OWASP Shanghai chapter meeting
Mar 2014
Managing Web & Application Security with OWASP – bringing it all together

Tobias Gondrom

(OWASP Global Board Member)

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

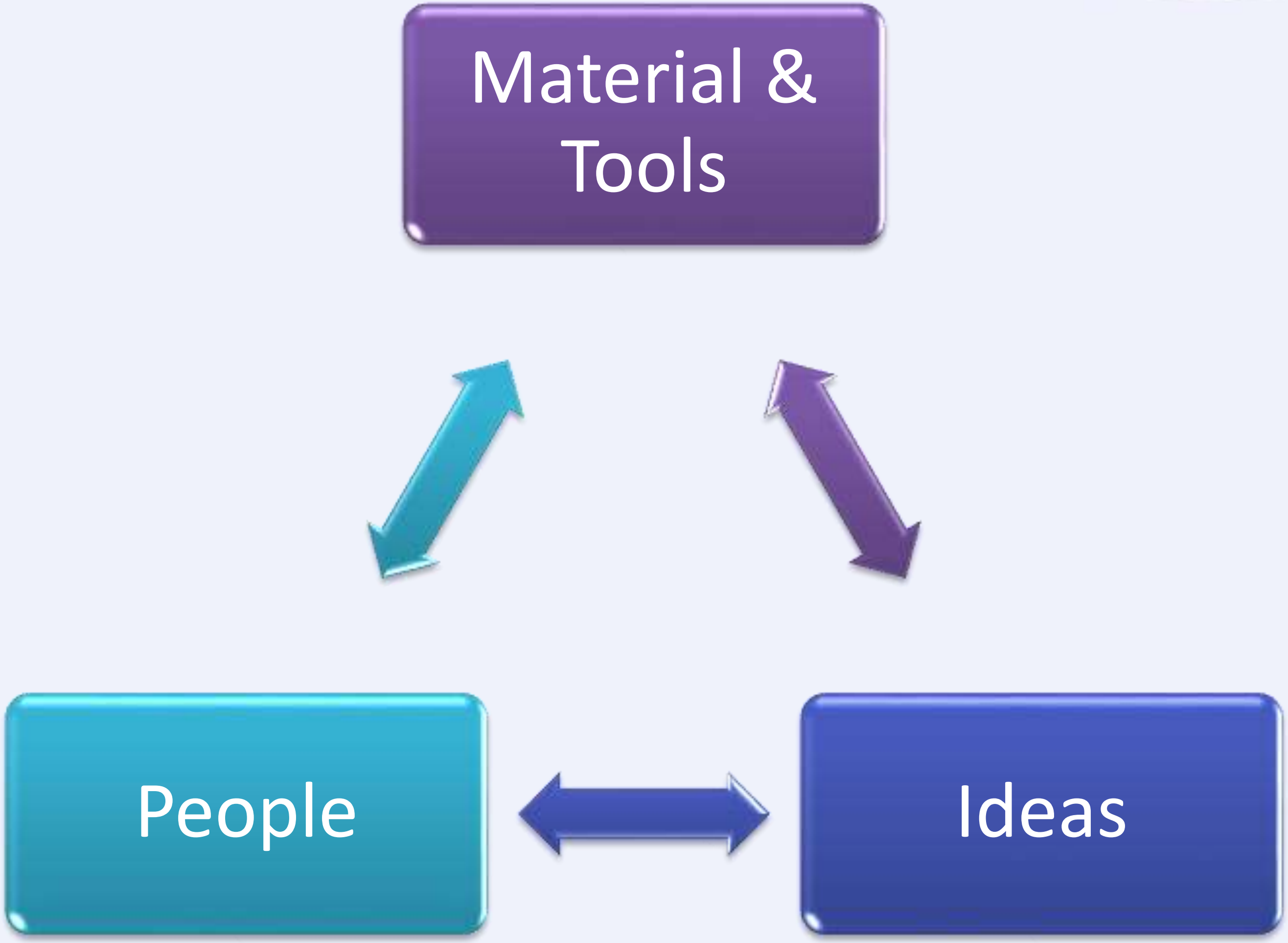
OWASP
The Open Web Application Security Project

- 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
- OWASP Global Board member, OWASP Project Leader for the CISO Survey, www.owasp.org
- 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
  IETF Administrative Oversight Committee (IAOC),
  Chair of the IETF Trust
- Cloud Security Alliance, Hong Kong chapter, Vice Chairman

