Managing Web & Application Security with OWASP – bringing it all together

Tobias Gondrom
(OWASP Project Leader)

OWASP
The Open Web Application Security Project

OWASP

The Open Web Application Security Project

http://www.owasp.org

OWASP is a worldwide free and open community focused on improving the security of application software.

Our mission is to make application security visible so that people and organizations can make informed decisions about application security risks.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

Tobias Gondrom

OWASP

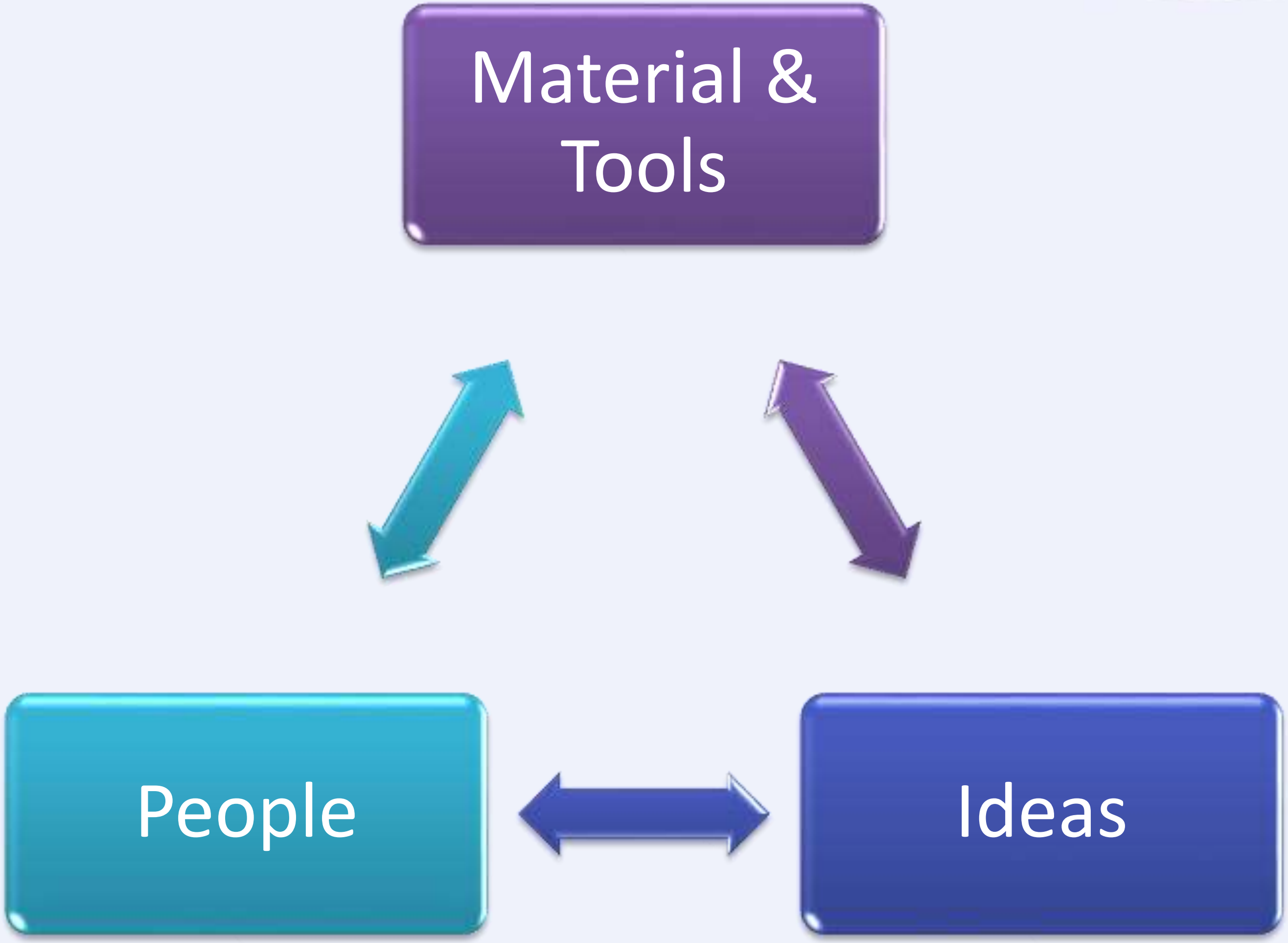
The Open Web Application Security Project

- 15 years information security experience
  (Global Head of Security, CISO, CTO)
  CISSP, CSSLP, CCISO
- 12 years management of application development experience
- Sloan Fellow M.Sc. In Leadership and Strategy, London Business School
- Thames Stanley: Managing Director,
  CISO Advisory, Information Security & Risk Management, Research and Advisory
- Author of Internet Standards on Secure Archiving, CISO training and co-author of the OWASP CISO guide
- Chair of IETF Web Security Working Group
  http://datatracker.ietf.org/wg/websec/charter/
  Member of the IETF Security Directorate
- Cloud Security Alliance, Hong Kong chapter board member
- OWASP Project Leader for the CISO Survey
  member of OWASP London, previous chapter lead of OWASP Germany, previous chair of the OWASP Global Industry Committee, www.owasp.org

- What was in it for me.
- What’s in it for you.
- How you can bring it all together.

How OWASP can help you

OWASP
The Open Web Application Security Project



But which of the currently 148 active projects is good and can help me solve my problems?

