www.pwc.com

Maturity Models Hands-on

SecAppDev 2019

Bart De Win

pwc

Bart De Win ?

- 20 years of Information Security Experience
  - Ph.D. in Computer Science - Application Security
- Author of >60 scientific publications
- ISC² CSSLP & CISSP certified
- Director @ Cyber&Privacy PwC Belgium:
  - Leading the Threat & Vuln. Mngt. team
  - (Web) Application tester (arch. review, code review, dynamic review, …)
  - Proficiency in Secure Software Development Lifecycle (SDLC) and Software Quality (ISO25010)
- OWASP SAMM co-leader
- Contact me at bart.de.win@pwc.com

Agenda

1. **Introduction**
2. Assessment
3. Improvements
4. Tips & Challenges
5. Discussion

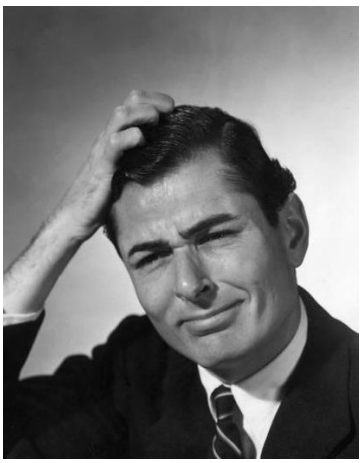
What's your Company Maturity ?

- In terms of IT **strategy** and application **landscape**
- In terms of software **Development** practices
  - Analysis, Design, Implementation, Testing, Release, Maintenance
- In terms of **ITSM** practices
  - Configuration, Change, Release, Vulnerability -Mngt.

Company Maturity ≈ **Feasibility SDLC Program**

Complicating factors, anyone ?

- Different development teams
- Different technology stacks
- Business-IT alignment issues
- Outsourced development
- …

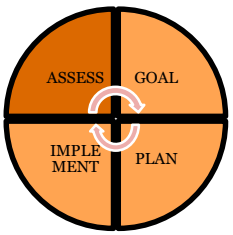


Typical Project Approach

Agenda

1. Introduction
2. **Assessment**
3. Improvements
4. Tips & Challenges
5. Discussion

As-Is



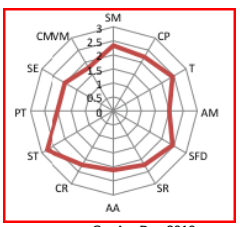
Maturity Evaluation (in your favourite model)

Depending on (your knowledge of) the organisation, you might be able to do this on your own

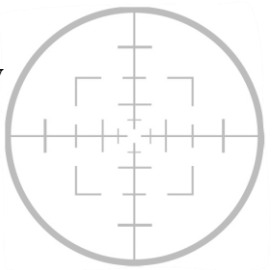
If not, interviews with different stakeholders will be necessary

Analyst, Architect, Tech Lead, QA, Ops, Governance

Discuss outcome with the stakeholders and present findings to the project advisory board



Scoping



For large companies, teams will perform differently

=> difficult to come up with a single result

Consider

- Reducing the scope to a single, uniform unit
- splitting the assessment into different organizational subunits

Splitting might be awkward at first, but can be helpful later on for motivational purposes

Assessment Exercise

Use OWASP SAMM to evaluate the development practices in your own company

Focus on 2 Business Functions:

- SAMM 1.5: Governance and Construction
- SAMM 2.0beta: Implementation and Verification

https://owaspsamm.org/ for the core documents

Assessment wrap-up

What's your company's score ?

What's the average scores for the group ?

Any odd ratings ?

