(SAM)M v Korporaciq

Building Security Maturity with OWASP SAMM

George Ribarski

Product Security Engineer
𝕏 @lenny_z

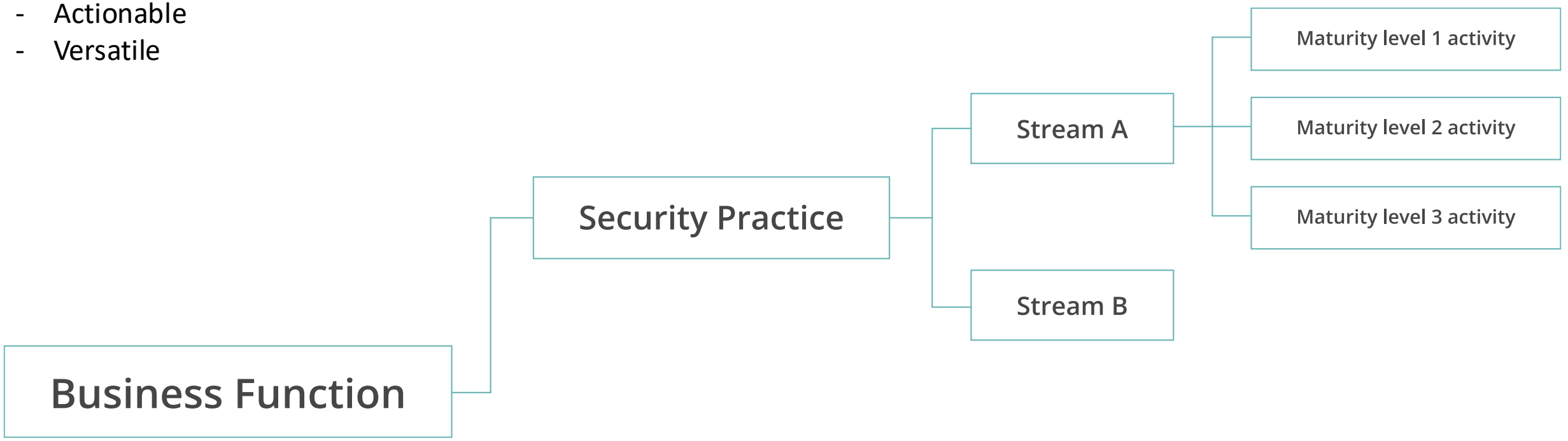
Agenda

01	What’s SAMM
02	Who SAMM
03	How SAMM
04	Why SAMM

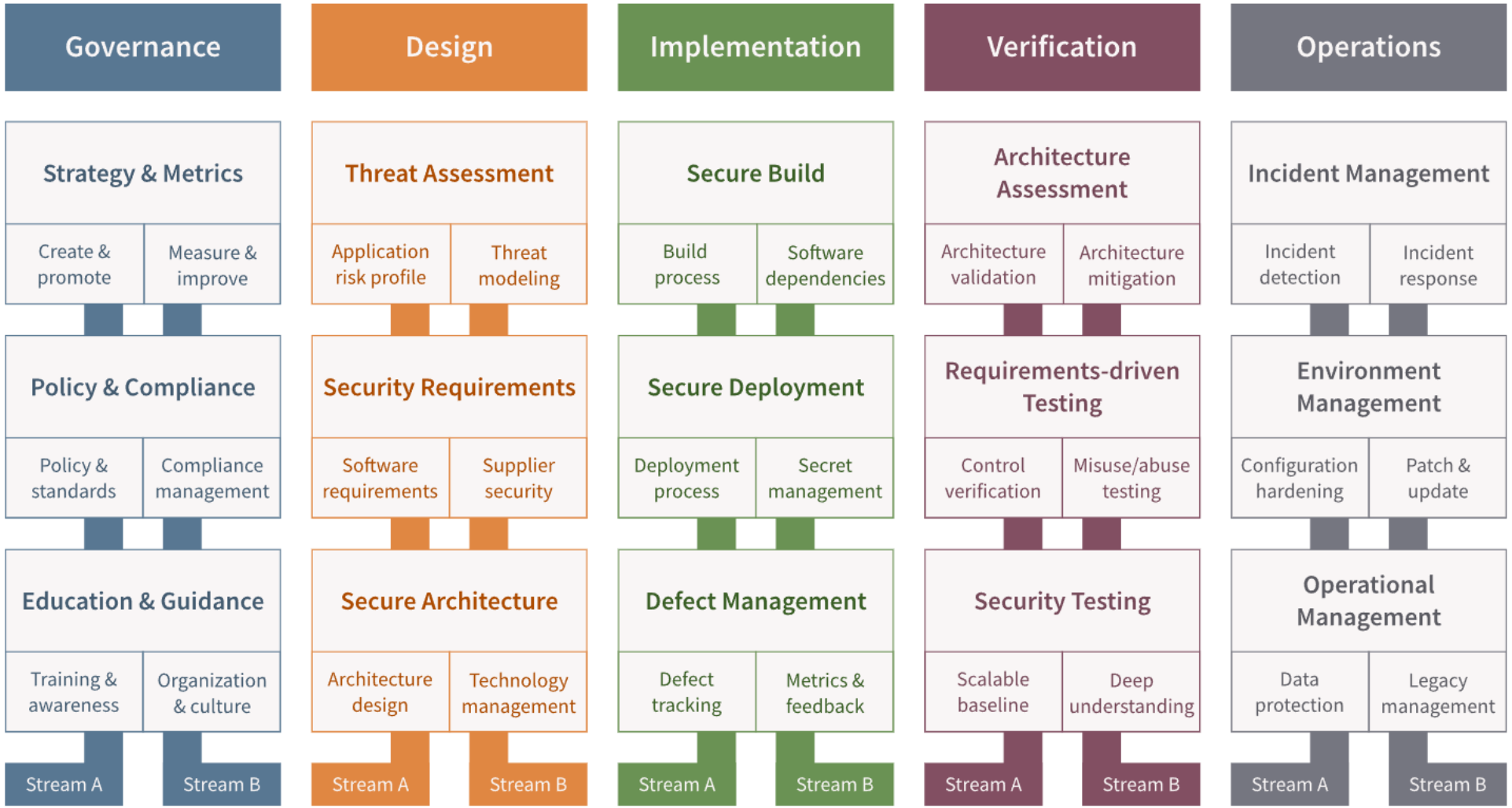
What’s SAMM

A mission is to provide an effective and measurable way for all types of organizations to analyze and improve their software security posture.

- Measurable
- Actionable
- Versatile

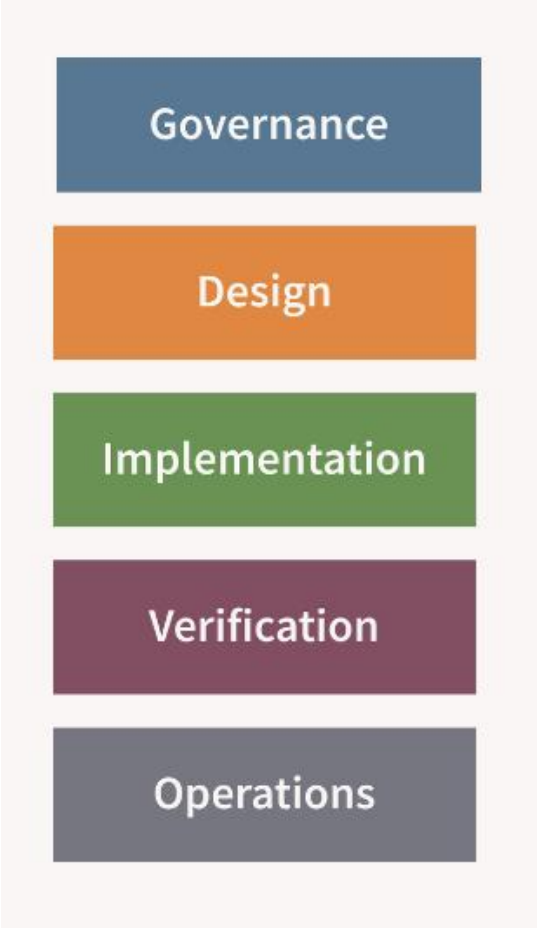


What's SAMM


Governance
Strategy & Metrics
Create & promote
Measure & improve
Policy & Compliance
Policy & standards
Compliance management
Education & Guidance
Training & awareness
Organization & culture
Stream A
Stream B
Design
Threat Assessment
Application risk profile
Threat modeling
Security Requirements
Software requirements
Supplier security
Secure Architecture
Architecture design
Technology management
Stream A
Stream B
Implementation
Secure Build
Build process
Software dependencies
Secure Deployment
Deployment process
Secret management
Defect Management
Defect tracking
Metrics & feedback
Stream A
Stream B
Verification
Architecture Assessment
Architecture validation
Architecture mitigation
Requirements-driven Testing
Control verification
Misuse/abuse testing
Security Testing
Scalable baseline
Deep understanding
Stream A
Stream B
Operations
Incident Management
Incident detection
Incident response
Environment Management
Configuration hardening
Patch & update
Operational Management
Data protection
Legacy management
Stream A
Stream B

What’s SAMM (Business Functions)

