Table of Contents

Overview 1

What is OWASP SAMM? 1

The OWASP SAMM Model 1

OWASP SAMM structure 1

Overview of Business Functions 2

Governance 2

Design 2

Implementation 2

Verification 2

Operations 2

Overview of the Security Practices 3

Governance 3

Strategy & Metrics 3

Streams 3

Policy & Compliance 3

Streams 3

Education & Guidance 3

Streams 4

Design 4

Threat Assessment 4

Streams 4

Security Requirements 4

Streams 4

Security Architecture 4

Streams 5

Implementation 5

Secure Build 5

Streams 5

Secure Deployment 5

Streams 5

Defect Management 5

Streams 6

Verification 6

Architecture Assessment 6

Streams 6

Requirements-driven Testing 6

Streams 6

Security Testing 7

Streams 7

Operations 7

Incident Management 7

Streams 7

Environment Management 8

Streams 8

Operational Management 8

Streams 8

Overview of Security Activities 8

Governance 8

Strategy & Metrics (SM1) 8

Activities 9

[Stream A] Identify the organization’s risk appetite 9

[Stream B] Define basic security metrics 9

Strategy & Metrics (SM2) 10

Activities 10

[Stream A] Define the security strategy 10

[Stream B] Set strategic KPIs 11

Strategy & Metrics (SM3) 11

Activities 11

[Stream A] Align security and business strategies 11

[Stream B] Drive the security program through metrics 12

Policy & Compliance (PC1) 12

Activities 12

[Stream A] Define policies and standards 12

[Stream B] Identify compliance requirements 13

Policy & Compliance (PC2) 14

Activities 14

[Stream A] Develop test procedures 14

[Stream B] Standardize policy and compliance requirements 14

Policy & Compliance (PC3) 15

Activities 15

[Stream A] Measure compliance to policies and standards 15

[Stream B] Measure compliance to external requirements 15

Education & Guidance (EG1) 16

Activities 16

[Stream A] Train all stakeholders for awareness 16

[Stream B] Identify security champions 17

Education & Guidance (EG2) 17

Activities 17

[Stream A] Customize security training 17

[Stream B] Implement centers of excellence 18

Education & Guidance (EG3) 19

Activities 19

[Stream A] Standardize security guidance 19

[Stream B] Establish a security community 19

Design 20
Threat Assessment (TA1) 20
Activities 20
[Stream A] Perform application risk assessments 20
[Stream B] Perform basic threat modeling 21
Threat Assessment (TA2) 21
Activities 21
[Stream A] Inventorize risk profiles 21
[Stream B] Standardize and scale threat modeling 22
Threat Assessment (TA3) 22
Activities 23
[Stream A] Periodic review of risk profiles 23
[Stream B] Optimize threat modeling 23
Security Requirements (SR1) 24
Activities 24
[Stream A] Identify security requirements 24
[Stream B] Perform vendor assessments 24
Security Requirements (SR2) 25
Activities 25
[Stream A] Standardize and integrate security requirements 25
[Stream B] Discuss security responsabilities with suppliers 25
Security Requirements (SR3) 26
Activities 26
[Stream A] Develop a security requirements framework 26
[Stream B] Align security methodology with suppliers 26
Security Architecture (SA1) 27
Activities 27
[Stream A] Adhere to basic security principles 27
[Stream B] Identify tools and technologies 27
Security Architecture (SA2) 28
Activities 28
[Stream A] Provide preferred security solutions 28
[Stream B] Promote preferred tools and technologies 29
Security Architecture (SA3) 29
Activities 29
[Stream A] Build reference architectures 29
[Stream B] Enforce the use of recommended technologies 30
Implementation 30
Secure Build (SB1) 30
Activities 30
[Stream A] Define a consistent build process 30
[Stream B] Identify application dependencies 31
Secure Build (SB2) 31
Activities 31
[Stream A] Automate the build process 31
[Stream B] Review application dependencies for security 32
Secure Build (SB3) 33
Activities 33
[Stream A] Enforce a security baseline during build 33