- 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



Material & Tools

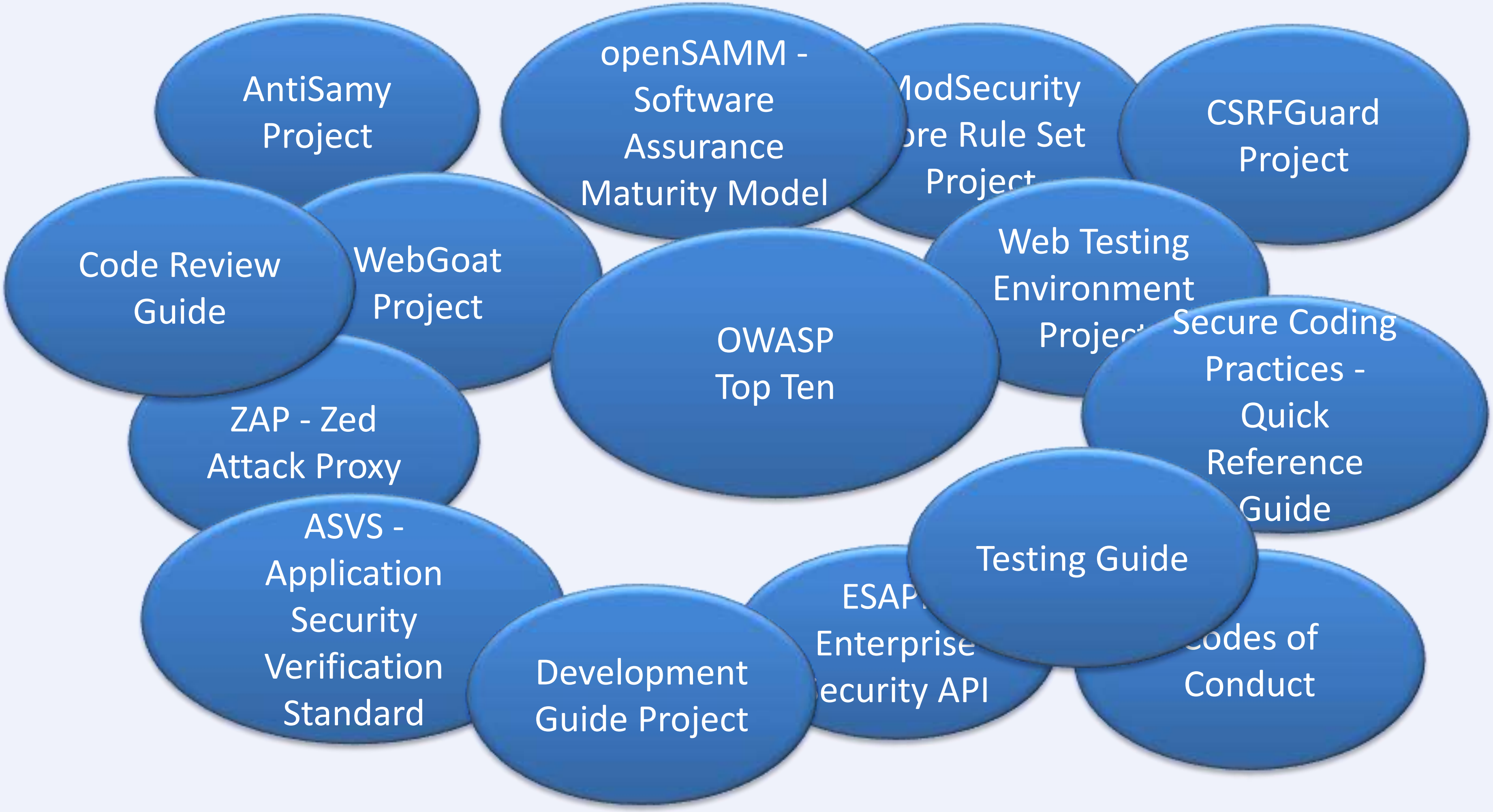
People

Ideas

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

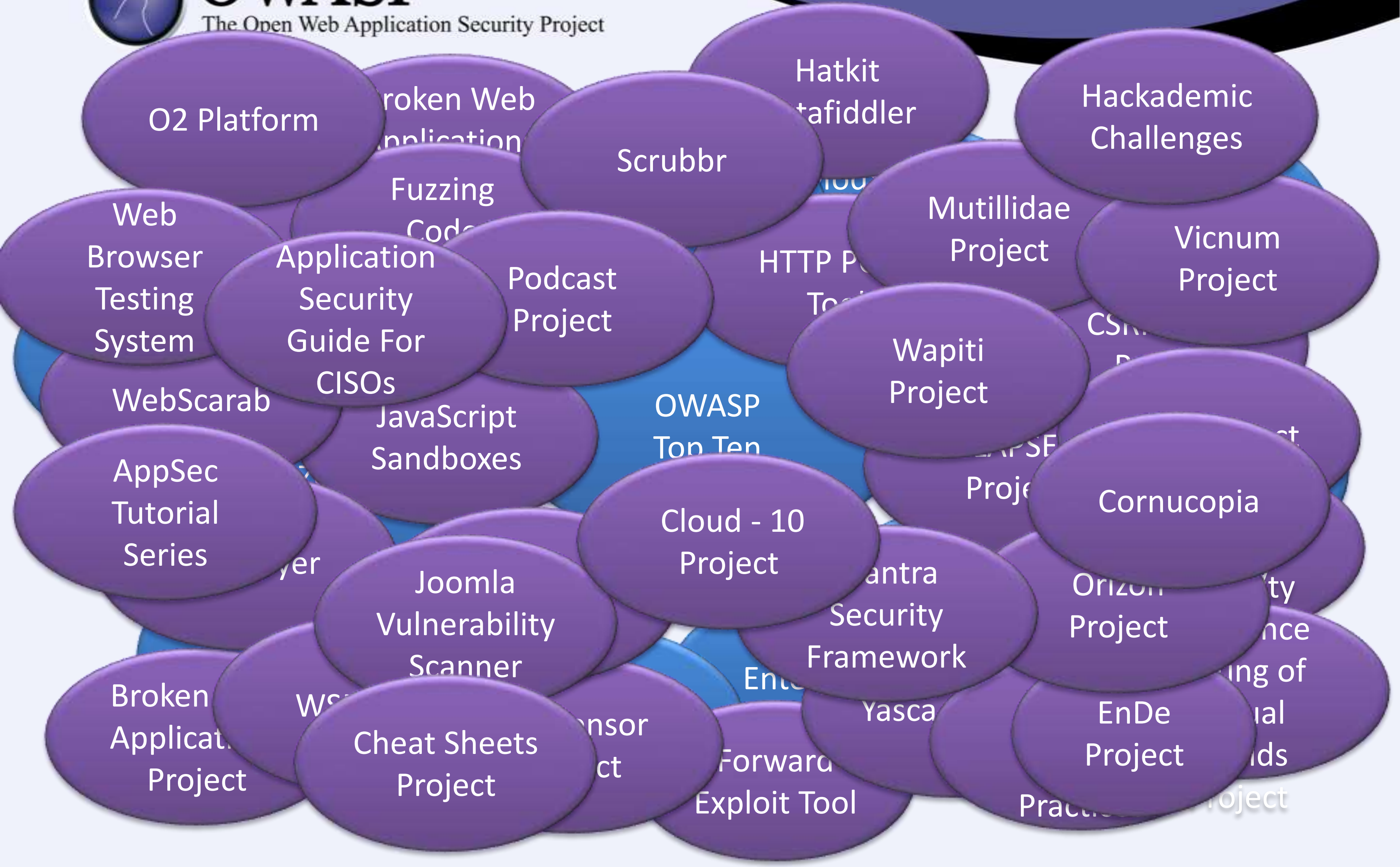
OWASP Flagship Projects

OWASP
The Open Web Application Security Project


AntiSamy Project
openSAMM - Software Assurance Maturity Model
ModSecurity
ore Rule Set
Project
CSRFGuard Project
Code Review Guide
WebGoat Project
OWASP Top Ten
Web Testing Environment Projec
Secure Coding Practices - Quick Reference Guide
ZAP - Zed Attack Proxy
ASVS - Application Security Verification Standard
Development Guide Project
ESAP
Enterprise
ecurity API
Testing Guide
odes of Conduct

OWASP Labs Projects and more

OWASP
The Open Web Application Security Project



O2 Platform

roken Web
pplication

Hatkit
tafiddler

Scrubbr

Hackademic
Challenges

Fuzzing
Code

Web
Browser
Testing
System

Application
Security
Guide For
CISOs

Podcast
Project

HTTP P
To

Mutillidae
Project

Vicnum
Project

CSR
P

Wapiti
Project

WebScarab

JavaScript
Sandboxes

OWASP
Top Ten

APSE
Proje

ct

AppSec
Tutorial
Series

yer

Cloud - 10
Project

Cornucopia

Joomla
Vulnerability
Scanner

antra
Security
Framework

Orizon
Project

ty
nce
ing of
ual
lds
oject

Broken
Applicat
Project

WS

nsor
ct

Cheat Sheets
Project

Ent

Yasca

Forward
Exploit Tool

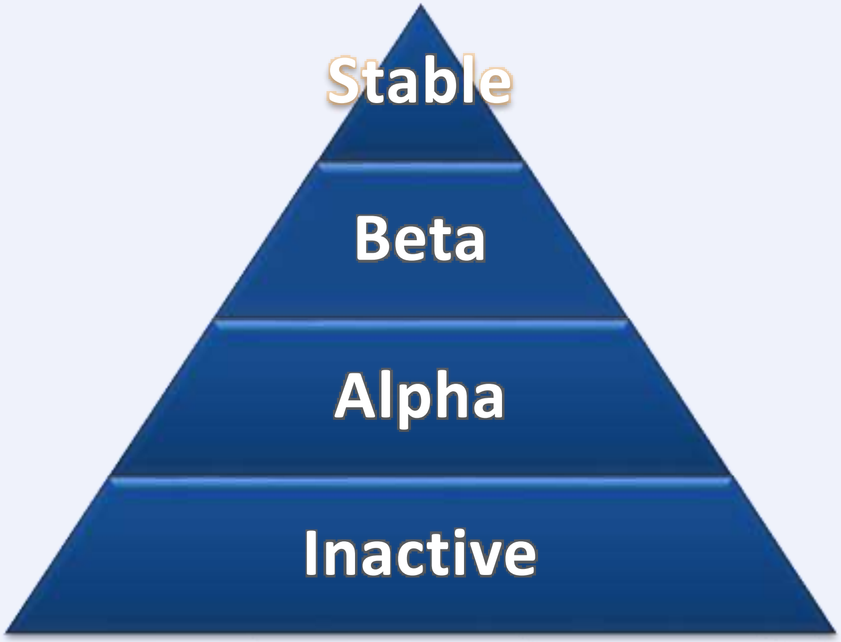
EnDe
Project

Practi

OWASP - Projects

OWASP
The Open Web Application Security Project

- Project Status



Stable

Beta

Alpha

Inactive

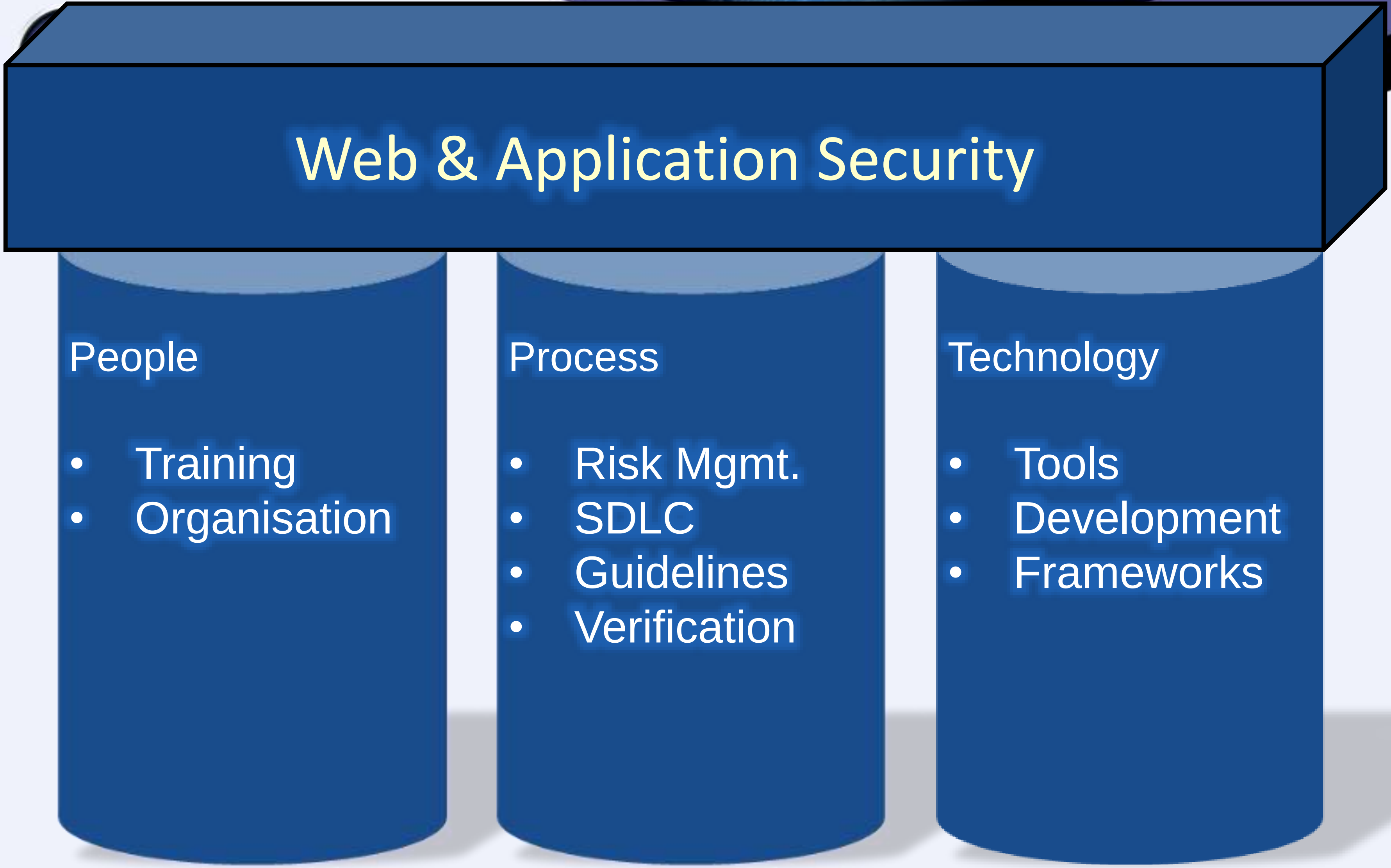
Categories

- Tools
- Documentation
- Protect
- Detect
- Life Cycle

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

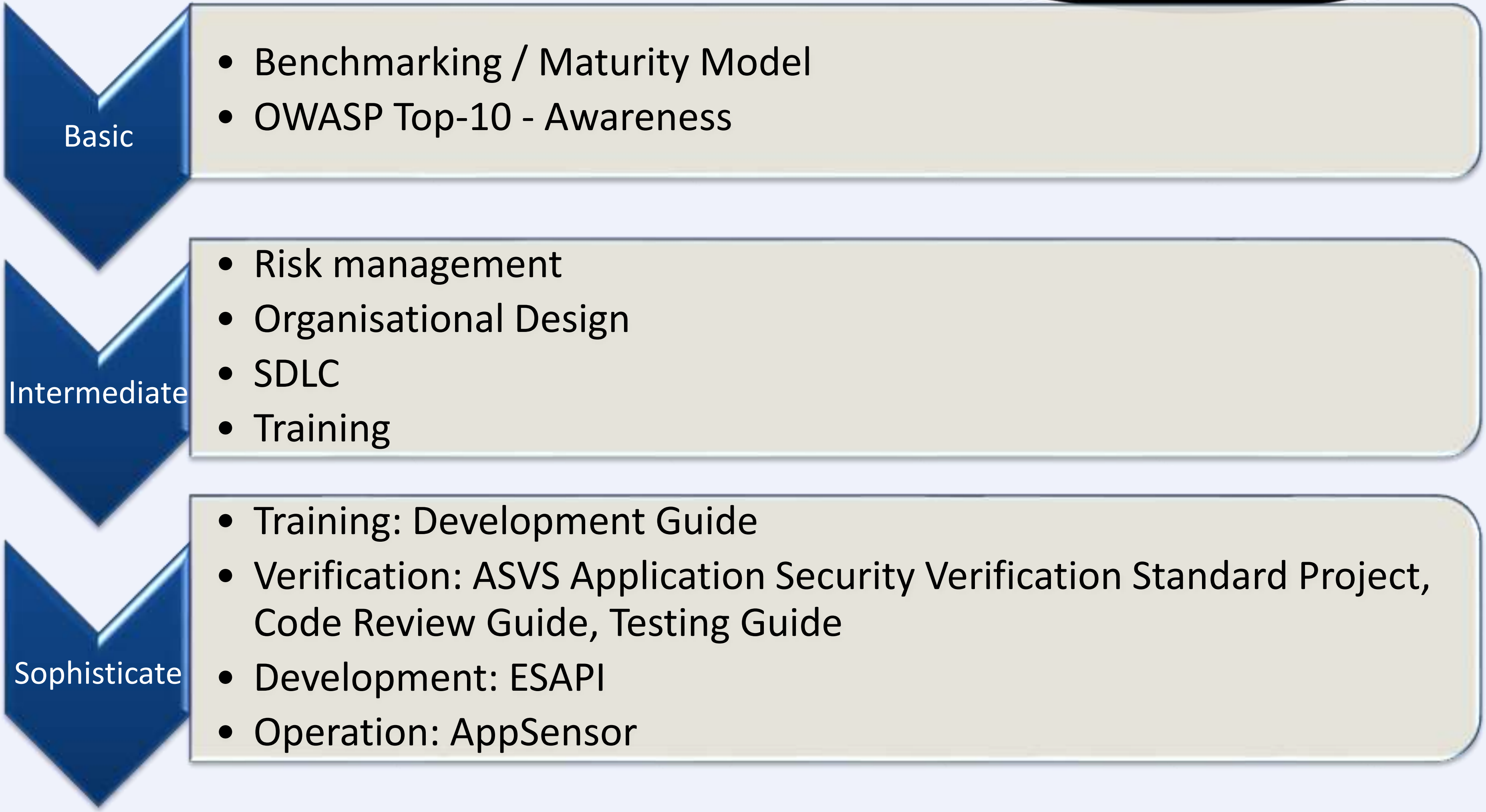
- Tools
- Development
- Frameworks

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
- WebGoat Project
- Testing Guide
- ESAPI - Enterprise Security API
- ASVS - Application Security Verification Standard
- AntiSamy Project
- AppSensor Project
- O2 Platform

