TRAINING KIT – SSDLC1

Secure Software Development Live Cycle

EXCELLIUM

Your first call when it comes to IT and Security!

March 16, 2017

TLP: WHITE

Agenda

EXCELLIUM
Your first call when it comes to IT and Security!

- **Introduction**
  - Some basic questions
  - What is a Secure Software Development Life Cycle ?
  - Purpose
  - Benefits
- **How setup a SSDLC**
  - Overview of OWASP Open SAMM
  - Why use this referential to define my SSDLC ?
  - How use Open SAMM ?
- **Practical example**
  - Select “Security Practices” according to my business
  - Define a roadmap
  - Focus on “Verification” business function

Introduction: Some basic questions...

EXCELLIUM
Your first call when it comes to IT and Security!

How do you code ?

Introduction: Some basic questions...

EXCELLIUM
Your first call when it comes to IT and Security!

- When do you include security into your development process ?
  - In business requirement ?
  - In risk analysis ?
  - In software architecture design ?
  - In infrastructure architecture design ?
  - In compliance process (PCI DSS) ?
  - In secure coding ?
  - In vulnerability management ?
  - In hardening ?

Introduction: Some basic questions...

EXCELLIUM
Your first call when it comes to IT and Security!

- But the security in a continuous process...
  - Analysis
  - Design
  - Implementation
  - Maintenance

Introduction: What is a SSDLC ?

EXCELLIUM
Your first call when it comes to IT and Security!

a **S**ecure **S**oftware **D**evelopment **L**ife **C**ycle is a continuous process that contains different steps in order to ensure security level of a software (product / application) according to a referential or laws.

Introduction: What is a SSDLC ?

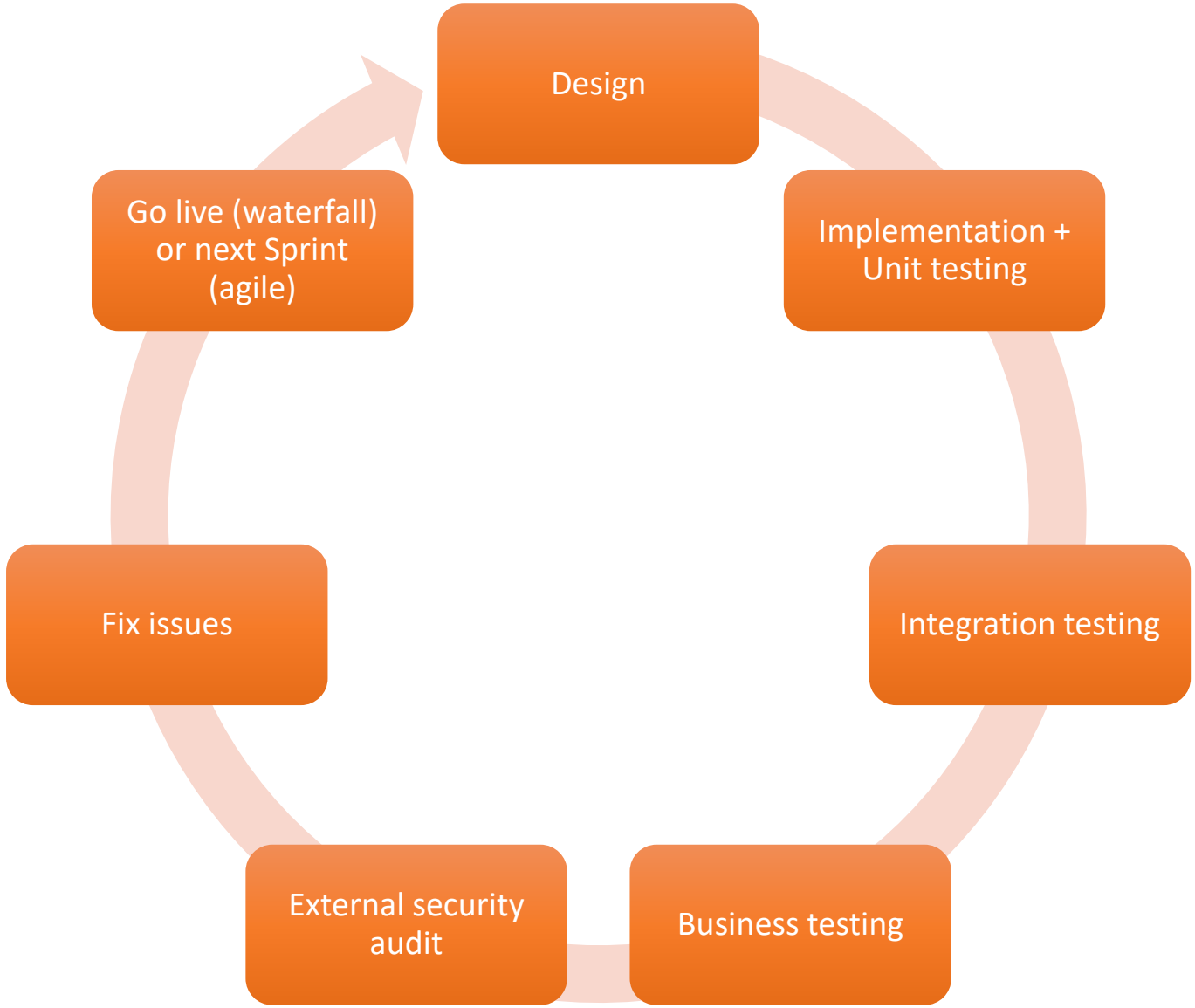
EXCELLIUM
Your first call when it comes to IT and Security!

Most of the time, the

Software Development

Life Cycle looks something

like this →



Introduction: What is a SSDLC ?

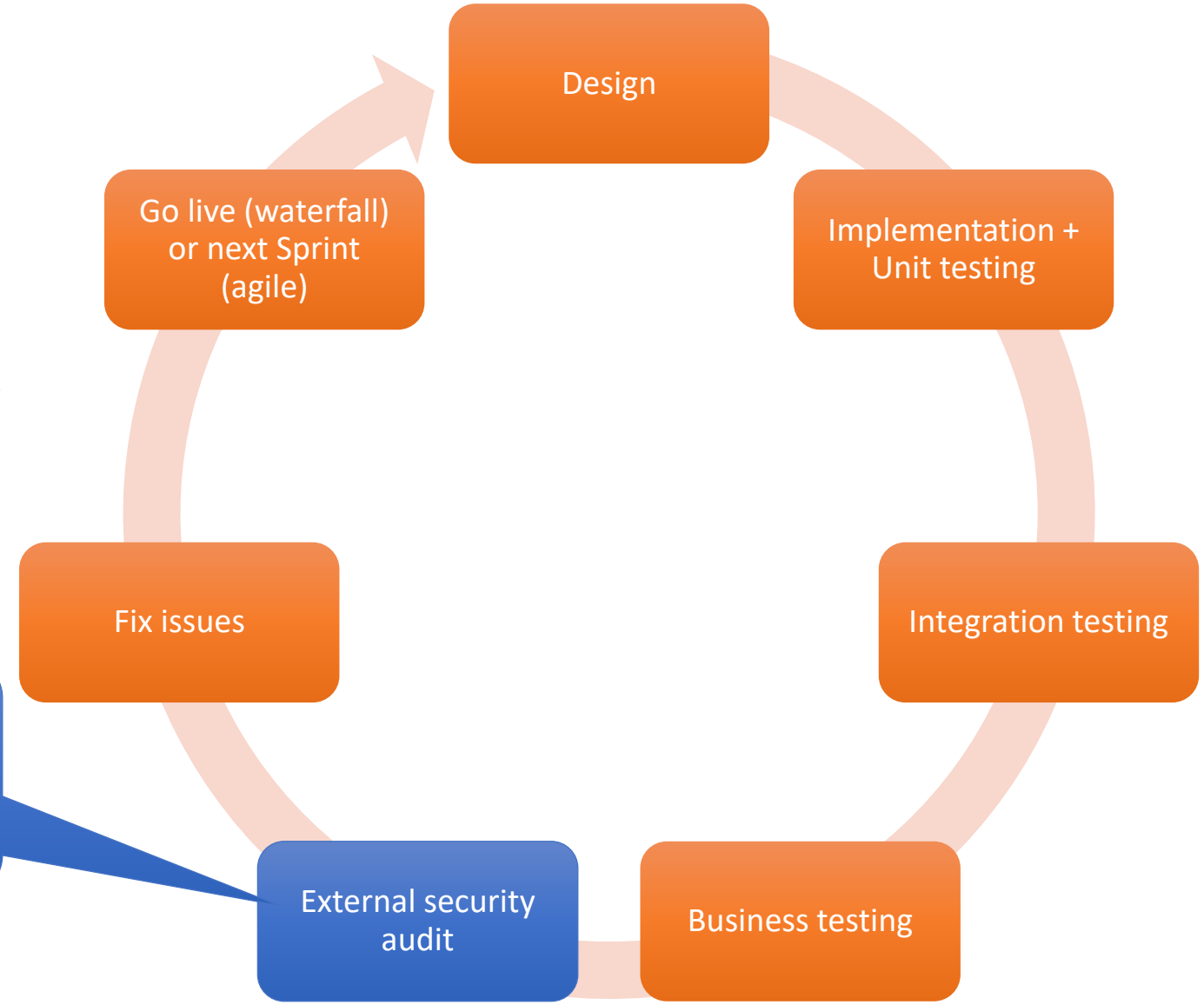
EXCELLIUM
Your first call when it comes to IT and Security!