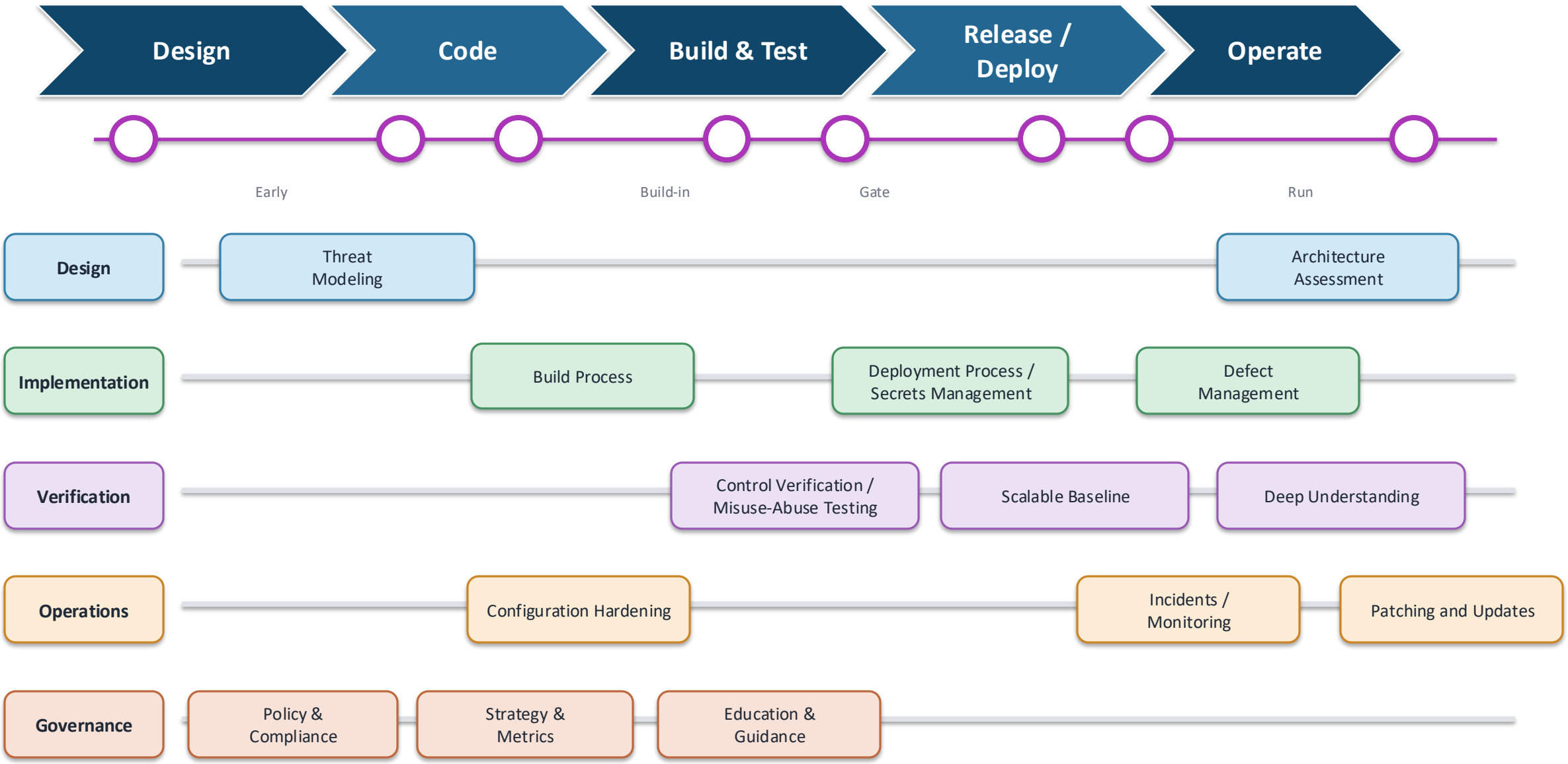
- Start with the core activities tied to any organization performing software development
- Named generically, but should resonate with any development stakeholder



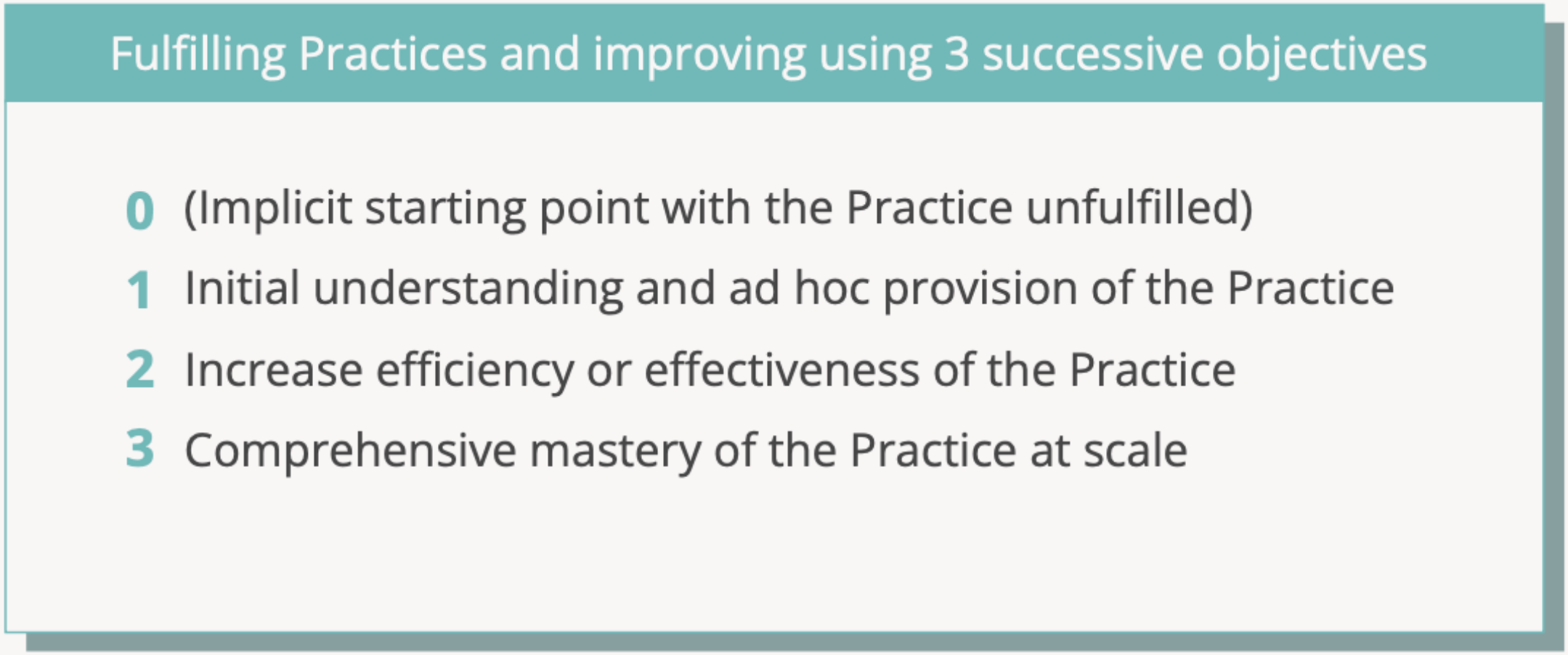
What’s SAMM (Security Practices)