One Roadmap Example



Basic

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

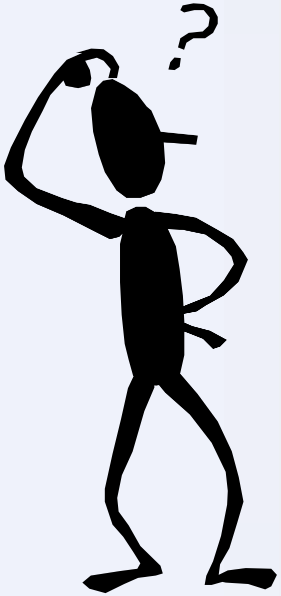
Intermediate

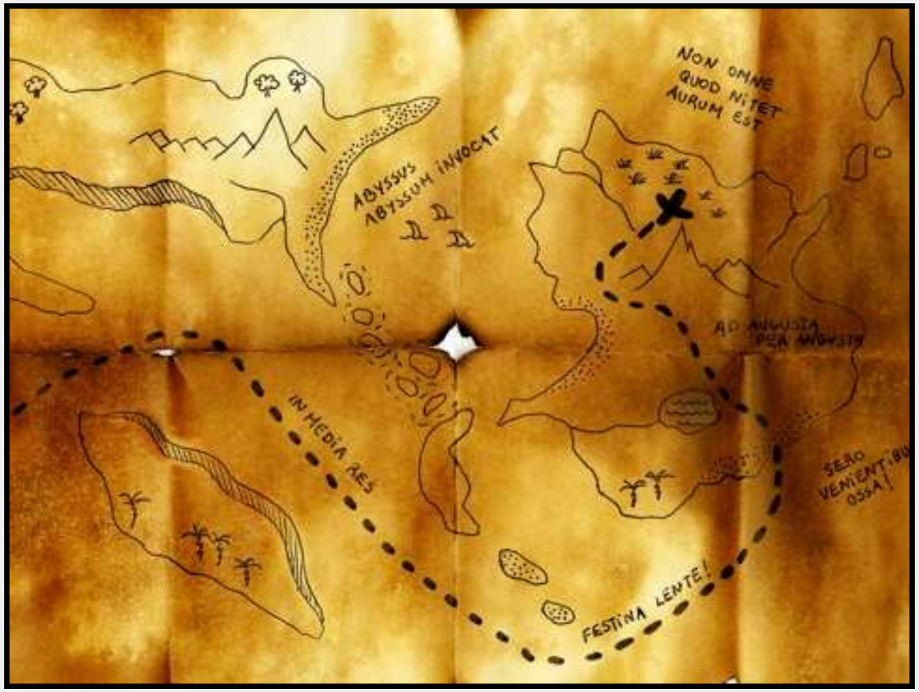
- Risk management
- Organisational Design
- SDLC
- Training

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

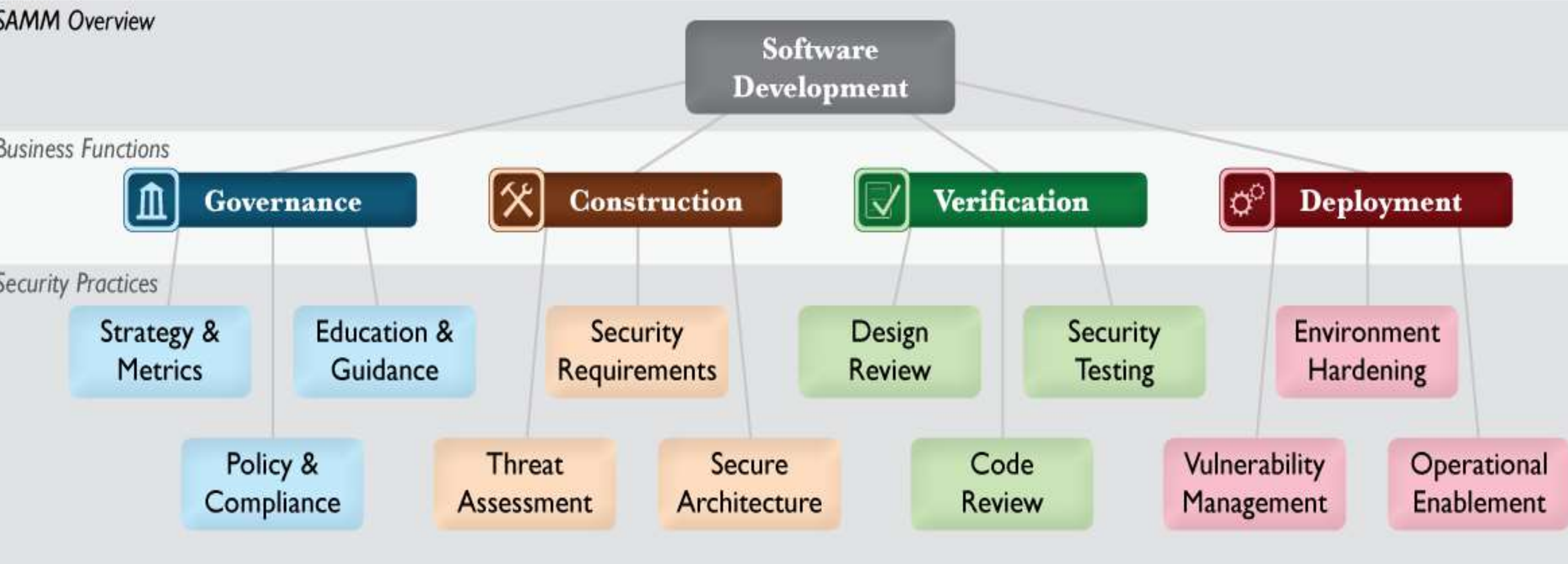
- Review of existing security efforts
- Benchmarking, Measuring Progress and Maturity Models

- 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

OWASP
The Open Web Application Security Project

- 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

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

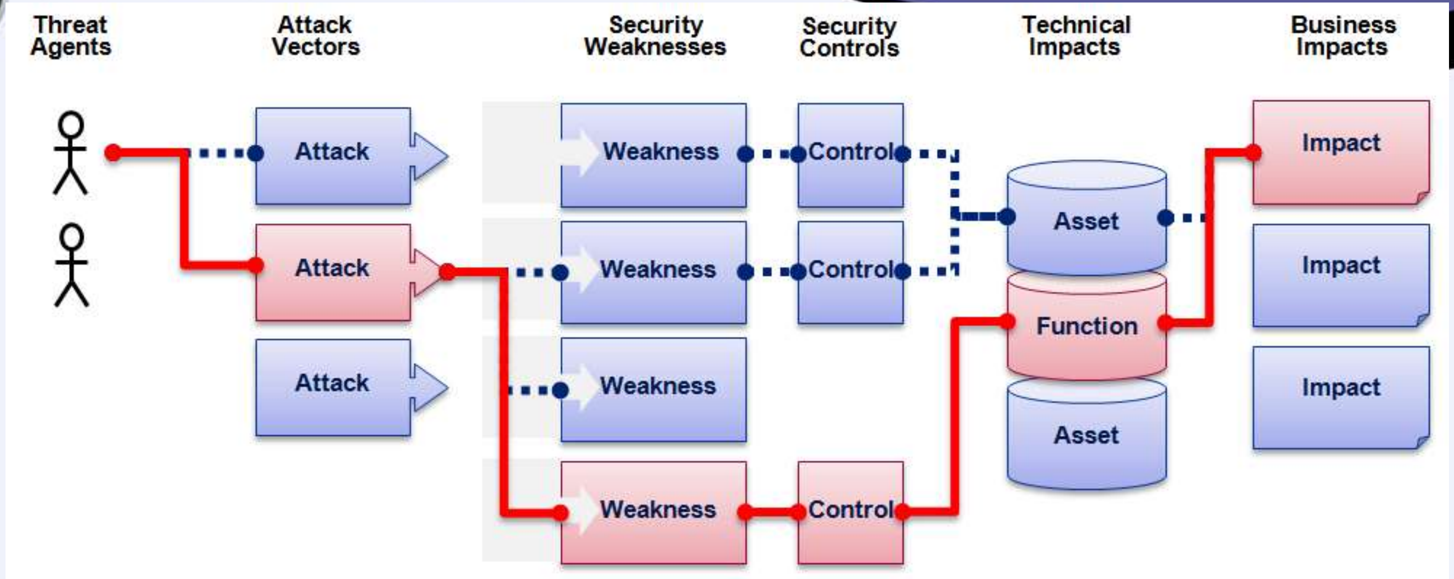
Why / Benefits:

