



OWASP

Open Web Application  
Security Project

# OWASP SAMM

## Software Assurance Maturity Model

Antonio Fontes

Chapter Meeting - 19 octobre 2015

OWASP Geneva Chapter



# Bio

## Antonio Fontes

*Sécurité et protection des données dans  
les opérations de développement et  
acquisition de logiciels*



L7 Sécurité Sarl, Directeur  
OWASP Suisse, membre du Comité  
OWASP Genève, *co-chapter leader*

sur Twitter: @starbuck3000

# Agenda

- Contexte et problématique
- Présentation de l'outil
- Exemples de rapports
- Opportunités

# Contexte

SAMM adresse la problématique de **qualification du niveau de maturité des actions entreprises à des fins de sécurité** dans les activités d'acquisition et de développement software.

## Scénarios envisagés:

- Développement et exploitation en interne
- Développement externalisé, exploitation interne
- Développement en interne, exploitation dans les nuages sécurisés
- Développement en Inde, hébergement on ne sait pas trop où, maintenance on ne sait pas trop par qui
- Etc.

# Problématique

Trois stratégies principales:

- La stratégie «tests d'intrusion»
- La stratégie «produits» ou «j'achète tout!»
- La stratégie «je fais les choses bien»

La question qui dérange:

- *«Dans quel groupe votre organisation se situe-t-elle?»*

# Problématique

## Des interrogations légitimes:

- Nos tests sont-ils exhaustifs? Suffisants?
- Avons-nous oublié un détail?
- Nos efforts sont-ils judicieusement choisis?
  - Aurions-nous pu investir dans l'activité A au lieu de B?
  - Notre choix est-il légitime?

# Problématique

Quel écart de gouvernance entre A et B?

- Oui. Mais encore?
- Selon quel référentiel?
- Qu'est-ce qui caractérise «catastrophique», «insuffisant», «suffisant», «excellent»?
- Que sais-je sans mes tests d'intrusion?
- Quels systèmes dans mon parc applicatif bénéficient-ils du meilleur contrôle opérationnel?
  - Selon quelle unité? Quelle mesure?



# Problématique

Acheter, acquérir, louer du *software*:

- Comment évaluer, mesurer ou comparer mes fournisseurs?
- Comment communiquer mes attentes à mes fournisseurs?
- Que puis-je demander à mes fournisseurs?
  - «*L'option sécurité, vous nous la facturez combien?*»
  - «*On va revenir vers vous avec une offre!*»



# Problématique

## Communiquer avec l'exécutif:

- Comment rassurer la Direction?
  - «Faites-vous autre chose que des tests d'intrusion?»
- Quel référentiel ou modèle adopter pour communiquer?

# Problématique

## Environnements hétérogènes:

### – Parcs applicatifs complexes:

- Fournisseurs multiples, dispersés, de maturité variable
- Environnements et technologies divers
- Cycles de développement à itération courtes: quid du test d'intrusion sur la release 372?
- Etc.

# Problématique

## Priorisation des efforts:

- Dans quoi investir?
- Pourquoi? Selon qui?

# SAMM



*Defender  
Project*



# SAMM: S... A... M... M...?

- Software Assurance Maturity Model
- Traduction: *Modèle de maturité d'assurance logicielle*

# Auteurs du projet

## **ACKNOWLEDGEMENTS**

The Software Assurance Maturity Model (SAMM) was originally developed, designed, and written by Pravir Chandra (chandra@owasp.org), an independent software security consultant. Creation of the first draft was made possible through funding from Fortify Software, Inc. This document is currently maintained and updated through the OpenSAMM Project led by Pravir Chandra. Since the initial release of SAMM, this project has become part of the Open Web Application Security Project (OWASP). Thanks also go to many supporting organizations that are listed on back cover.

## **CONTRIBUTORS & REVIEWERS**

This work would not be possible without the support of many individual reviewers and experts that offered contributions and critical feedback. They are (in alphabetical order):

Fabio Arciniegas	Brian Chess	Matteo Meucci	John Steven
Matt Bartoldus	Dinis Cruz	Jeff Payne	Chad Thunberg
Sebastien Deleersnyder	Justin Derry	Gunnar Peterson	Colin Watson
Jonathan Carter	Bart De Win	Jeff Piper	Jeff Williams
Darren Challey	James McGovern	Andy Steingruebl	