- 3 Security Practices for each Business Function
- They cover key areas relevant to software security assurance
- Each one is a silo for improvement

What’s SAMM (SLDC Mapping)



What’s SAMM (Maturity Levels)



What’s SAMM (Assessment)

What is the SAMM Assessment?

- Evaluates the current software security posture against SAMM’s 15 practices
- Measures maturity levels (0–3) across each practice using quality criteria
- Identifies gaps and provides a baseline for building a targeted improvement roadmap

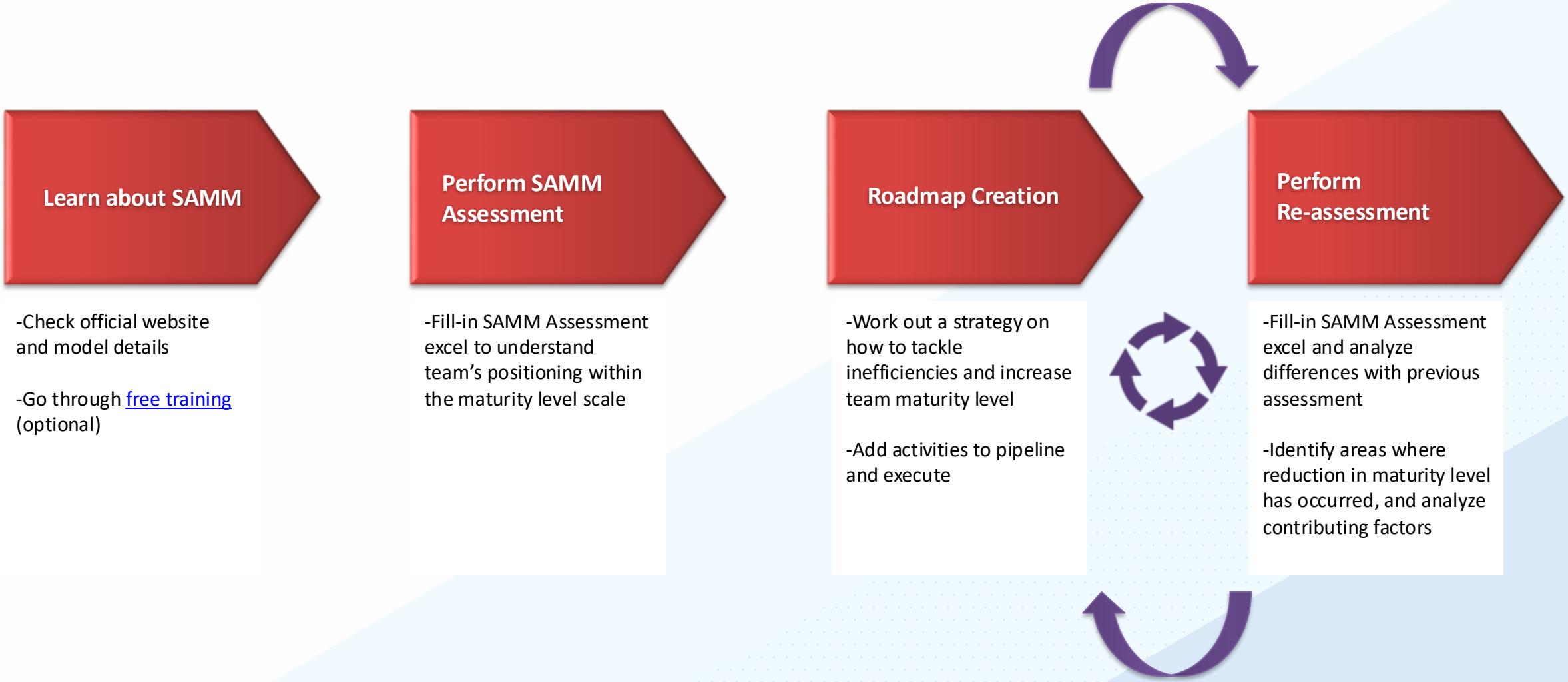
How We Do It

- **Interview-style sessions** with each product team (2–3 senior engineers)
- **Core team** facilitates and scores each session
- We walk through SAMM questions on screen, discuss evidence, and score together

