GOTHAM
DIGITAL SCIENCE

Matt Bartoldus
matt@gdssecurity.com

Security in the SDLC: It Doesn’t Have To Be Painful

Introduction

- Me
- Who Are You?
  - Assessment (Penetration Tester; Security Auditors)
  - Developer
  - IT Architect
  - Management
  - Application Owner
  - Consultant (2 or more above)
  - Other

Agenda

- Information Security Industry
  - It is all so very young!
- The Building Blocks
  - Business Case
  - People, Process, Technology
  - Frameworks
- How?
- Problems You Will Create

The above to include war stories, examples, trivia, things to look out for and other random things …

Young Discipline in a Young Industry

- BS7799 came out mid-90s
- Shifting Focus within Industry
  - PBX to Infrastructure to Database/Application hacking

- PCI-DSS
  - CISP – 2001 – mention of change control as a best practice item
  - PCI-DSS v1.2 – late 2008 – Requirement 6

Common Excuses

- “No Time”
- “No Skills”
- “No Budget”

Translation

- Business reasons for security have not been defined and/or communicated … (or communicated well enough)!

- *Example – Spend £60,000 to encrypt our laptops please?*

Business Case- Drivers

- Relatively Same Drivers Across Industries
  - Compliance
    - PCI-DSS, SOX, DPA, etc
  - Protection
    - Brand/reputation; from criminals (cyber-crime)
  - Governance
    - Function of good corporate governance; enterprise risk management

Business Case- Quality

- What is Quality?
  - Subjective
  - Depends on context

ISO 9001

"Degree to which a set of inherent characteristics fulfills requirements."

Six Sigma

"Number of defects per million opportunities."