Most of the time, the

Software Development

Life Cycle looks something

like this →

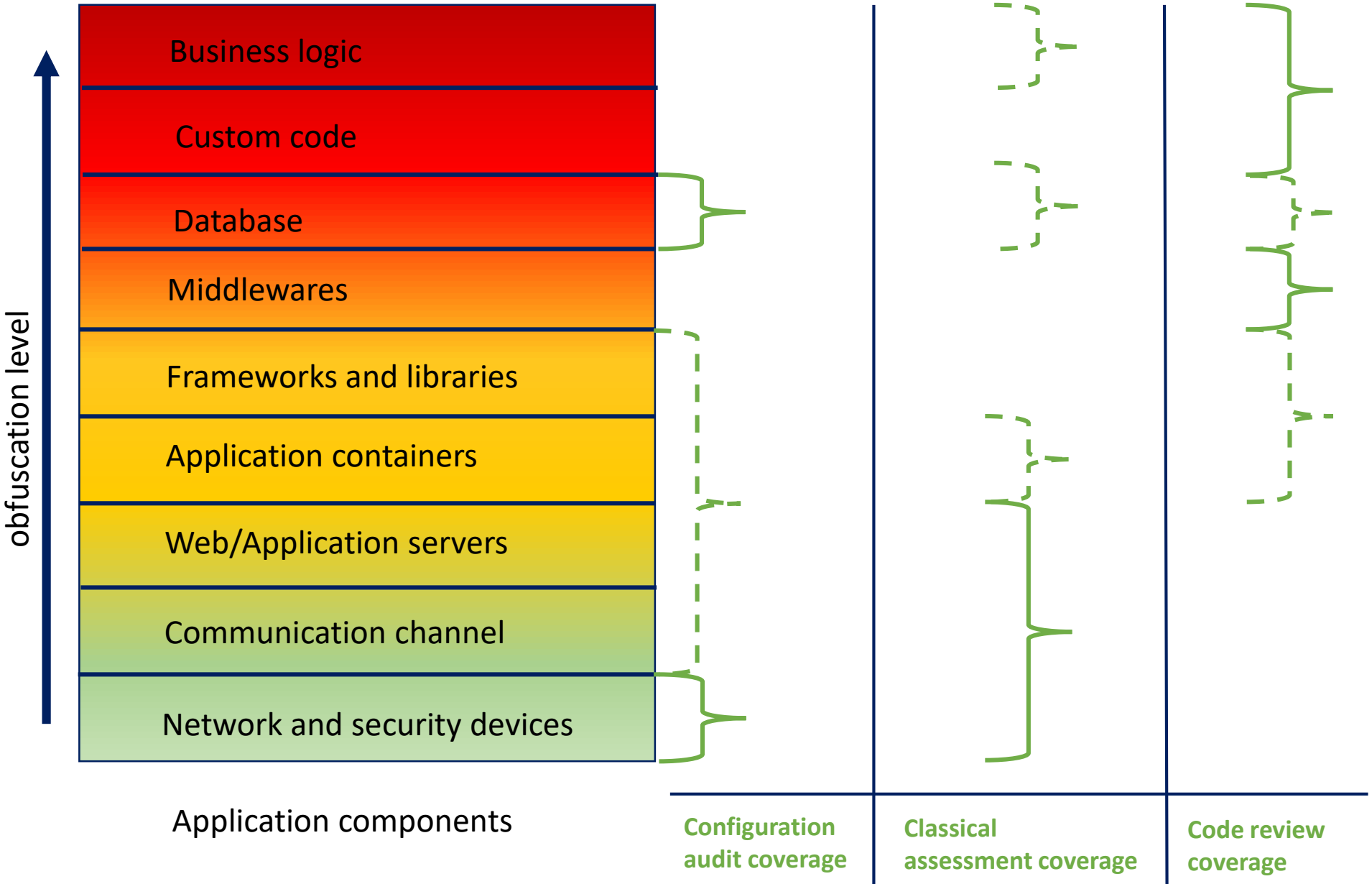


Security validation happen only at process end !

Introduction: What is a SSDLC ?

EXCELLIUM
Your first call when it comes to IT and Security!

Ways to identify threats in applications



Introduction: Purpose

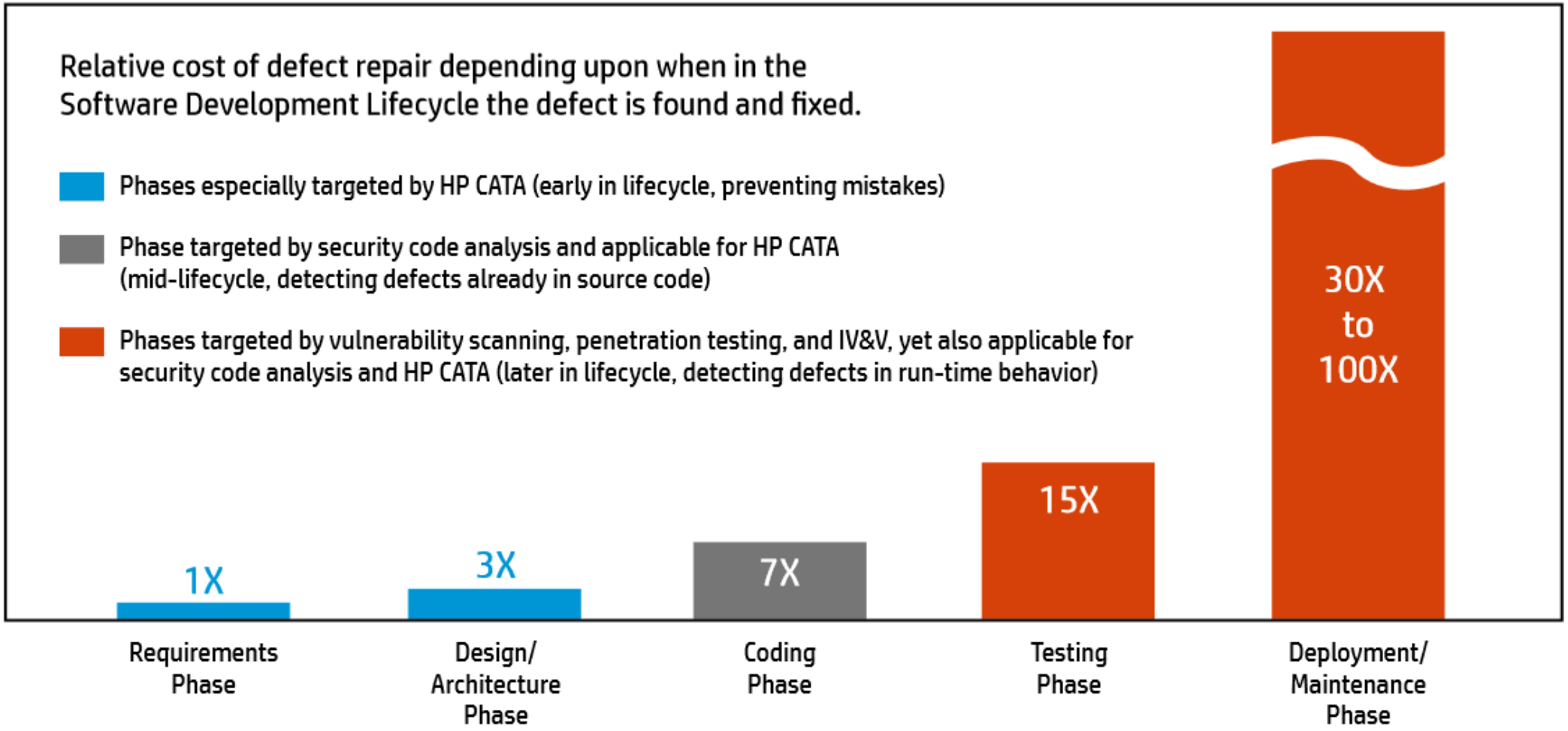
EXCELLIUM
Your first call when it comes to IT and Security!

- Bring security in each key phase of a Software Development Life Cycle
- Avoid unexpected cost at process end due to security issues to fix
- Avoid software development delivery delay due to security issues to fix
- Enable possibility of budgeting cost implied by security enforcement/requirements of a software
- Make visible job done for security enforcement of a software
- Ensure security level regardless of your developer/software provider by imposing your process to them contractually !

Introduction: Purpose

EXCELLIUM
Your first call when it comes to IT and Security!

Cost of Defect Repair



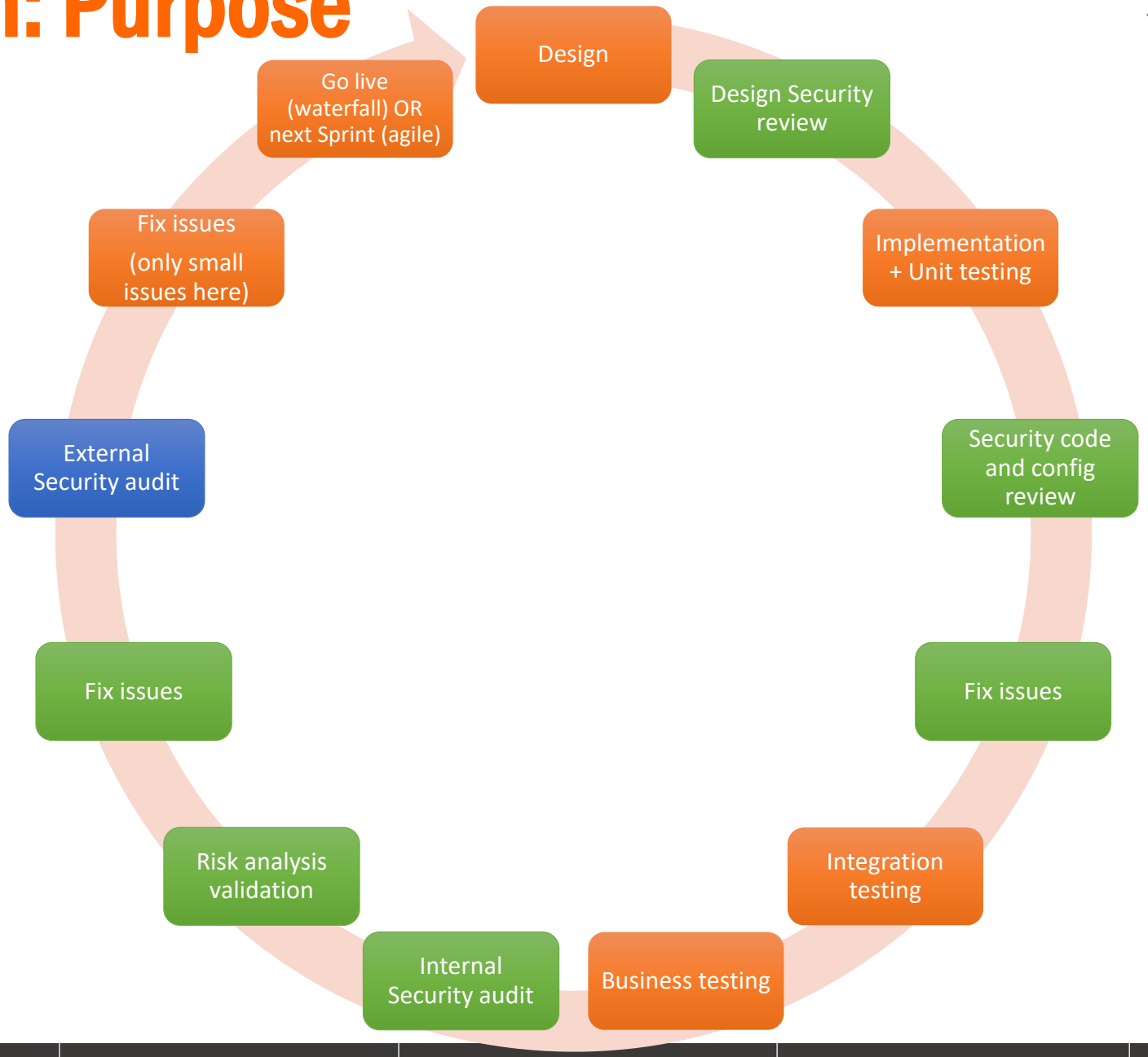
Introduction: Purpose

EXCELLIUM
Your first call when it comes to IT and Security!

Software Development

Life Cycle looks now like

this →



Introduction: Benefits

EXCELLIUM
Your first call when it comes to IT and Security!