- 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

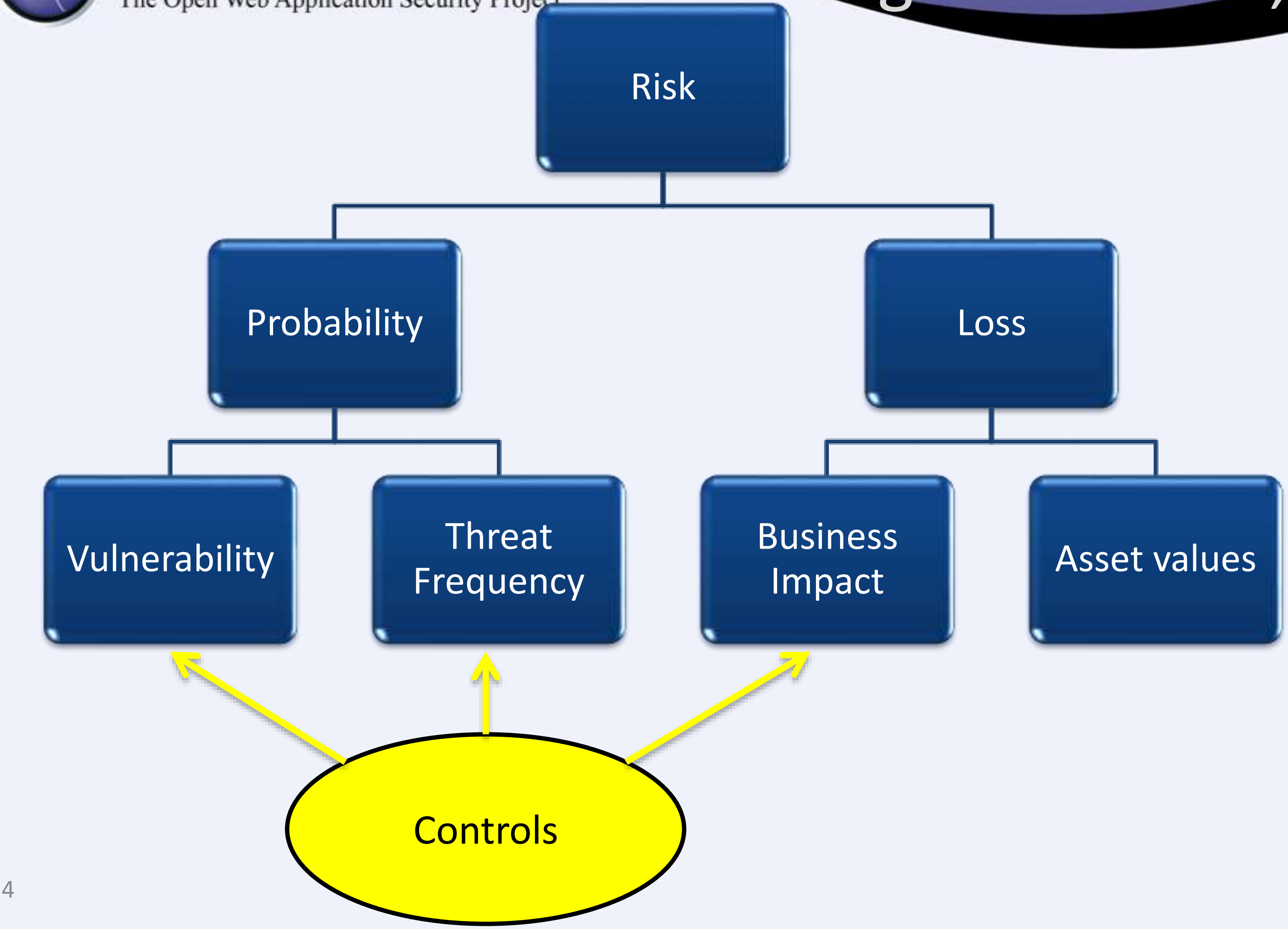


Injection Example

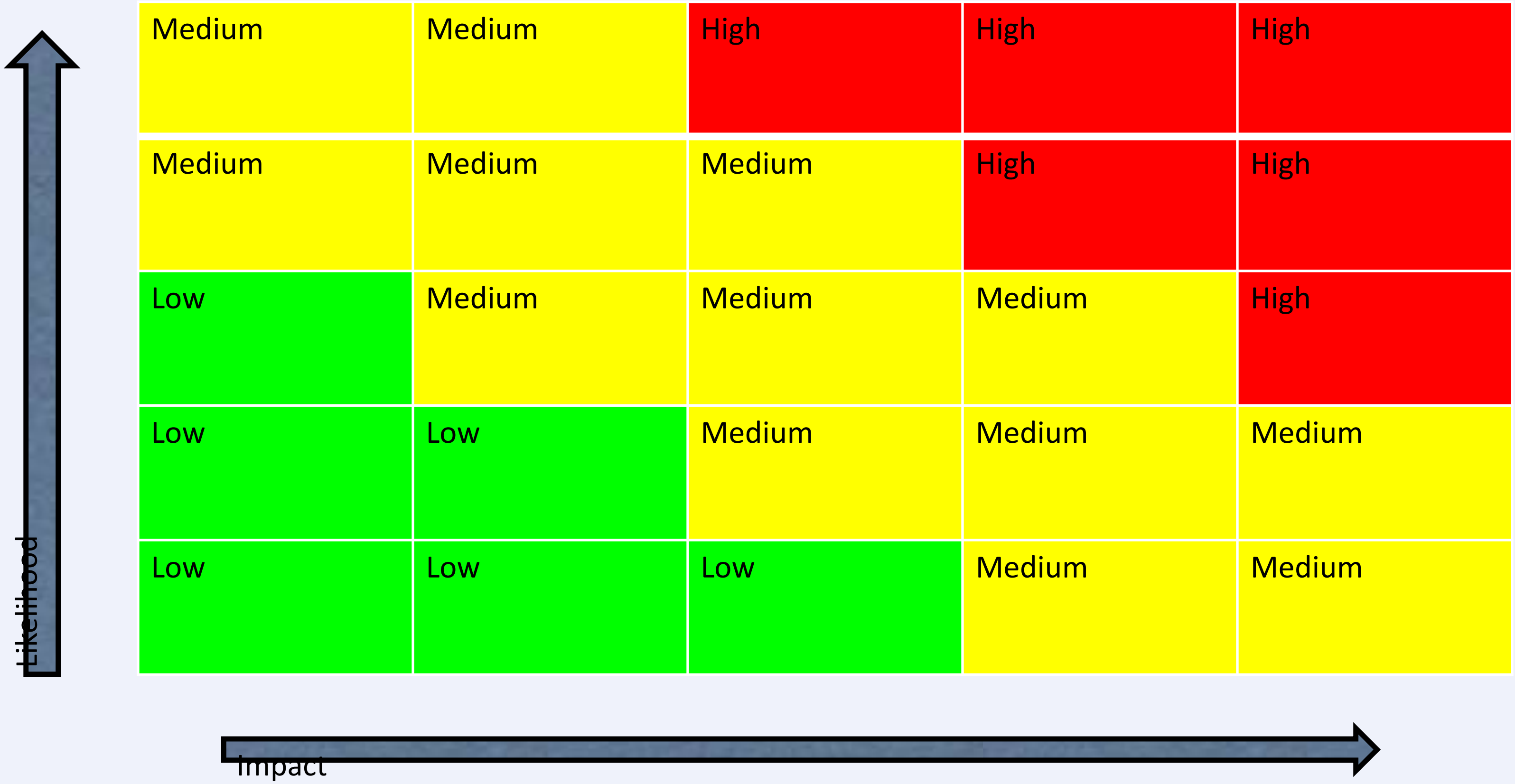
Threat Agent		Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	1	Easy	Widespread	Easy	Severe	?
	2	Average	Common	Average	Moderate	
	3	Difficult	Uncommon	Difficult	Minor	
		1	2	2	1	
			1.66	*	1	

1.66 weighted risk rating

Other methods: e.g. ISO 27005, …



Risk Heat Map – Threat Level



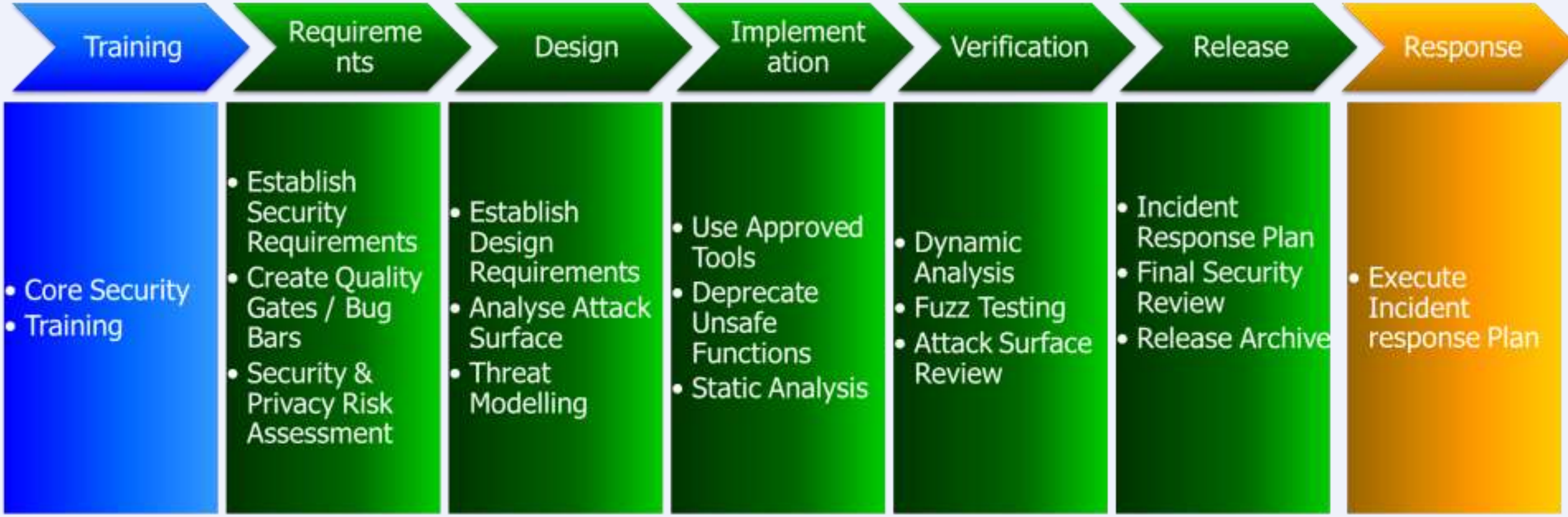
Medium	Medium	High	High	High
Medium	Medium	Medium	High	High
Low	Medium	Medium	Medium	High
Low	Low	Medium	Medium	Medium
Low	Low	Low	Medium	Medium

SDLC(s)