Quality Assurance

- Prevention of defects

Quality Control

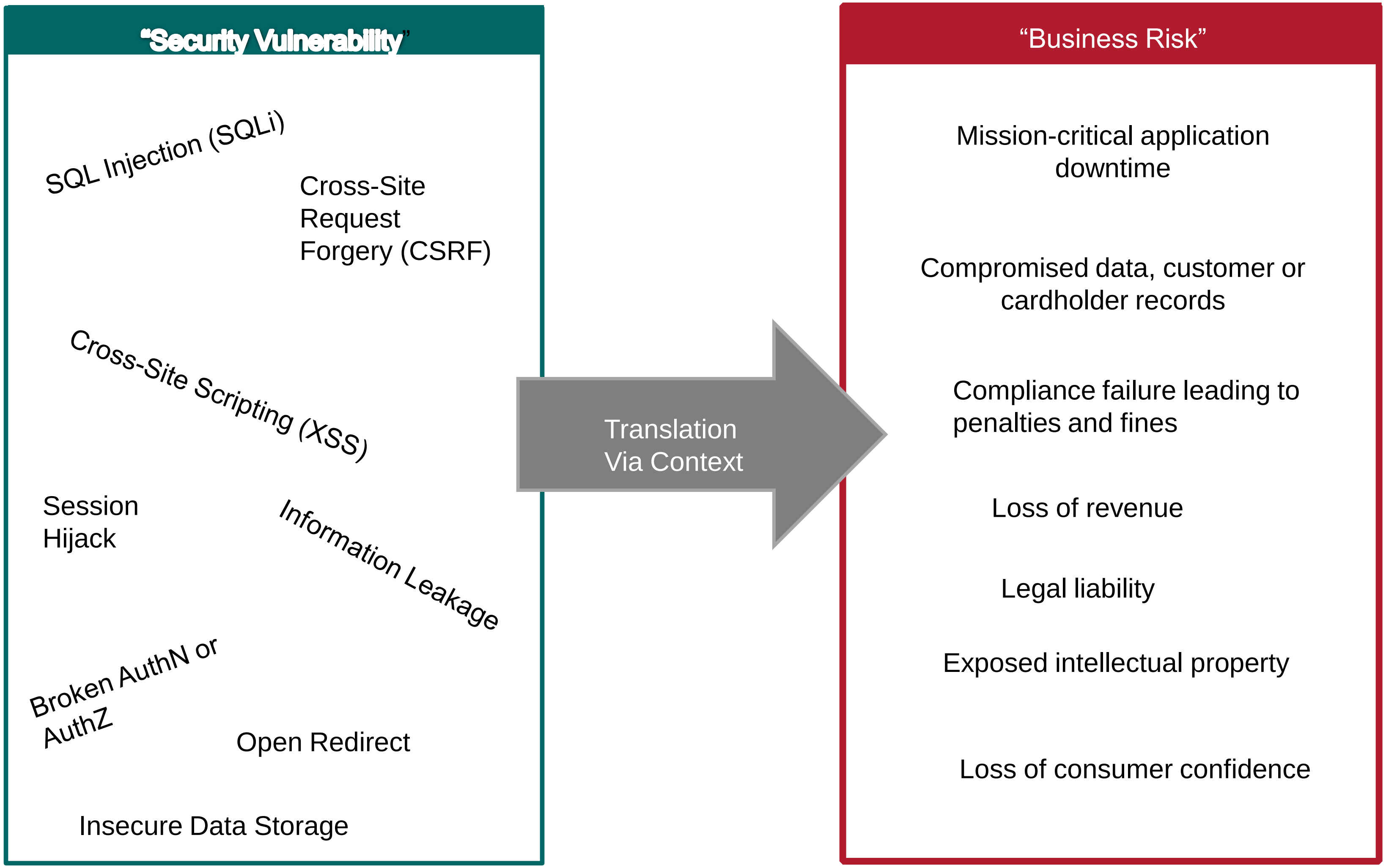
- Detection of defects

Security Defect?

✓ My application is vulnerable to SQL Injection which allows an anonymous attacker the ability to pull down the contents of the backend database without authentication.

- So what?
- Is this vulnerability a defect?
- Quality Issue?
- Requirements met?

Business Case – Translate Technical Risk to Business Risk



“Security Vulnerability”

SQL Injection (SQLi)

Cross-Site Request Forgery (CSRF)

Cross-Site Scripting (XSS)

Session Hijack

Information Leakage

Broken AuthN or AuthZ

Open Redirect

Insecure Data Storage

Translation Via Context

“Business Risk”