- SSDLC allow you to:
  - Avoid cost due to security issues found by users / user's security department after production release → Avoid as much as possible hidden/unexpected cost !
  - Use the security level of your software as a marketing advantage to differentiate your product face to your competitor
  - Minimize risk of compromission and then minimize risk of :
    - Financial penalty (ex: customer sensitive data loss)
    - Reputation issue (ex: disclose of your compromission in media or local market)
    - Lost of Intellectual property (ex: theft of industrial secrets)
  - Reach security level imposed by law (ex: PCI DSS) by explicitly demonstrating your security level to external auditor
  - Measure the quality of your software provider according to the result obtained after being assessed using your SSDLC

Introduction: Benefits

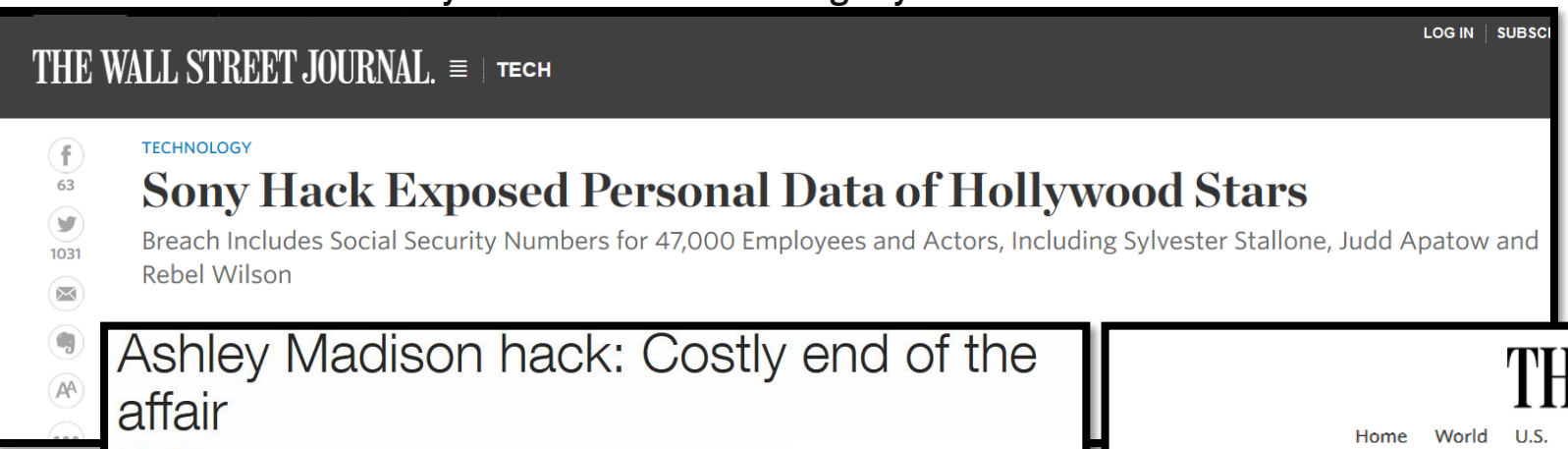
EXCELLIUM
Your first call when it comes to IT and Security!

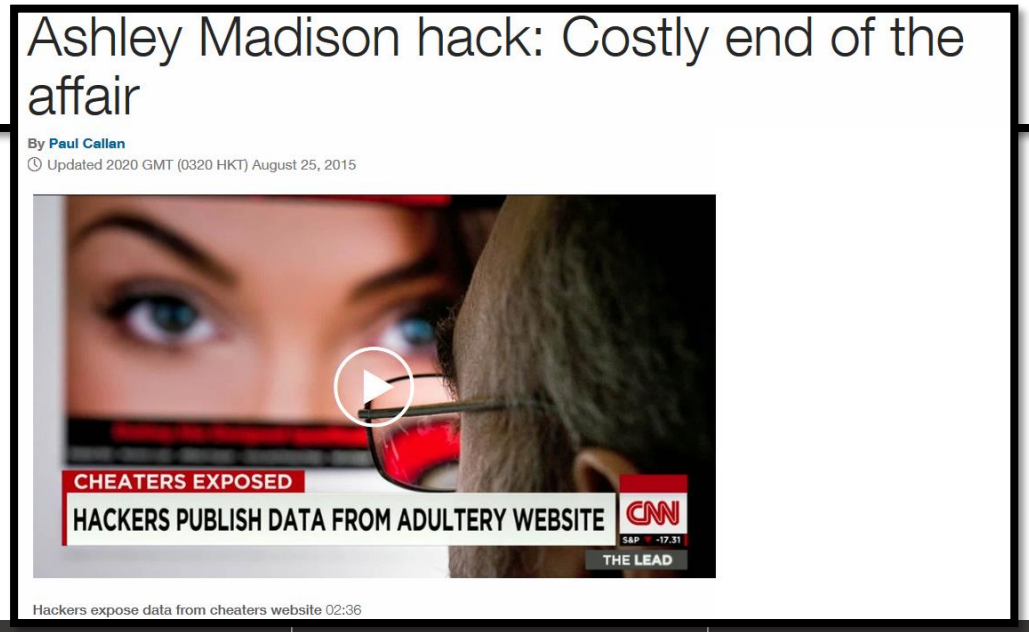
- If the Security is not included in the core of your SDLC:
  - You will face cost due to security issues found by users / user's security department after production release
  - Your competitor can use the security level of your/their software as a marketing advantage to differentiate their product facing yours (ex: Using security vulnerability disclosed into media to base their sales pitch)
  - You will face a higher risk of compromission and then higher risk of Financial penalty, Reputation issue, Lost of Intellectual property (see previous slide for examples)
  - You will face difficulty and additional cost to reach security level imposed by law (ex: PCI DSS) and perhaps financial penalty if you cannot reach the expected level in allowed timeframe of in case of compromission
  - It's will be difficult to measure the quality of your software provider
  - It's will be harder to detect malicious code injected by rogue employee

Introduction: Benefits

EXCELLIUM
Your first call when it comes to IT and Security!

- OK, include the security in the core of your SDLC in order to have a SSDLC have a cost but do you want that media talk about you in this way ? What will be the feeling of your shareholder ?



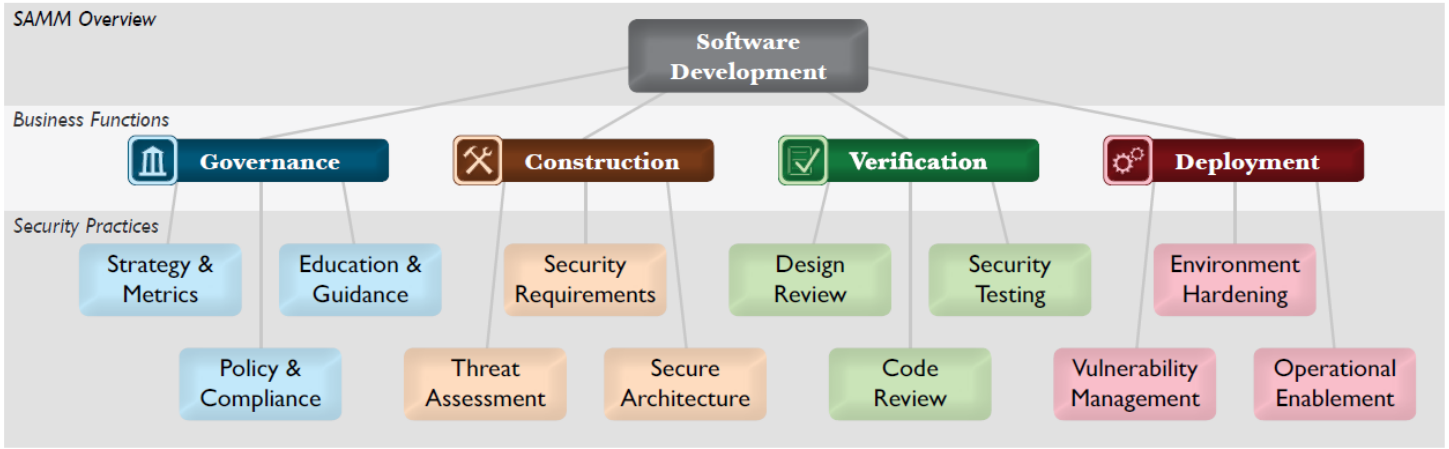


How to setup a SSDLC: OpenSAMM

EXCELLIUM
Your first call when it comes to IT and Security!

The Open Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:

- Evaluating an organization's existing software security practices
- Building a balanced software security assurance program in well-defined iterations
- Demonstrating concrete improvements to a security assurance program
- Defining and measuring security-related activities throughout an organization



How to setup a SSDLC: Why OpenSAMM ?

EXCELLIUM
Your first call when it comes to IT and Security!

- Open SAMM is provided by the OWASP foundation that is recognized as a standard provider in the domain of application security
- As is it Open it don't stick you to a proprietor referential and don't make you dependent of a specific consulting company or group
- The number of company using Open SAMM make you benefits of the practical feedback and update through the guide evolution
- Gartner recognize quality of Open SAMM guide (OK it's not the point that make you decide to use it but it help on marketing side)
- Contains example roadmap and sample to start building a SSDLC with a pragmatic point of view
- Can be read in 1 day (96 pages) and approach is easy to understand
- Easy to spread : Book version cost is 25$ - Pdf version is free
- Available in English / Spanish / Japanese

How to setup a SSDLC: OpenSAMM Pillars

EXCELLIUM
Your first call when it comes to IT and Security!

Open SAMM is based on following pillar:

- "**Business Function**" also called "**Function**" : Category of activities related to the software development
- "**Security Practices**" also called "**Practice**": For each "Business Function", SAMM defines 3 Security Practices.

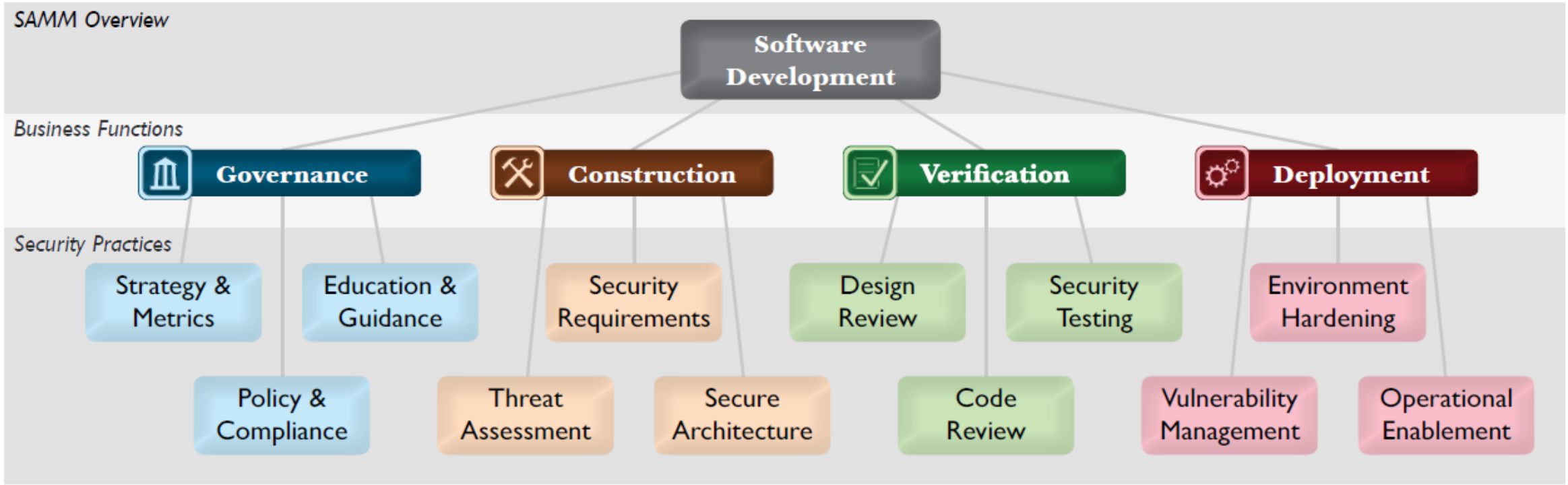
  Each Security Practice is an area of security-related "Activities" that build assurance for the related "Business Function"
- "**Maturity Levels**" also called "**Level**": For each Security Practice, SAMM defines 3 Maturity Levels as

  Objectives. Each Level within a Security Practice is characterized by a successively more sophisticated

  Objective defined by specific activities and more stringent success metrics than the previous level

How to setup a SSDLC: OpenSAMM Pillars

EXCELLIUM
Your first call when it comes to IT and Security!