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

Secure Software Development Lifecycle - SDLC

- 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

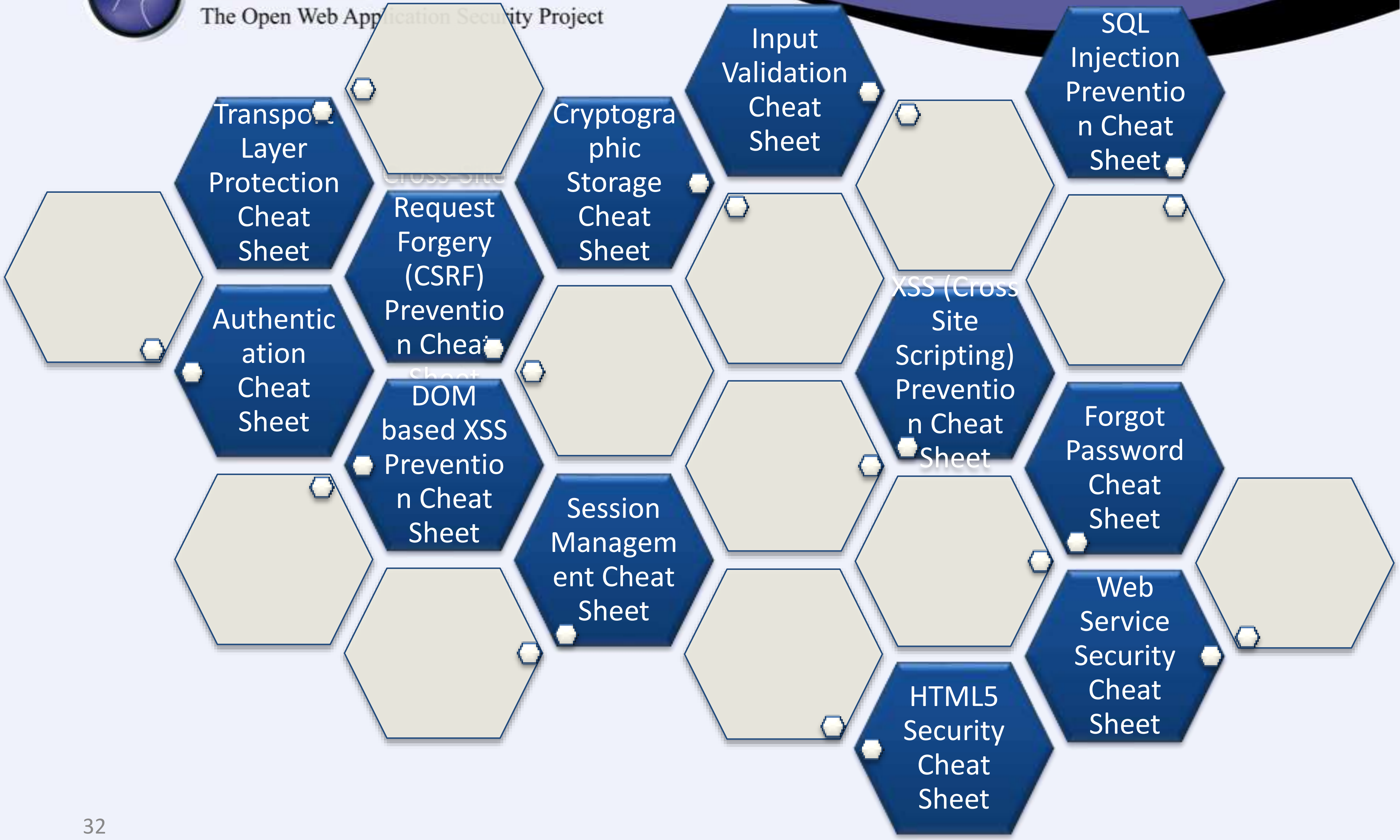
Assist defining requirements and adding them to policies and contracts

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

Authentication Cheat Sheet

Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

DOM based XSS Prevention Cheat Sheet

Cryptographic Storage Cheat Sheet

Session Management Cheat Sheet

Input Validation Cheat Sheet

XSS (Cross Site Scripting) Prevention Cheat Sheet

HTML5 Security Cheat Sheet

SQL Injection Prevention Cheat Sheet

Forgot Password Cheat Sheet

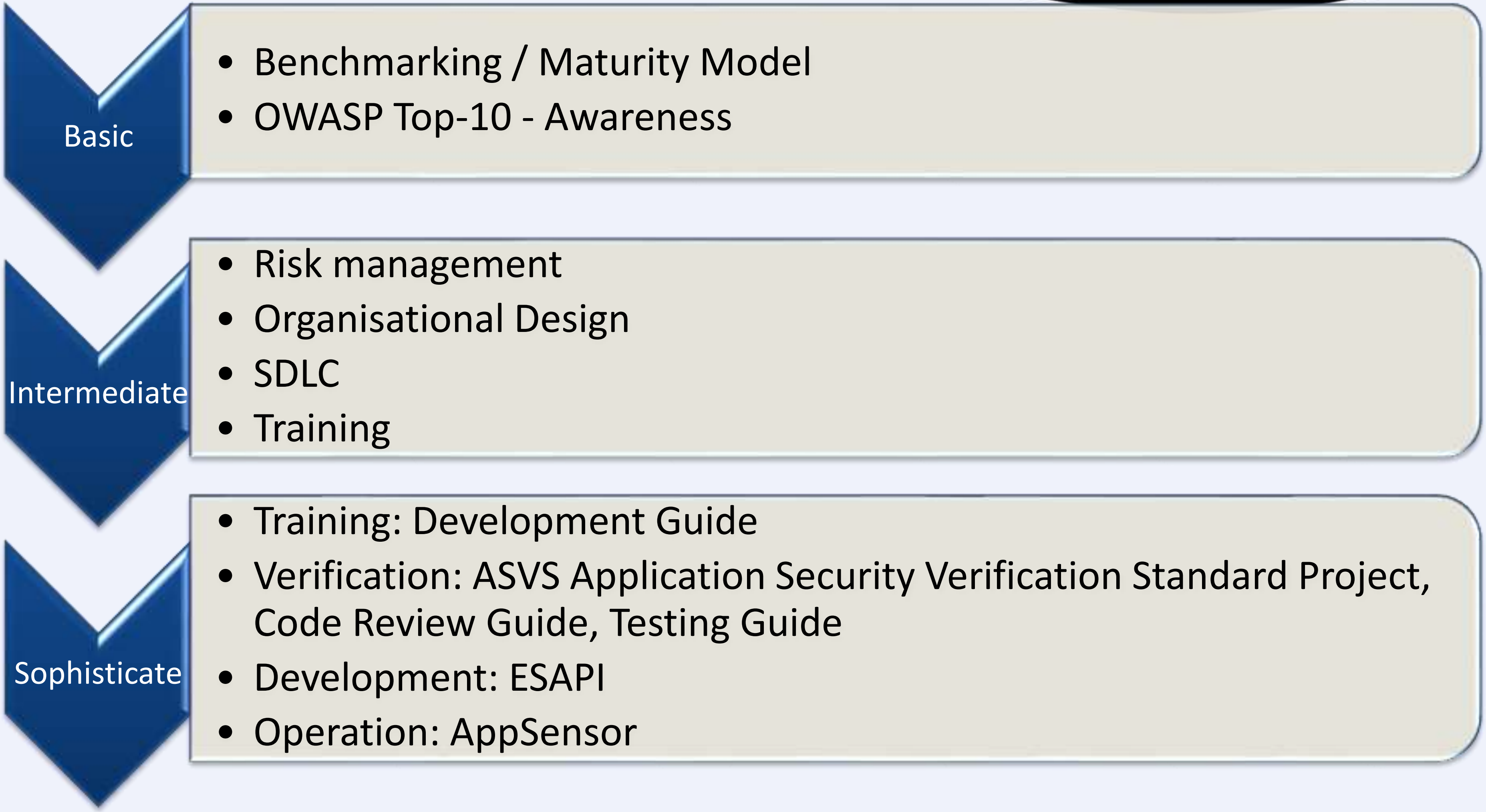
Web Service Security Cheat Sheet

Webgoat

- 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 https://www.owasp.org/index.php/OWASP_CISO_Survey

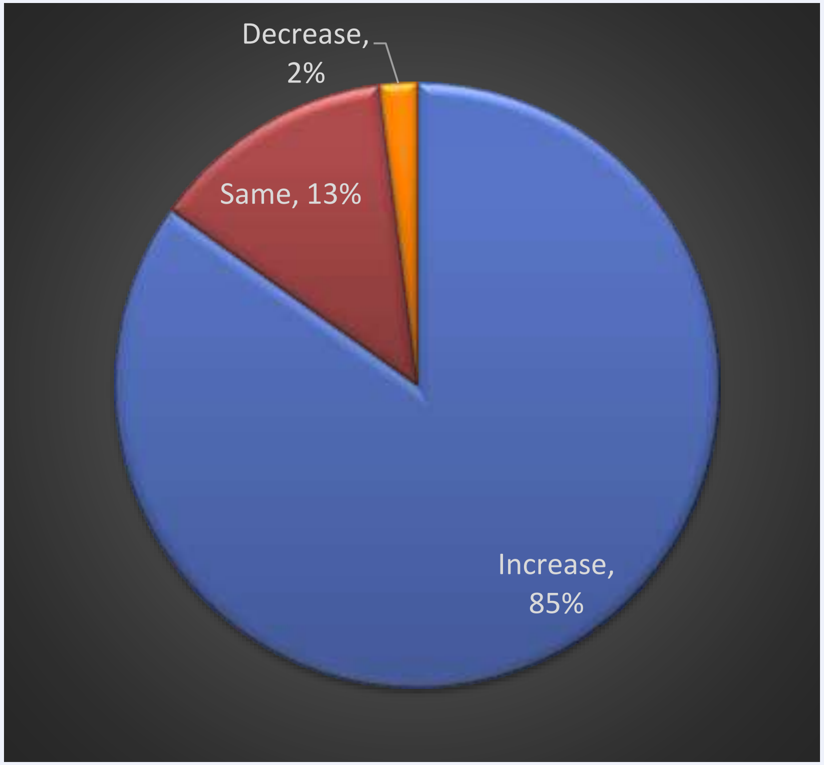
  - Email me: tobias.gondrom@owasp.org

- Methodology
  - Phase 1: Online Survey sent to CISOs and Information Security Managers
  - Phase 2: Followed by selective personal interviews
  - More than 100 replies from various industries and counting…

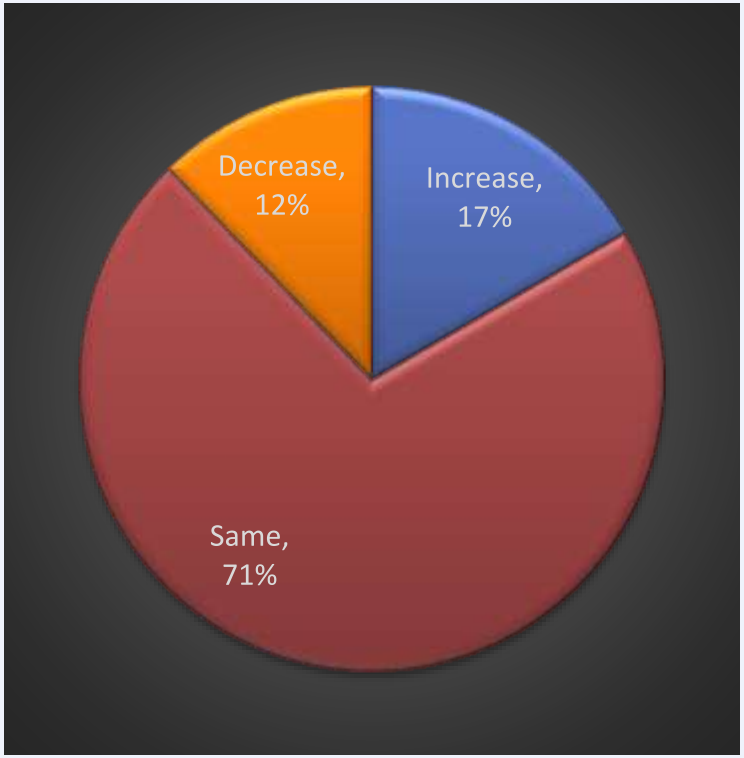
CISO Survey: External Threats are on the Rise!