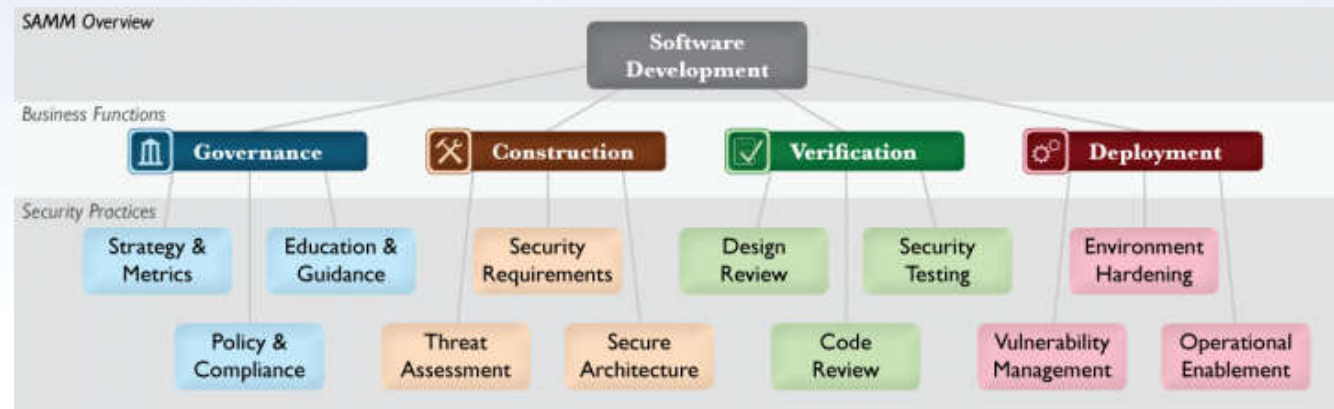
# SAMM: comment cela se présente-t-il?

- Document téléchargeable (gratuit):  
<https://www.owasp.org/index.php/SAMM>
- Ou imprimable (payant):  
<http://www.lulu.com/shop/opensamm-project/software-assurance-maturity-model-samm-bw/paperback/product-4749935.html>
- 95 pages
- Anglais, Espagnol, Japonais, Allemand



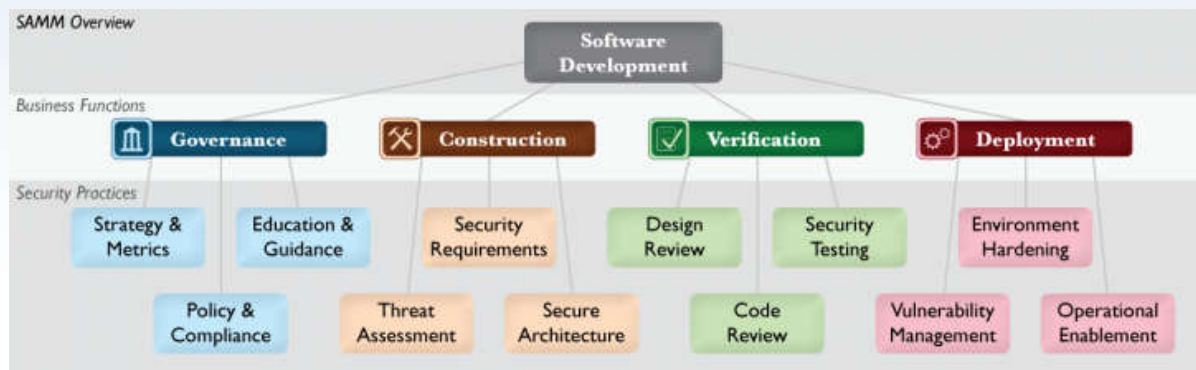
# SAMM: un processus simple

- 3 étapes:
  - J'évalue mes dispositifs de développement/achat
  - J'identifie mon «niveau de maturité» recherché
  - Je formalise un plan d'action



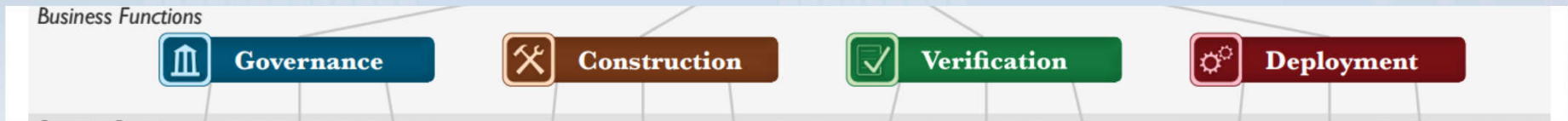
# SAMM: organisation du modèle

- 3 niveaux:
  - *Pôle Direction des développements / acquisitions*
  - *Pôle Fonctions métier*
  - *Pôle Activités de sécurité*