How to setup a SSDLC: Business functions

EXCELLIUM
Your first call when it comes to IT and Security!

"Business Function" are the following:

- "Governance" : Governance is centered on the processes and activities related to how an organization manages overall software development activities. More specifically, this includes concerns that cross-cut groups involved in development as well as business processes that are established at the organization level.

How to setup a SSDLC: Business functions

EXCELLIUM
Your first call when it comes to IT and Security!

"Business Function" are the following:

- "Construction": Construction concerns the processes and activities related to how an organization defines goals and creates software within development projects. In general, this will include product management, requirements gathering, high-level architecture specification, detailed design, and implementation.

How to setup a SSDLC: Business functions

EXCELLIUM
Your first call when it comes to IT and Security!

"Business Function" are the following:

- "Verification": Verification is focused on the processes and activities related to how an organization checks and tests artifacts produced throughout software development. This typically includes quality assurance work such as testing, but it can also include other review and evaluation activities.

How to setup a SSDLC: Business functions

EXCELLIUM
Your first call when it comes to IT and Security!

"Business Function" are the following:

- "Deployment": Deployment entails the processes and activities related to how an organization manages release of software that has been created. This can involve shipping products to end users, deploying products to internal or external hosts, and normal operations of software in the runtime environment.

How to setup a SSDLC: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

"Security Practices" for the Business Function "Governance" are :

- "*Strategy & Metrics*" : Involves the overall strategic direction of the software assurance program and instrumentation of processes and activities to collect metrics about an organization's security posture.

- "*Policy & Compliance*" : Involves setting up a security and compliance control and audit framework throughout an organization to achieve increased assurance in software under construction and in operation.

- "*Education & Guidance*" : Involves increasing security knowledge amongst personnel in software development through training and guidance on security topics relevant to individual job functions.

How to setup a SSDLC: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

"Security Practices" for the Business Function "Construction" are :

- "*Threat Assessment*" : Involves accurately identifying and characterizing potential attacks upon an organization's software in order to better understand the risks and facilitate risk management.

- "*Security Requirements*" : Involves promoting the inclusion of security-related requirements during the software development process in order to specify correct functionality from inception.

- "*Secure Architecture*" : Involves bolstering the design process with activities to promote secure-by-default designs and control over technologies and frameworks upon which software is built.

How to setup a SSDLC: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

"Security Practices" for the Business Function "Verification" are :

- "*Design Review*" : Involves inspection of the artifacts created from the design process to ensure provision of adequate security mechanisms and adherence to an organization's expectations for security.

- "*Code Review*" : Involves assessment of an organization's source code to aid vulnerability discovery and related mitigation activities as well as establish a baseline for secure coding expectations.

- "*Security Testing*" : Involves testing the organization's software in its runtime environment in order to both discover vulnerabilities and establish a minimum standard for software releases.

How to setup a SSDLC: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

"Security Practices" for the Business Function "Deployment" are :

- "*Vulnerability Management*" : Involves establishing consistent processes for managing internal and external vulnerability reports to limit exposure and gather data to enhance the security assurance program.

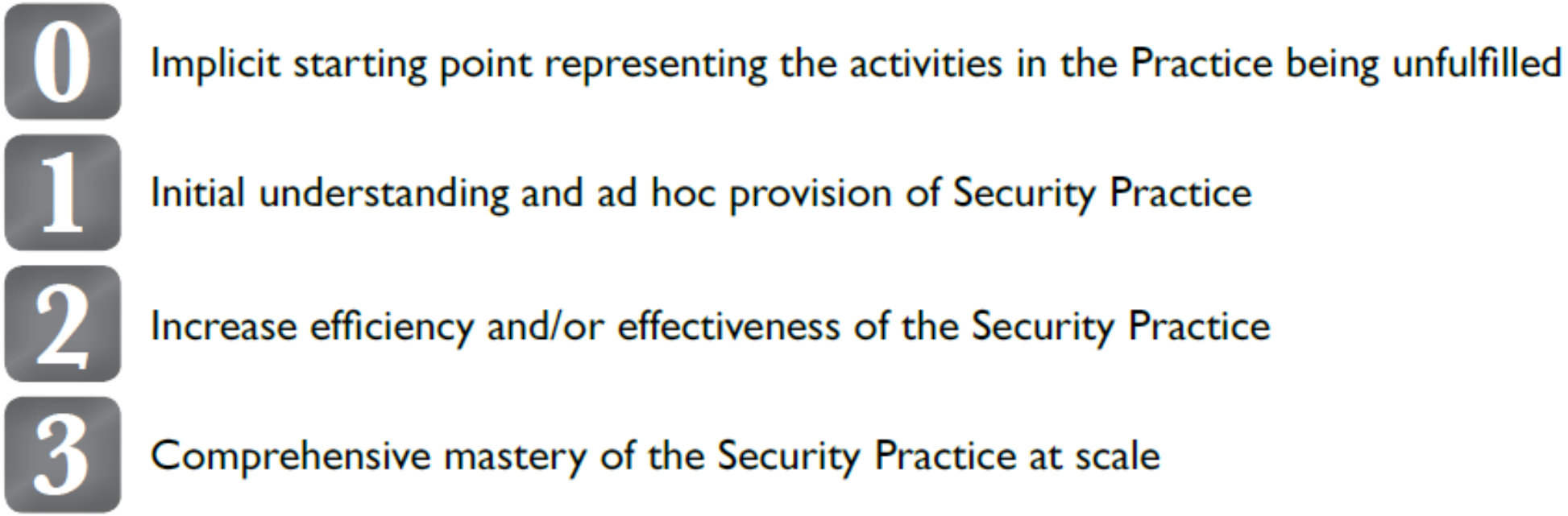
- "*Environment Hardening*" : Involves implementing controls for the operating environment surrounding an organization's software to bolster the security posture of applications that have been deployed.

- "*Operational Enablement*" : Involves identifying and capturing security-relevant information needed by an operator to properly configure, deploy, and run an organization's software.

How to setup a SSDLC: Maturity levels

EXCELLIUM
Your first call when it comes to IT and Security!

"**Maturity levels**" for a Security Practices are the following:



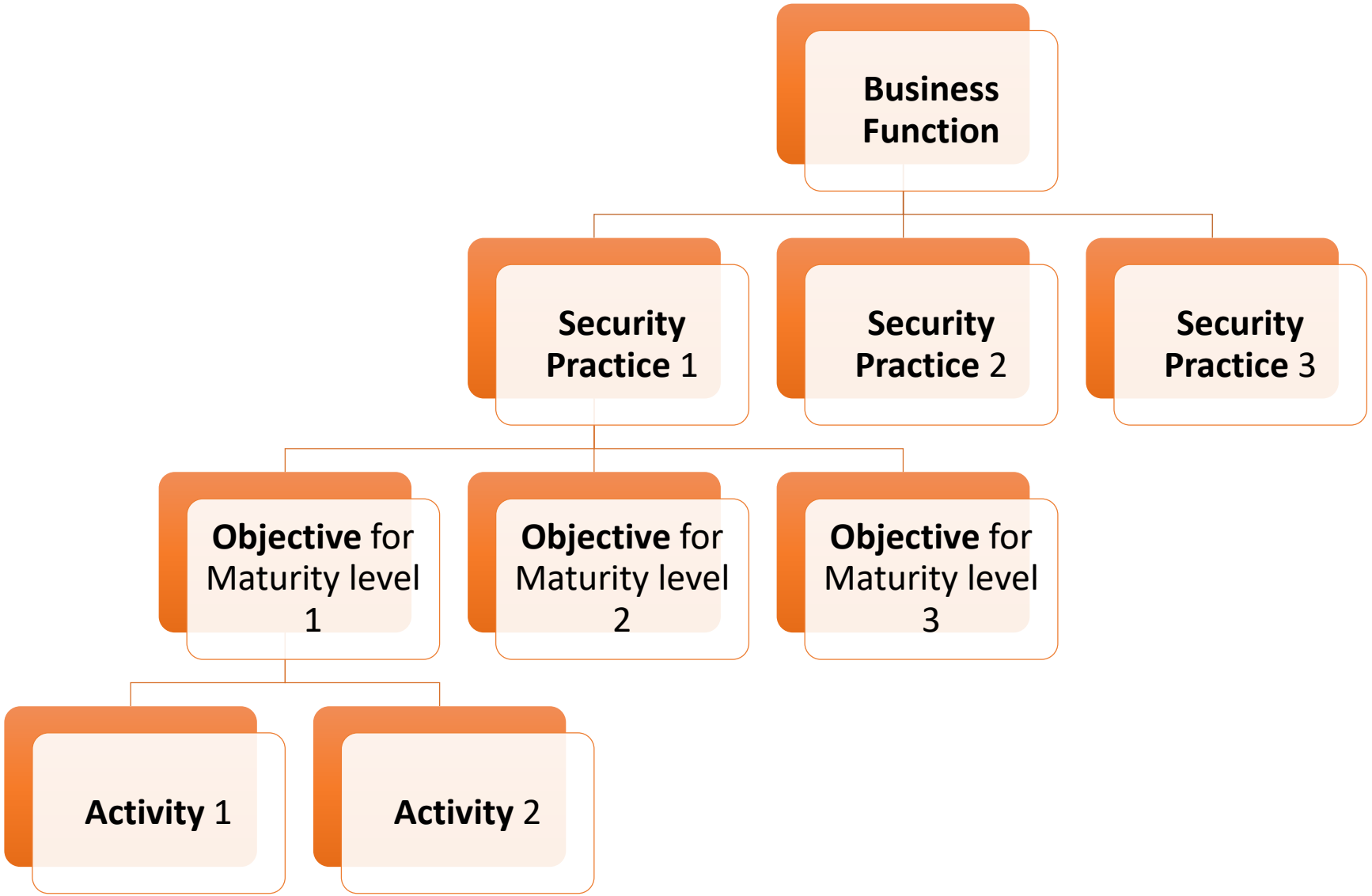
How to setup a SSDLC: Maturity levels

EXCELLIUM
Your first call when it comes to IT and Security!