OWASP
The Open Web Application Security Project

- External attacks or fraud (e.g., phishing, website attacks)

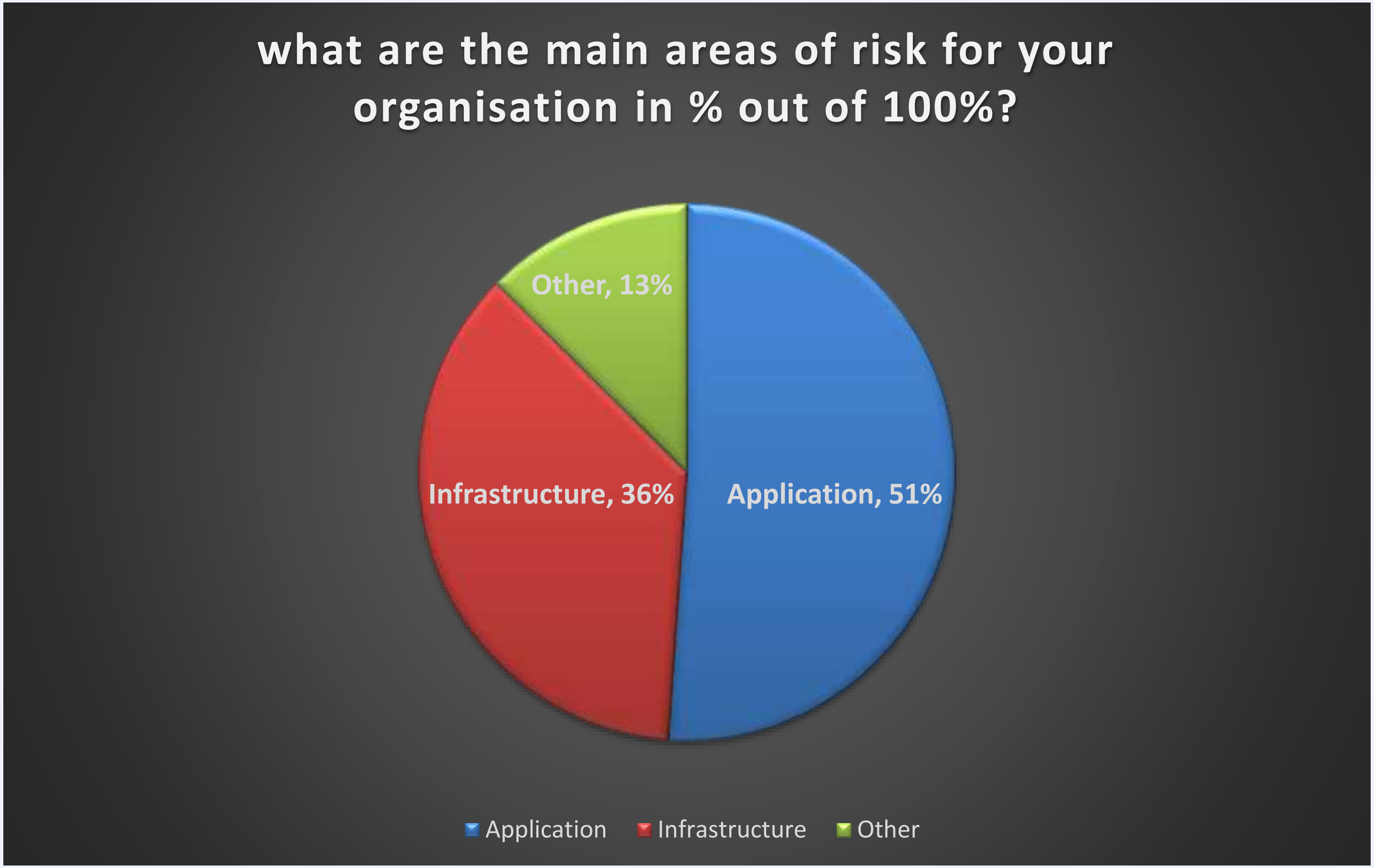


Internal attacks or fraud (e.g., abuse of privileges, theft of information)



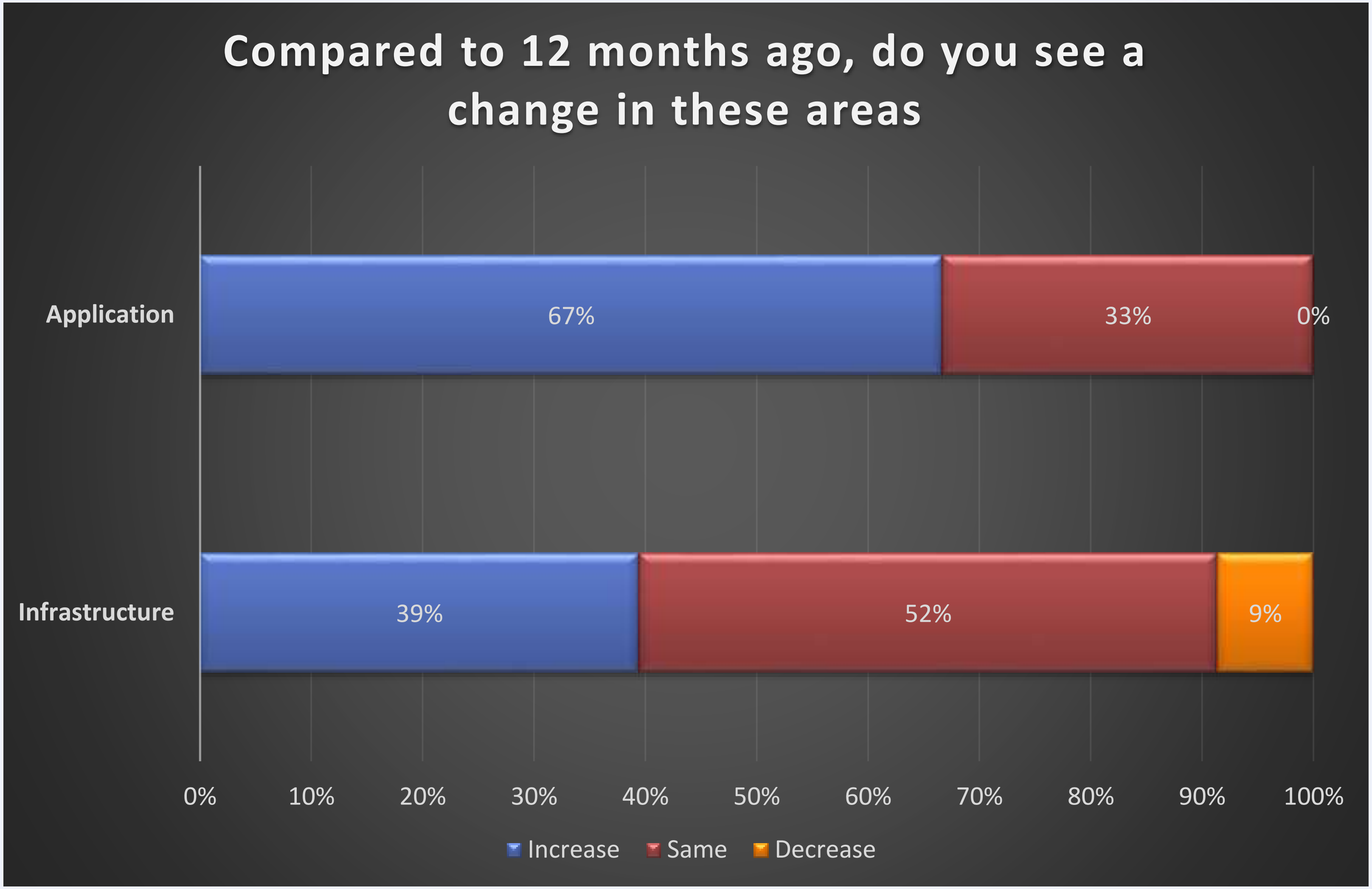
CISO Survey: Change in the threats facing your organization