OWASP

The Open Web Application Security Project

http://www.owasp.org

OWASP Flagship Projects

OWASP
The Open Web Application Security Project

AntiSamy Project

openSAMM - Software Assurance Maturity Model

ModSecurity Core Rule Set Project

CSRFGuard Project

Code Review Guide

WebGoat Project

OWASP Top Ten

Web Testing Environment Project

Secure Coding Practices - Quick Reference Guide

ZAP - Zed Attack Proxy

ASVS - Application Security Verification Standard

Development Guide Project

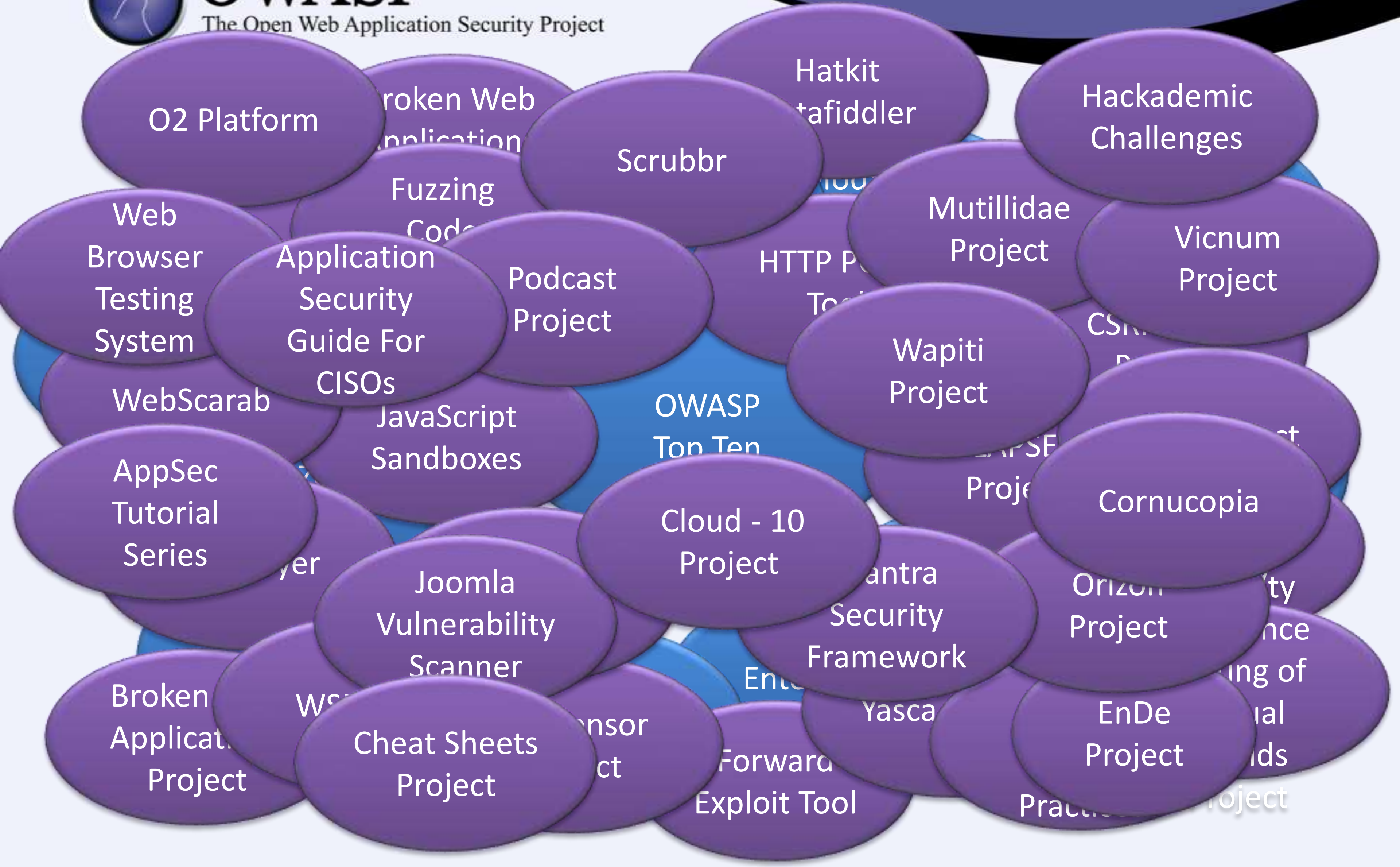
ESAPI Enterprise Security API

Testing Guide

Codes of Conduct

OWASP Labs Projects and more

OWASP
The Open Web Application Security Project



Hatkit
tafiddler

Hackademic Challenges

O2 Platform

roken Web
pplication

Scrubbr

Fuzzing
Cod

Web Browser Testing System

Application Security Guide For CISOs