Tools

- **OWASP SAMM Toolbox (XLSX):** Excel/Google Sheets spreadsheet with all questions, scoring, and auto-generated scorecards
- **SAMMY by Codific (online):** Web-based platform for assessments, SMART improvement plans, progress dashboards, and multi-team tracking

Progress SAMM Adoption Process



SAMM Who

- **Founded:** 1981 | Headquartered in Burlington, Massachusetts
- **Employees:** ~3000 across 16+ countries
- **Mission:** Trusted provider of AI-powered digital experience and infrastructure software

- **Application Development:** Telerik, Kendo UI, Sitefinity CMS
- **DevOps & Automation:** Chef, WhatsUp Gold
- **Data Connectivity:** DataDirect, Corticon
- **Network & Security:** Flowmon, LoadMaster
- **Secure File Transfer:** MOVEit, WS_FTP
- **AI & Innovation:** Progress Agentic RAG, AI-powered capabilities across the portfolio
- **Database & App Platform:** OpenEdge

- 30+ Solutions with 100+ Applications
- Tech Stack
  - C/C++,.NET, Java, JavaScript/TypeScript, Python, Rust, Ruby, Go … many others
  - AWS, Azure, GCP
  - OnPrem and SaaS product lines
  - ~ 100M LoC

How SAMM (Where We Struggled)

Honest lessons from the road — the challenges that tested our program and what we learned

Competing Priorities

Constant tension between features and security optimizations. Business priorities often pushed SAMM improvements down the backlog. Winning time on the roadmap required repeated justification.

Engagement & Mindset

Some teams misunderstood the purpose and saw security as a blocker, not an enabler. Overcoming the “security slows us down” mentality required persistent education and framing.

Communication Gaps

Top-down communication isn’t perfect. Despite C-level sponsorship, some teams simply didn’t know about the program or their role in it. Messages got lost in the cascade.

Legacy Products

How do you assess products that are 40 years old? Legacy codebases don’t map cleanly to modern maturity frameworks. We had to adapt scoring and expectations for a different era of software.

How SAMM (Why We're Successful)

Five pillars that turned our SAMM initiative from a checkbox exercise into a lasting cultural shift

Top-Down Approach

Company-wide OKR with C-level sponsorship. Leadership didn't just approve it — they championed it.

Program, Not a Project

Communicated as a continuous program, not a one-time project. It never ends — security maturity is a journey.

Trust, Not Compliance

No evidence gathered. This isn't an audit — it's a self-assessment built on trust and honest conversation.

Gamification

Teams competed against each other. Winners were publicly praised and celebrated — turning security into a source of pride.

Centralized Support

Detailed documentation, guidelines, trainings, communities, ongoing engagement, and regular reminders.

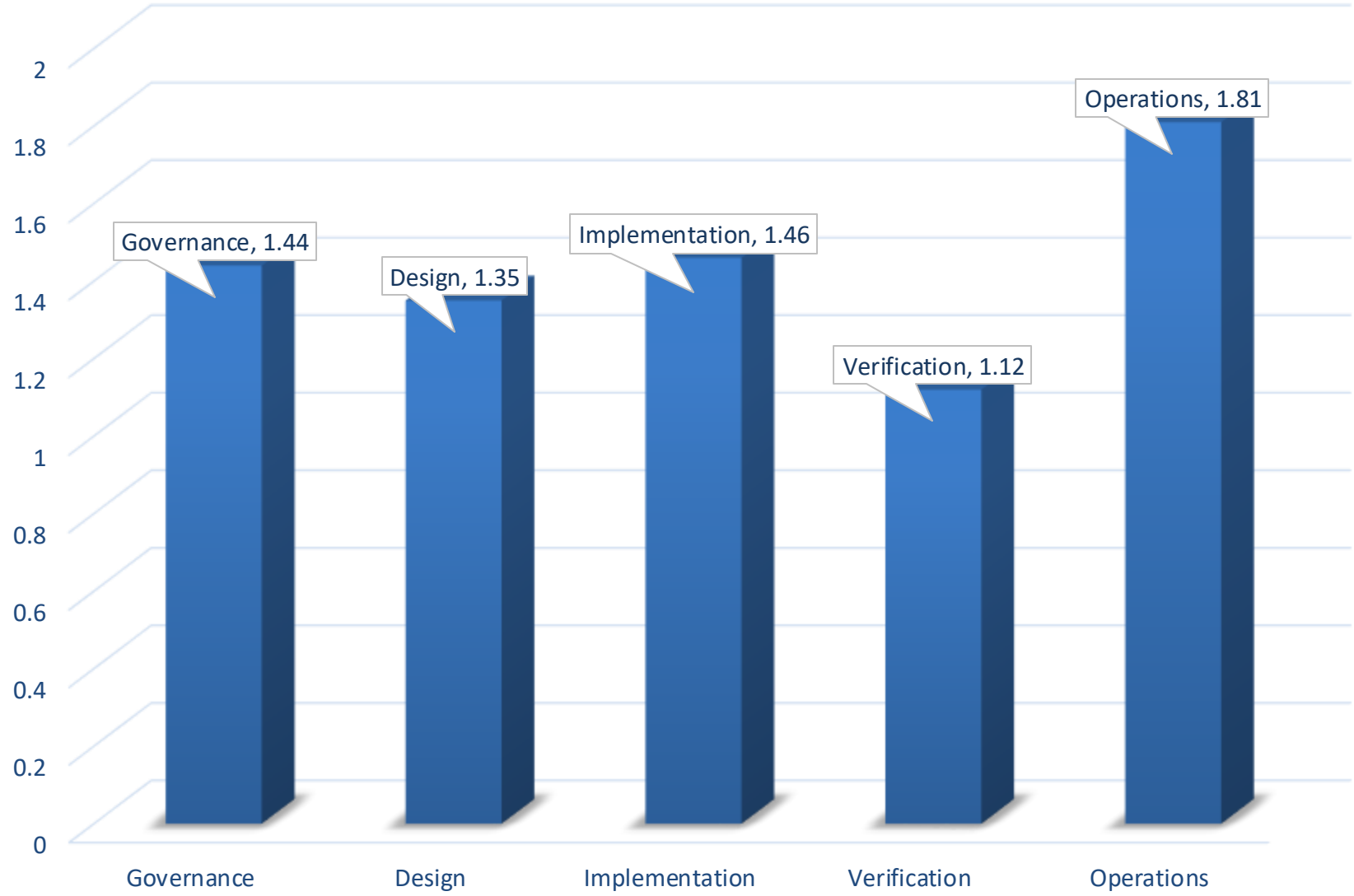
How SAMM (OWASP SAMM Global Benchmark)

