensive outcomes are not just security metrics, they are business insights that help organizations make smarter, faster, more resilient decisions.

We cannot buy our way to resilience, and we cannot audit our way to readiness. But we can practice, measure, and improve. That is what ARMOR is about: giving organizations a practical path to transform testing into continuous validation and resilience into a sustained capability.

— **Greg Anderson**
Creator, The ARMOR Model ™

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

TABLE OF CONTENTS

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

EXECUTIVE SUMMARY

Organizations today invest heavily in cybersecurity; millions of dollars annually on controls, technology, and compliance programs; yet measurable readiness remains elusive. Despite this spend, attackers continue to exploit vulnerabilities faster than defenders can respond, and expanding attack surfaces across cloud, SaaS, and third-party ecosystems make exposure management increasingly complex.

Most organizations still approach validation as a series of point-in-time events: annual penetration tests, quarterly vulnerability scans, and isolated red team exercises. These activities serve important purposes, but they fail to measure how well an organization can detect, respond, and recover under real conditions. The result is a widening gap between perceived preparedness and operational resilience.

The ARMOR Model provides a structured, vendor-agnostic roadmap to close that gap. ARMOR provides a five-level progression that guides organizations from reactive, compliance-driven testing toward continuous, adaptive validation, integrated with operations and governance.

THE ARMOR MODEL IS

- **Progressive:** Each level builds on the one before it, ensuring maturity is both achievable and sustainable.
- **Practical:** Every stage defines outcomes, actions, sustainment criteria, and Governance so organizations know what maturity looks like and how to achieve it.
- **Universal:** Applicable to organizations of any size or sector. Smaller teams can leverage trusted partners; larger enterprises can scale internally.
- **Aspirational:** The upper levels are designed to stretch capabilities toward integrated, continuous validation. Few will reach full resilience, but all gain strength by advancing incrementally.

THE ARMOR MODEL HELPS ORGANIZATIONS

- Benchmark their current offensive security maturity.
- Identify practical actions to advance to the next level.
- Ensure practices are sustained before moving forward.
- Connect offensive security directly to business resilience.

Offensive security cannot deliver its full value when reduced to audits and checklists. With ARMOR, organizations gain a roadmap to evolve testing into a continuous discipline that strengthens detection, response, and resilience against modern adversaries.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

INTRODUCTION

THE STATE OF EXPOSURE AND READINESS

The modern attack surface is expanding faster than most organizations can secure it. Hybrid infrastructures, cloud workloads, SaaS platforms, and third-party dependencies have replaced the perimeter with a constantly shifting landscape of exposures. Each new service, integration, or deployment introduces potential entry points, while patch cycles, monitoring, and remediation workflows across this disparate infrastructure often lag behind real-world exploitation.

Meanwhile, global security spending continues to rise; projected to exceed $240 billion in 2026; though much of that investment still focuses on prevention and compliance rather than measurable readiness. Controls exist, but their effectiveness under pressure remains largely untested against real-world, persistent, adversarial behavior.

THE STATE OF OFFENSIVE SECURITY

For many organizations, offensive security remains a snapshot exercise. Penetration tests are conducted annually to satisfy auditors or customers. Red team engagements occur once every year or two, while vulnerability scans identify missing patches and misconfigurations. These efforts drive break-fix remediation processes but rarely deliver insights that meaningfully contribute to operational improvement or resilience.

Reports become static artifacts: vulnerabilities are triaged, remediations tracked, and metrics are centered around isolated, point-in-time responsiveness. What's missing is a sustained feedback loop where offensive results inform detection engineering, risk management, and executive decision-making.

GAPS CREATE WEAKNESSES

This unfortunate state has created a widening array of gaps that leave organizations in a state of unknown unknowns that ultimately leads to real weaknesses when faced with the threat of persistent adversaries.

- **Point-in-time testing/remediation:** Most organizations test and remediate annually or semi-annually, leaving long windows where exposures go unvalidated. Mean time to Remediate, gets tracked, ignoring that some vulnerabilities had existed for months prior.

- **Compliance-driven scope:** Testing is frequently shaped by regulatory requirements rather than the organization's true exposure. PCI-DSS, for example, only requires the systems within the flow of cardholder data are tested, leaving large parts of the organization untested.

- **Tool dependence:** Many organizations equate buying a tool with solving the problem. Few organizations are evaluating their security spend against the results of offensive security exercises and how effective their teams are at tuning, monitoring and using these tools.

- **Limited integration:** Results are rarely considered in enterprise risk management or used to influence strategic decisions. Are you asking questions like: "*Were likely adversarial attack paths tested?*" or "*What changes as a result of these findings?*"

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

HOW ARMOR IS DIFFERENT

The ARMOR Model addresses these gaps by offering a clear, progressive roadmap from compliance-driven testing to continuous resilience. It defines not just what maturity looks like at various levels, but how to achieve, sustain and grow from one level to the next.

PROGRESSIVE NATURE

The ARMOR Model is sequential by design. Organizations cannot skip levels, nor should they attempt to. Each stage establishes a foundation that supports the next. For example, without consistent inventories and remediation cycles at Level 2, it is impossible to strategically align offensive security activities in Level 3. Similarly, advanced adversary simulations at Level 4 will fail to deliver value without a well-documented strategy and integrated processes from earlier levels.

This progression reflects the reality of how organizations mature: not through sudden transformation, but through incremental improvements in visibility, governance, process, and culture. Each level builds directly on the practices and sustainment criteria of the previous one, ensuring that progress is durable and not superficial.

- **From Ad Hoc to Repeatable (Levels 1–2**): Organizations move from compliance-driven testing toward predictable, recurring practices, creating the operational rhythm necessary for consistency.

- **From Repeatable to Managed (Level 3):** Testing becomes strategic, broadening in scope to include cloud, SaaS, and supply chain exposures, while remediation is governed by SLAs. Organizations begin to connect offensive security to business risk.