Podcast Project

HTTP P
To

Mutillidae Project

Vicnum Project

CSR

Wapiti Project

WebScarab

JavaScript Sandboxes

OWASP Top Ten

APSE
Proje

ct

Cornucopia

AppSec Tutorial Series

yer

Cloud - 10 Project

Joomla Vulnerability Scanner

antra Security Framework

Orizon Project

ty
nce
ing of
ual
ds
oject

Broken Applicat Project

WS

nsor
ct

Cheat Sheets Project

Ent

Yasca

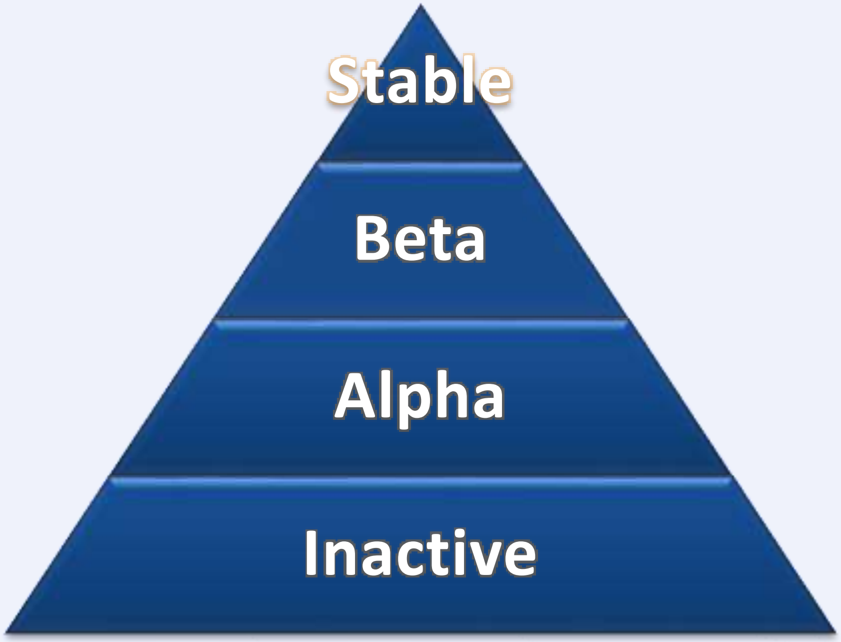
Forward Exploit Tool

EnDe Project

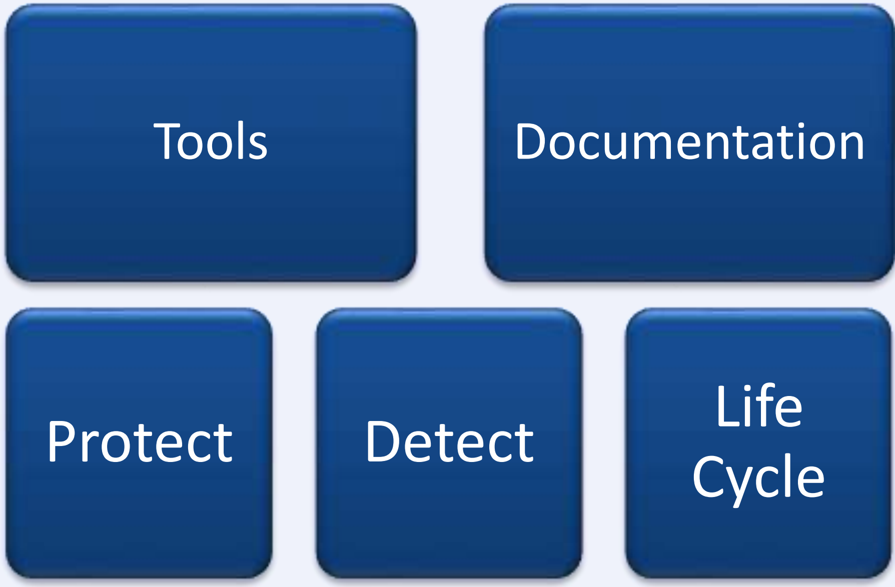
Practi

OWASP - Projects

- Project Status



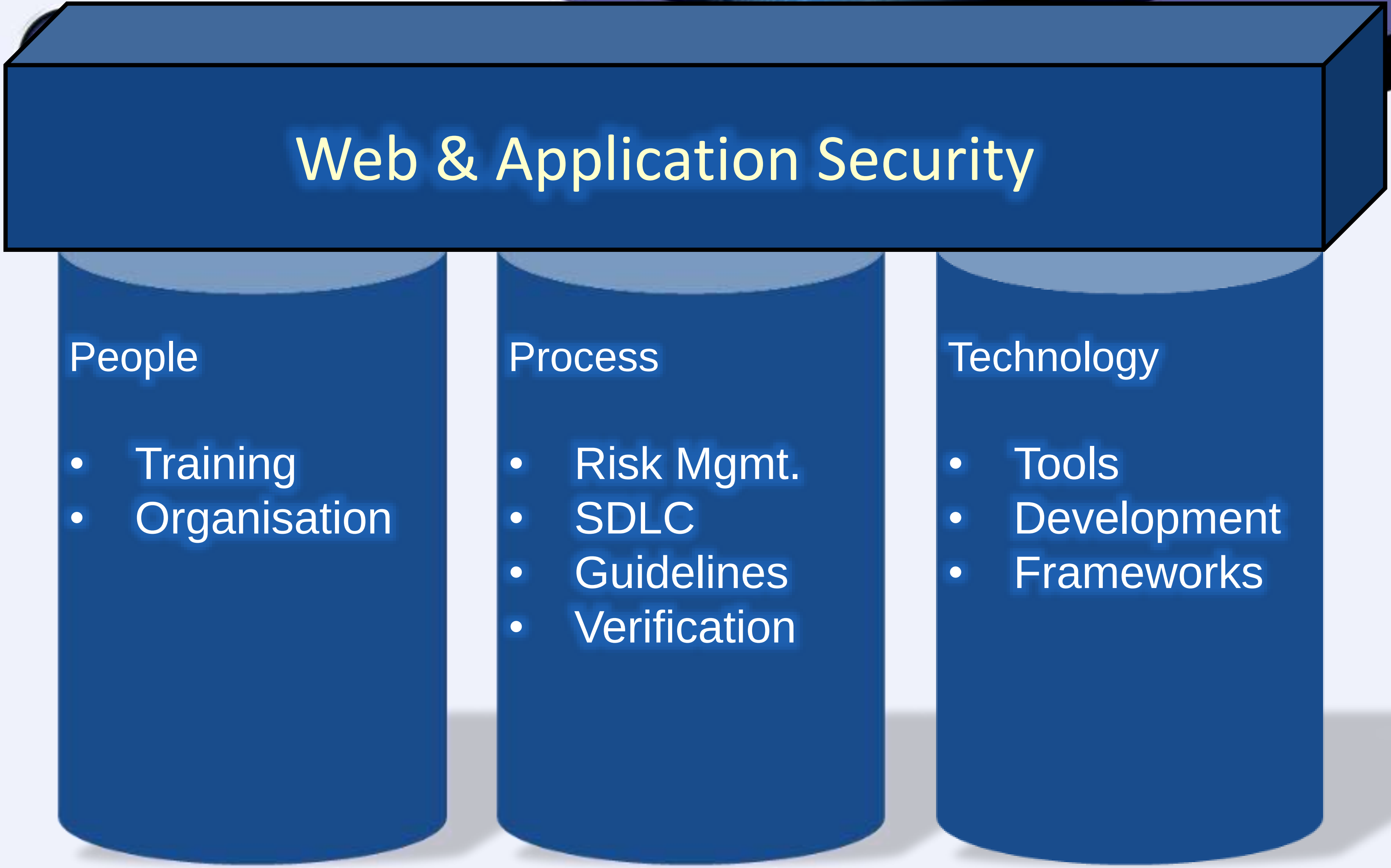
Categories



e.g. OWASP Top-10: Stable, Documentation, Protect

Multitude of Standards and Documents

- OWASP
- ISO 2700x, ISO 31000
- Cobit, Risk IT (ISACA)
- ITIL, NIST, PCI-DSS, ISF “Standard of Good Practice for Information Security”
- CSA (Cloud Security Alliance)
- ….



