SYNOPSYS®

www.synopsys.com |

Maturity Action Plan
(MAP)

Clear directions for establishing or maturing your software security program

Our Maturity Action Plan (MAP) is a strategic solution that helps organizations build a detailed plan and roadmap with a prioritized list of recommendations to enhance your software security program.

Build, evolve, and maintain your software security initiative

While a current-state measurement, such as the Building Security In Maturity Model (BSIMM) shows you what you're doing. MAP helps you set objectives, outline a strategy to get from where you are today to your objectives, and clarify the resources you'll need. We work closely with your key stakeholders to understand your organization's current state, define an achievable future state, and develop a MAP to advance your software security initiative. The plan covers three SSI execution capability groups:

1. People

Equip staff with knowledge and information to specify, create, and operate secure software. Three of the most common capabilities:

- **Satellite** ensures that a knowledgeable group of software security practitioners are adequately distributed across all your development teams.
- **Competency Management** provides all software stakeholders with sufficient skills to execute the evolving tasks associated with their role.
- **Attack Intelligence** brings relevant and timely information about attacker actions, security defects, and mitigation techniques into your firm and transforms it into actionable guidance.

2. Process

Identify and characterize the organization's software assets and define how and when to engage with each development and acquisition activity. Six of the most common process capabilities:

- **Software Development Life Cycle (SDLC)** Gates to ensure people and tools are including or applying the appropriate software security controls in each software project.
- **Open Source Management** assures that all open source software used in the firm's portfolio is known, tracked, maintained, tested, and used in accordance with SSI policies and standards.
- **Risk and Compliance** enable subject matter experts to periodically determine the risk posture and compliance status of all software in the SSI's purview.
- **Policy and Standards** assure appropriate roles maintain complete and current documentation on mandatory actions, events, and characteristics applicable to all the people, process, and technology in the SSI and its application portfolio.
- **Metrics** ensure all SSI processes are appropriately instrumented, that measurement data become valuable metrics, and metrics are distributed to everyone who requires them for decision-making.

- **Vendor Management** to prevent third-party acquired software unacceptably increasing the firm's software security risk and ensure clear assignment of software security responsibility.

3. Verification

Utilize traditional software security activities to verify your software security program. Four of the most common verification techniques include:

- **Penetration Testing** finds exploitable defects through manual and automated white box and black box testing.
- **Architecture and Design Review** uncovers exploitable defects in software architecture through manual white box analysis.
- **Secure Code Review** identifies exploitable defects through manual code review and automated static analysis.
- **Quality Assurance** finds functional defects and exploitable defects through manual and automated testing.

Once your MAP is developed, we can help you socialize it to get the buy-in, resources, and support you need to implement it.

Sized to fit

Take advantage of our 20+ years of experience implementing successful software security initiatives. Once your MAP is developed, we can help you socialize it to get the buy-in, resources, and support you need to implement it. Find out which MAP solution best fits your organization's needs:

	MAP - Standard	MAP - Comprehensive
Current State Measurement	Capability maturity 20 capabilities @ 4 levels each	BSIMM 113 activities @ 2 levels each
Roadmap Period	24 months	24 months
Capabilities Planned	8-12	3-6
Milestones per Capability	3	5-15
Deliverable Format	Executive PowerPoint with current state and roadmap views	Report including spider charts, BSIMM, scorecards, and comparisons

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com