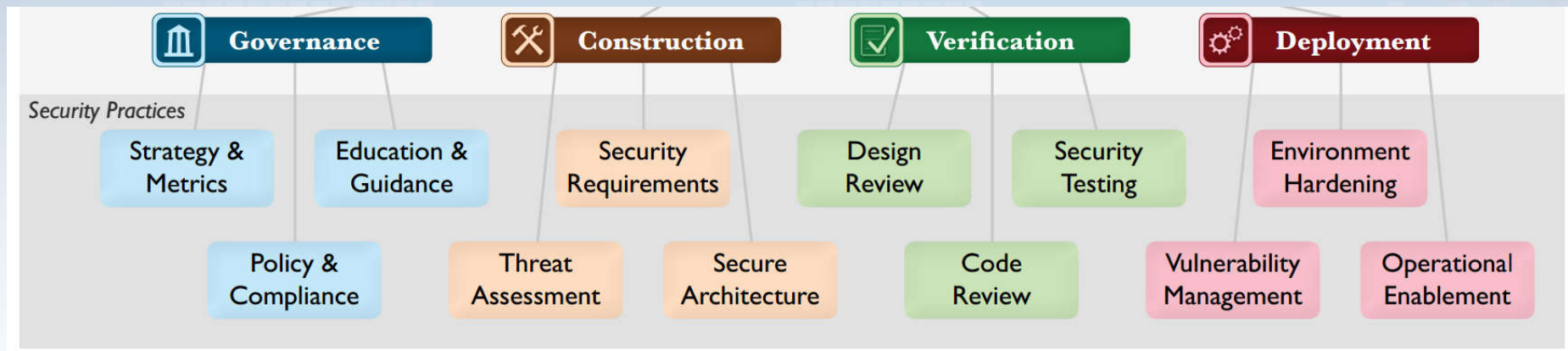
# SAMM: organisation du modèle

- 4 fonctions métier:






# SAMM: organisation du modèle

- 12 activités de sécurité:



# SAMM: organisation du modèle




- 3(4) niveaux de maturité par activité:

Threat Assessment <span>...more on page 46</span>			
	 TA 1	 TA 2	 TA 3
<b>OBJECTIVE</b>	Identify and understand high-level threats to the organization and individual projects	Increase accuracy of threat assessment and improve granularity of per-project understanding	Concretely tie compensating controls to each threat against internal and third-party software
<b>ACTIVITIES</b>	<b>A.</b> Build and maintain application-specific threat models <b>B.</b> Develop attacker profile from software architecture	<b>A.</b> Build and maintain abuse-case models per project <b>B.</b> Adopt a weighting system for measurement of threats	<b>A.</b> Explicitly evaluate risk from third-party components <b>B.</b> Elaborate threat models with compensating controls



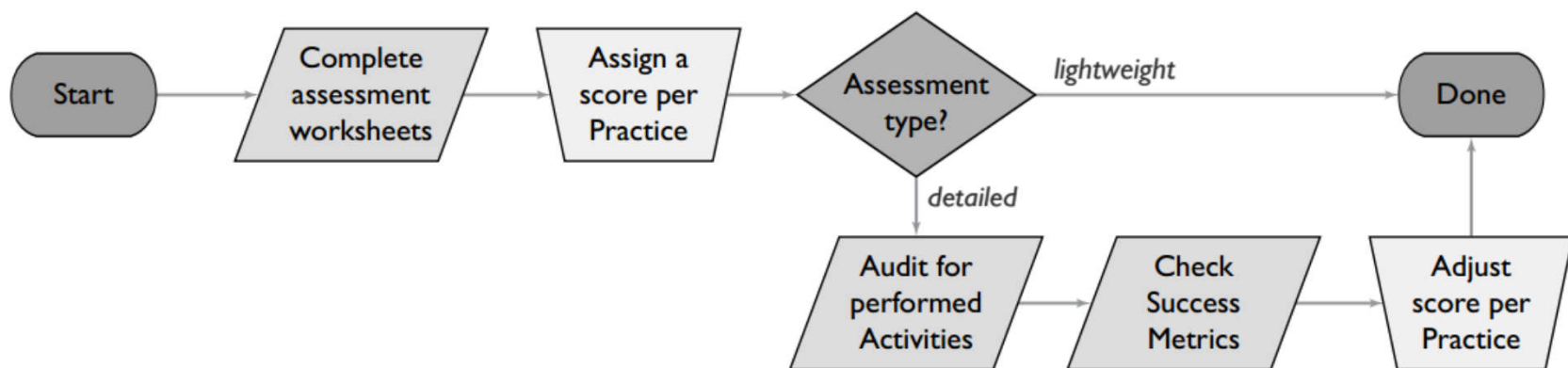
# SAMM: organisation du modèle

- 3(4) niveaux de maturité par activité:

Design Review <span>...more on page 58</span>			
	 DR 1	 DR 2	 DR 3
<b>OBJECTIVE</b>	Support ad hoc reviews of software design to ensure baseline mitigations for known risks	Offer assessment services to review software design against comprehensive best practices for security	Require assessments and validate artifacts to develop detailed understanding of protection mechanisms
<b>ACTIVITIES</b>	A. Identify software attack surface B. Analyze design against known security requirements	A. Inspect for complete provision of security mechanisms B. Deploy design review service for project teams	A. Develop data-flow diagrams for sensitive resources B. Establish release gates for design review