- **From Managed to Optimized (Level 4):** Red and purple teaming, adversary simulations, and resilience metrics are introduced. The A/B split provides achievable milestones, allowing organizations to begin with annual exercises and structured tabletop reviews (4A) before scaling to quarterly, intelligence-driven simulations that include business and executive participation (4B).

- **From Optimized to Resilient (Level 5):** Validation becomes continuous, adaptive, and fully integrated into enterprise governance. Foundational resilience (5A) includes regular crisis-focused tabletop and simulation exercises, while advanced resilience (5B) represents the aspirational standard where these exercises are institutionalized across technical, operational, and executive functions.

The ARMOR Model is intentionally challenging but achievable. Smaller organizations can make meaningful progress in the early levels, while enterprises with greater resources can pursue advanced resilience. By adopting the model incrementally, organizations demonstrate measurable improvements at every stage, without the risk of overreach or wasted investment.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

THE FOUR ELEMENTS OF EACH LEVEL

Each ARMOR level is described through four consistent elements:

- **Outcomes** define what the organization achieves at that stage.
- **Actions** describe the steps organizations must take to reach those outcomes.
- **Sustainment Criteria** outline what must be in place to hold maturity before advancing.
- **Governance** ensures the outcomes and sustainment criteria are institutionalized as part of normal business operations.

Together, these elements provide a holistic view of maturity. Outcomes describe the "what," actions outline the "how," sustainment ensures stability, and supporting practices connect offensive security to the broader organization.

THE LEVELS OF THE ARMOR MODEL

LEVEL 1: AD HOC

At the Ad Hoc level, organizations are beginning their offensive security journey. Activities are typically driven by compliance or customer requirements, but they provide an important foundation for visibility and awareness. By completing annual assessments, identifying critical assets, and consistently tracking vulnerabilities, organizations establish the first essential steps toward structured practices and build the accountability needed to progress toward more proactive security.

OUTCOMES

- Compliance needs are satisfied through at least one penetration test or vulnerability assessment each year.
- Initial asset awareness is established by identifying core systems, applications, and data critical to business operations.
- Security visibility is improved by documenting vulnerabilities and exposures, creating a baseline understanding of the attack surface.
- Basic prioritization of risks occurs using standard severity ratings (e.g., Critical, High, Medium, Low).

ACTIONS

- Perform an annual penetration test or vulnerability scan to meet regulatory or customer obligations and to gain an initial view of the attack surface.
- Create a simple asset inventory that includes critical business systems, applications, and data stores. This can be maintained in a spreadsheet, shared drive, or simple asset management tool.
- Document test results centrally so they are easy to review, reference, and track over time.
- Prioritize remediation efforts by addressing "Critical" and "High" vulnerabilities first, ensuring the most significant issues are managed.
- Engage business and IT stakeholders following each test to review results and ensure that findings are understood and connected to operational priorities.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

SUSTAINMENT CRITERIA

- An annual penetration test or vulnerability assessment is consistently completed and retained for records.
- An asset inventory exists, covering all known critical business systems, and is reviewed at least once per year.
- All identified “Critical” vulnerabilities are remediated or have a documented mitigation plan.
- Test results and remediation actions are tracked in a central location accessible to security and IT teams.

GOVERNANCE

- Testing activities are managed within existing compliance or IT functions and approved through basic audit or assurance processes.
- Leadership acknowledges the importance of testing for visibility and external validation.
- Governance at this stage focuses on maintaining accountability for completion, retaining documentation, and using results to inform future planning.
- Policies or procedures may be informal but establish an initial foundation for consistent oversight and recordkeeping.

LEVEL 2: REPEATABLE

At the Repeatable level, organizations move beyond single, compliance-driven assessments and establish a regular cadence for offensive security. Testing becomes scheduled and predictable, assets are tracked more thoroughly, and remediation is validated through retesting. By embedding testing into the operational rhythm, organizations gain greater visibility into vulnerabilities, reduce repeated findings, and create the foundation for aligning offensive security with broader business risk.

OUTCOMES

- Testing is predictable: Penetration testing and/or vulnerability assessments are scheduled on a recurring basis (at least annually, often biannually or quarterly).
- Asset visibility improves: Inventories of systems, applications, and data are expanded and updated more frequently, reducing blind spots.
- Remediation is closed-loop: Vulnerabilities are tracked until resolution, with retesting to confirm effectiveness.
- Risk awareness grows: Early threat modeling begins, helping to identify potential attack paths and inform scoping decisions.

ACTIONS

- Establish a testing cadence (e.g., annual, semi-annual, or quarterly) and ensure it is formally documented and budgeted.
- Maintain an updated asset and application inventory, expanding coverage beyond critical systems identified at Level 1.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

- Introduce a remediation workflow: Use ticketing systems or project management tools to log vulnerabilities, assign ownership, and track them through closure.
- Confirm fixes through retesting, ensuring vulnerabilities are not just marked “closed” but validated by follow-up.
- Apply basic threat modeling during scoping discussions to identify high-value assets and likely attack vectors.

SUSTAINMENT CRITERIA

- Security testing occurs on a predictable schedule, not just in response to compliance demands and has appropriate funds/budget assigned.
- Asset inventories are reviewed and updated at least quarterly.
- All vulnerabilities are prioritized, have a documented remediation plan, and are tracked until resolved.
- Retesting of remediated vulnerabilities occurs to confirm effectiveness.
- Threat modeling workshops or exercises are conducted at least annually to inform scoping.

GOVERNANCE

- Governance structures begin to define accountability for testing and remediation activities.
- Security or IT management assumes responsibility for scheduling, scope, and coordination of assessments.
- Testing frequency, ownership, and documentation requirements are outlined in policy or standard operating procedures.
- Leadership reviews test results and progress against previous assessments to ensure follow-through and improvement.
- Oversight ensures consistency, visibility, and traceability of testing activities, setting the stage for program-level management.