Average maturity scores across 30 organizations worldwide — scale of 0 to 3

Benchmark

1.448

SAMM Benchmark Analysis v1.2 (DC 2025)



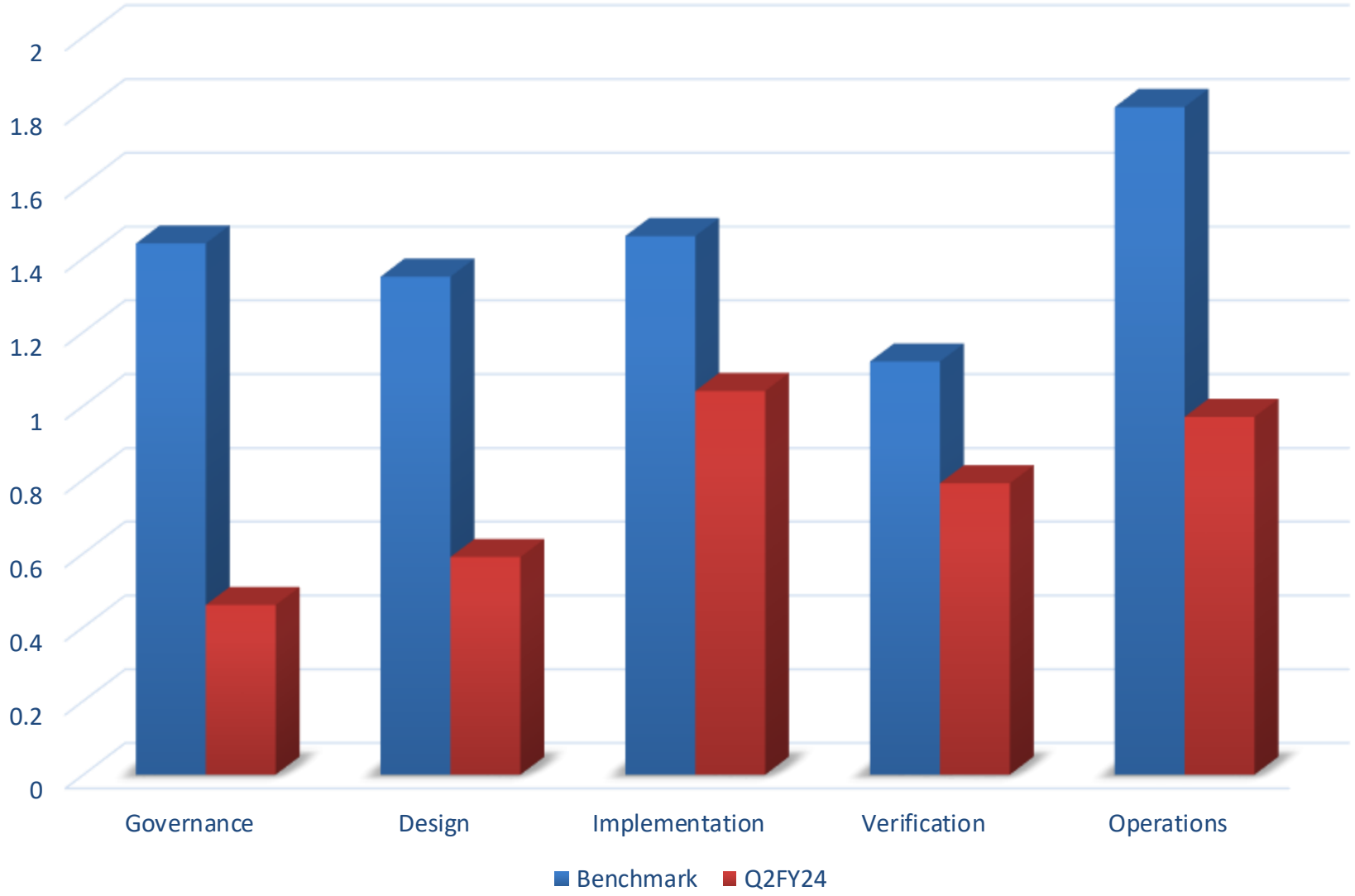
How SAMM (OWASP SAMM Global Benchmark)

Average maturity scores across 30 organizations worldwide — scale of 0 to 3

BEFORE • Q2 FY24

0.94

First baseline assessment across 30 teams. Early-stage practices with limited consistency.