[Stream B] Test application dependencies 33
Secure Deployment (SD1) 34
Activities 34
[Stream A] Use a repeatable deployment process 34
[Stream B] Protect application secrets in configuration and code 34
Secure Deployment (SD2) 35
Activities 35
[Stream A] Automate deployment and integrate security checks 35
[Stream B] Include application secrets during deployment 35
Secure Deployment (SD3) 36
Activities 36
[Stream A] Verify the integrity of deployment artifacts 36
[Stream B] Enforce lifecycle management of application secrets 36
Defect Management (DM1) 37
Activities 37
[Stream A] Track security defects centrally 37
[Stream B] Define basic defect metrics 38
Defect Management (DM2) 38
Activities 38
[Stream A] Rate and track security defects 38
[Stream B] Define advanced defect metrics 39
Defect Management (DM3) 39
Activities 39
[Stream A] Enforce an SLA for defect management 39
[Stream B] Use metrics to improve the security strategy 40
Verification 40
Architecture Assessment (AA1) 40
Activities 40
[Stream A] Assess application architecture 40
[Stream B] Evaluate architecture for typical threats 41
Architecture Assessment (AA2) 41
Activities 41
[Stream A] Verify the application architecture for security methodically 41
[Stream B] Structurally verify the architecture for identified threats 42
Architecture Assessment (AA3) 42
Activities 42
[Stream A] Verify the effectiveness of security components 42
[Stream B] Feed review results back to improve reference architectures 43
Requirements-driven Testing (RT1) 43
Activities 43
[Stream A] Test the effectiveness of security controls 43
[Stream B] Perform fuzz testing 44
Requirements-driven Testing (RT2) 44
Activities 44
[Stream A] Define and run security test cases from requirements 44
[Stream B] Define and run security abuse cases from requirements 45
Requirements-driven Testing (RT3) 45
Activities 45
[Stream A] Automate security requirements testing 45
[Stream B] Perform security stress testing 46
Security Testing (ST1) 46
Activities 47
[Stream A] Perform automated security testing 47
[Stream B] Test high risk application components manually 47

Security Testing (ST2) 48
Activities 48
[Stream A] Develop application-specific security test cases 48
[Stream B] Establish a penetration testing process 49
Security Testing (ST3) 49
Activities 49
[Stream A] Integrate security testing tools in the delivery pipeline 49
[Stream B] Establish continuous, scalable security verification 50
Operations 50
Incident Management (IM1) 50
Activities 51
[Stream A] Use best-effort incident detection 51
[Stream B] Create an incident response plan 51
Incident Management (IM2) 51
Activities 52
[Stream A] Define an incident detection process 52
[Stream B] Define and incident response process 52
Incident Management (IM3) 53
Activities 53
[Stream A] Improve the incident detection process 53
[Stream B] Establish an incident response team 53
Environment Management (EM1) 54
Activities 54
[Stream A] Use best-effort hardening 54
[Stream B] Practice best-effort patching 54
Environment Management (EM2) 55
Activities 55
[Stream A] Establish hardening baselines 55
[Stream B] Formalize patch management 55
Environment Management (EM3) 56
Activities 56
[Stream A] Perform continuous configuration monitoring 56
[Stream B] Enforce timely patch management 56
Operational Management (OM1) 57
Activities 57
[Stream A] Organize basic data protections 57
[Stream B] Identify unused applications 57
Operational Management (OM2) 58
Activities 58
[Stream A] Establish a data catalog 58
[Stream B] Formalize decommissioning process 58
Operational Management (OM3) 59
Activities 59
[Stream A] Respond to data breaches 59
[Stream B] Review application lifecycle state regularly 59
Credits 60
Sponsors 60
Proceeds 61
Sponsorship levels 61
Sponsorship benefits 61
Join as a sponsor 61
License 61