LEVEL 3: MANAGED

At the Managed level, offensive security evolves into a deliberate program aligned with organizational goals. A documented strategy guides testing, the scope expands to include cloud, SaaS, and third-party environments, and results are tied to structured remediation and governance. Offensive security becomes integrated into IT and business change cycles, ensuring new initiatives are validated before introducing risk. This marks a turning point: security is no longer performed just for compliance or consistency, but as a strategic discipline that supports business priorities and acts as a proactive partner in innovation.

OUTCOMES

- Documented offensive security strategy: A written strategy exists and is reviewed regularly to ensure alignment with business objectives.
- Broader coverage: Testing expands beyond traditional IT infrastructure to include cloud, SaaS, APIs, and third-party services.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

- Threat-informed scoping: Threat modeling is structured and formalized, ensuring test scenarios reflect realistic attack paths.
- Change-driven testing: Security testing is triggered not only by cadence but also by significant business or IT changes (e.g., acquisitions, application launches, infrastructure shifts).
- Formal remediation governance: Service-level agreements (SLAs) define timelines for fixing vulnerabilities by severity.

ACTIONS

- Develop and maintain an offensive security strategy that ties testing to organizational risk and business objectives, review annually.
- Expand testing scope to include cloud environments, SaaS platforms, APIs, and critical supply chain integrations.
- Formalize threat modeling using methodologies such as STRIDE, PASTA, or MITRE ATT&CK to guide test planning.
- Integrate testing into change cycles, making offensive security part of ITIL, DevOps, or digital transformation workflows.
- Define remediation SLAs (e.g., Critical issues fixed within 15 days, High within 30 days) and hold teams accountable.
- Introduce social engineering testing to evaluate user and process resilience.

SUSTAINMENT CRITERIA

- A documented and approved offensive security strategy is reviewed and updated annually.
- Testing covers on-premises, cloud, SaaS, and third-party environments.
- Remediation SLAs are consistently applied and tracked for accountability.
- Security testing is formally included in IT and business change management processes.
- Social engineering assessments (e.g., phishing, pretexting) are part of the testing program.
- Threat modeling sessions are conducted before major initiatives and at least annually for core assets and are used to inform both scoping and scenario-based exercises and associated incident response procedures in future stages.

GOVERNANCE

- Formal governance mechanisms oversee testing strategy, resource allocation, and remediation performance.
- Policies define testing objectives, required coverage, and SLA expectations for remediation. Executive sponsors or risk committees review results, trends, and strategic alignment with business goals.
- Findings are tracked through established governance workflows with escalation for unresolved issues.
- Governance ensures that offensive security is integrated into change management, project approval, and risk reporting processes, enabling predictable, strategic outcomes.

LEVEL 4: OPTIMIZED

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

At the Optimized level, offensive security evolves into a sustained program that goes beyond identifying vulnerabilities to measuring resilience, validating detection and response, and informing business risk decisions. Because organizations vary in resources and maturity, Level 4 is divided into two sub-levels:

- **4A (Foundationally Optimized):** Represents the minimum practices that demonstrate optimization is underway. Organizations conduct regular red and purple team exercises, supported by structured tabletop exercises that simulate both technical and executive-level incident response scenarios. These TTX events help validate coordination between technical responders, business units, and leadership teams. Early resilience metrics are introduced to measure detection, response, and recovery performance. The focus is on establishing repeatable testing rhythms, improving cross-team communication, and beginning to quantify resilience outcomes.

- **4B (Fully Optimized):** Represents full maturity at this stage. Adversary simulations are ongoing, with tabletop exercises integrated into the broader test cycle to validate readiness across operations, executive management, and communications functions. Threat intelligence is embedded into both technical and scenario-driven tests, ensuring exercises reflect evolving adversary behaviors and organizational priorities. Results directly inform enterprise risk management, enabling leadership to evaluate not only control performance but also decision-making, communication, and resilience under simulated stress.

LEVEL 4A: FOUNDATIONALLY OPTIMIZED

OUTCOMES

- Annual red and purple team exercises are conducted to validate security controls and testing resilience of SOC/IR functions.
- Adversary simulations are incorporated, simulating realistic attack paths.
- Introductory tabletop exercises begin to validate coordination, escalation, and communication processes in response to simulated incidents.
- Initial resilience metrics (MTTD, MTTR, detection coverage) are collected for critical systems.
- Findings are remediated and retested to confirm closure.
- Results are reviewed by security leadership and used to inform remediation priorities.

ACTIONS

- Develop a documented red/purple team testing plan with defined scope, objectives, and cadence.
- Partner with external specialists to lead exercises while internal teams participate and learn.
- Measure and document how quickly attacks are detected and contained.
- Facilitate tabletop exercises at least annually to evaluate IR coordination and validate communication between SOC, IT, and management teams.
- Perform after-action reports and lessons-learned workshops to ensure improvements are applied.
- Share results with security leadership and incorporate outcomes into security program planning.

SUSTAINMENT CRITERIA

- Annual red/purple team exercises occur consistently, with evidence of lessons learned and remediation validated.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

- At least one tabletop exercise is completed annually and reviewed for effectiveness in communication and decision-making.
- At least one resilience metric is collected for each critical asset class (e.g., endpoints, cloud apps, perimeter).
- Test results are archived, and year-over-year comparisons demonstrate progress.
- Security leadership formally reviews results within 30 days of each exercise.

GOVERNANCE

- Executive sponsorship for offensive security is formalized within governance committees or steering bodies that also oversee risk and operations.
- Policies and standards codify the role of advanced testing, such as red and purple team exercises, defining cadence, approval, and reporting expectations.
- Leadership ensures that results are reviewed, tracked, and incorporated into process and policy improvements.
- Governance requires that outcomes from exercises and initial tabletop reviews are used to strengthen coordination between IT, security, and operations teams.