Mission-critical application downtime

Compromised data, customer or cardholder records

Compliance failure leading to penalties and fines

Loss of revenue

Legal liability

Exposed intellectual property

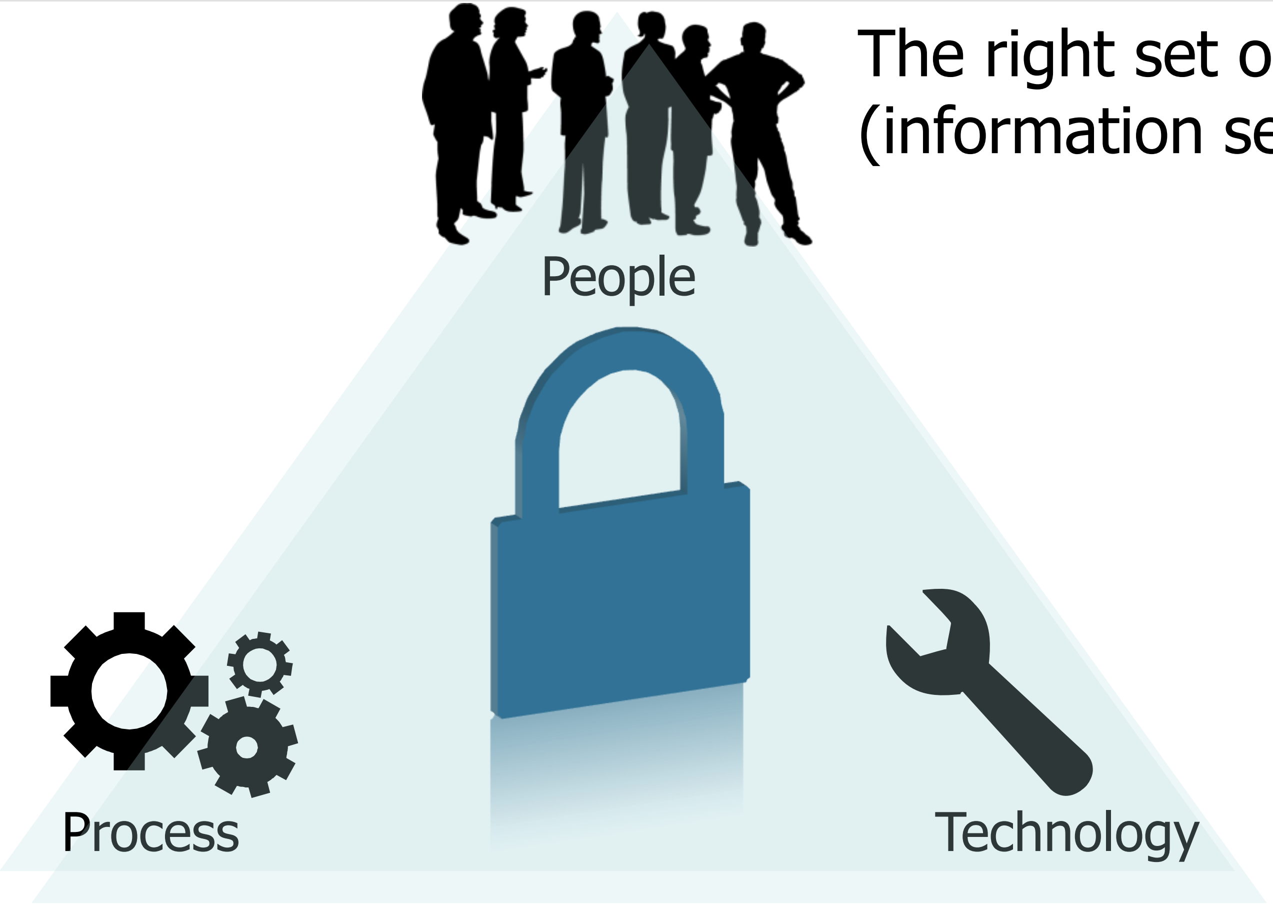
Loss of consumer confidence

Business Case - Customer Expectations

The pricing for my application is as follows:

- £19.99 for the Application
- £29.99 for the Application + reliability
- £39.99 for the Application + reliability + performance
- £49.99 for the application + reliability + performance + security

Building Block - Standard Approach to IT Delivery



The right set of skills (information security)

Industry proven processes

Industry leading tools and research

Building Block – Technology

Technology

- Technology is used to automate processes, provide efficiency and cost savings, and drive innovation.

However

- Technology is useless if PEOPLE do not know how to use
- Technology can be dangerous if PEOPLE use incorrectly
- The benefits of using technology can be wasted if not part of a PROCESS

Building Block - People

People

- Building Software
  - Design
  - Architecture
  - Development
  - Testing
  - Project Management
    - Project Risk
    - Project Costing

- Information Security
  - Secure Design
  - Security Architect
  - Secure Development
  - Security Testing
  - Project Management
    - Risk Assessment
    - Resource Allocation

Building Block - Process

Process

- Systems Development
  - Development methodologies
    - Waterfall
    - RUP
    - Agile
  - Development Activities
    - Planning
    - Design
    - Develop
    - Test
    - Release

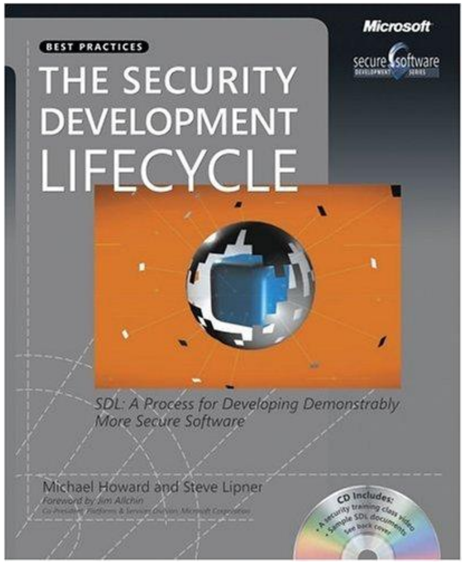
- Information Security (Infosec)
  - **Infosec** Methodologies
    - ?
    - ?
    - ?
  - **Infosec** Activities
    - Risk Analysis
    - Threat Modelling/Assessment
    - Testing