Web & Application Security

People

- Training
- Organisation

Process

- Risk Mgmt.
- SDLC
- Guidelines
- Verification

Technology

- Tools
- Development
- Frameworks

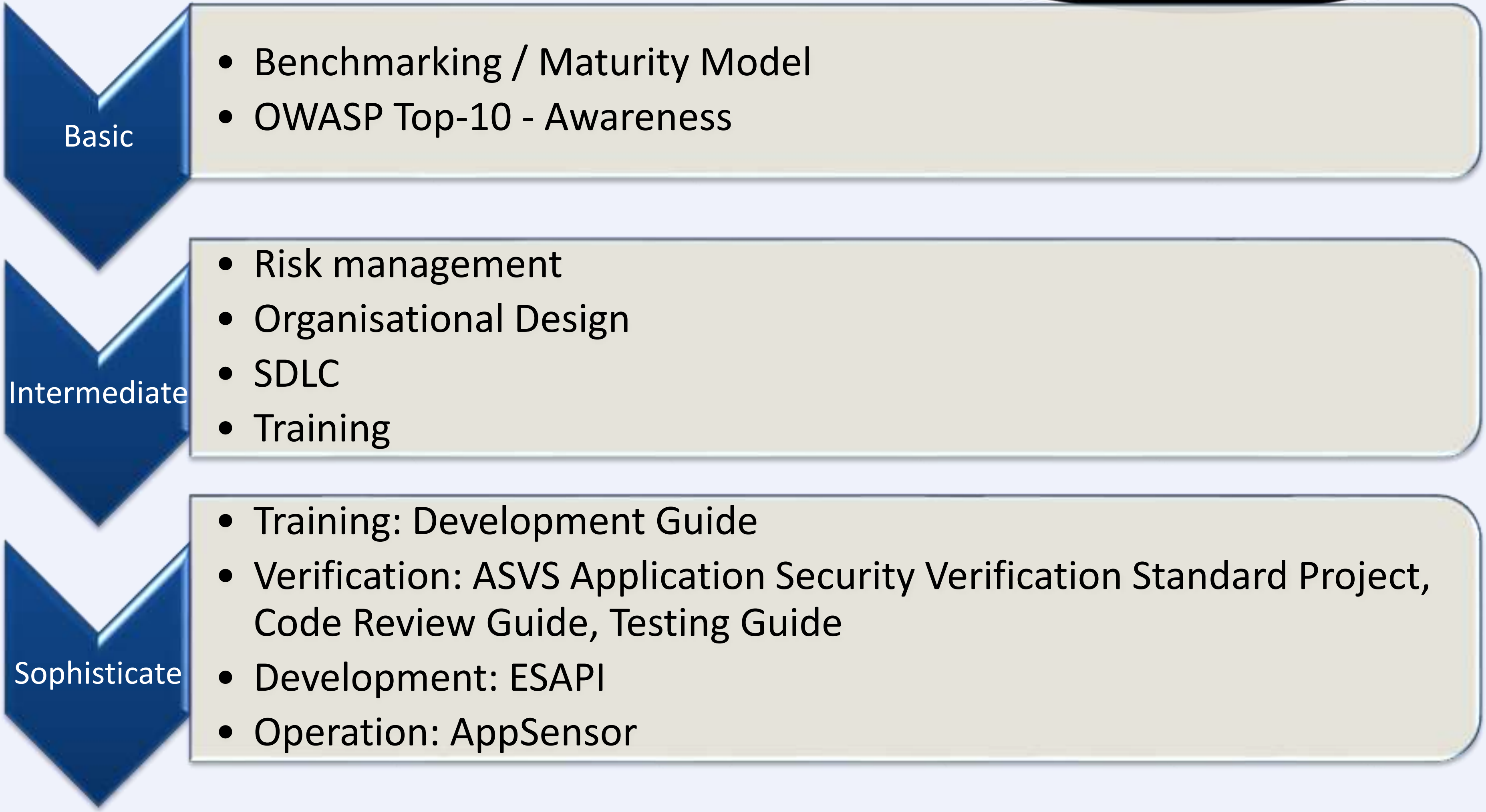
OWASP Projects for an industry or development company

OWASP
The Open Web Application Security Project

- OWASP Top Ten
- openSAMM - Software Assurance Maturity Model
- Application Security Guide For CISOs
- Secure Coding Practices - Quick Reference Guide
- Cheat Sheets Project
- Code Review Guide
- Development Guide Project
- ESAPI - Enterprise Security API
- WebGoat Project
- Testing Guide
- ASVS - Application Security Verification Standard
- AntiSamy Project
- AppSensor Project
- O2 Platform

One Roadmap Example

OWASP
The Open Web Application Security Project



Basic

- Benchmarking / Maturity Model
- OWASP Top-10 - Awareness

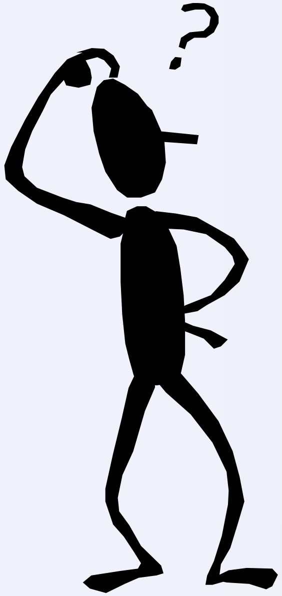
Intermediate

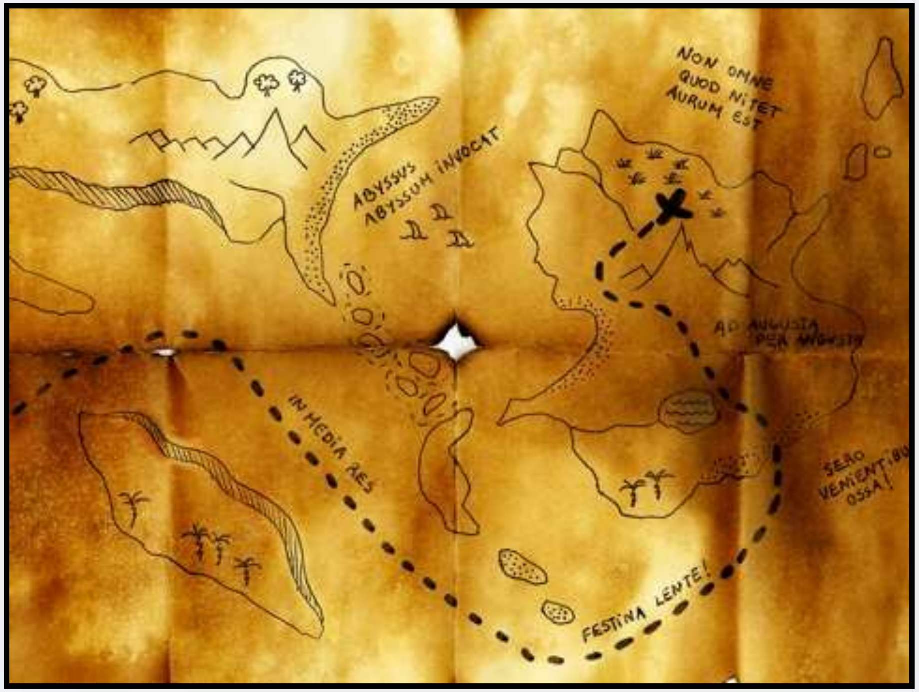
- Risk management
- Organisational Design
- SDLC
- Training

Sophisticate

- Training: Development Guide
- Verification: ASVS Application Security Verification Standard Project, Code Review Guide, Testing Guide
- Development: ESAPI
- Operation: AppSensor

Or:
Where are we? – And where are we going?