- There also intermediate level to indicate if you fulfill a level but also a part of the next levels
- In this case you add a "+" after the level that you fully fulfill
- Example:
  - An organization that is performing all Level 1 Activities for Operational Enablement as well as one Level 2 or 3 Activity would be assigned a “1+” score
  - An organization performing all Activities for a Security Practice, including some beyond the scope of SAMM, would be given a "3+" score

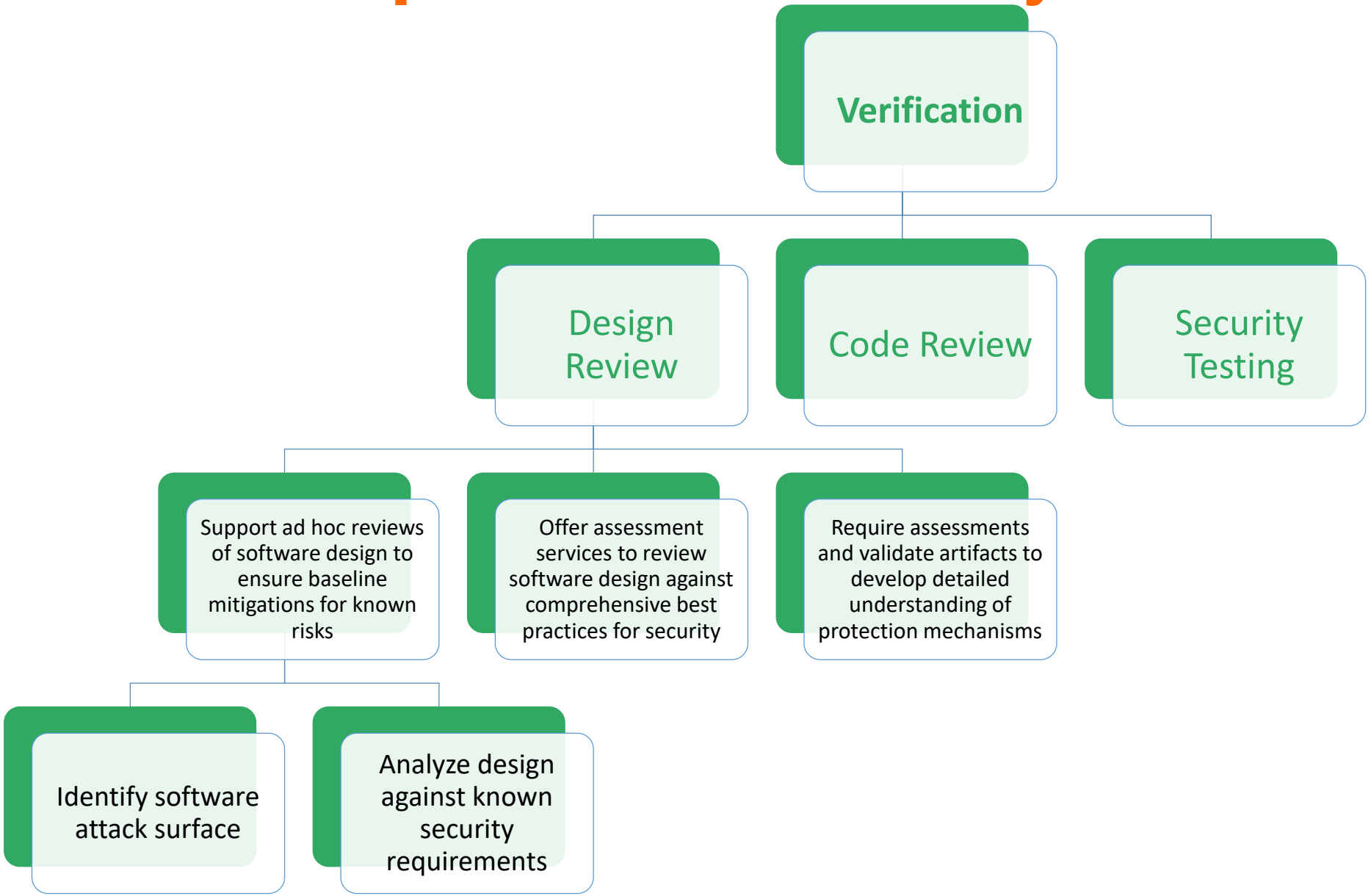
How to setup a SSDLC: Hierarchy

EXCELLIUM
Your first call when it comes to IT and Security!



How to setup a SSDLC: Hierarchy

EXCELLIUM
Your first call when it comes to IT and Security!



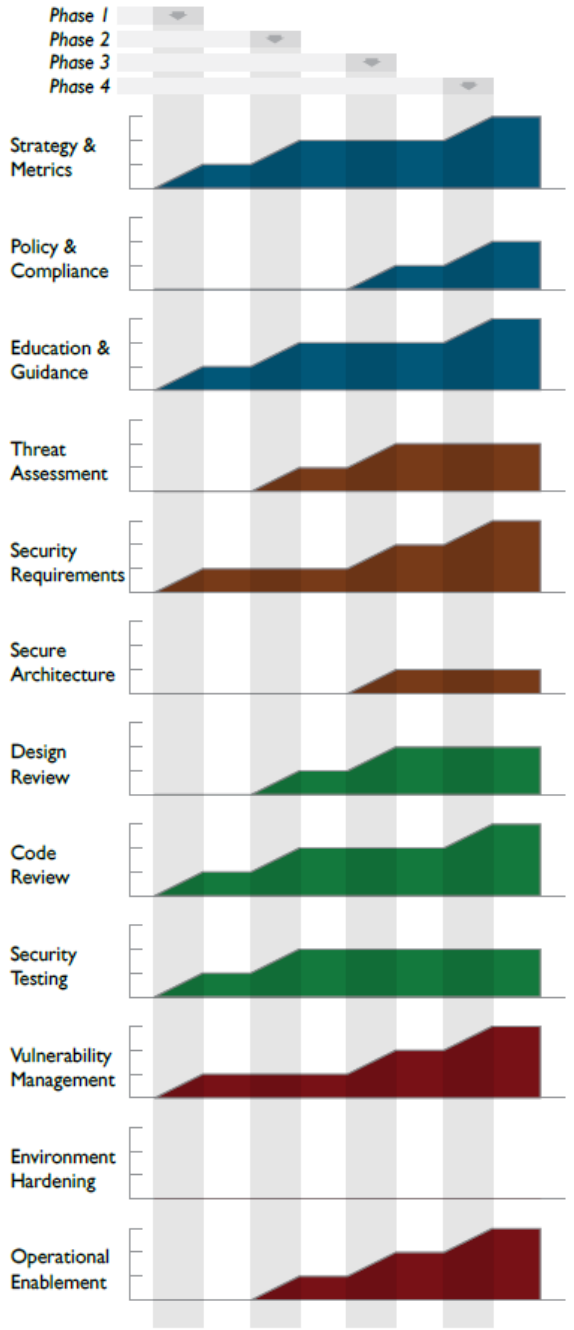
How to setup a SSDLC: The roadmap

EXCELLIUM
Your first call when it comes to IT and Security!

- The first thing is to create a "**Roadmap**" in order to define the vision of application security level that you actually have and one that you want to reach in a timeframe
- To achieve the creation of the roadmap, you will perform the step below:
  a) Select a set of "**Security Practices**" for each "**Business Function**" according to you business (software vendor, financial service,...)
  b) Define a set of phase (for example time based like quarter or half year) in which several "**Security Practices**" are each improved by one maturity level
  c) Perform a assessment for each "**Security Practices**" in order determine your current maturity level:
     - You can perform a detailed assessment or you can use assessment worksheet provided by Open SAMM in order to quickly determine your level.

How to setup a SSDLC: The roadmap

- A Open SAMM roadmap consist of phases (the vertical bars) in which several “Security Practices” are each improved by one maturity level.
- First phase is the starting point of your SSDLC setup and contains the current maturity level for all “Security Practices” selected for the first version of your roadmap.
- Last phase indicate the end of the first version of your roadmap.

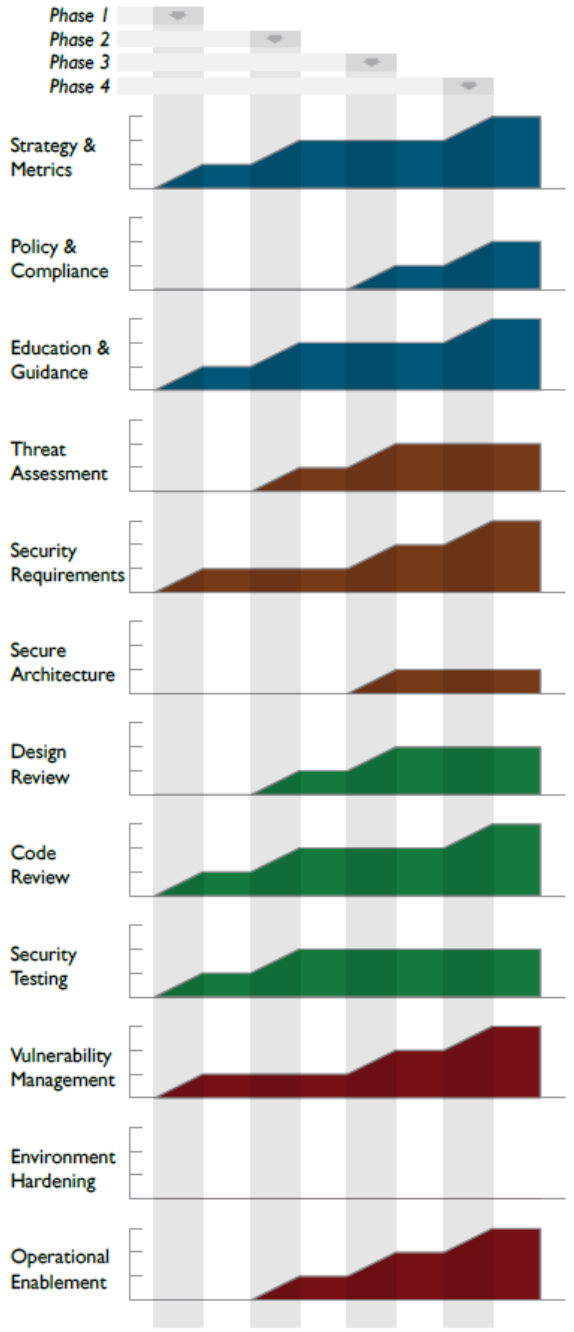


How to setup a SSDLC: The roadmap

- SSDLC is generally a iterative process and version of the roadmap can be considered as iteration

- For the next version of your roadmap you can include “Security Practices” that has not be part of the initial version

- It’s possible, according to your business, to choose to reach only the maturity level 1,1+,2,2+ in the first version of your roadmap in order to apply focus on more important “Security Practices” for which you want to reach the maturity level 3 or 3+