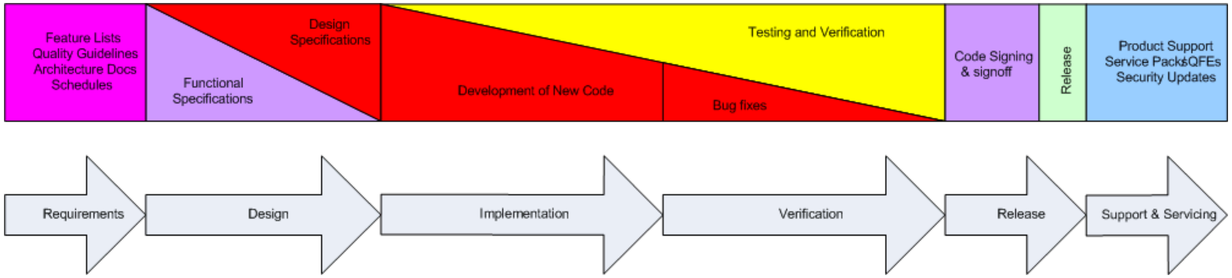
Development Method Independent

Security is independent of development methodologies whether using Agile, RUP, Waterfall, Scrum, RAD, Iterative, etc

Building Block – Framework (Approach)

This is an OWASP Project
OWASP
The Open Web Application Security Project


Microsoft
secure software
BEST PRACTICES
THE SECURITY DEVELOPMENT LIFECYCLE
SDL: A Process for Developing Demonstrably More Secure Software
Michael Howard and Steve Lipner
Foreword by Jim Allchin
CD Includes:



Motivation for a framework approach

- Changing an organisation is difficult

Simple, well-defined, measurable
preferred over
complex

- Application security is a result of many activities
  - Combination of people, process, and automation
- There is no single formula for all organisations
  - Business risk from software depends on the nature of the business
- An assurance program must be built over time
  - Organisations can't change overnight. Use a phased approach.

Questions from Business

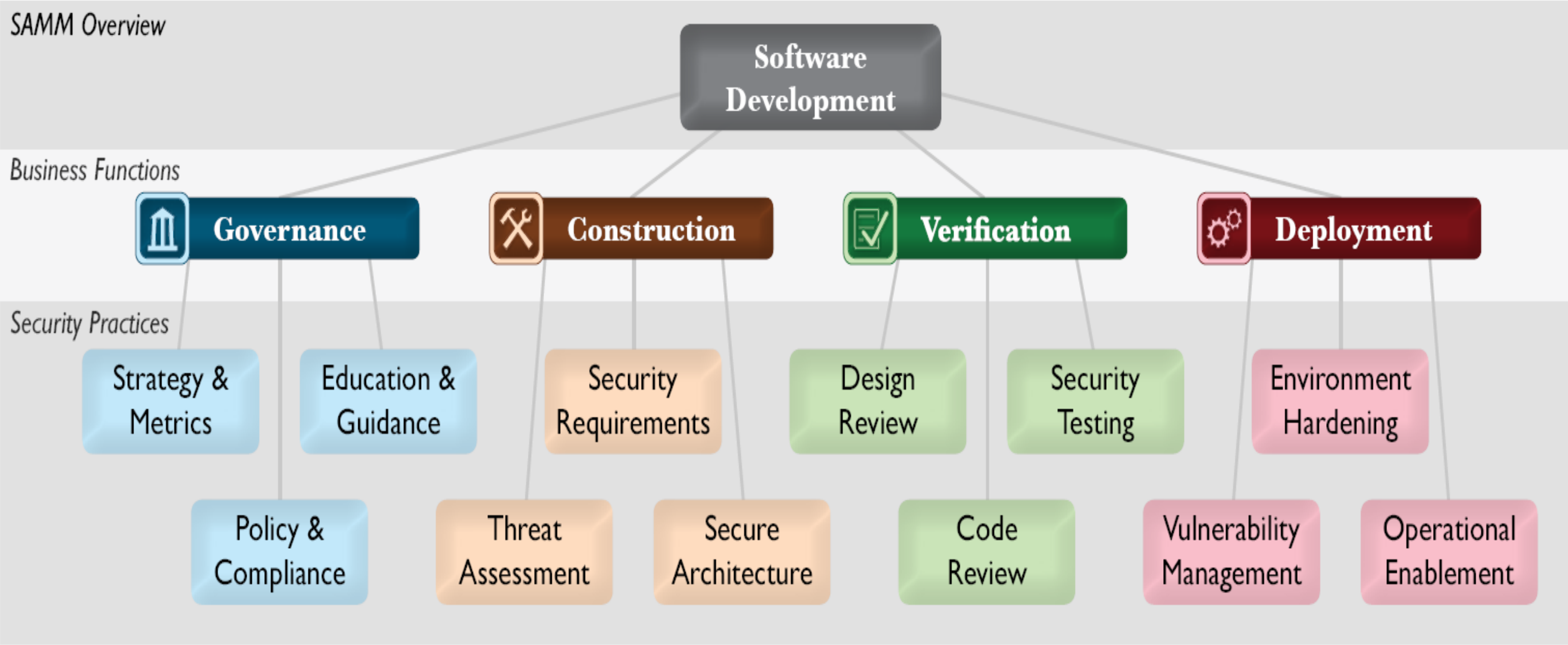
- » What does ‘it’ look like?
- » How can we understand and manage ‘this’?
- » Do we have enough resources / skills to do ‘this’?
- » How does ‘this’ fit in with the Security function, shouldn’t they do ‘it’?
- » We are used to security projects that implement tools or systems but now we need to change our processes?
- » Isn’t there an established method or model for all ‘this’?