Why SAMM

From first baseline to measurable security maturity — a 119% improvement

BEFORE • Q2 FY24

0.94

First baseline assessment across 30 teams. Early-stage practices with limited consistency.

NOW • Q2 FY26

2.06

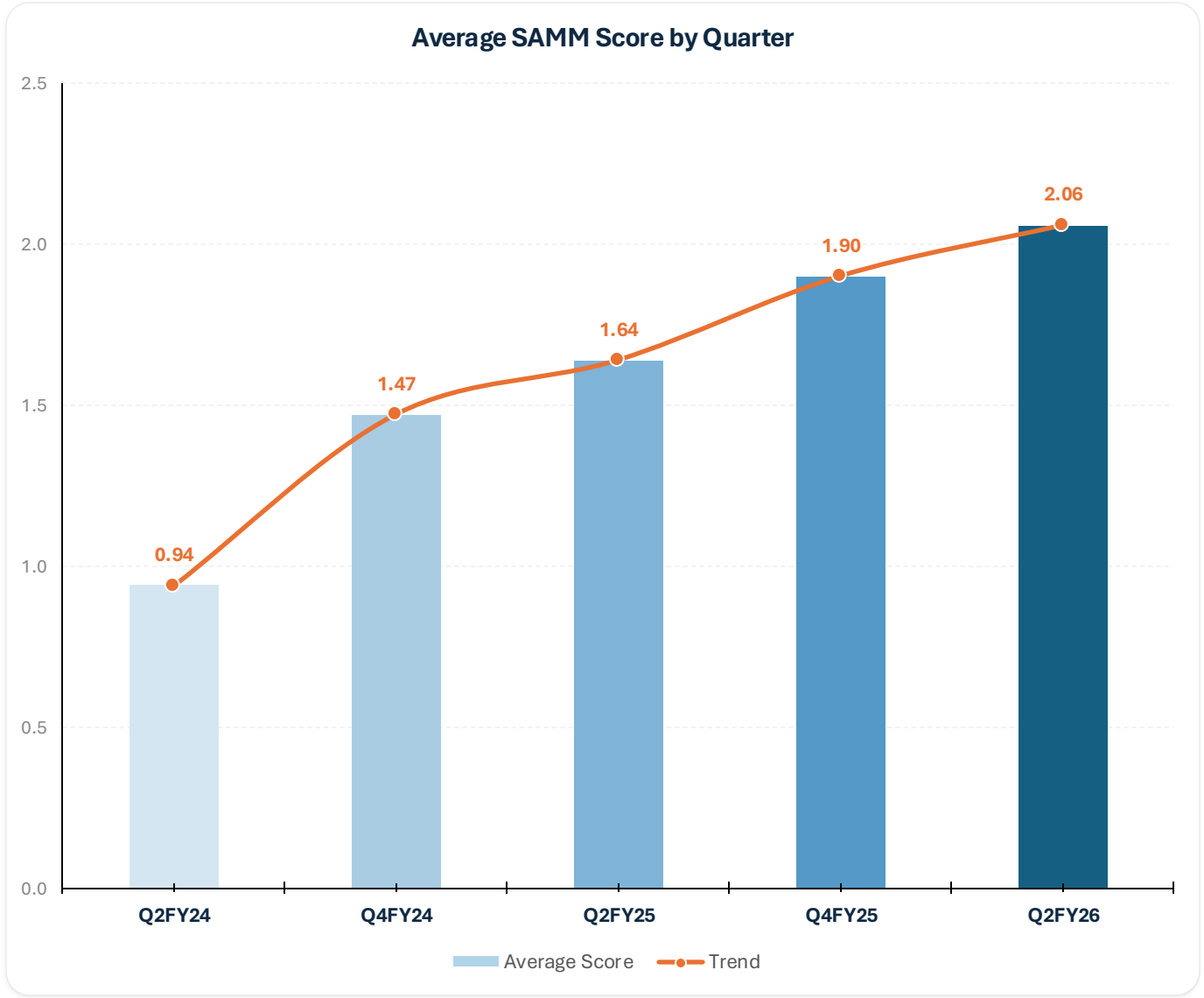
Mature, repeatable practices embedded across the organization with structured improvement plans.