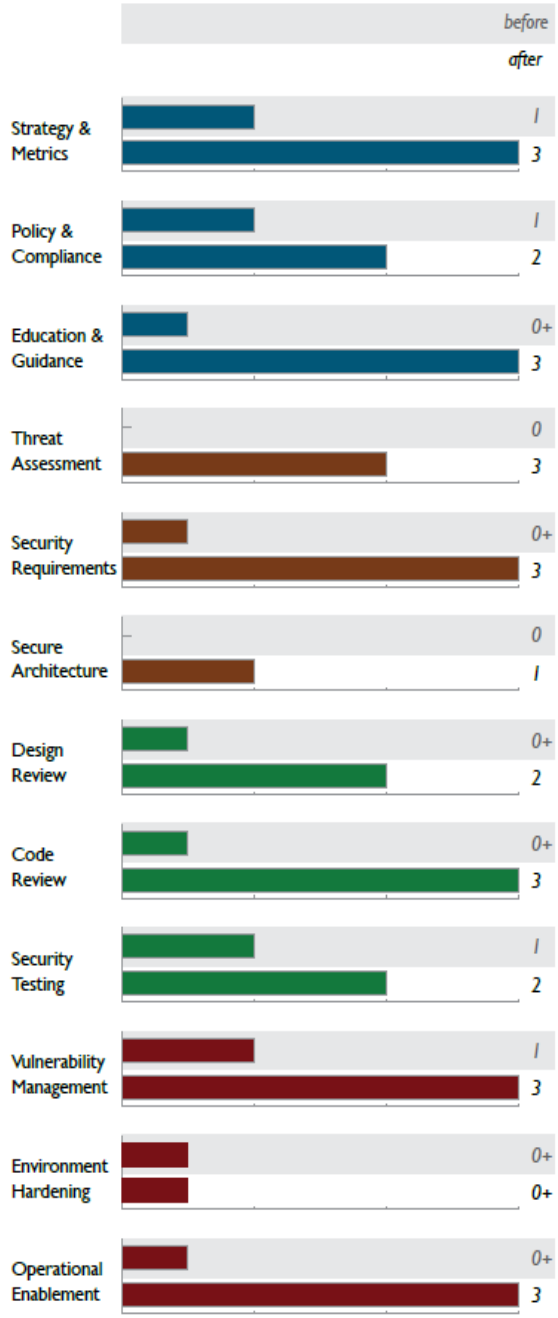
How to setup a SSDLC: Work in a phase

EXCELLIUM
Your first call when it comes to IT and Security!

- When the roadmap is ready, the work in phase is the following for each "Security Practices" :
  a) Look at "Activities" related to "Objective" for the next maturity level to reach or the job to do to keep the same level if the level must not be increased for the current phase
  b) Look at success metrics defined by Open SAMM for the current targeted "Objective", adapt them if needed (stick to it if possible):
     - Example for "Code Review" maturity level 1 of the Objective "Opportunistically find basic code-level vulnerabilities and other high-risk security issues":
       - >80% of project teams briefed on relevant code review checklists in past 6 months
       - >50% of project teams performing code review on high-risk code in past 6 months
  c) Plan and dispatch task to team
  d) Use success metrics to measure evolution during phase

How to setup a SSDLC: The scorecards

- Based on the scores (maturity level) assigned to each “Security Practice”, an organization can create a scorecard to capture those values
- Selecting a time interval over which to generate a scorecard facilitates understanding of overall changes in the assurance program during the time frame
- Using interval scorecards is encouraged for several situations:
  - "**Gap analysis**" : Capturing scores from detailed assessments versus expected performance levels
  - "**Demonstrating improvement**" : Capturing scores from before and after an iteration of assurance program build-out
  - "**Ongoing measurement**" : Capturing scores over consistent time frames for an assurance program that is already in place



Practical example: Business context

EXCELLIUM
Your first call when it comes to IT and Security!

- We are an IT service (50 peoples) of a non IT company (bank, insurance,..)
- Due to historical reason, application security is not part of the current SDLC but we use Continuous Integration
- We always perform a vulnerability assessment audit by an external security company before to consider a application “ready for production”
- We develop more and more web/mobile oriented application in order to allow our customers to perform operations by themselves as much as possible (customer portal, self service,...)
- The number/type of security issues gathered by vulnerability assessment performed at the end of application implementation take more and more time to fix and production deployment is often delayed
- Due the previous point development team are forced to have heavy working days or work on week end (implying additional cost on IT service to cover/pay extra time) and then our turnover rate is increasing
- We decide to spread an iteration timeframe of a year for the initial roadmap in order to take the time to lay the foundation of your SSDLC
- We use a new strategic project which have a development timeframe of 1 years to start our new SSDLC

Practical example: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

- According to the context, we choose the "Security Practices" below as priority for the first roadmap iteration:
  - For "Governance":
    - "*Strategic & Metrics*" → To define and manage the long term objectives
    - "*Policy & Compliance*" → Target the minimum in iteration n°1 in order to "start small & quick"
    - "*Education & Guidance*" → To spread security knowledge and motivate IT teams

Practical example: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

- According to the context, we choose the "Security Practices" below as priority for the first roadmap iteration:
  - For "Construction":
    - "*Threat Assessment*" →To identity the attack from which our application will be exposed
    - "*Security Requirements*" & "*Secure Architecture*" →To prepare inclusion of security into project requirements and start awareness of our analysts (technical & business) and architects (technical & business)

Practical example: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

- According to the context, we choose the "Security Practices" below as priority for the first roadmap iteration:
  - For "Verification":
    - "*Design Review*" → To validate/challenge architect/analyst work
    - "*Code Review*" → To validate/challenge developer work
    - "*Security testing*" → We will ask to our security services provider to help us on integration of security during project implementation phases

Practical example: Security Practices

EXCELLIUM
Your first call when it comes to IT and Security!

- According to the context, we choose the “Security Practices” below as priority for the first roadmap iteration:
  - For “Deployment”:
    - “*Vulnerability Management*” →Target the minimum in iteration n°1 in order to “start small & quick”
    - “*Environment Hardening*” →To complete to the work done on application level and validate/challenge architect/operator/developer on infrastructure side
    - “*Operational Enablement*” → Target the minimum in iteration n°1 in order to “start small & quick”

Practical example: Initial Roadmap it. 1

EXCELLIUM
Your first call when it comes to IT and Security!

Based on Excel provided by Open SAMM to help in roadmap creation, this is our roadmap for iteration n°1 →

Software Assurance Maturity Model (SAMM) Roadmap

Organization: My company
Project: My project
Version 1

Source Data

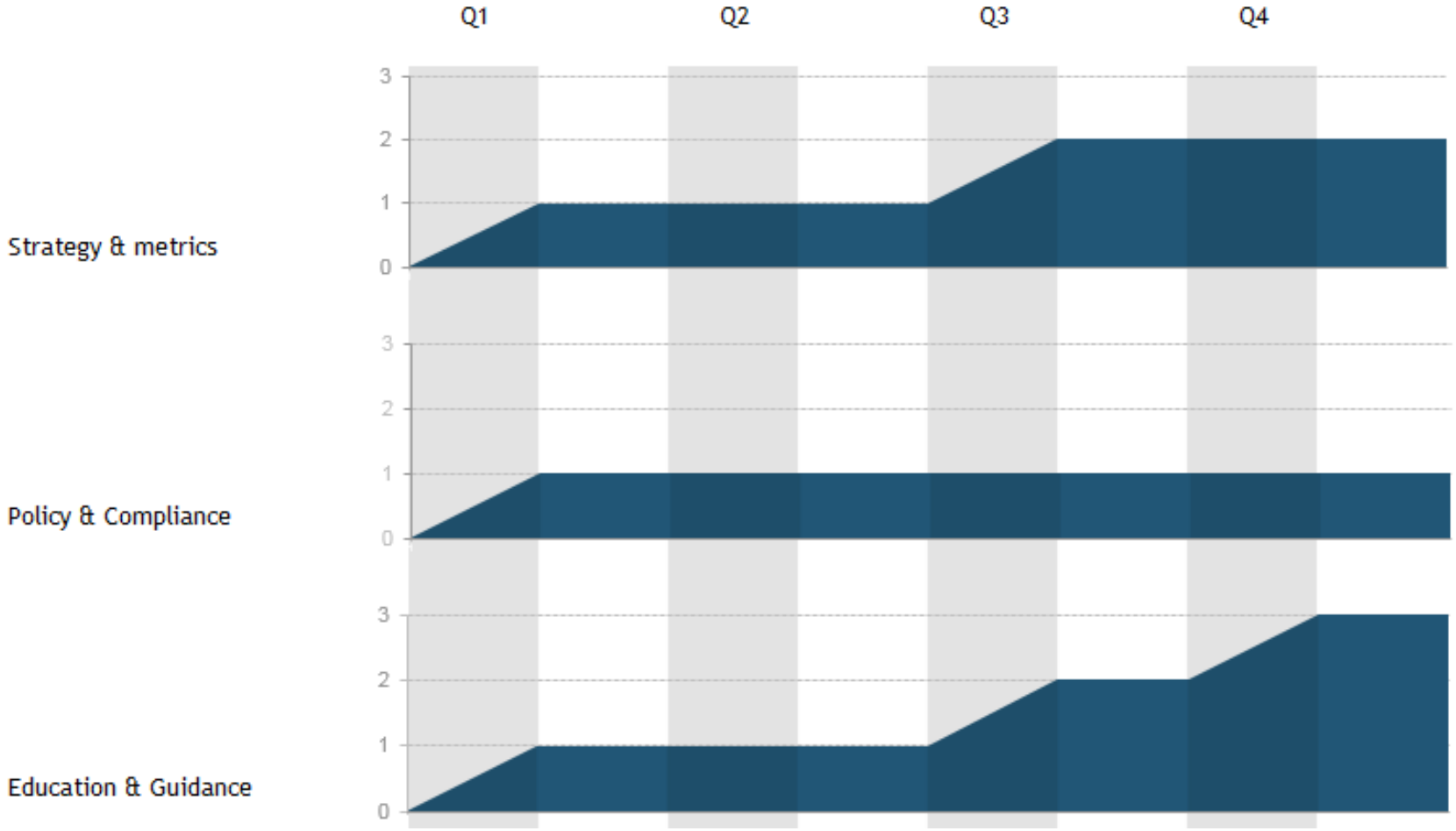
Security Practices/Phase	Start	Q1	Q2	Q3	Q4
Strategy & metrics	0	1	1	2	2
Policy & Compliance	0	1	1	1	1
Education & Guidance	0	1	1	2	3
Threat Assessment	0	1	1	2	3
Security Requirements	0	1	1	2	3
Secure Architecture	0	1	1	2	3
Design Analysis	0	1	1	2	3
Code Review	0	1	1	2	3
Security Testing	0	1	1	2	2
Vulnerability Management	0	1	1	1	1
Environment Hardening	0	1	1	2	3
Operational Enablement	0	1	1	1	1

Valid Maturity Levels	
	0
	1
	2
	3

Practical example: Initial Roadmap it. 1

EXCELLIUM
Your first call when it comes to IT and Security!