# SAMM: évaluation d'une organisation




- Méthode à choix: accélérée (*lightweight assessment*) ou approfondie (*detailed assessment*):








# SAMM: évaluation d'une organisation

- Guides d'évaluation:

Threat Assessment	Yes/No	
◆ Do most projects in your organization consider and document likely threats?		
◆ Does your organization understand and document the types of attackers it faces?		
◆ Do project teams regularly analyze functional requirements for likely abuses?		 TA 1
◆ Do project teams use a method of rating threats for relative comparison?		
◆ Are stakeholders aware of relevant threats and ratings?		
◆ Do project teams specifically consider risk from external software?		 TA 2
◆ Are all protection mechanisms and controls captured and mapped back to threats?		 TA 3

# SAMM: évaluation d'une organisation

- Guides d'évaluation:

Design Review	Yes/No
◆ Do project teams document the attack perimeter of software designs?	
◆ Do project teams check software designs against known security risks?	
◆ Do most project teams specifically analyze design elements for security mechanisms?	 DR 1
◆ Are most project stakeholders aware of how to obtain a formal design review?	 DR 2
◆ Does the design review process incorporate detailed data-level analysis?	
◆ Does routine project audit require a baseline for design review results?	 DR 3

# Modèles de maturité par industries

## Financial Services Organization

Roadmap template



### RATIONALE

A Financial Services Organization involves the core business function of building systems to support financial transactions and processing. In general, this implies a greater concentration of internal and back-end systems that interface with disparate external data providers.

Initially, effort is focused on improving the Practices related to Governance since these are critical services that set the baseline for the assurance program and help meet compliance requirements for the organization.

Since building secure and reliable software proactively is an overall goal, Practices within Construction are started early on and ramped up sharply as the program matures.

Verification activities are also ramped up smoothly over the course of the roadmap to handle legacy systems without creating unrealistic expectations. Additionally, this helps ensure enough cycles are spent building out more proactive Practices.

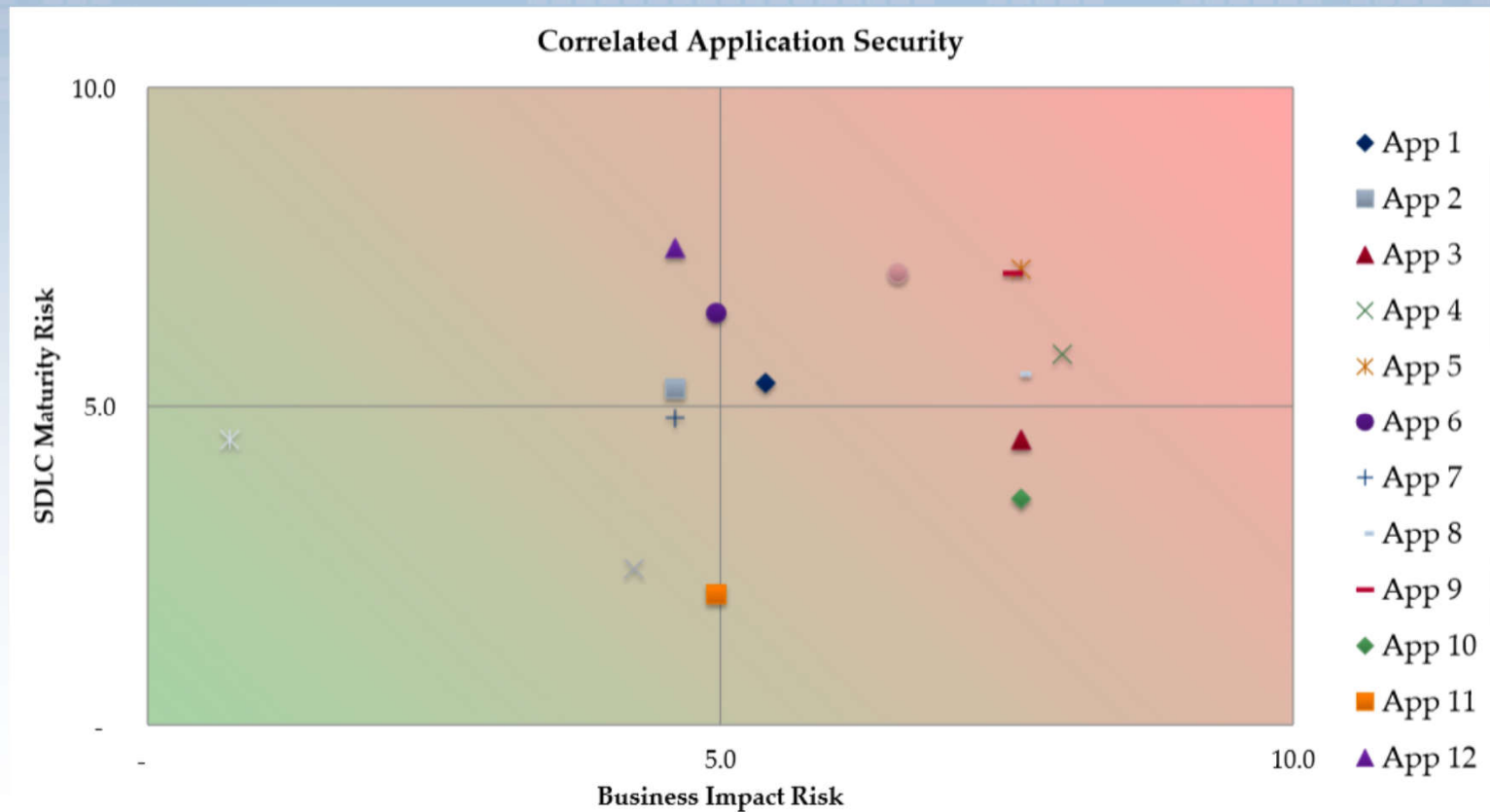
Since a financial services organization often operates the software they build, focus is given to the Practices within Deployment during the middle of the roadmap after some initial Governance is in place but before heavy focus is given to the proactive Construction Practices.