LEVEL 4B: FULLY OPTIMIZED

OUTCOMES

- Red and purple team exercises are performed quarterly or in response to significant changes in the business or IT environment.
- Adversary simulations are designed and executed using live threat intelligence to mirror realistic attacker behaviors.
- Tabletop exercises evolve into structured cross-functional simulations conducted alongside red/purple team activities.
- Resilience metrics (MTTD, MTTR, detection coverage, recurring exposure rates) are collected, trended over time, and compared against defined targets.
- Testing results are incorporated into enterprise risk dashboards reviewed by executives and risk committees.
- Offensive security outcomes are consistently linked to measurable improvements in detection engineering, SOC performance, and incident response readiness.

ACTIONS

- Establish a quarterly (or event-driven) testing cadence that includes red/purple team exercises and advanced adversary simulations.
- Integrate live threat intelligence into scenario design, ensuring testing reflects emerging attacker tactics.
- Conduct tabletop exercises bi-annually to test IR procedures, executive escalation paths, and decision-making under simulated stress.
- Translate simulation findings into concrete detection engineering content (e.g., SIEM rules, EDR analytics, log correlation enhancements).
- Share results with executive stakeholders through risk dashboards, executive briefings, or steering committees.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

- Maintain formalized lessons-learned workshops and assign clear ownership for closing identified detection and response gaps.

SUSTAINMENT CRITERIA

- Red/purple team exercises and adversary simulations occur at least quarterly or following significant business/technology changes.
- Tabletop results are documented and correlated with live test findings to identify systemic or process-level gaps.
- Multiple resilience metrics along with remediation cycle times are consistently collected, benchmarked, and trended to demonstrate progress.
- Results are integrated into enterprise risk dashboards and reviewed by executive leadership at least quarterly.
- Evidence exists that testing has directly influenced improvements in SOC operations, IR playbooks, or risk prioritization.

GOVERNANCE

- Governance expands into an integrated oversight framework connecting offensive validation, resilience metrics, and business risk management.
- Policy defines requirements for threat-informed adversary simulations, red/purple team integration, and follow-up review cycles.
- Executive risk committees evaluate metrics and simulation outcomes as part of enterprise risk and performance dashboards.
- Tabletop exercise results and threat trend analyses are incorporated into policy, training, and governance updates.
- Oversight ensures that offensive validation is sustained, repeatable, and adaptive to evolving threats and business conditions

LEVEL 5: RESILIENT

At the Resilient level, offensive security becomes continuous, adaptive, and deeply embedded into organizational culture and enterprise governance. Testing is no longer an isolated event but an ongoing process of validation and improvement, ensuring that defenses can adapt as quickly as threats evolve. Because few organizations will achieve all aspects of this level, it is divided into two sub-levels:

- **5A (Foundational Resilience):** Represents foundational resilience, where continuous validation begins across critical assets and systems. Advanced adversary simulations and crisis-focused tabletop exercises are conducted regularly to evaluate both technical response and executive decision-making under pressure. These exercises stress-test communication, coordination, and leadership readiness in realistic, time-constrained scenarios. Results are reviewed by senior leadership and used to validate detection capabilities, recovery processes, and business continuity planning. The organization begins treating resilience as a measurable outcome, not an abstract goal.

- **5B (Fully Resilient):** Represents full resilience, where continuous validation is automated across all major environments, and adversary simulations are conducted in tandem with strategic crisis simulations involving executive and board participation. These high-fidelity exercises emulate

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

enterprise-wide disruptions—such as data loss, destructive attacks, or supply chain compromise—to validate response speed, decision clarity, and strategic adaptability. Results are embedded directly into board-level risk reporting and strategic decision-making, ensuring offensive validation, business continuity, and governance operate as a unified discipline.

LEVEL 5A: FOUNDATIONAL RESILIENCE

OUTCOMES

- Continuous validation is established for critical systems, business applications, and key controls.
- Semi-annual adversary simulations validate detection, response, and recovery against realistic attacker behaviors.
- Tabletop exercises expand into crisis simulations involving technical, operational, and leadership participants.
- Security leaders use offensive security results in quarterly strategy and investment discussions.
- Exposure management shifts from remediation of discrete vulnerabilities to reduction of systemic risk.

ACTIONS

- Deploy continuous validation for mission-critical systems and high-risk assets (e.g., production cloud workloads, payment platforms, customer-facing apps).
- Conduct semi-annual adversary simulations, integrating threat intelligence into scenario design.
- Introduce crisis tabletop simulations focused on validating containment and recovery procedures, communication plans, and coordination between departments.
- Align offensive security reporting with enterprise risk registers and strategy planning cycles.
- Set measurable exposure reduction targets (e.g., reducing time-to-remediation or mean exposure days).

SUSTAINMENT CRITERIA

- Continuous validation is maintained across at least critical systems with documented scope and results.
- Adversary simulations are conducted semi-annually and reviewed at the executive level.
- Tabletop and crisis simulation findings are tracked, and remediation actions are verified through follow-up testing or audits.
- Risk dashboards reflect exposure reduction trends, not just point-in-time vulnerability counts.
- Results are directly linked to resourcing, budget adjustments, or risk mitigation initiatives.

GOVERNANCE

- Governance fully integrates continuous validation, adversary simulation, and resilience measurement into enterprise risk management.
- Policy mandates the ongoing alignment of offensive security activities with business continuity, crisis management, and incident response programs.
- Leadership regularly reviews validation outcomes and resilience metrics, using them to adjust priorities and resource allocation.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

- Governance ensures structured accountability, defined ownership, and documentation to sustain continuous improvement.

LEVEL 5B: FULLY RESILIENT

OUTCOMES

- Continuous validation extends across the enterprise environment, including on-premises, cloud, SaaS, and supply chain exposures.
- Adversary simulations are ongoing and adaptive, with new threat intelligence automatically shaping test scenarios.
- Enterprise-level tabletop and crisis simulations are institutionalized to validate governance, communication, and strategic decision-making.
- Resilience metrics (e.g., mean time to detect/respond, percent of coverage, exposure reduction rate) are tracked at the enterprise level.
- Offensive security outcomes are embedded into board-level risk discussions and capital allocation.
- Continuous improvement cycles (plan–do–check–act) are institutionalized across security operations.