Maturity Models & Benchmarking

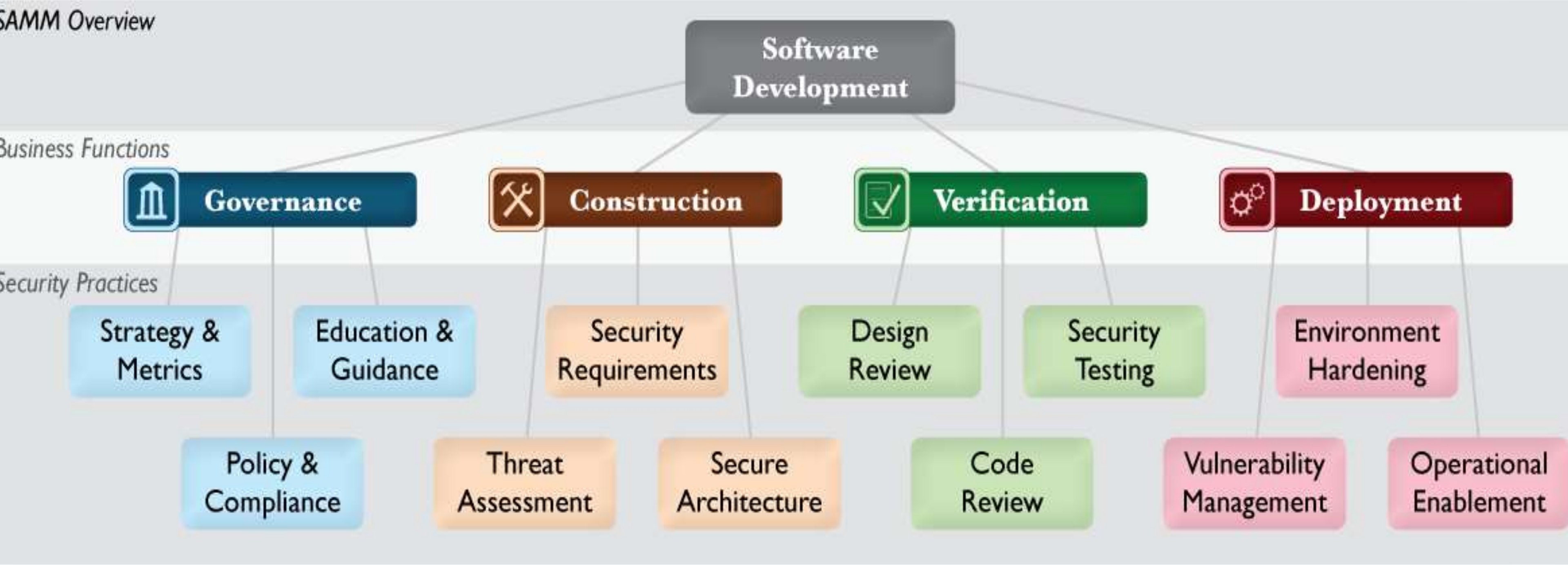
- Review of existing security efforts
- Benchmarking, Measuring Progress and Maturity Models

- Software Assurance Maturity Model (SAMM, http://www.opensamm.org)
- ISO 27000s
- Capability Maturity Model (CMM)
- …

SAMM Security Practices

OWASP
The Open Web Application Security Project

- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one can be targeted individually for improvement



OWASP Top 10 – Awareness & Training

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Failure to Restrict URL Access
- A8: Insecure Cryptographic Storage
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

OWASP Top-10

OWASP
The Open Web Application Security Project

- Top 10 Most Critical Web Application Security Risks
  - there exist more risks beyond top-10!
- Referenced by many external standards and best practices, e.g. PCI DSS etc.
- Great tool for awareness programs and training
- Available in many languages: e.g. Chinese, German, …
- Currently in revision for new version in 2013 (review stage of RC1)

OWASP Top-10 - how

OWASP
The Open Web Application Security Project

- Easy to use to start a first discussion and awareness
  - Initial developer training (1.5 hours)
  - Management awareness
  - Available in many languages (Spanish, Chinese, Japanese, Korean, Vietnamese, Indonesian, …)
  - Also other Top-10 for cloud, …
- But: there exist more risks beyond top-10!
- Referenced by many external standards, regulation and best practices, e.g. PCI DSS etc.

3. Risk Management

OWASP
The Open Web Application Security Project

What & How much is enough?

Risk Management

Risk: The probable frequency and probable magnitude of future loss

- Why – or where do you put your resources?
- Methods: OWASP, ISO-27005, ITIL, NIST SP 800-30, OCTAVE
- Asset Classification, Threat Analysis & Vulnerability Assessment
- What do you do with Risks?
- Quality vs. quantity, Human behavior & risk

Risk management

OWASP
The Open Web Application Security Project

Why / Benefits:

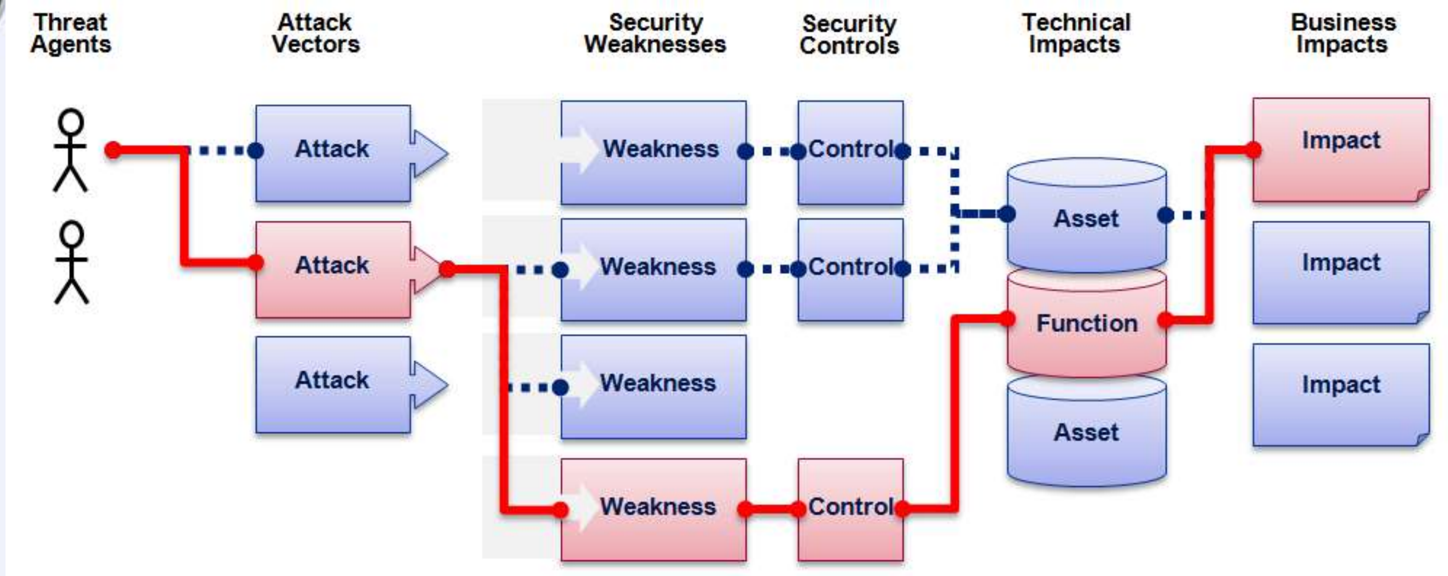
- Allocation of resources
  - Asset Classification and values?
  - Threats Analysis & Scenarios?
- Establish ownership of assets, risk and controls