So what is ‘this’ discipline called?

- » Software Assurance
- » BSA – Business Software Assurance
- » SSA - Software Security Assurance
- » SDL – Security Development Lifecycle
- » SDLC – to confuse everyone
- » sSDLC – secure Software Development Lifecycle
- » SPLC – Secure Project Lifecycle
- » CLASP - Comprehensive, Lightweight Application Security Process
- » 7 Touchpoints
- » SSF – System Security Framework

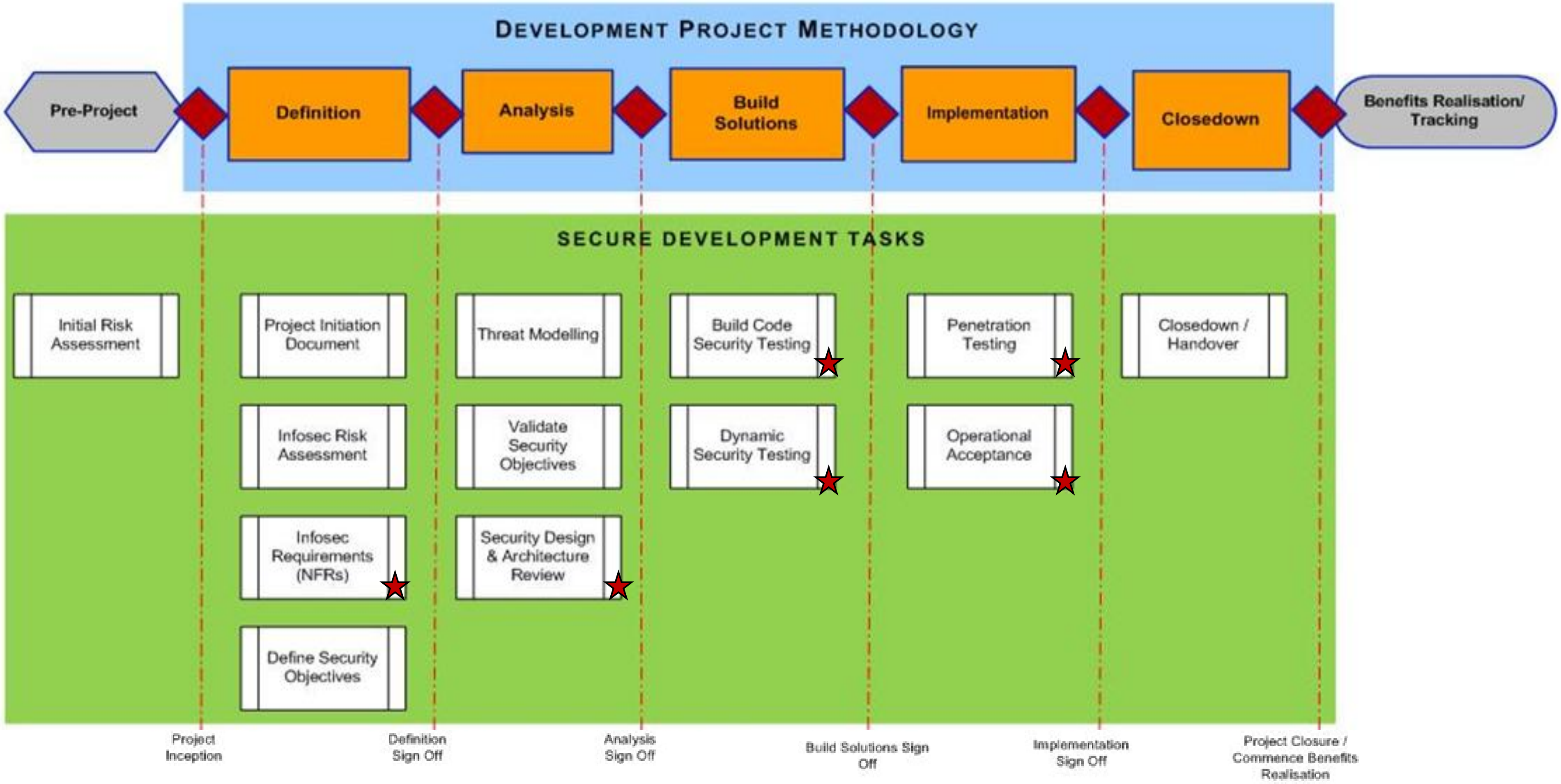
Business Functions and Security Practices

- Using OpenSAMM as a framework for security in software development
- Security Practices that are the independent silos for improvement that map underneath the Business Functions of software development.



GOTHAM DIGITAL SCIENCE

Security within a Generic Development Project



DEVELOPMENT PROJECT METHODOLOGY

Pre-Project

Definition

Analysis

Build Solutions

Implementation

Closedown

Benefits Realisation/ Tracking

SECURE DEVELOPMENT TASKS

Initial Risk Assessment

Project Initiation Document

Infosec Risk Assessment