ACTIONS

- Expand continuous validation to cover all significant business systems, cloud environments, and third-party integrations.
- Establish an adaptive adversary simulation program, continuously updated by real-time threat intelligence.
- Conduct quarterly enterprise tabletop and crisis simulations that test executive communication, governance coordination, and business continuity.
- Integrate resilience metrics into enterprise scorecards and risk dashboards.
- Formalize a PDCA cycle:
    - **Plan**: Define objectives for offensive security aligned with risk.
    - **Do**: Execute continuous validation and adversary simulations.
    - **Check:** Review outcomes with executives and the board.
    - **Act**: Adjust strategy, budgets, and processes based on lessons learned.

SUSTAINMENT CRITERIA

- Continuous validation is active across the enterprise, with results consistently maintained and monitored.
- Adversary simulations are executed on an ongoing basis.
- Crisis simulation metrics (response time, communication accuracy, decision velocity) are tracked and reported to executive leadership. Cross-functional teams including legal, HR, and corporate communications regularly participate in enterprise tabletop exercises.
- Enterprise resilience metrics show sustained improvement over multiple review cycles.
- Board-level oversight includes offensive security as a standard input to enterprise risk governance.

GOVERNANCE

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

- At this final stage, offensive security governance is institutionalized at the enterprise level and embedded into board oversight.
- Policy, risk frameworks, and operational governance all incorporate continuous validation, TTX results, and resilience performance as ongoing strategic inputs.
- Executive and board-level reporting includes offensive security as a key indicator of organizational readiness and operational risk.
- Governance ensures adaptability, transparency, and sustained integration across security, IT, operations, and business leadership, treating resilience as a measurable, managed business discipline.

PRACTICAL NEXT STEPS: USING ARMOR

The ARMOR Model provides structure and clarity, but its value lies in how organizations apply it. Offensive security maturity cannot be achieved by purchasing tools or commissioning isolated tests. It requires consistent evaluation, prioritization, and follow-through. The following steps provide a roadmap for putting ARMOR into practice.

SELF-ASSESSMENT

Begin with an honest evaluation of your organization against the Outcomes, Actions, Sustainment Criteria, and Governance defined in the model. Compare your current testing practices with the descriptions at each level and determine where you most closely align. To provide more targeted guidance on where to begin, ARMOR provides a self-assessment worksheet in Appendix B as well as an online assessment tool at www.armormodel.org.

After you determine your current maturity, first re-review the sustainment criteria for the previous level. Confirm there are no gaps in process, coverage, or metrics. If issues remain, resolve them before advancing. Once you are confident you can hold your current level, focus on the next logical level. The model is sequential, and progress is earned step by step.

- Verify last level's sustainment evidence is current and complete.
- Close any gaps in process, coverage, or metrics.
- Reconfirm ownership and cadence.
- Advance only when sustainment is demonstrated, then plan actions for the next level.

HOW TO PROGRESS

1. Use the ARMOR actions at your target level as the foundation for planning. Translate them into projects or initiatives in your security roadmap. Assign clear ownership, set timelines, and connect each action to business objectives, not just technical goals.

2. Progression is only durable if sustainment is in place. Validate that asset inventories are accurate, remediation timelines are enforced, strategies are reviewed, and metrics are collected and applied. Advancement should occur only when practices are consistently demonstrated.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

3. Maturity requires more than testing; it requires an ecosystem. Strengthen the supporting Governance at each level:
   - **Governance**: Establish steering committees or executive sponsorship.
   - **People**: Invest in staff development, hiring, or trusted partners.
   - **Process**: Embed testing into change management, risk, and business workflows.
   - **Technology**: Adopt tools to support practices, not replace them.

4. Treat higher levels as aspirational. Not every organization will reach the Resilient stage, but all can benefit from its principles. Even partial adoption of continuous validation or adversary simulation practices brings measurable gains. Stabilizing at earlier levels is not failure, it still represents meaningful, sustainable progress.

5. Maturity is not static. Technology stacks, business priorities, and adversary tactics constantly shift. Reassess your ARMOR level annually or after major organizational changes. Use results to update your roadmap, celebrate progress, and identify new opportunities to advance.

CONCLUSION

Organizations are investing more in cybersecurity than ever before, yet many still struggle to measure whether those investments translate to true readiness. Annual penetration tests, vulnerability scans, and compliance audits continue to provide value, but they offer only momentary insight into an environment that changes daily. Attack surfaces evolve, adversaries adapt, and without continuous validation, even mature programs risk operating on assumptions rather than evidence.

The ARMOR Model addresses this gap by providing a structured, progressive roadmap for evolving from point-in-time assessments to continuous resilience. It defines what maturity looks like at each stage and how to achieve it through sustained actions, measurable outcomes, and operational integration. By treating offensive security as a continuous discipline, rather than a periodic audit, organizations can connect validation directly to governance, operations, and business risk.

The model offers clarity by defining maturity in practical terms; alignment by connecting offensive outcomes to enterprise objectives; sustainability by emphasizing sustainment before advancement; and universality by making maturity achievable regardless of organization size or industry.

Reaching the highest levels of ARMOR is intentionally aspirational. Few organizations will achieve full resilience immediately, but every step forward improves visibility, coordination, and confidence. The journey itself is where resilience is built.

Next steps are clear: assess your current maturity, identify your next logical level, and focus on building the people, processes, and governance needed to sustain each improvement. Whether progress comes through internal development or trusted partnerships, the outcome is the same, stronger validation, more adaptive defenses, and a measurable increase in organizational resilience.

The ARMOR Model is not a checklist; it is a roadmap for growth. In a world of constant threats and accelerating change, continuous validation is no longer optional, it is essential.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

APPENDIX A - GLOSSARY OF TERMS

Ad Hoc (ARMOR Level 1)
The initial stage of offensive security maturity. Activities are irregular, often compliance-driven, and provide basic visibility but limited repeatability or integration into business risk management.