# Piloter en se basant sur SAMM

	Application 1	Application 2	Application 3	Application 4	Application 5	Application 6
Governance: Strategy & Metrics	0+	2+	0+	0+	0+	0+
Governance: Policy & Compliance	0+	1+	0+	0+	0+	0+
Governance: Education & Guidance	0+	2	2+	2+	2+	2+
Construction: Threat Assessment	0+	1+	1+	0+	1+	1+
Construction: Security Requirements	0	2+	0+	0+	1+	0+
Construction: Security Architecture	1+	2	1+	1+	1+	1+
Verification: Design Review	1+	0+	1+	0+	1	0+
Verification: Code Review	1	2	3	1+	0+	3
Verification: Security Testing	1+	1+	1+	0+	1+	0+
Deployment: Vulnerability Management	1+	2+	1+	1+	1+	1+
Deployment: Environment Hardening	0	2	0+	0	0	0+
Deployment: Operational Enablement	0	2	0+	0+	0+	0+

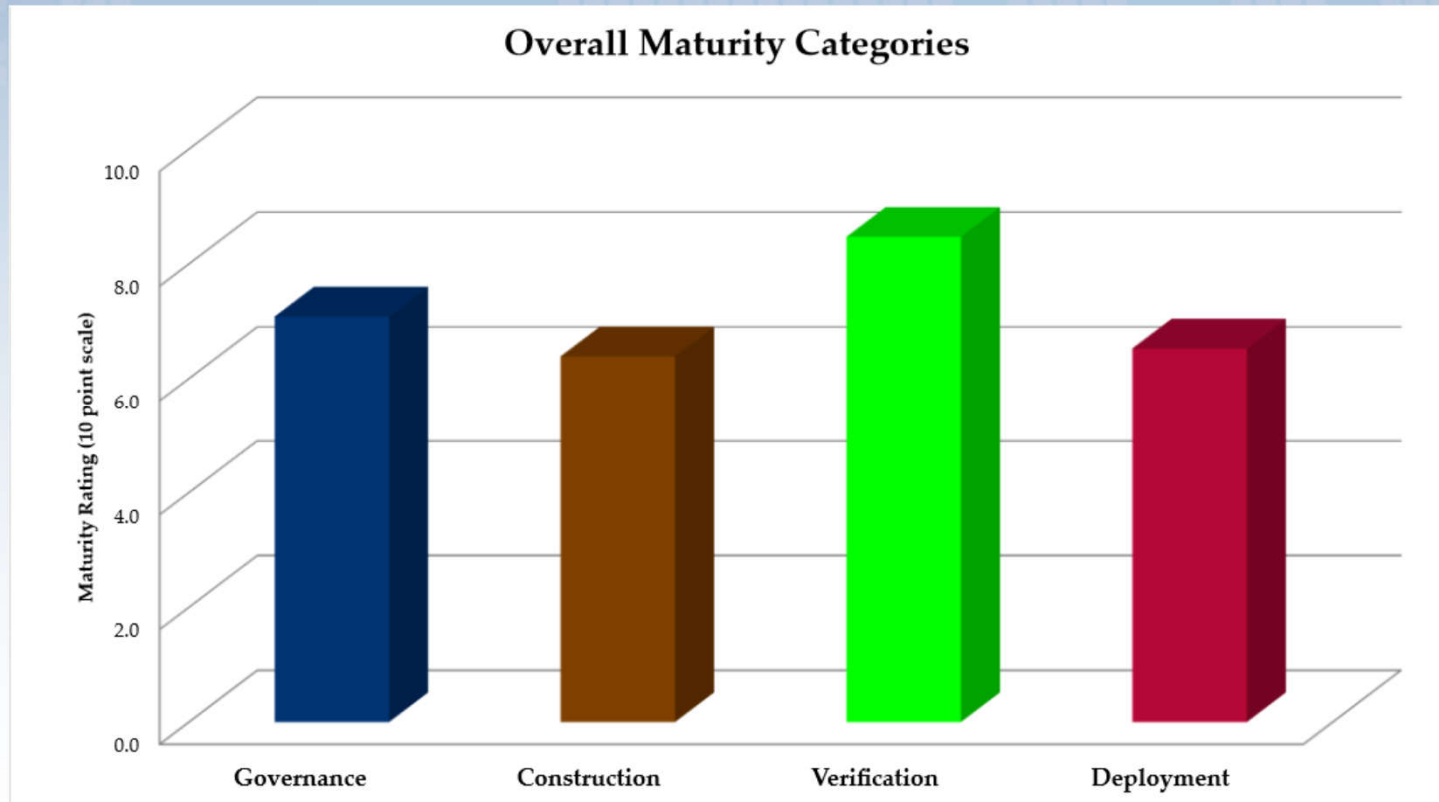
Source: Yan Kravchenko

# Piloter en se basant sur SAMM



Source: Yan Kravchenko

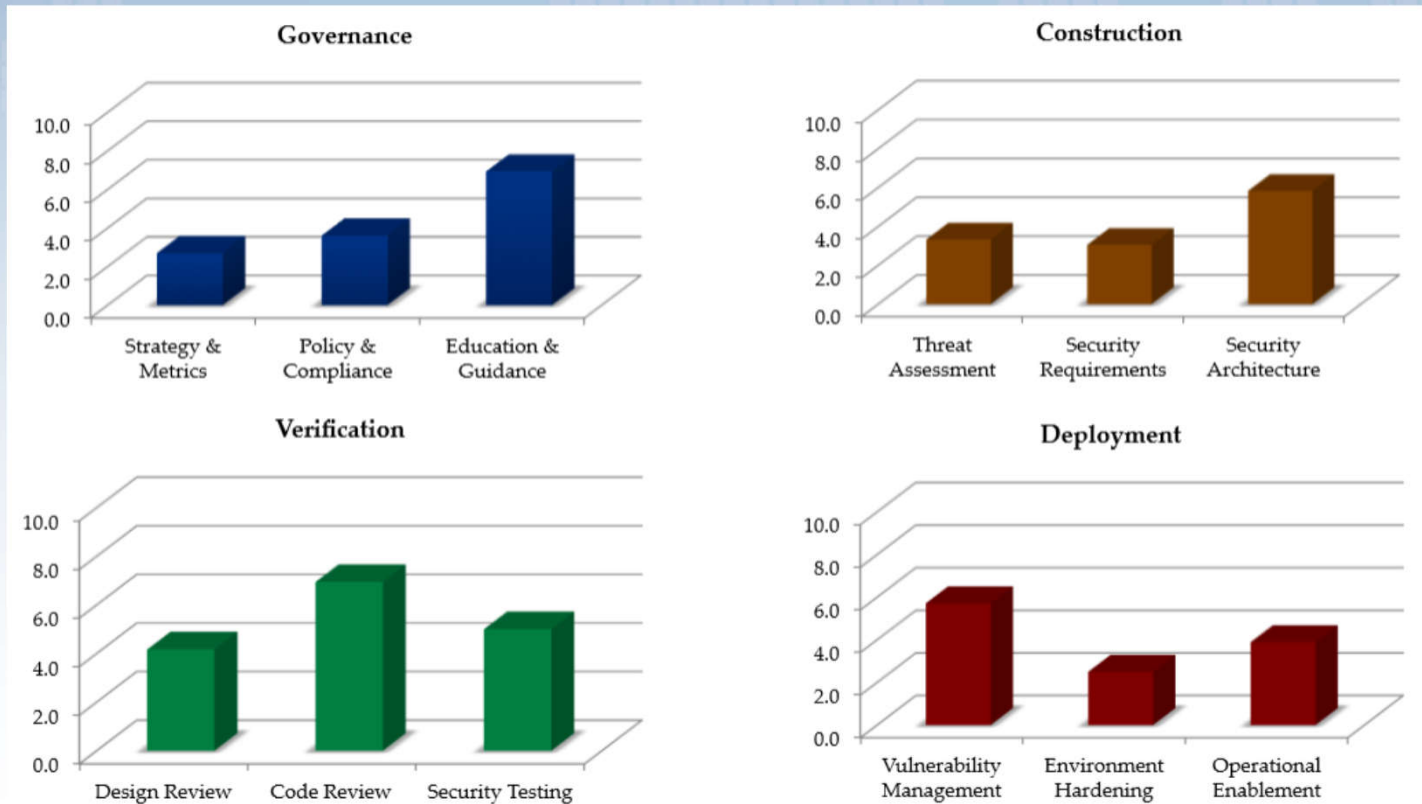
# Piloter en se basant sur SAMM



Source: Yan Kravchenko



# Piloter en se basant sur SAMM



Source: Yan Kravchenko



# Piloter en se basant sur SAMM

**OpenSAMM** Home BU Summary Assessments About Contact Maintenance ▾ Hello, Michael Craigue

## Cyber Security announces its new OpenSAMM Assessment Tool!

The HP Product Security Workgroup has chosen OWASP's Software Assurance Maturity Model (OpenSAMM) to measure the maturity of HP's software development processes. These assessments will help product development groups identify potential gaps in their security activities. The tool also provides instant feedback on how any software program measures up against both internal HP and industry averages.