Assessment - Lessons Learned Organisation Specific

Pre-screen general software development maturity

Define assessment scope in organisation:

- Organisation wide
- Selected Business Units
- Development Groups (internal, supplier)
- IT infrastructure Groups (hosting internal, cloud)

Involve key stakeholders

Invaluable for awareness & education

Apply CONSISTENT (same interviewers) within same organisation

Assessment - Lessons Learned
Interview / Scoring

Adapt & select subset questionnaire per profile
(risk management, development, IT infrastructure, …)

Try different formats: interview style, workshops

Capture more details:

- "Adjusted" scoring
- Ask percentage instead of Yes/No
- If Yes: request CMM level for activity
- Ask about strengths & weaknesses

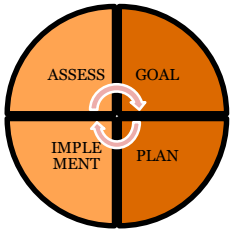
Validate results:

- Repeat questions to several people
- Lightweight vs full approach
- Anonymous interviews
- Aggregate gathered information

Agenda

1. Introduction
2. Assessment
3. **Improvements**
4. Tips & Challenges
5. Discussion

To-Be



Identify the targets for your company

Define staged roadmap and overall planning

Define application migration strategy

Gradual improvements work better than big bang

Have this validated by the project advisory board

Staged Roadmap

Security Practices/Phase	Start	One	Two	Three
Strategy & metrics	0,5	2	2	2
Policy & Compliance	0	0,5	1	1,5
Education & Guidance	0,5	1	2	2,5
Threat Assessment	0	0,5	2	2,5
Security Requirements	0,5	1,5	2	3
Secure Architecture	0,5	1,5	2	3
Design Review	0	1	2	2,5
Code Review	0	0,5	1,5	2,5
Security Testing	0,5	1	1,5	2,5
Vulnerability Management	2,5	3	3	3
Environment Hardening	2,5	2,5	2,5	2,5
Operational Enablement	0,5	0,5	1,5	3
Total Effort per Phase		7,5	7,5	7,5

Improvement Exercise

Define a target for your company and the phased roadmap to get there

Focus on the most urgent/heavy-impact practices first

Try balancing the complexity and effort of the different step-ups

Goal – Lessons Learned

Link to the organisational context

- Specific Business Case (ROI)
- Organisation objectives / risk profile

Think carefully about target SAMM level

- So you want to achieve all 3's. (Hmm. Who are you, NSA ?)
- Link to industry level
- Respect practice dependencies
- It can make sense not to include particular low-level activities, or to lower a current level

Goal – Lessons Learned

Get consensus, management support

Be ready for budget questions (linked to Plan phase)

- man days, CAPEX, OPEX
- General stats about % impact overall budget

Create & reuse own organisation template

Plan – Lessons Learned

Identify quick wins (focus on success cases)

Start with awareness / training

Adapt to upcoming release cycles / key projects

Spread effort & "gaps to close" over realistic iterations

Spread work, roles & responsibilities

SW security competence centre, development, security, operations

For instance service portfolio and guidelines: when and who ?

Take into account dependencies

Be ready to adapt planning

Plan – Budgeting

Average budget impact 5%-15% on project

Cost of tooling

- Central procurement vs per development group

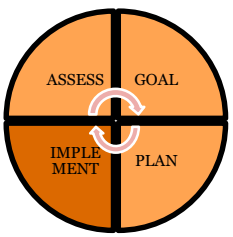
Cost of training

- Do not forget internal/external time spent

Cost of external suppliers / outsourcing

Different technology stacks will impact budget

Implementation



Implementation of dedicated activities according

Iterative, Continuous Process

Leverage good existing practices

Implement – Lessons Learned

Adapt & reuse SAMM to your organisation

Categorize applications: High, Medium, Low
based on risk: e.g. Internet facing, transactions, …

Recheck progress & derive lessons learned at each iteration

Create & improve reporting dashboard

Application & process metrics

Treat new & legacy code bases differently

Agile: differentiate between Every Sprint, Bucket & one-time AppSec activities

Balance planning on people, process, knowledge and tools

Lessons Learned – AppSec Competence Centre

Inject & spread best practices

"market & promote" – do not become risk/audit function

Do not become operational bottle-neck

Spread/hand-over knowledge to champions throughout organisation

Create & nurture AppSec community

Agenda

1. Introduction
2. Assessment
3. Improvements
4. **Tips & Challenges**
5. Discussion

The importance of a Business Case

If you want your company to improve, management buy-in is crucial

⇒ You will need a business case to convince them

Typical arguments:

- Improved security quality
- Better cost efficiency
- Compliance
- Risk management
- Customer satisfaction
- Reputation management

Entry Points

- Pick the weak spots that can demonstrate short-term ROI
- Typical examples
  - Awareness training
  - Coding Guidelines
  - External Pentesting
- Success will help you in continuing your effort

Application categorization

Granularity !

Inter-Connectivity !

Use this to rationalize security effort (according to the application risk)

Communication & Support

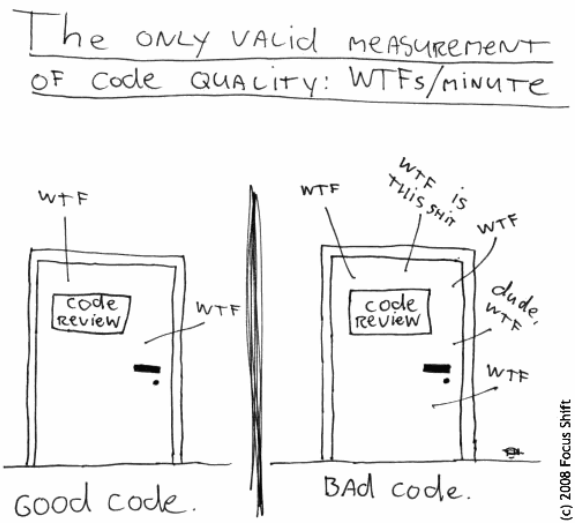
Critical success factor !

Spreading the message – broad audience

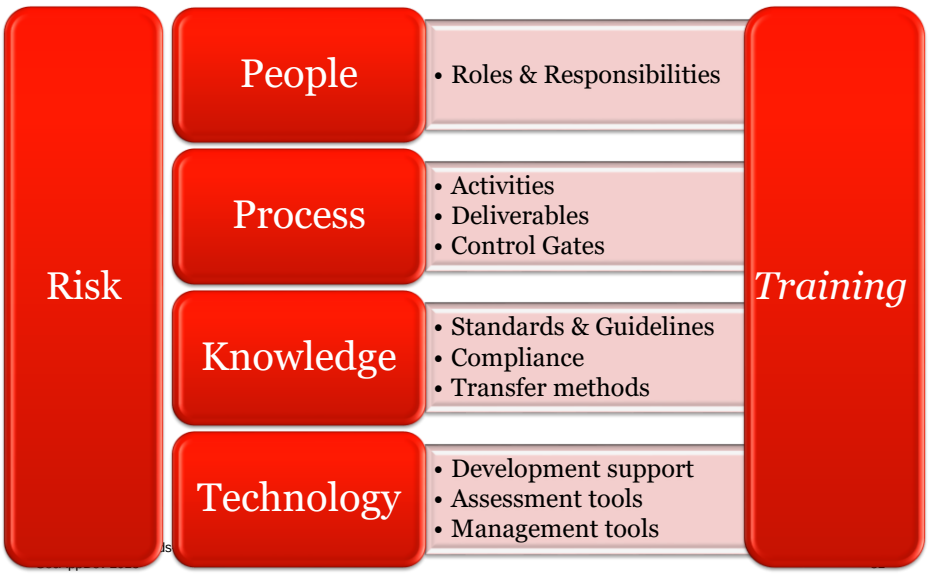
Setup a secure applications portal !

Regular status updates towards management

Monitoring & Metrics



SDLC Cornerstones (recap)



Conclusions

SDLC is the overall framework for most of this week's sessions

Models need to be adapted to your situation

Find balance for all cornerstones

Risk Management is key for rationalizing effort

Beware of the big bang