OWASP
The Open Web Application Security Project



CISO Survey : Change in the Threats

OWASP
The Open Web Application Security Project

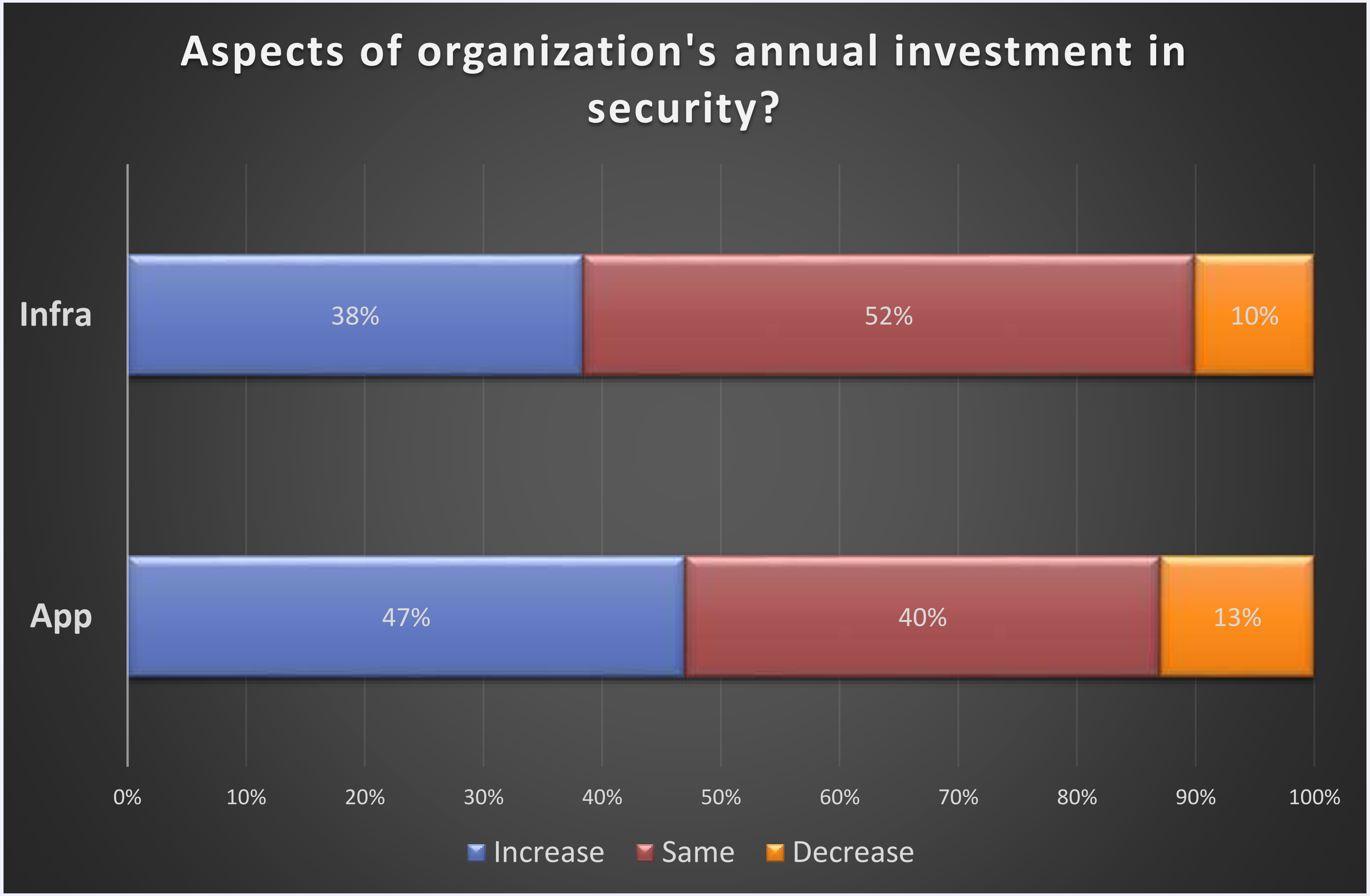


•Top five sources of application security risk within your organization?

- **Lack of awareness of application security issues within the organization**
- **Insecure source code development**
- **Poor/inadequate testing methodologies**
- **Lack of budget to support application security initiatives**
- Staffing (e.g., lack of security skills within team)

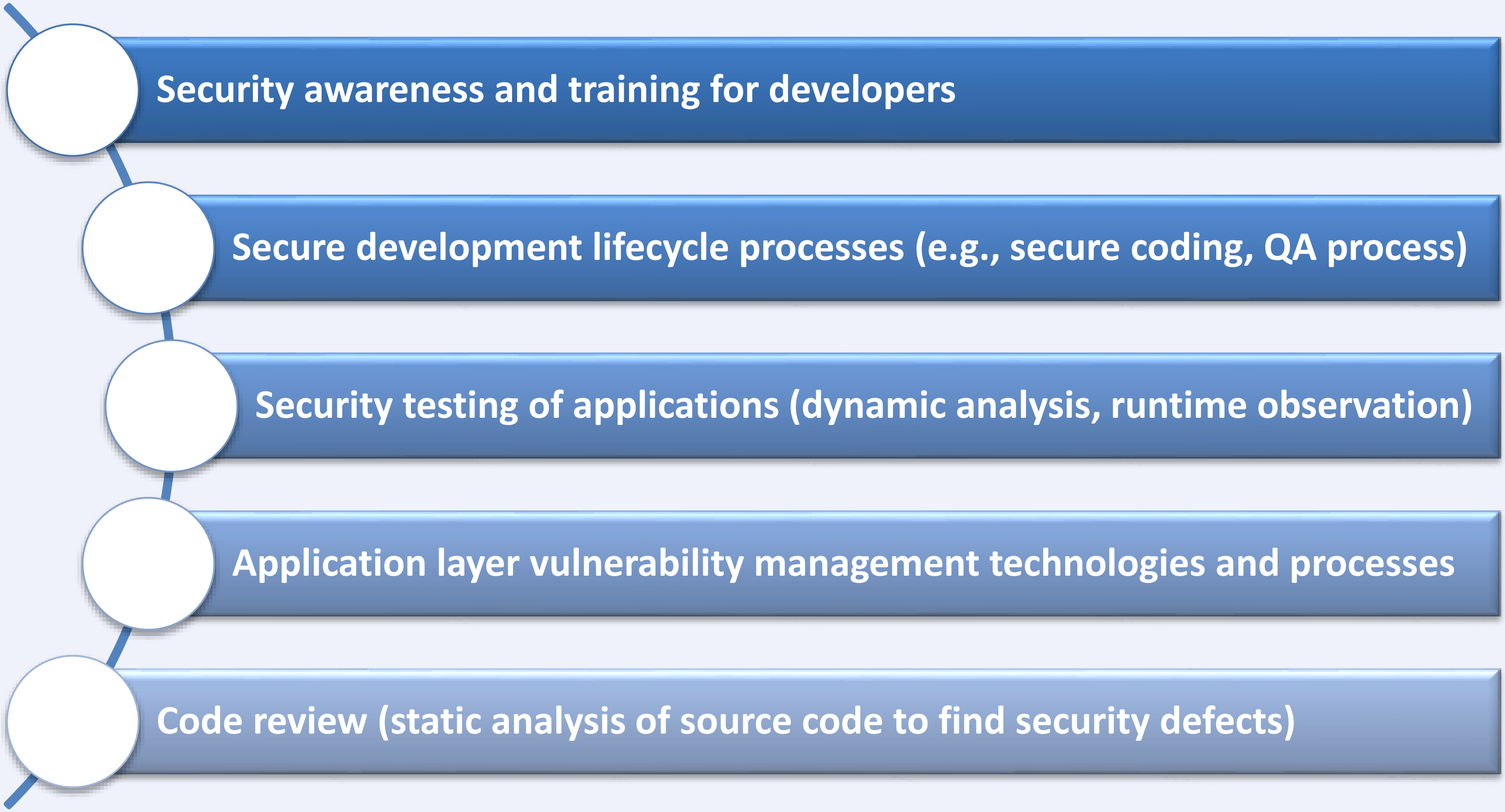
CISO Survey & Report: Investments in Security

OWASP
The Open Web Application Security Project



OWASP
The Open Web Application Security Project

- Top application security priorities for the coming 12 months.



Security awareness and training for developers

Secure development lifecycle processes (e.g., secure coding, QA process)

Security testing of applications (dynamic analysis, runtime observation)

Application layer vulnerability management technologies and processes

Code review (static analysis of source code to find security defects)

CISO Survey & Report 2013: Security Strategy

- Security Strategy:
  - **Only 27% believe their current application security strategy adequately addresses the risks** associated with the increased use of social networking, personal devices, or cloud
  - Most organisations define the strategy for 1 or 2 years:

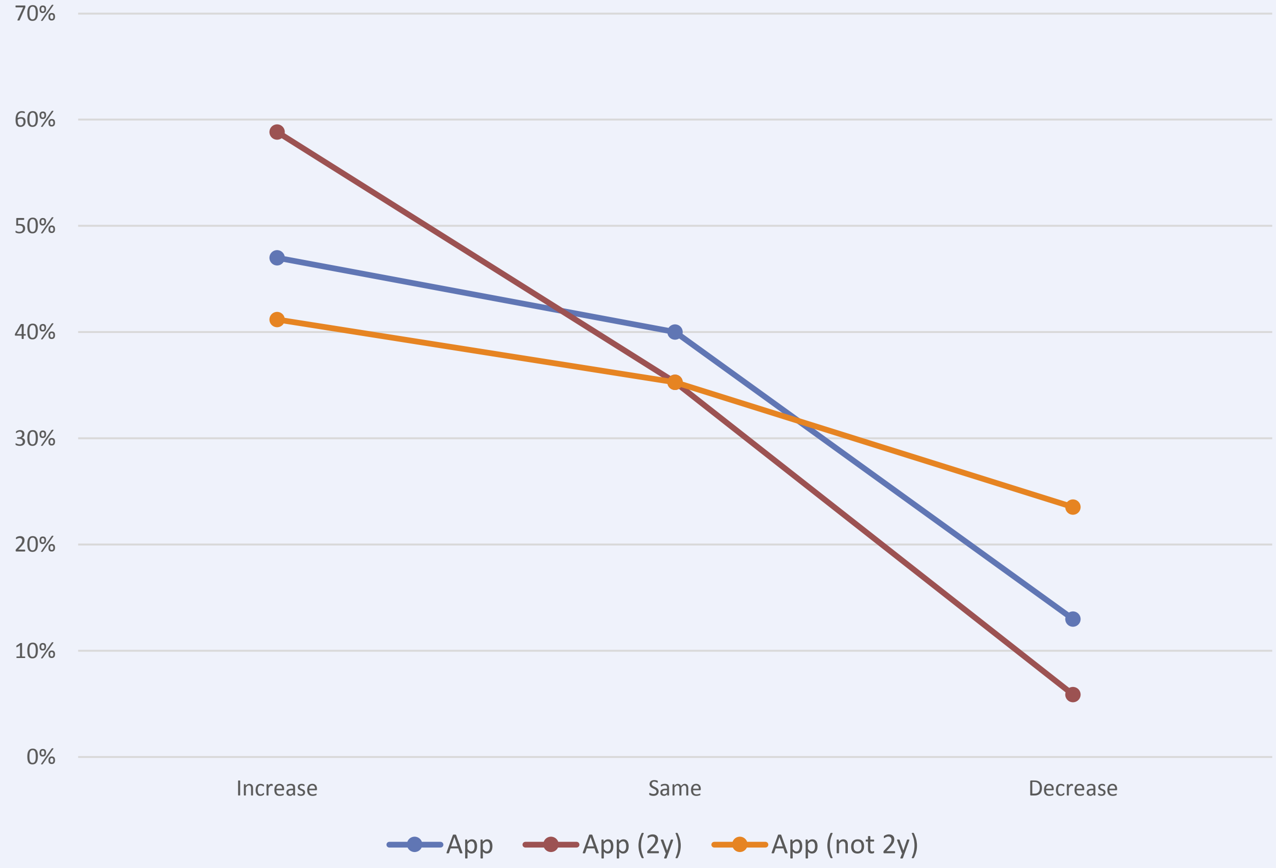
Time Horizon	Percent
3 months	9.3%
6 months	9.3%
1 year	37.0%
2 years	**27.8%**
3 years	11.1%
5 years+	5.6%

CISO Survey & Report 2013: Security Strategy

OWASP
The Open Web Application Security Project

•Benefits of a security strategy for application security investments:

Correlation between investments in Application Security and a 2year Application Security Strategy