### Who can use OpenSAMM

This assessment tool can be used by any team at HP involved in the software development process.

### How to use OpenSAMM

1. To start an assessment, go to the [Assessment](#) page, click on the [Create New Assessment](#) button and enter your information.
2. Answer the questions within each of the four tabs – Governance, Construction, Verification and Deployment.
3. You can save your work for later at any time by using the save button at the bottom of the page; your OpenSAMM score is updated automatically as the answers are populated.
4. When complete, click the Scorecard link to view your results.

### Benefits

The OpenSAMM assessment tool provides a consistent method to evaluate the maturity of your organization's software development processes and offers a solid foundation for further improvement.

### Need more resources?

- [Contact information would go here](#)

*Source: Michael Craigue*

# Outiller SAMM

The screenshot shows the OpenSamm web application interface. The browser address bar displays `http://127.0.0.1/OpenSamm/Assessments`. The application has a blue header with the following navigation links: OpenSamm, Home, BU Summary, Assessments, About, Contact, and Maintenance. The user is logged in as "Hello, Michael Craigue".

The main content area is titled "Assessments" and includes a "Create New Assessment" button. Below this, there are two sections:

- My Assessments**: A table with one entry.

Product Name	Organization	Final	Owner	Updated	Created	Options
Opensamm test			demouser1	2/23/2015	2/23/2015	<a href="#">Details</a>   <a href="#">Delete</a>   <a href="#">Scorecard</a>
- All Other Assessments**: A table with no data.

Product Name	Organization	Final	Owner	Updated	Created	Options
No Assessments Found						

At the bottom left, the copyright notice "© 2015 - OpenSamm" is visible.

*Source: Michael Craigue*

10/19/2015

OWASP Geneva Chapter - SAMM

# Piloter en se basant sur SAMM

OpenSAMM Home BU Summary Assessments About Contact Maintenance ▾ Hello, Michael Craigue

## Assessment

Product Name: **Opensamm test**

Governance Construction Verification Deployment

### Strategy & Metrics Score: 0+

Is there a software security assurance program already in place?	<input checked="" type="checkbox"/>
Do most of the business stakeholders understand your organization's risk profile?	<input checked="" type="checkbox"/>
Is most of your development staff aware of future plans for the assurance program?	<input type="checkbox"/>
Are most of your applications and resources categorized by risk?	<input type="checkbox"/>
Are risk ratings used to tailor the required assurance activities?	<input checked="" type="checkbox"/>
Does most of the organization know about what's required based on risk ratings?	<input type="checkbox"/>
Is per-project data for cost of assurance activities collected?	<input type="checkbox"/>
Does your organization regularly compare your security spend with other organizations?	<input checked="" type="checkbox"/>