Infosec Requirements (NFRs) ★

Define Security Objectives

Threat Modelling

Validate Security Objectives

Security Design & Architecture Review ★

Build Code Security Testing ★

Dynamic Security Testing ★

Penetration Testing ★

Operational Acceptance ★

Closedown / Handover

Project Inception

Definition Sign Off

Analysis Sign Off

Build Solutions Sign Off

Implementation Sign Off

Project Closure / Commence Benefits Realisation

Security Testing Lifecycle

DR 2

Offer assessment services to review software design against comprehensive best practices for security

A. Inspect for complete provision of security mechanisms

B. Deploy design review service for project teams

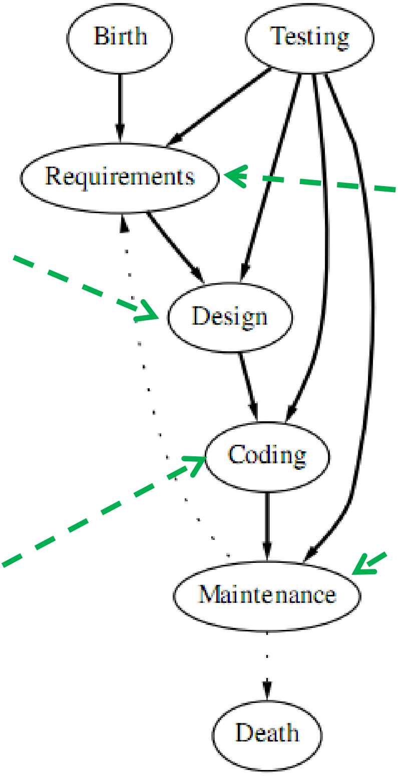
CR 2

Make code review during development more accurate and efficient through automation

A. Utilize automated code analysis tools

B. Integrate code analysis into development process

Testing is for "Life"



Early identification of defects & prevention of defect migration are key goals of the testing process.