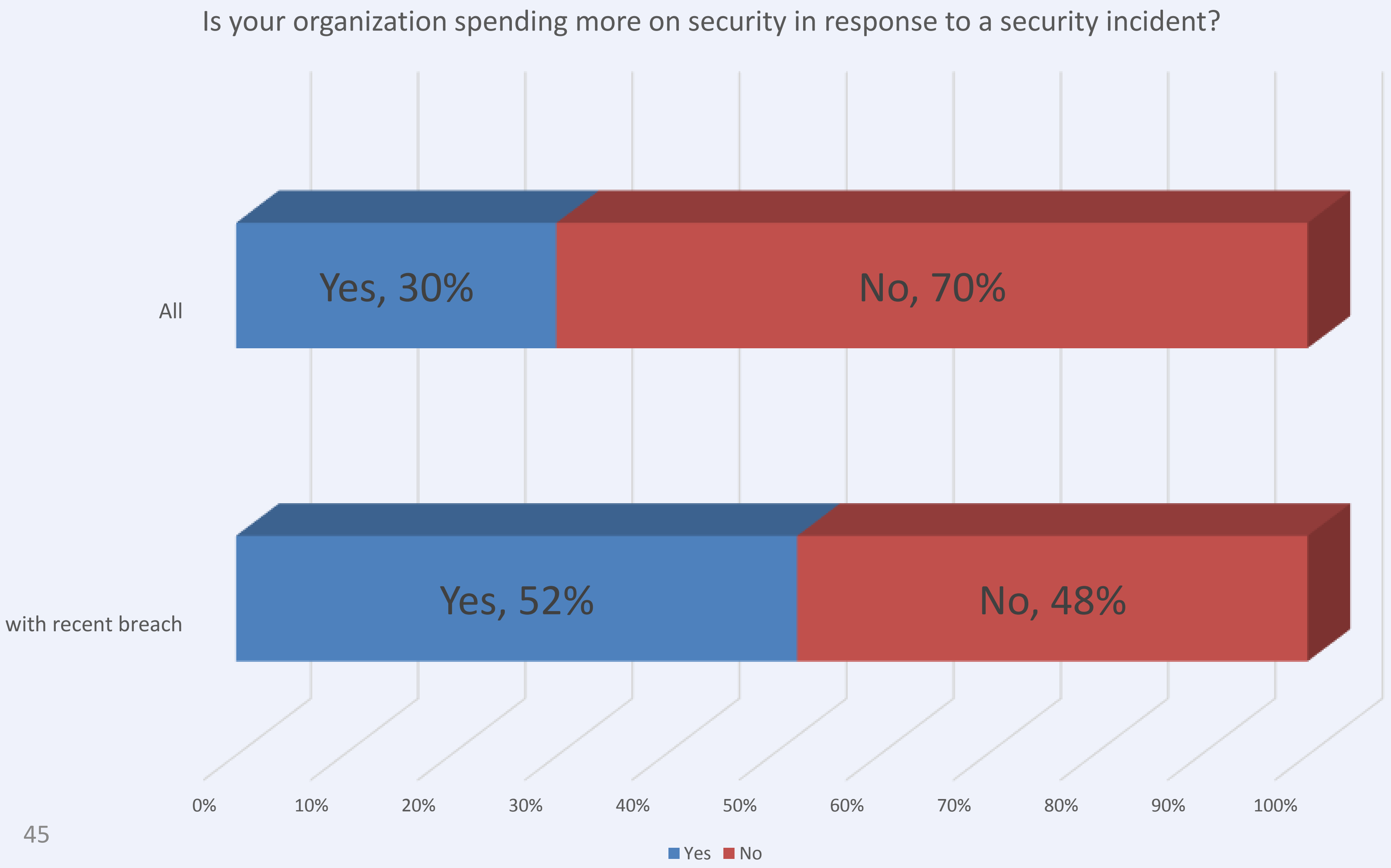


Analysis for correlations with:

- Recent security breach
- Has a ASMS
- Company size
- Role (i.e. CISO)
- Has a Security Strategy
- **Time horizon of security strategy (2 years)**

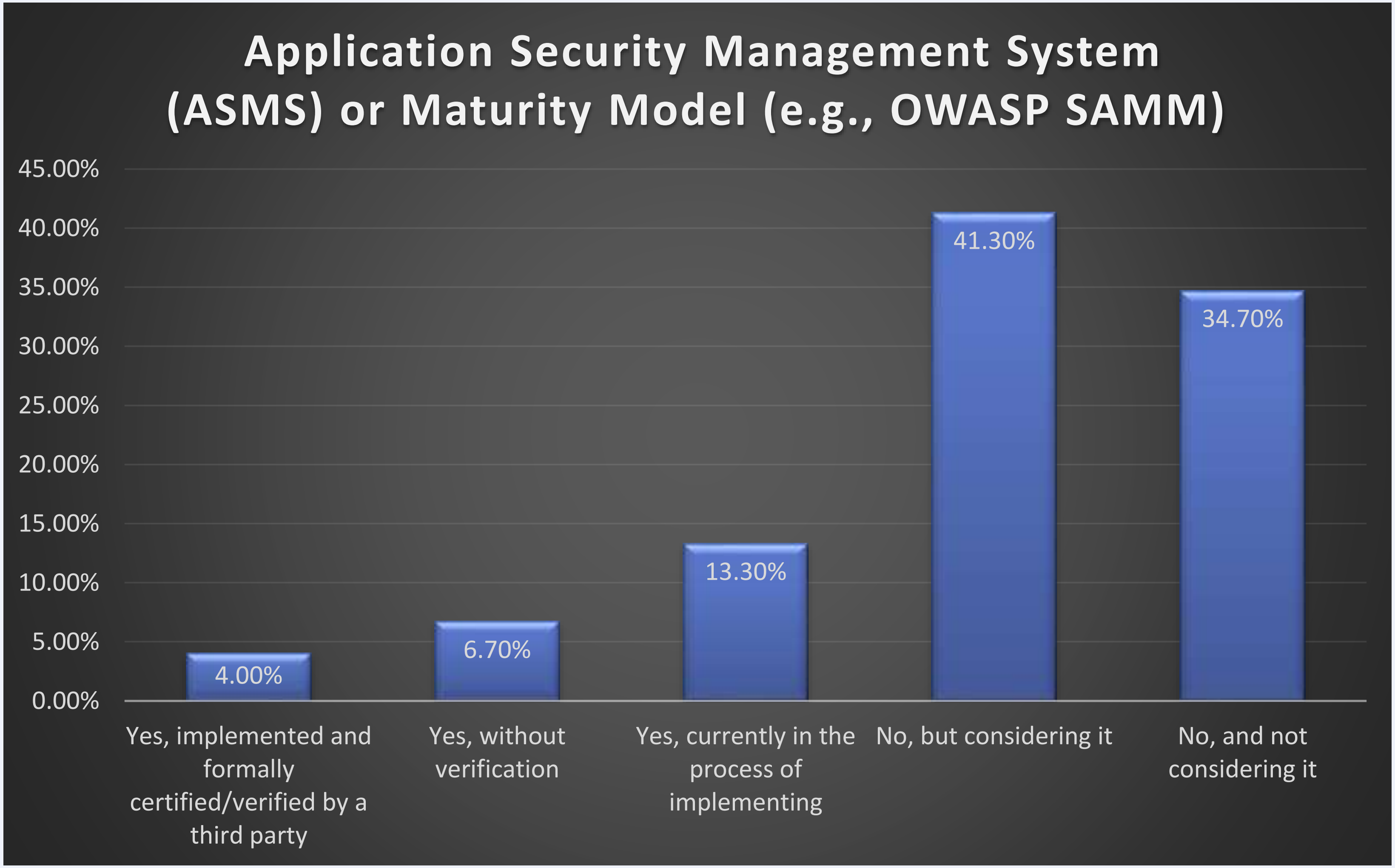
Spending after security incident

OWASP
The Open Web Application Security Project



CISO Survey & Report 2013: ASMS

OWASP
The Open Web Application Security Project



- Top five challenges related to effectively delivering your organization's application security initiatives

- Availability of skilled resources
- Level of security awareness by the developers
- Management awareness and sponsorship
- Adequate budget
- Organizational change

•CISOs found the following OWASP projects most useful for their organizations (note: we did not have a full list of all 160 active projects)

- OWASP Top-10
- Cheatsheets
- Development Guide
- Secure Coding Practices Quick Reference
- Application Security FAQ

Acknowledgements & References

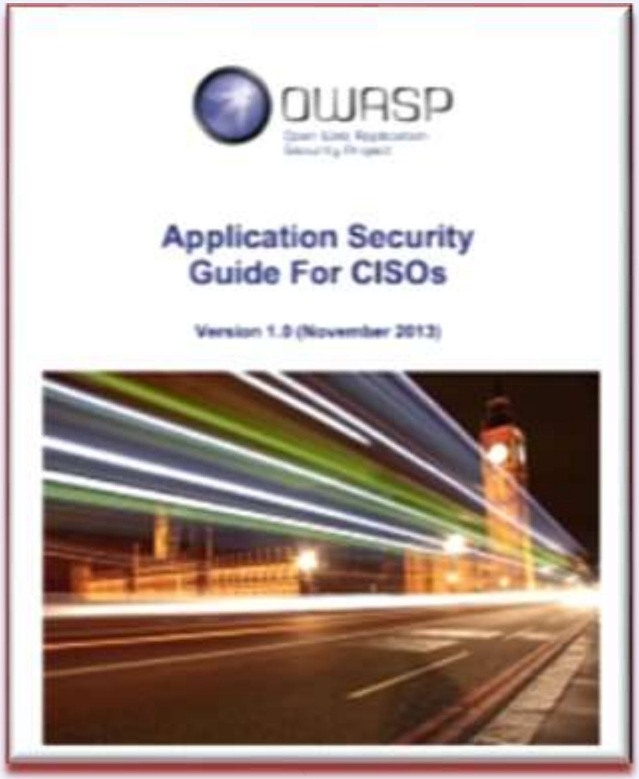
OWASP
The Open Web Application Security Project

OWASP CISO Guide authors, contributors and reviewers:

- Tobias Gondrom
- Eoin Keary
- Any Lewis
- Marco Morana
- Stephanie Tan
- Colin Watson

Further References:

- **OWASP CISO Guide:** https://www.owasp.org/images/d/d6/Owasp-ciso-guide.pdf
- **OWASP CISO Survey:** www.owasp.org/index.php/OWASP_CISO_Survey



OWASP

Application Security Guide For CISOs

Version 1.0 (November 2013)

Register to receive future CISO updates and CISO survey reports

OWASP
The Open Web Application Security Project

Register to receive future updates and survey reports

- to receive only updates about future releases of the OWASP CISO Survey and related CISO projects, you can **register your email address** here: https://docs.google.com/forms/d/1DBYIpWcx6IAZNHOXufdkLZKLIQXetwgbxxd7h_mqWN0/viewform
- **(or in short URL: http://ow.ly/tHeT9)**

(Your contact details will of course be kept strictly confidential and only used to send you updates about new releases of OWASP CISO projects and invitations to participate in the OWASP CISO Survey. And you can of course unsubscribe from this service at any time.)

OWASP
Open Web Application Security Project

CISO Survey and Report 2013

Version 1.0.2 (January 2014)

- 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