### Policy & Compliance Score: 0+

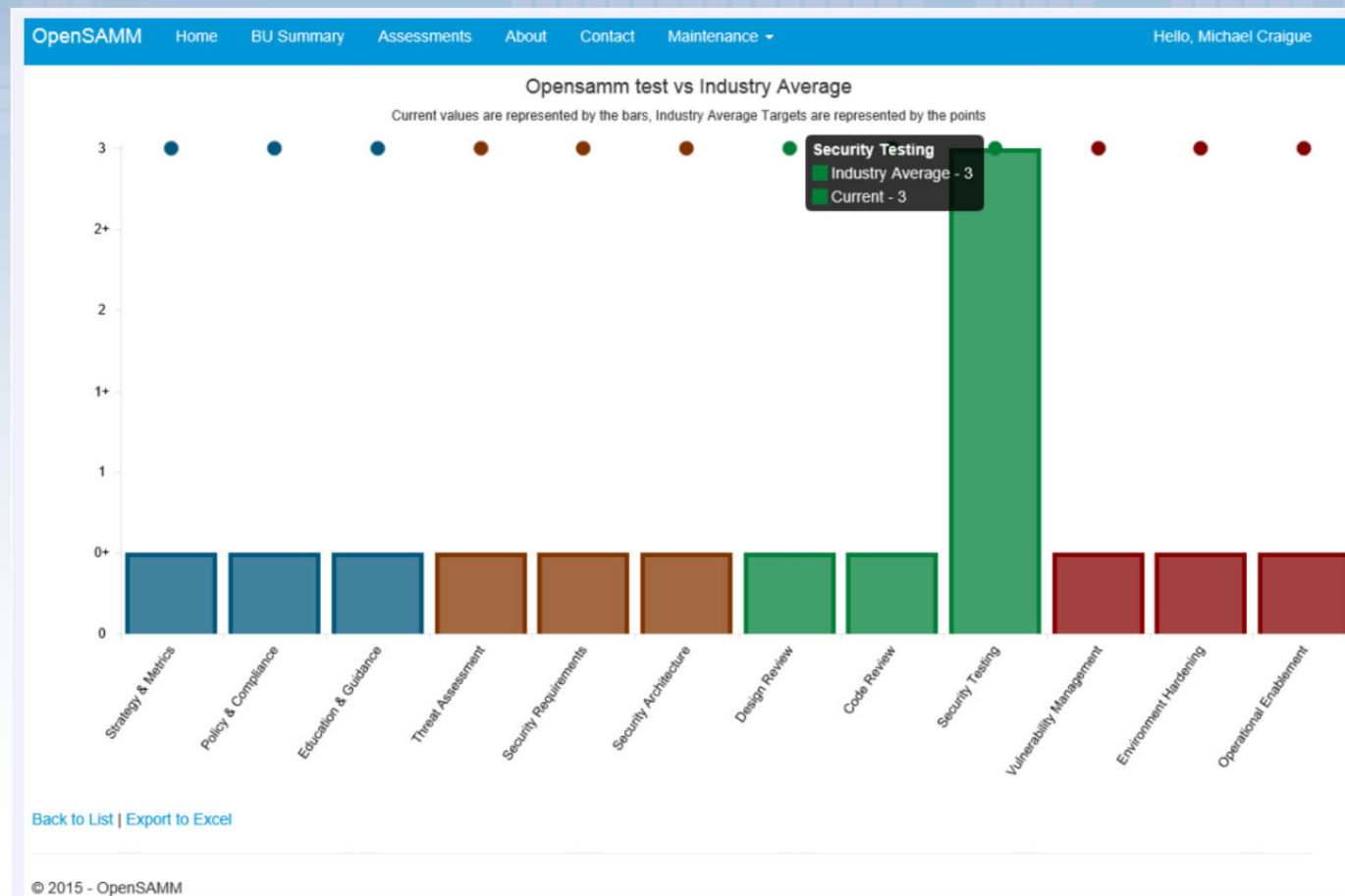
Do most project stakeholders know their project's compliance status?	<input checked="" type="checkbox"/>
Are compliance requirements specifically considered by project teams?	<input type="checkbox"/>

*Source: Michael Craigue*

10/19/2015

OWASP Geneva Chapter - SAMM

# Piloter en se basant sur SAMM



Source: Michael Craigue

10/19/2015

OWASP Geneva Chapter - SAMM

# Points forts de SAMM

- Langage simple, «coût technique» faible
- C'est un modèle, il n'est pas nécessaire de le respecter à la lettre
- Référentiel en adoption croissante
- Agnostique:
  - Compatible toutes opérations de développement/acquisition
  - Le pilotage peut être soutenu par du software

# Adoption/sponsors de SAMM

- Bloomberg
- Dell
- Denim Group
- Elavon / Bancorp
- Fortify
- Gotham Digital Science
- HP
- ING
- JTI
- Kimberly-Clark
- McAfee
- PwC
- SITA
- Toreon
- Whitehat Security
- ...

# Historique - Evolutions

- Publication originale: 2004, version 1
  - Inchangée depuis
  - Nombreux outils publiés par la communauté (feuilles Excel, etc.)
- En cours d'édition:
  - Version 1.1 en cours de finalisation (SAMM Summit (Dublin, 27 mars 2015))



# Questions?

# ?

antonio.fontes@L7s.ch  
@starbuck3000

Merci.

# Liens

Projet SAMM

<https://www.owasp.org/index.php/SAMM>

Téléchargement (en Anglais):

<https://www.owasp.org/images/c/c0/SAMM-1.0.pdf>

Présentation par Yan Kravchenko (*App Security? Is there a metric for that?*)

[https://www.owasp.org/images/2/21/OpenSAMM\\_App\\_Prioritization\\_Overview\\_v3.pdf](https://www.owasp.org/images/2/21/OpenSAMM_App_Prioritization_Overview_v3.pdf)

Présentation par Michael Craigue (OpenSAMM at HP)

[https://www.owasp.org/images/b/b1/OpenSAMM\\_March\\_2015\\_Michael\\_Craigue\\_HP\\_Final.pdf](https://www.owasp.org/images/b/b1/OpenSAMM_March_2015_Michael_Craigue_HP_Final.pdf)