Adversary Simulation
A controlled engagement that emulates tactics, techniques, and procedures (TTPs) of real-world threat actors. Unlike traditional penetration tests, these simulations validate detection, response, and coordination across security and business teams.

After-Action Review (AAR)
A structured post-exercise analysis that captures successes, failures, and corrective actions. AARs convert testing results into lessons learned for measurable improvement.

Annual Penetration Test
A point-in-time assessment required for compliance or customer assurance. Identifies exploitable vulnerabilities but does not provide continuous validation of defenses.

ARMOR Model
A five-level maturity framework—Ad Hoc, Repeatable, Managed, Optimized, Resilient—guiding organizations from compliance-driven testing to continuous, adaptive resilience.

Attack Surface
All potential points where an adversary could gain unauthorized access. Includes networks, endpoints, cloud services, applications, and third-party integrations.

Board-Level Risk Reporting
Formal presentation of offensive security outcomes and resilience metrics to executive and board leadership, ensuring cyber risk is evaluated as business risk.

Change-Driven Testing
Triggering offensive testing based on material business or technology changes—such as new applications, infrastructure migrations, or acquisitions—to validate new exposures.

Continuous Improvement (CI)
The process of iteratively refining controls and processes based on feedback, findings, and metrics. Within ARMOR, CI is formalized through the Plan–Do–Check–Act (PDCA) cycle.

Continuous Validation
Ongoing automated or semi-automated testing of controls and exposures to ensure defenses remain effective as systems and threats evolve.

Crisis Simulation

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

A high-impact tabletop or live-fire exercise that replicates a significant cyber or business disruption, testing leadership, communication, and strategic decision-making under pressure.

Detection Engineering
The design and tuning of detection logic—SIEM rules, endpoint analytics, and telemetry correlation—based on insights from adversary behavior and offensive exercises.

Exposure Management
The continuous identification, prioritization, and reduction of attack surface and exploitable weaknesses, extending beyond vulnerability management to include misconfigurations and third-party risks.

Exposure Reduction Metrics
Quantitative indicators of how effectively exposures are closed or mitigated over time, such as mean exposure days or recurring issue rates.

Governance Integration
The alignment of offensive security results with enterprise risk, compliance, and strategic planning so testing outcomes inform executive decision-making.

Lessons-Learned Workshop
A collaborative meeting following an exercise or incident to discuss findings, assign ownership, and track improvements to completion.

Managed (ARMOR Level 3)
The stage where offensive security becomes strategic, documented, and governed. Testing expands in scope and is tied to risk, service-level agreements, and change management.

Mean Time to Detect (MTTD)
The average duration between an adversary action and its detection by the organization.

Mean Time to Respond (MTTR)
The average duration between detection and containment or recovery from a security event.

Metrics (Resilience Metrics)
Quantitative measures—such as MTTD, MTTR, exposure reduction, and detection coverage—that track resilience performance and program progress.

Governance
The supporting ecosystem of governance, people, process, and technology that sustains each ARMOR level's maturity.

Optimized (ARMOR Level 4)
A maturity stage where red and purple team exercises, adversary simulations, and resilience metrics validate both control effectiveness and organizational coordination. Tabletop exercises become structured and recurring.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

Outcomes
The measurable results expected at each level of the model that define success (e.g., predictable testing cadence, integration into governance, or continuous validation).

PDCA Cycle (Plan–Do–Check–Act)
A four-step framework for continuous improvement:

1. **Plan:** Define objectives and metrics.
2. **Do:** Execute testing and validation.
3. **Check:** Review outcomes and data.
4. **Act:** Implement improvements and update strategy.

Penetration Test (Pentest)
A time-boxed, authorized attempt to exploit vulnerabilities in systems or applications to assess real-world risk exposure.

Purple Team Exercise
A cooperative engagement where offensive and defensive teams work together in real time to validate detection and response capabilities.

Red Team Exercise
A stealth, goal-oriented simulation of an advanced adversary conducted to measure detection, response, and resilience across people, process, and technology.

Repeatable (ARMOR Level 2)
The stage where organizations establish a predictable cadence for testing and remediation, enabling consistency and trend analysis.

Resilience
An organization's capacity to anticipate, withstand, recover from, and adapt to cyber threats without loss of mission or critical business operations.

Resilient (ARMOR Level 5)
The aspirational stage of continuous, adaptive validation integrated into enterprise governance and board oversight. Offensive security becomes a sustained business discipline.

Risk Dashboard
A consolidated visual display of resilience metrics, exposures, and trends used for executive communication and decision support.

Sustainment Criteria
Defined requirements that demonstrate a level's maturity is stable and repeatable before progressing further. Ensures advancement is durable.

Tabletop Exercise (TTX)

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

A guided, discussion-based simulation that tests coordination, escalation, and decision-making during an incident scenario. Used to validate processes without impacting live systems.

Threat Intelligence Integration
Incorporating current adversary tactics and motivations into test planning to ensure simulations reflect realistic, evolving threats.

Threat Modeling
A structured analysis used to identify potential threats, attack paths, and control weaknesses for prioritizing testing and defense efforts.

Validation
The act of confirming that security controls, processes, and response mechanisms perform as intended during realistic testing or simulations.

Vulnerability Scanning
Automated scanning to identify known vulnerabilities and misconfigurations across assets, forming the foundation for higher-level offensive testing.

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

APPENDIX B - SELF-ASSESSMENT WORKSHEET

ASSESSMENT & SCORING GUIDANCE

For each question, select the value that best represents your organization's current practice.

Score	Description
1 – Emerging	Practices are ad hoc or inconsistently applied. Activities are primarily reactive or compliance-driven.
2 – Developing	Practices are defined and repeatable but not yet strategic. Processes exist, though integration and sustainment vary across teams or systems.
3 – Established	Practices are formalized, sustained, and measured. Outcomes are consistently used to drive improvement and inform tactical, operational, and management decisions.