What Changed

- Expanded from **30 to 36 teams** assessed, proving scalability
- Consistent quarter-over-quarter score growth across every assessment cycle
- Crossed the **2.0 maturity threshold** — moving from ad-hoc to repeatable
- Biggest jump in the first year (+0.53), sustaining momentum since

What It Means

- Security practices are now **documented, measured, and improving** rather than ad-hoc
- Teams own their security posture with clear roadmaps to Level 3
- The program is delivering **compounding returns** on security investment



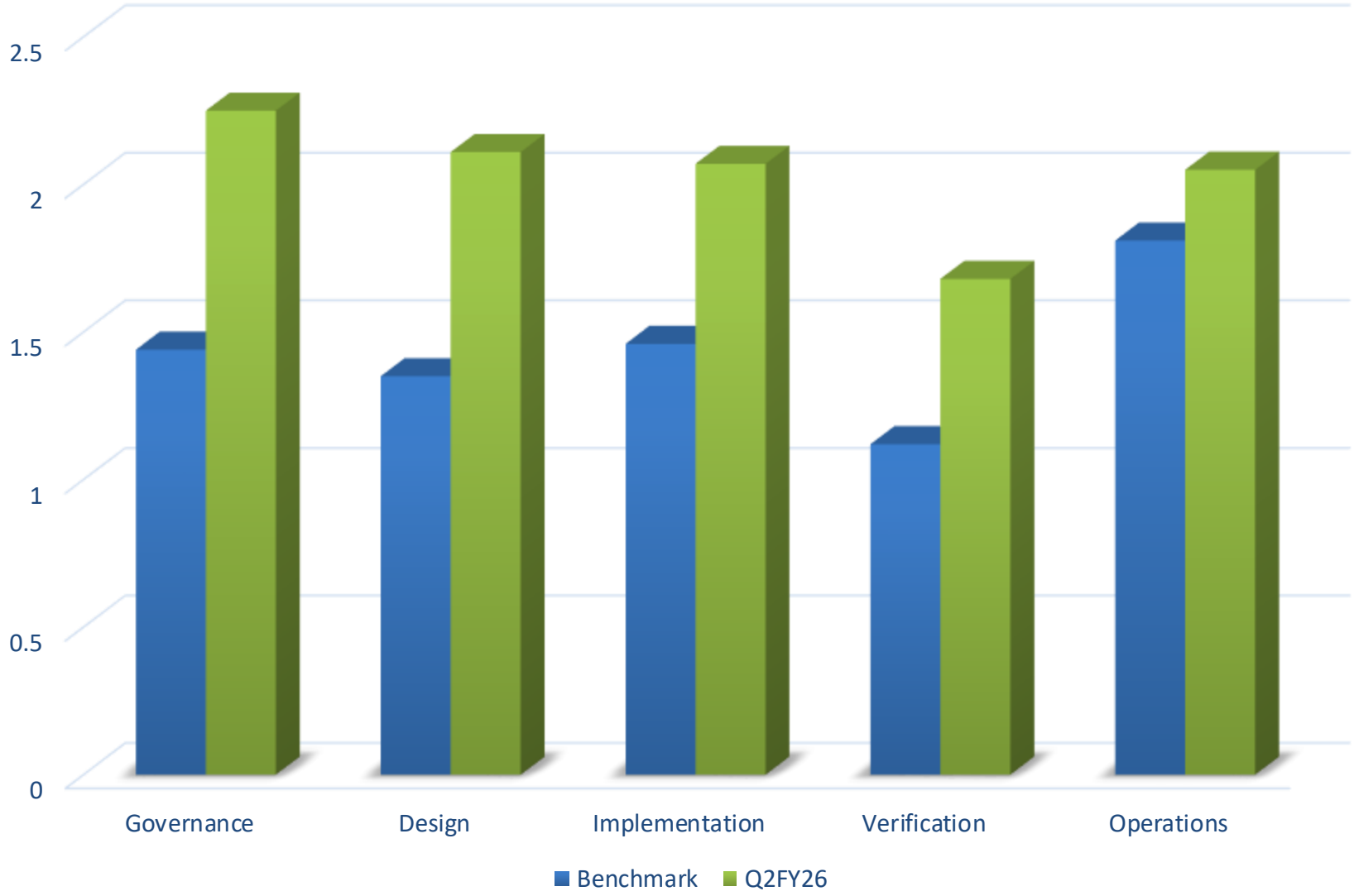
Why SAMM (OWASP SAMM Global Benchmark)

Average maturity scores across 30 organizations worldwide — scale of 0 to 3

NOW • Q2 FY26

2.06

Mature, repeatable practices embedded across the organization with structured improvement plans.



Why SAMM (Lessons Learned)

Key takeaways from running the SAMM program — what the journey has taught us so far

Productivity & ROI

~20% initial capacity investment, but teams report increased productivity, visibility, and confidence when presenting security practices to clients.

Faster Response Times

SAMM ≠ no vulnerabilities. Findings still exist, but SLO/SLA resolution times dropped up to 40% because teams are better prepared.

Community & Collaboration

The program drives teams and individuals into security community channels and workshops, boosting cross-team and cross-BU collaboration.

AI & Automation

AI-driven automation turned SAMM practices into pipeline steps — shortening delivery time while meeting security requirements, especially for on-prem products.

Compliance Enablement

Not marketed as compliance, but SAMM assessments help teams provide evidence and answers to GRC for SOC, ISO, PCI, and more.

Q & A