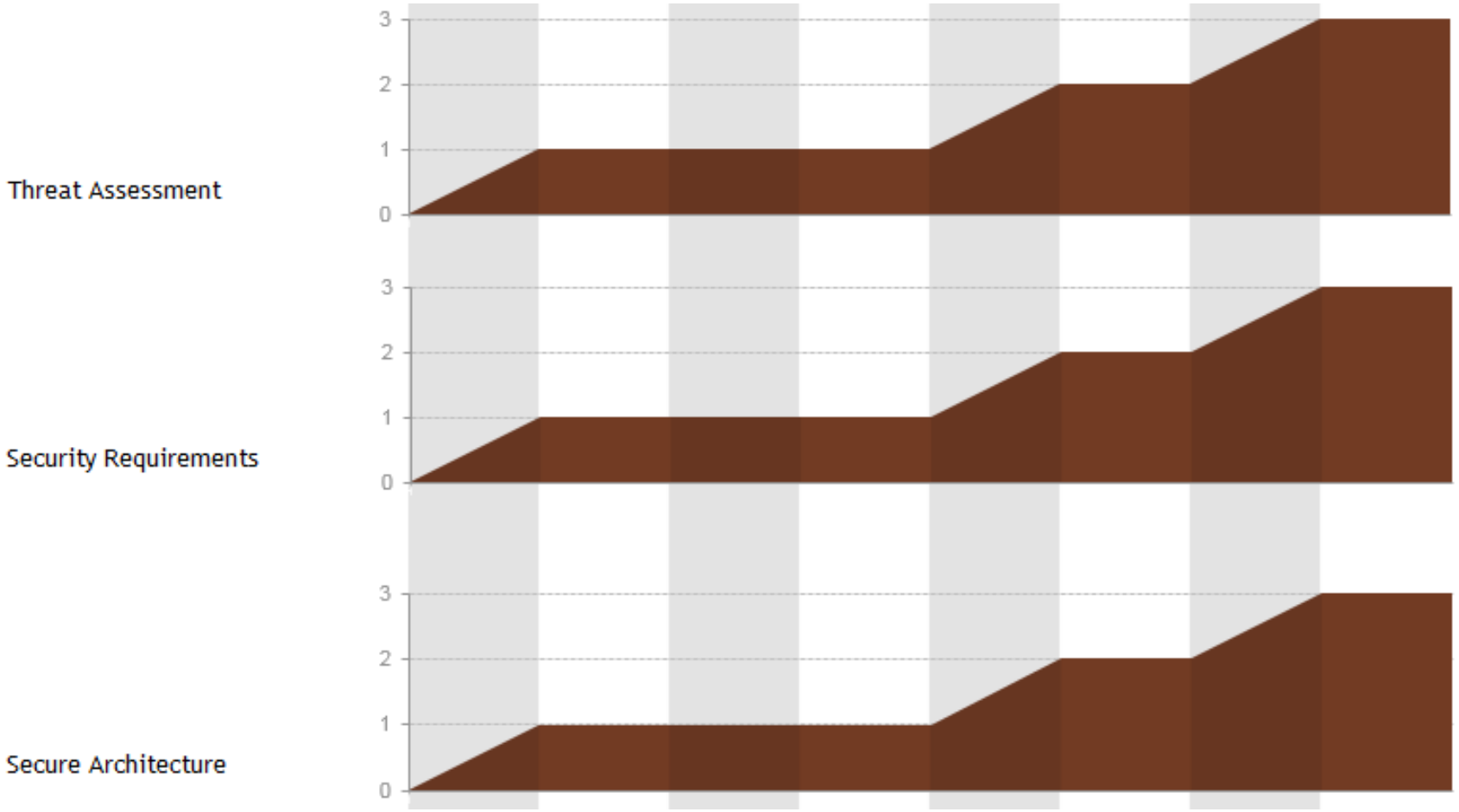
View for "Governance" business function for different quarters for the year



Practical example: Initial Roadmap it. 1

EXCELLIUM
Your first call when it comes to IT and Security!

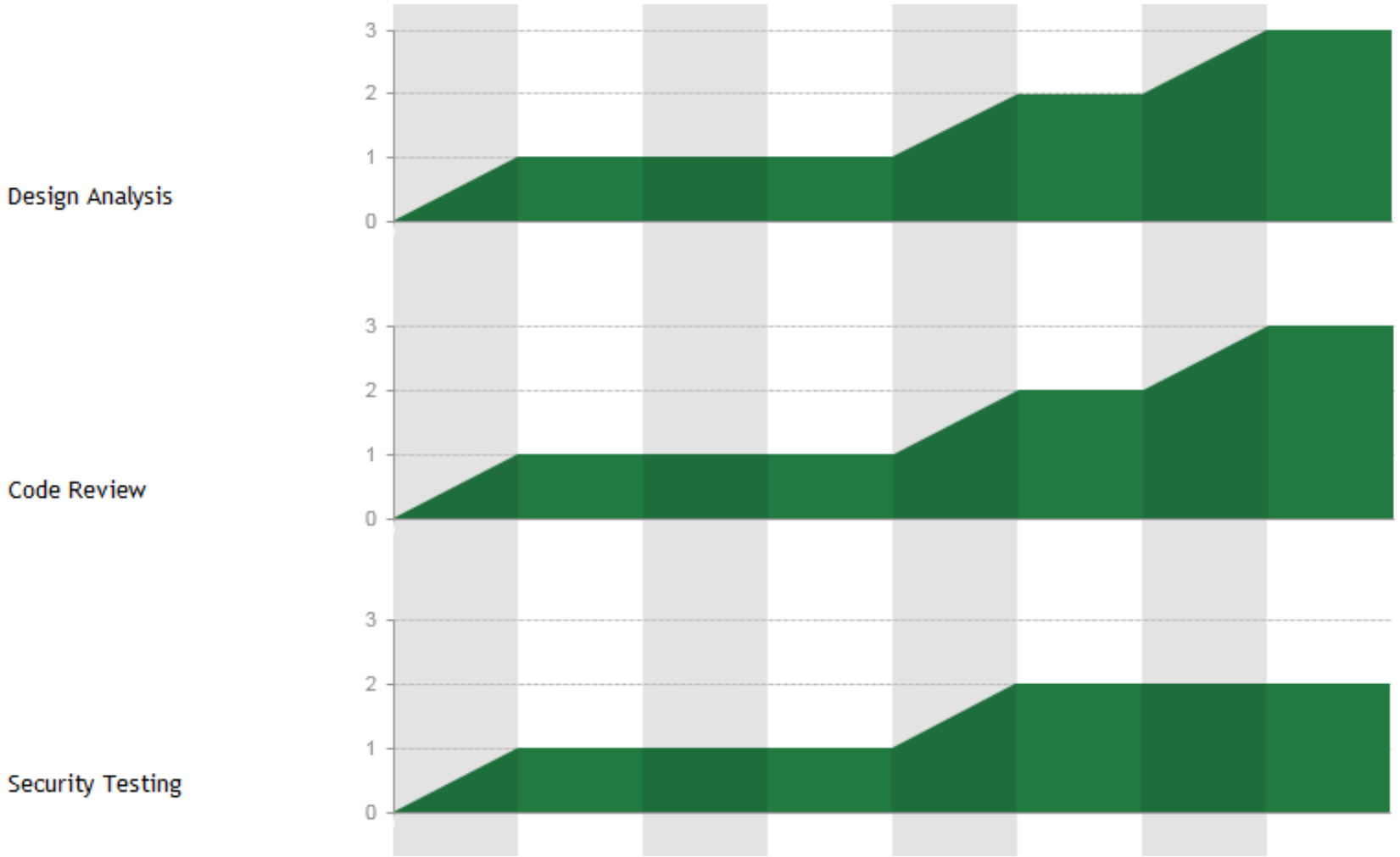
View for "Construction" business function for different quarters for the year



Practical example: Initial Roadmap it. 1

EXCELLIUM
Your first call when it comes to IT and Security!

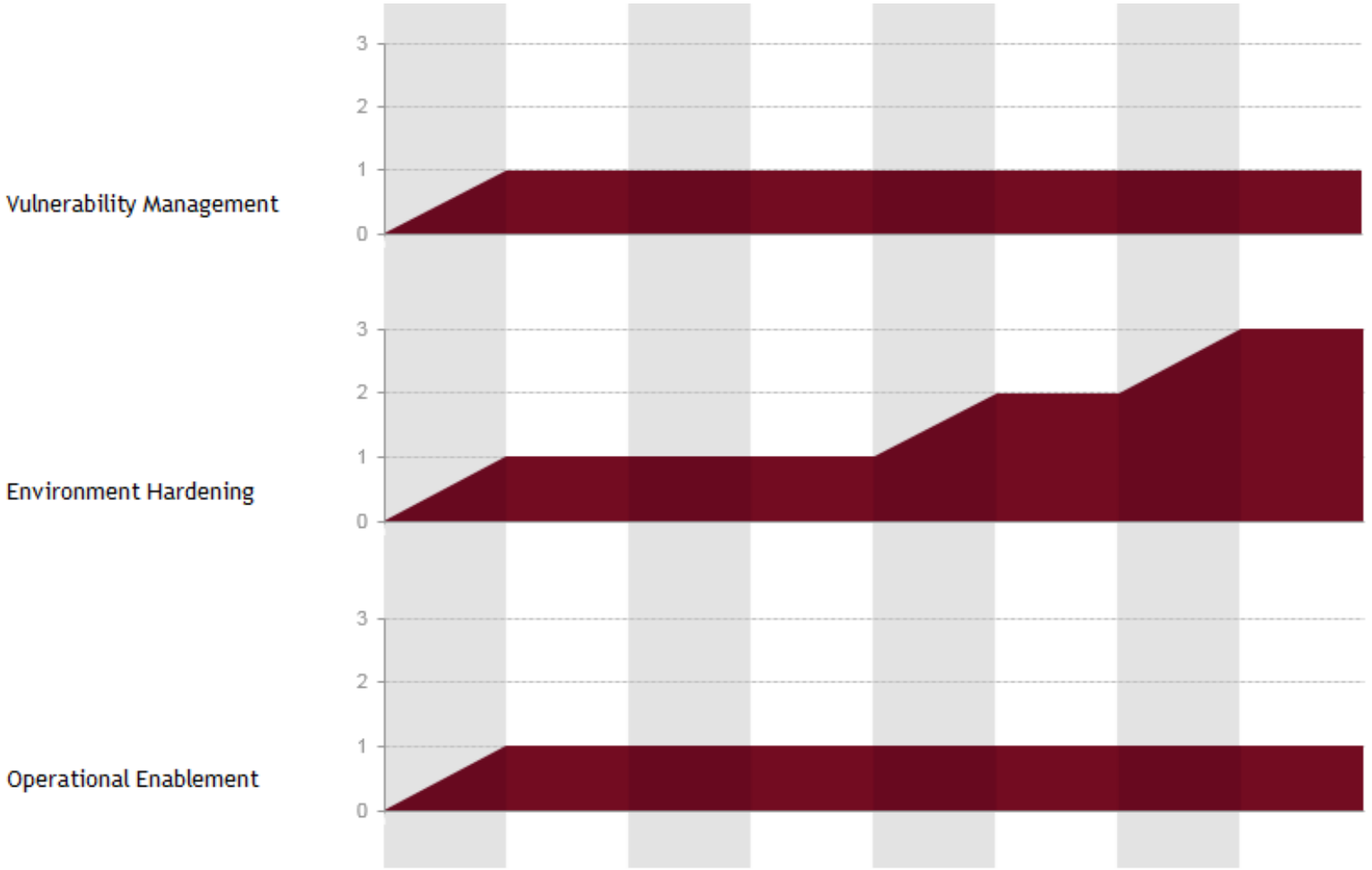
View for "Verification" business function for different quarters for the year



Practical example: Initial Roadmap it. 1

EXCELLIUM
Your first call when it comes to IT and Security!