Methods:

- OWASP
- FAIR (Factor Analysis of Information Risk)
- ISO 27005, ISO 31000
- Risk IT (ISACA)
- …

OWASP Top 10 Risk Rating Methodology

OWASP



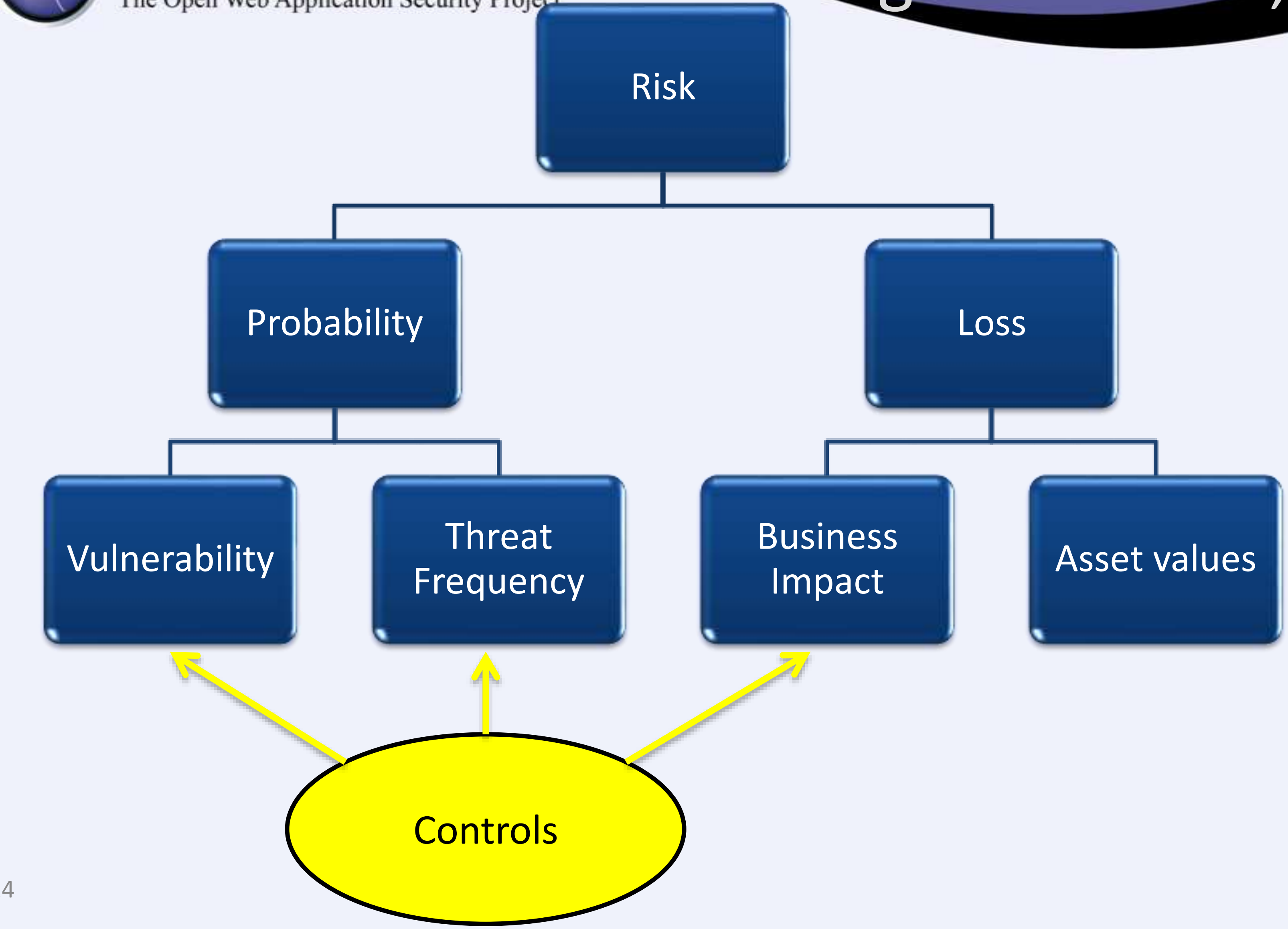
Threat Agent		Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	1	Easy	Widespread	Easy	Severe	?
	2	Average	Common	Average	Moderate	
	3	Difficult	Uncommon	Difficult	Minor	
		1	2	2	1	
			1.66	*	1	

Injection Example

1.66 weighted risk rating

Other methods: e.g. ISO 27005, …

OWASP
The Open Web Application Security Project



Risk Heat Map – Threat Level

Likelihood

Medium	Medium	High	High	High
Medium	Medium	Medium	High	High
Low	Medium	Medium	Medium	High
Low	Low	Medium	Medium	Medium
Low	Low	Low	Medium	Medium

Impact

SDLC(s)