Ref: Ireland, Andrew – Software Testing Life-Cycle

ST 1

Establish process to perform basic security tests based on implementation and software requirements

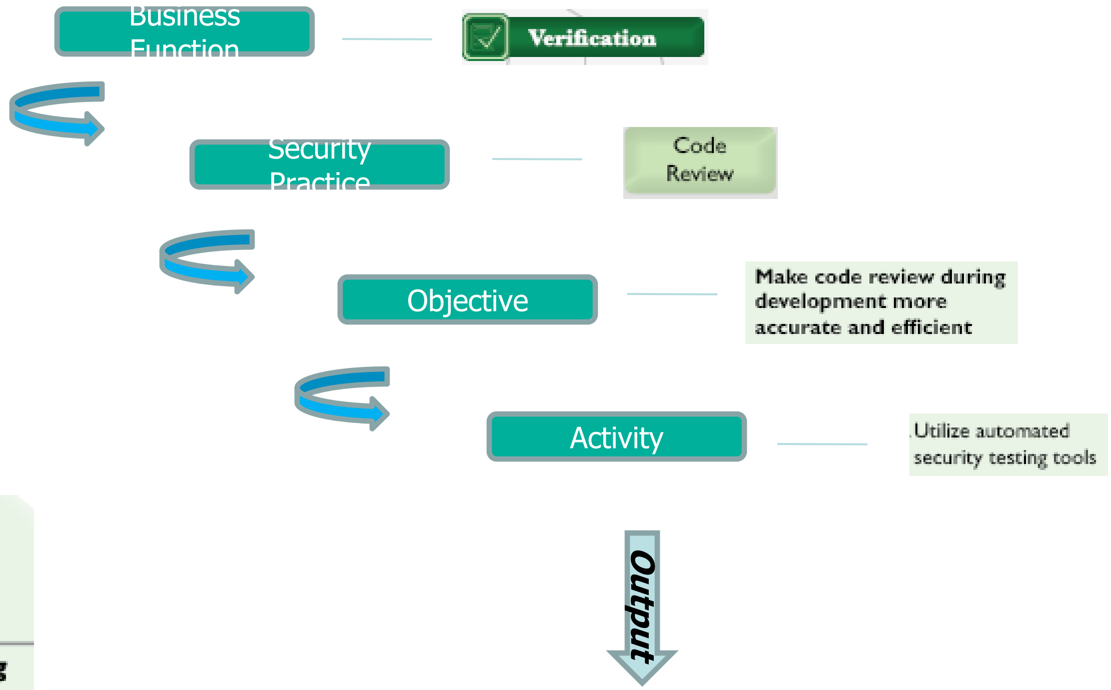
A. Derive test cases from known security requirements

B. Conduct penetration testing on software releases

B. Integrate security testing into development process

B. Establish release gates for security testing

Process Output Example: Compliance



Business Function

Verification

Security Practice

Code Review

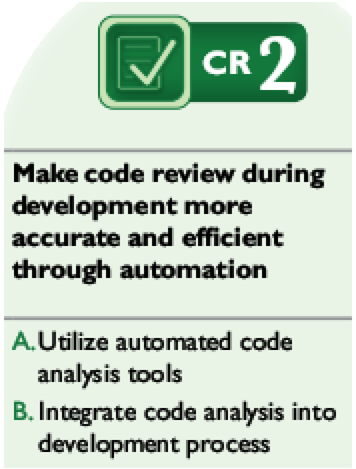
Objective

Make code review during development more accurate and efficient

Activity

Utilize automated security testing tools

Output



CR 2

Make code review during development more accurate and efficient through automation

A. Utilize automated code analysis tools

B. Integrate code analysis into development process

PCI

6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability

It's not the tool that enables compliance, it is the process in which the tool is used

How?