After completing all questions:

1. Sum the five scores in each section and divide by 5 to find your Section Average.
2. Add all section averages and divide by 4 to find your Overall Average.
3. Use the Overall Average to identify your corresponding ARMOR Level

SELF-ASSESSMENT SCORE

Section	***Worksheet Results***	
Governance & Strategy		
Testing Cadence & Scope		
Remediation & Sustainment		
Integration & Collaboration		
Overall Score (SUM ÷ 4)	*SUM:*	*AVG:*

Resulting ARMOR Level *(circle one)*

Level 1	Level 2	Level 3	Level 4	Level 5
Ad-Hoc	Repeatable	Managed	Optimized	Resilient
(1.0 – 1.4)	(1.5 – 2.0)	(2.1 – 2.4)	(2.5 – 2.8)	(2.9 – 3.0)

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

SECTION 1 – GOVERNANCE & STRATEGY

#	QUESTION	1	2	3
1	Does the organization have a documented risk-aligned offensive security strategy?	☐	☐	☐
2	Are roles and responsibilities for offensive security clearly defined across the organization?	☐	☐	☐
3	Is leadership regularly briefed on offensive security outcomes and risk implications?	☐	☐	☐
4	Are offensive security results used to inform policy, investment, or strategic decisions?	☐	☐	☐
5	Are threat intelligence and risk context incorporated into planning and prioritization?	☐	☐	☐

Section 1 Total: ____ **Section 1 Average (÷5):** ____

SECTION 2 – TESTING CADENCE & SCOPE

#	QUESTION	1	2	3
6	How consistently are penetration tests or security assessments performed?	☐	☐	☐
7	Does testing include cloud, SaaS, and third-party, and on-prem assets?	☐	☐	☐
8	Are red/purple team exercises conducted to measure detection and response capability?	☐	☐	☐
9	Are test scopes threat-informed (based on adversary behaviors or emerging risks)?	☐	☐	☐
10	Are tabletop exercises or crisis simulations conducted for critical systems and processes?	☐	☐	☐

Section 2 Total: ____ **Section 2 Average (÷5):** ____

SECTION 3 – REMEDIATION & SUSTAINMENT

#	QUESTION	1	2	3
11	Are findings triaged, prioritized, and tracked to resolution within defined SLAs?	☐	☐	☐
12	Is remediation validated through retesting or continuous validation processes?	☐	☐	☐
13	Are recurring or systemic findings analyzed for root causes and process improvement?	☐	☐	☐
14	Are sustainment metrics (e.g., remediation rate, mean time to validate) reviewed regularly?	☐	☐	☐
15	Are remediation and validation processes documented and reviewed for effectiveness?	☐	☐	☐

Section 3 Total: ____ **Section 3 Average (÷5):** ____

SECTION 4 – INTEGRATION & COLLABORATION

#	QUESTION	1	2	3
16	Are offensive security results communicated to defensive and operations teams?	☐	☐	☐
17	Are red/purple team insights used to improve detection and response capabilities?	☐	☐	☐
18	Do business units understand and act on relevant offensive security outcomes?	☐	☐	☐
19	Are results integrated with enterprise risk management reporting and dashboards?	☐	☐	☐
20	Are cross-functional reviews or after-action reports conducted following exercises?	☐	☐	☐

Section 4 Total: ____ **Section 4 Average (÷5):** ____

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

APPENDIX C - SELF-ASSESSMENT SIMULATION DATA

To validate the scoring structure and assess the natural distribution of maturity levels, a simulation of 1,000 organizations was conducted using the ARMOR self-assessment model. The simulation used realistic organizational profiles across four market segments (SMB, Mid-Market, Enterprise, and Large Enterprise) representing typical employee counts, IT/security staffing, and operational complexity.

Each simulated organization answered 20 representative questions covering governance, testing cadence, remediation, and integration. Scores ranged from 1 to 3 per question, and overall averages were mapped to the five ARMOR maturity levels. The simulation incorporated weighted sampling that mirrors the real-world distribution of company sizes in the United States, excluding very small organizations (< 200 employees) that typically fall outside ARMOR's intended audience.

OBJECTIVES

- Validate the scoring bands and ensure consistent mapping to ARMOR levels
- Assess expected maturity distributions by segment
- Confirm that the model scales predictably across organizational sizes

METHODOLOGY

Randomized scores were generated following a bell-curve distribution tuned for each segment's expected maturity and variance. The resulting dataset contains 1,000 simulated cases, summarized by both count and percentage. Confidence intervals were calculated for each segment and level.

> ***Confidence Note:*** *95 percent confidence intervals were within ±3.0 percent for all major levels, confirming representativeness of the 1,000-organization sample.*

The following tables and figures summarize the simulated results by segment and level.

INTERPRETATION

The results align closely with expected real-world trends. SMBs primarily cluster around Levels 1 and 2, where practices are emerging or repeatable but not yet strategic. Mid-Market organizations show stronger representation at Level 3, reflecting the development of managed programs and early strategic alignment. Enterprise and Large Enterprise organizations demonstrate a more even spread between Levels 3 and 4, with a small but significant proportion beginning to achieve Level 5 characteristics.

Overall, the distribution reinforces the model's intent: higher maturity requires deliberate investment, integrated governance, and sustained operational execution. Progression between levels is incremental and realistic, with the model exhibiting logical scalability across organizational types and sizes.

DATA AVAILABILITY

The full 1,000-organization simulation dataset and summary tables used in Appendix C are available at www.armormodel.org

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.