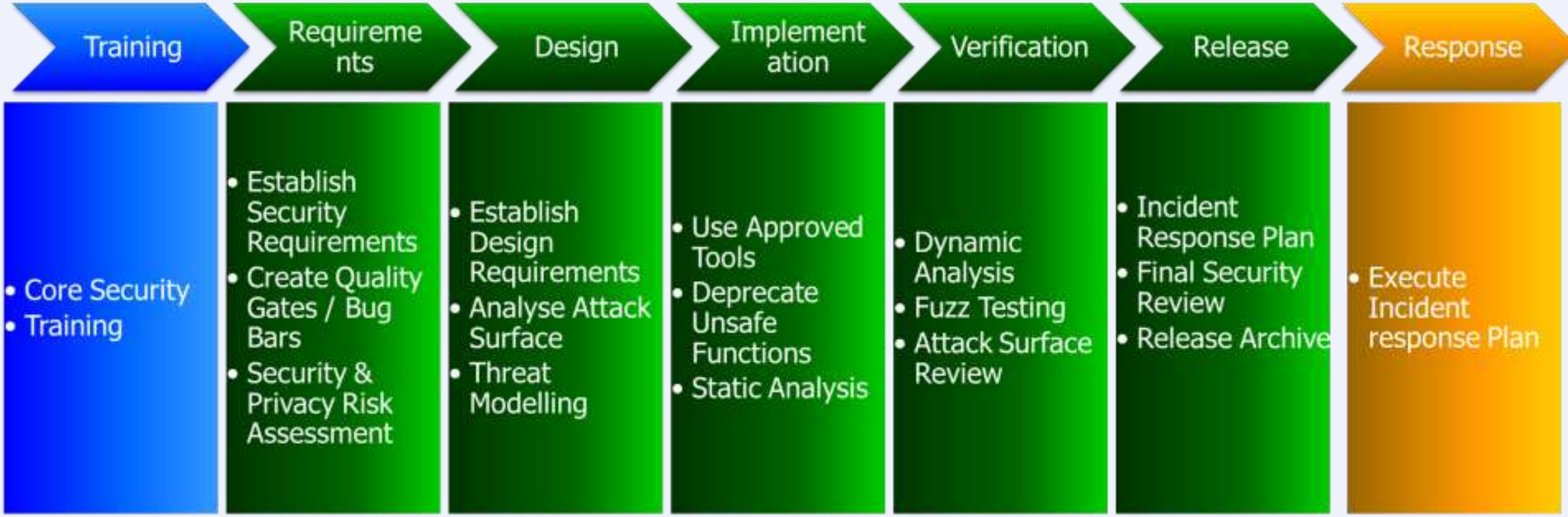
OWASP
The Open Web Application Security Project

- Microsoft SDL
- Adobe Secure Product Lifecycle
- OWASP’s CLASP
- …

Secure Software Development Lifecycle - SDLC

OWASP
The Open Web Application Security Project

- e.g. Microsoft SDL



Training	Requirements	Design	Implementation	Verification	Release	Response
• Core Security • Training	• Establish Security Requirements • Create Quality Gates / Bug Bars • Security & Privacy Risk Assessment	• Establish Design Requirements • Analyse Attack Surface • Threat Modelling	• Use Approved Tools • Deprecate Unsafe Functions • Static Analysis	• Dynamic Analysis • Fuzz Testing • Attack Surface Review	• Incident Response Plan • Final Security Review • Release Archive	• Execute Incident response Plan

Training

- OWASP Top-10
- Secure Coding Practices
- Cheatsheets
- Webgoat

OWASP Top-10

- Usually a good first awareness training for developers (~1-2 hours)
- Recommend to tailor it to your application landscape: make it meaningful for them as some of the security risks may not be as urgent in your organisation as others
- Enrich with examples / use cases from your applications

Secure Coding Practices Quick Reference Guide

OWASP
The Open Web Application Security Project

- Good next step of “To do” after initial “OWASP Top-10”
- Technology agnostic coding practices
- What to do, not how to do it
- Compact (17 pages), comprehensive checklist format
- Focuses on secure coding requirements, rather then on vulnerabilities and exploits
- Includes cross referenced glossary to get developers and security folks talking the same language
  - ➢ Tailor to your application landscape
    (not all parts may be equally important for your organisation).

- Goal: Build a secure coding kick-start tool, to help development teams quickly understand secure coding
- Originally developed for use inside The Boeing Company, July 2010, Boeing assigned copyright to OWASP

Secure Coding Practices Quick Reference Guide Summary

Help development teams to quickly understand secure coding practices

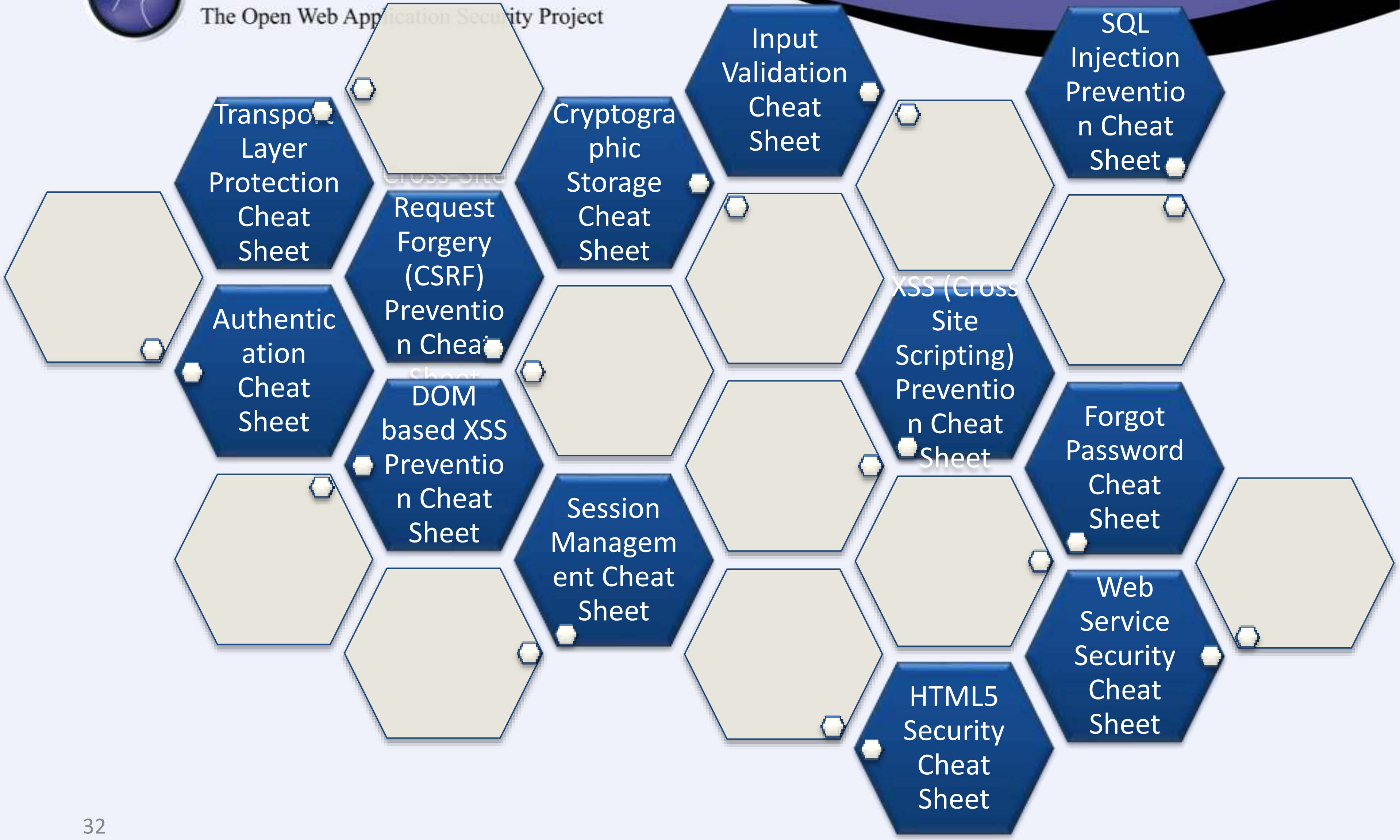
Assist defining requirements and adding them to policies and contracts