- Use Building Blocks
  - Business Case
    - Get funding, management commitment
- People, Process and Technology
  - Skills
  - Integrate into Existing Processes
- Framework
  - Use to Measure over time
  - Put into Business Context
  - Enable comparison

How? Security Skills

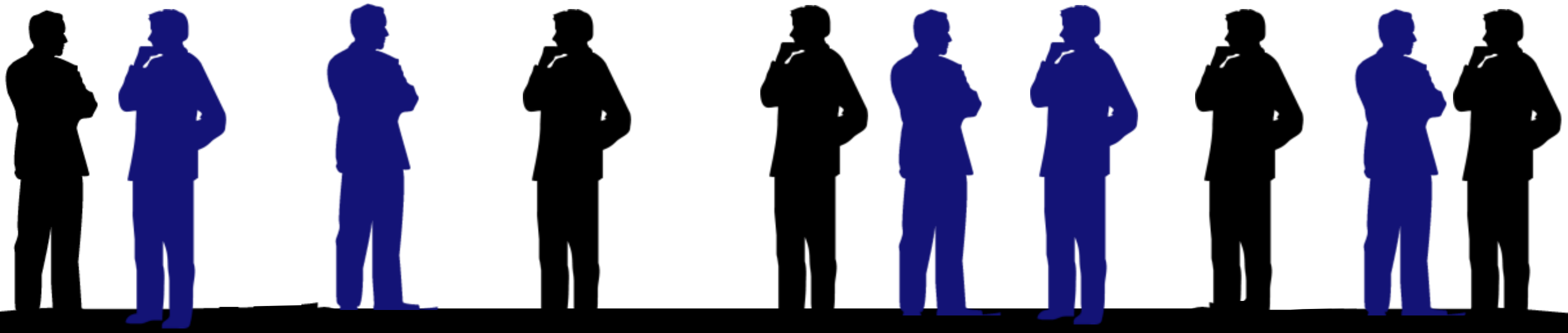
Security professionals are overwhelmed

Organisations must learn to bridge the gap

The business is overwhelmed by security

Where are your information security skills?

How? Security Skills



Security skills are deployed into the business

The business embeds security activities and skills

How? Augment Processes

- Embed security into existing business processes

  "We don't have a formal process, how can we embed security into something we don't have?"

  – You are DOING something .. so embed security as part of that DOING something!

How? Plan and Measure

- Use activities to make a plan
  - Start with a ‘current state’
    - Even if you think you know … document it
    - Draw up a plan
    - Measure at milestones

- Measure
  - Define metrics based on plan
    - Example: Use CMMI-ish ratings for activities (a la COBIT)
      - 0 -Nonexistent
      - 1- Ad-hoc
      - 2- Repeatable
      - 3- Defined Process
      - 4 -Managed and Measurable
      - 5- Optimised

Problems You Will Create

– More defects
  - How will this be perceived by management?
  - How will these be managed?
  - Who will prioritise remediation?
  - When will remediation be done?
  - Developer morale

(don't beat anyone up)

Problems You Will Create

– Skills gap
  - It will become apparent where your security skills are (or are not)
  - Never a good time for training
  - Consultants are a very costly long term option
  - That ONE ‘security person’ can not be involved with everything!
  - There is a difference between a ‘breaker’ and a ‘fixer’

Problems You Will Create

- Resource gap
  - Actually the case anyway, but will be further highlighted
  - Convincing senior management to invest more
  - Now that more is understood about your vulnerabilities, it can not be ignored .. but it can be considered and eventually managed

Problems You Will Create

– Political minefields

- Some organisations don’t manage change very well
- Middle managers
- Managing perceptions and pushback

About Gotham Digital Science

- Gotham Digital Science (GDS) is an international security services company specializing in Application and Network Infrastructure security, and Information Security Risk Management. GDS clients number among the largest financial services institutions and software development companies in the world.

- Offices in London and New York City