View for "Deployment" business function for different quarters for the year



Practical example: Next maturity level

EXCELLIUM
Your first call when it comes to IT and Security!

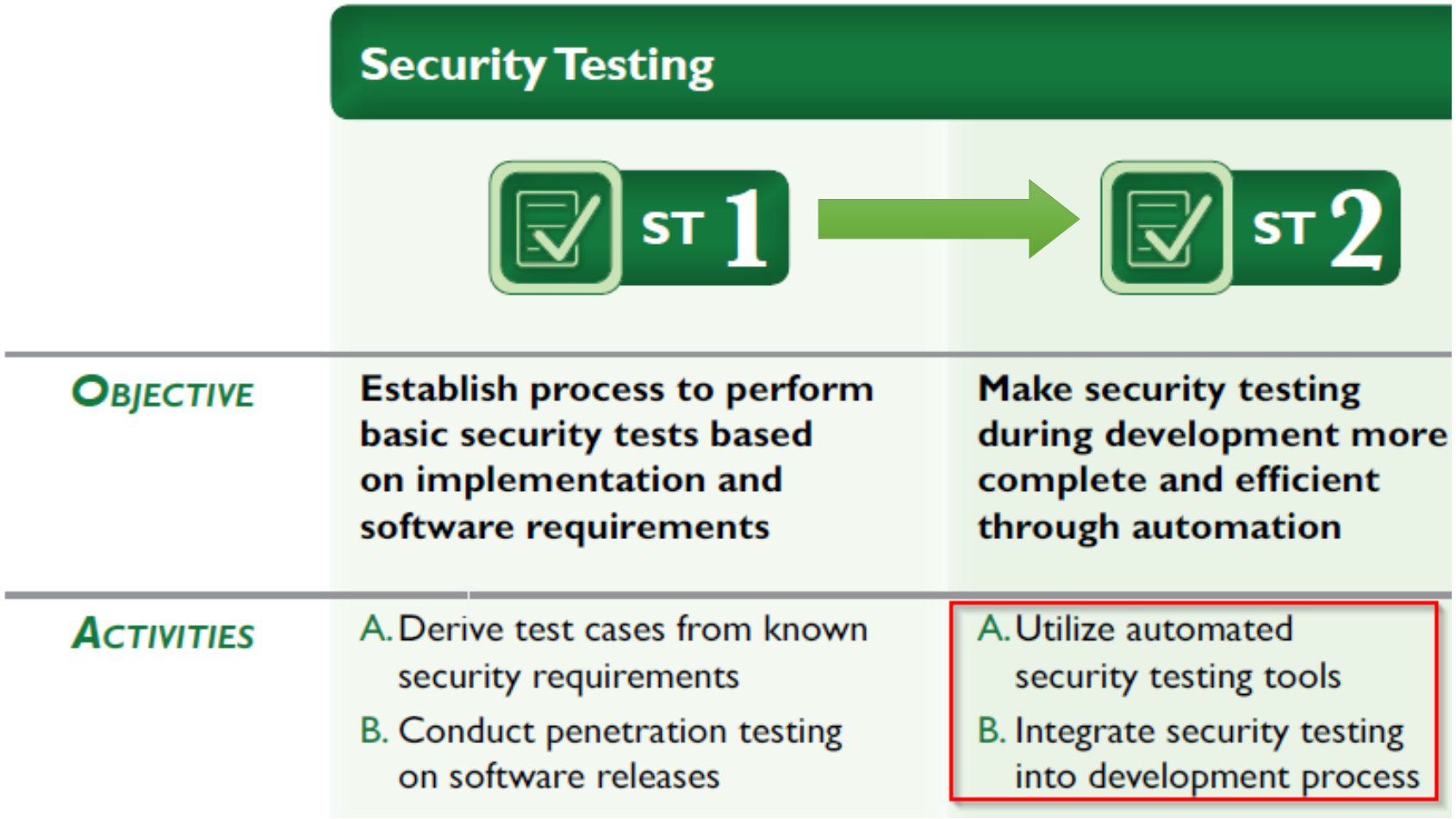
We will focus here on a way to pass from Security Practices "Security Testing" Maturity level 1 to level 2 planned on

Security Testing	ST 1	ST 2
OBJECTIVE	Establish process to perform basic security tests based on implementation and software requirements	Make security testing during development more complete and efficient through automation
ACTIVITIES	A. Derive test cases from known security requirements B. Conduct penetration testing on software releases	A. Utilize automated security testing tools B. Integrate security testing into development process

Practical example: Next maturity level

EXCELLIUM
Your first call when it comes to IT and Security!

We will focus here on a way to pass from Security Practices "Security Testing" Maturity level 1 to level 2 planned on



Practical example: Next maturity level

EXCELLIUM
Your first call when it comes to IT and Security!

What we need to do to fulfil this maturity level granting (specified by Open SAAM) ?

- Utilize automated security testing tools
- Integrate security testing into development process

What we will do ?

- Use security application scanners (free to avoid extra cost at the beginning because we start from scratch)
- Update the Continuous Integration Process (CIP) in order to integrate theses scanners

Practical example: Next maturity level

What we need ?

a) Help of our security services provider to :

- Propose us security application scanners and define appropriate initial scanning settings/profile according to threats from which our application will be exposed
- Help development team to implement defensive measures during project implementation
- Train project technical leader to analyze scanner reports and detect false-positive/false-negative
- Update scanning settings/profile during project evolution with sharing with project development team

b) Help of project technical leader in order to:

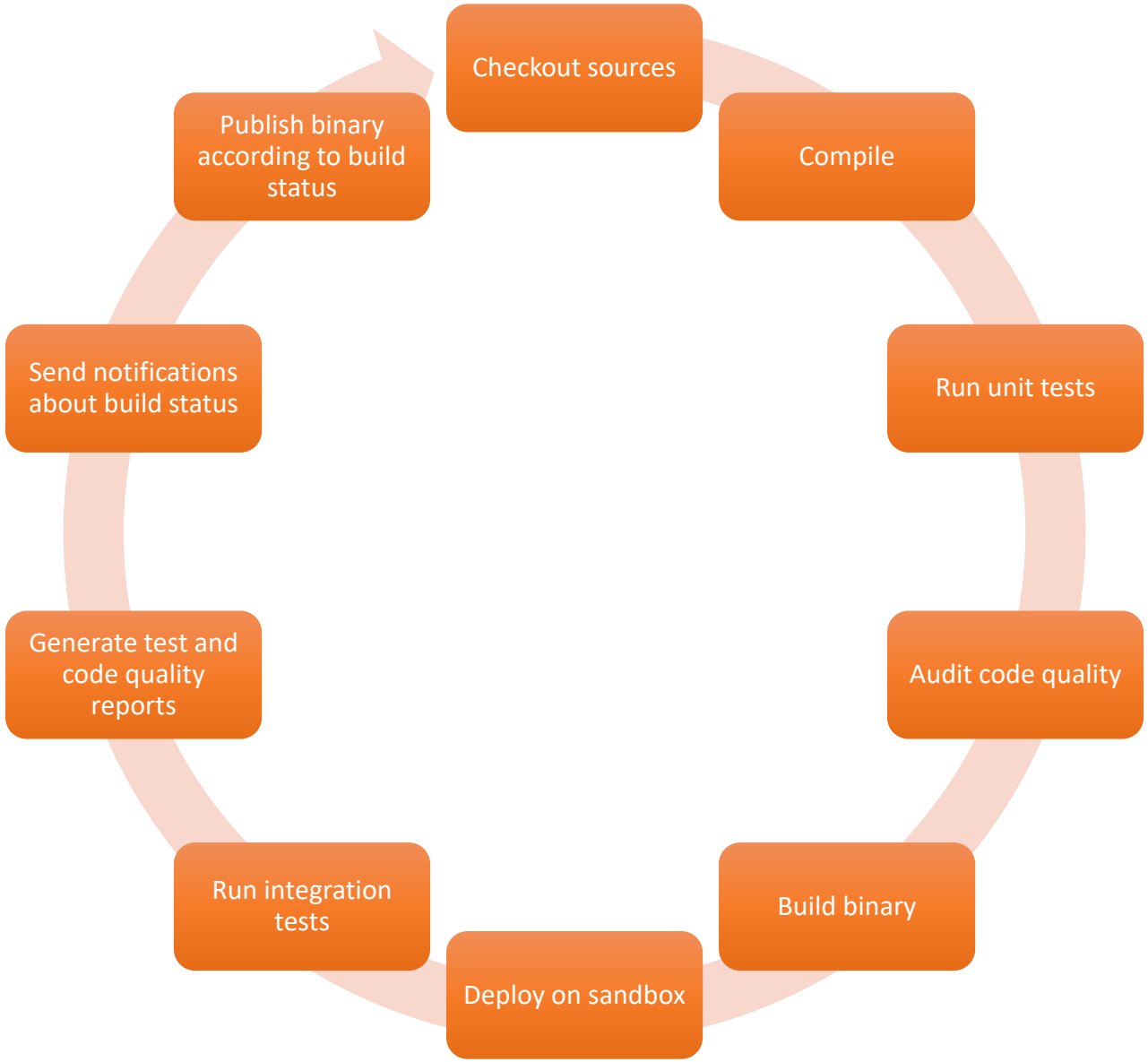
- Integrate the scanners into the CIP
- Analyze scanner reports to check for false-positive/false-negative
- Help project manager to plan tasks to fix real issues discovered by scanners between 2 CIP occurrences

Infrastructure part of the application will be covered by the Security Practices "Environment Hardening" maturity levels

Practical example: Next maturity level

EXCELLIUM
Your first call when it comes to IT and Security!

Our CIP move from this →



Practical example: Next maturity level

EXCELLIUM
Your first call when it comes to IT and Security!

To this →

Tools & Links

EXCELLIUM
Your first call when it comes to IT and Security!

Name	Goal	Link
OpenSAMM	OpenSAMM referential	http://www.opensamm.org/
Jenkins	Continuous Integration Platform	https://jenkins-ci.org/
SonarQube	Static code analyzer	http://www.sonarqube.org/
OWASP SonarQube	Set of security rules	https://www.owasp.org/index.php/OWASP_SonarQube_Project
SonarQube FindSecbug	Set of security rules	http://h3xstream.github.io/find-sec-bugs/
OWASP Dependency Check	Tool to check Java/.Net dependencies for CVE	https://www.owasp.org/index.php/OWASP_Dependency_Check
OWASP ZAP	Web local proxy and dynamic application analyzer	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Q&R

EXCELLIUM
Your first call when it comes to IT and Security!