SIMULATION RESULTS

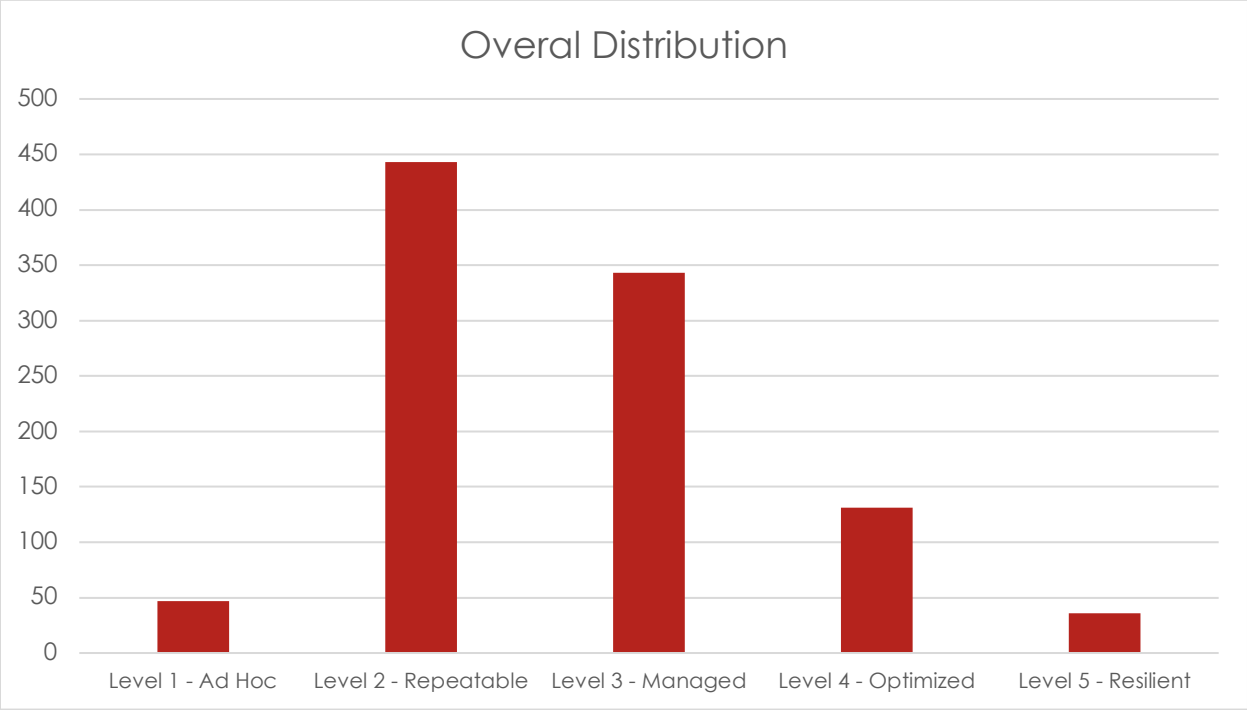

Figure C - 1: Overall Self-Assessment Distribution

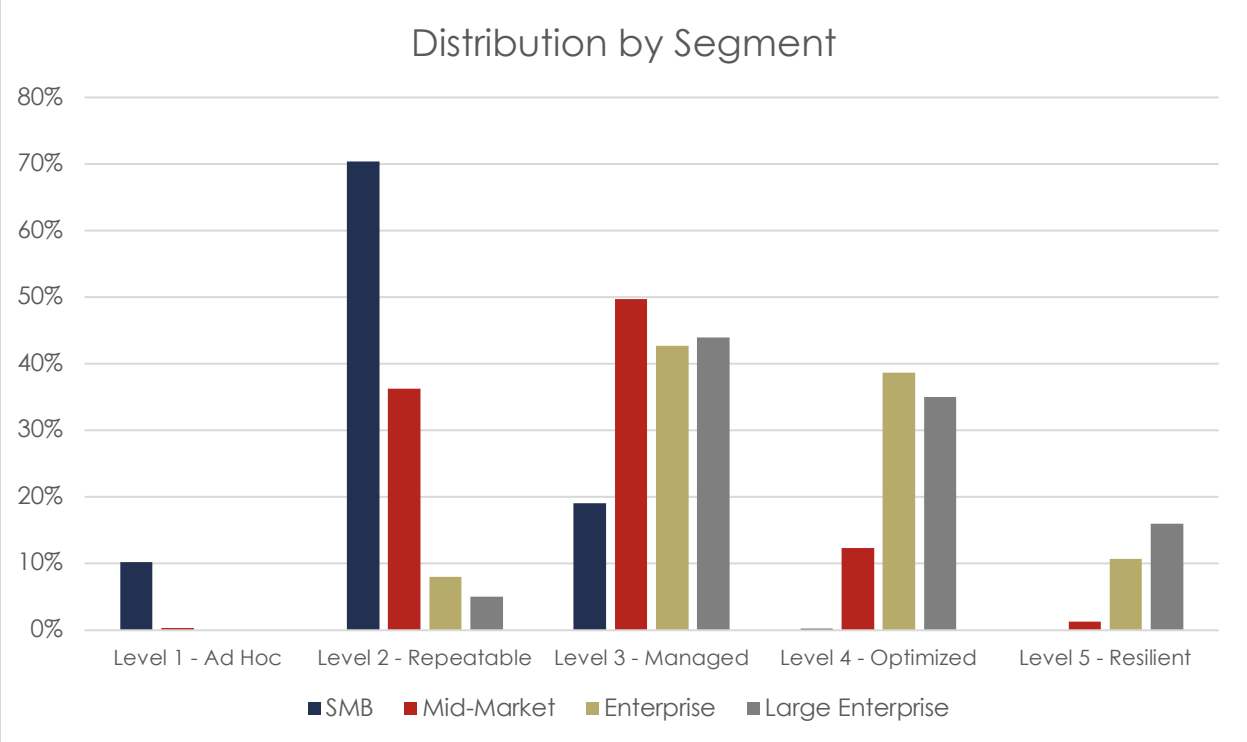

Figure C - 2: Self-Assessment Distribution by Segment

© 2025 Greg Anderson. Published at www.armormodel.org. Licensed under CC BY-NC-SA 4.0.