Context and vocabulary for interactions with security staff

Easy desk reference

OWASP Cheat Sheet Series

OWASP
The Open Web Application Security Project



Transport Layer Protection Cheat Sheet

Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

Cryptographic Storage Cheat Sheet

Input Validation Cheat Sheet

SQL Injection Prevention Cheat Sheet

Authentication Cheat Sheet

DOM based XSS Prevention Cheat Sheet

XSS (Cross Site Scripting) Prevention Cheat Sheet

Session Management Cheat Sheet

Forgot Password Cheat Sheet

Web Service Security Cheat Sheet

HTML5 Security Cheat Sheet

Webgoat

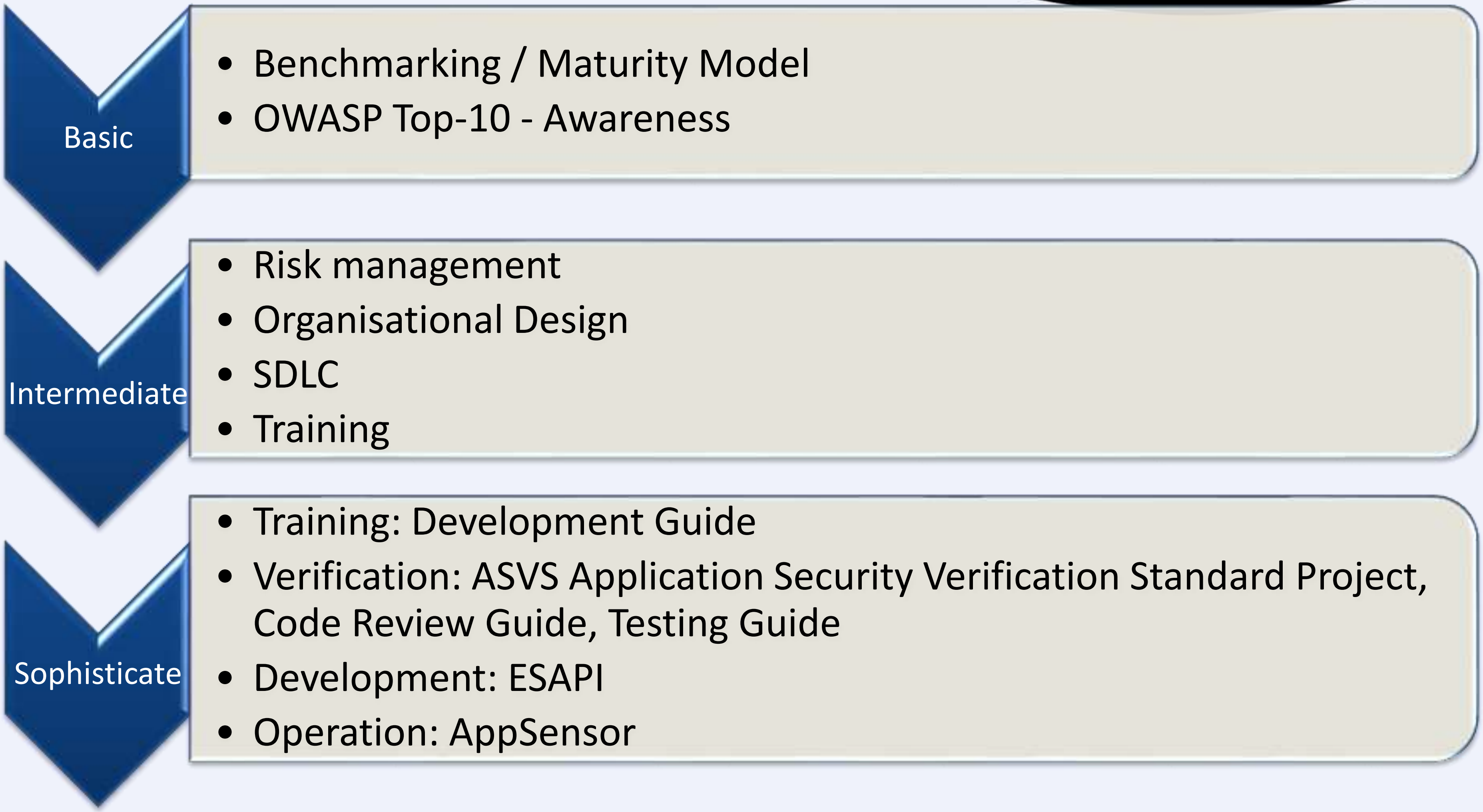
OWASP
The Open Web Application Security Project

- Exercise with Example Web Application to illustrate typical Security Flaws within Web-Applications
- Practice Lessons for Common Vulnerabilities
- Teach a Structured Approach to Testing and Exploiting
- Give Practical Training and Examples

One Roadmap Example

OWASP

The Open Web Application Security Project



Basic

- Benchmarking / Maturity Model
- OWASP Top-10 - Awareness

Intermediate

- Risk management
- Organisational Design
- SDLC
- Training

Sophisticate

- Training: Development Guide
- Verification: ASVS Application Security Verification Standard Project, Code Review Guide, Testing Guide
- Development: ESAPI
- Operation: AppSensor

- Further Resources:
  - OWASP CISO Guide:
- https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs
  - OWASP CISO Survey
  - Email me: tobias.gondrom@owasp.org

- Questions?
  - What OWASP tools do you think will be useful for you right away?
  - What would you like to have in the future?

Thank you

CISO Survey

https://www.surveymonkey.com/s/CISO2013Survey