Security Touchpoints When Acquiring Software

Dr Carsten Huth

Nadim Barsoum

Dawid Sroka

OWASP AppSecEU 15

Amsterdam, The Netherlands

Topics

- **Context**
- **Problem Definition**
- **SDLC and Security Touchpoints**
- **Acquisition Process**
- **Conclusions**

Acknowledgement

A substantial part of the research for this presentation was carried out as part of EBS Protect.on Security Improvement Programme (SIP) 034 - Application Security. It is planned to train employees at E.ON in matters of Security Touchpoints When Acquiring Software.

CONTEXT AND PROBLEM DEFINITION

OWASP AppSecEU 15
Amsterdam, The Netherlands

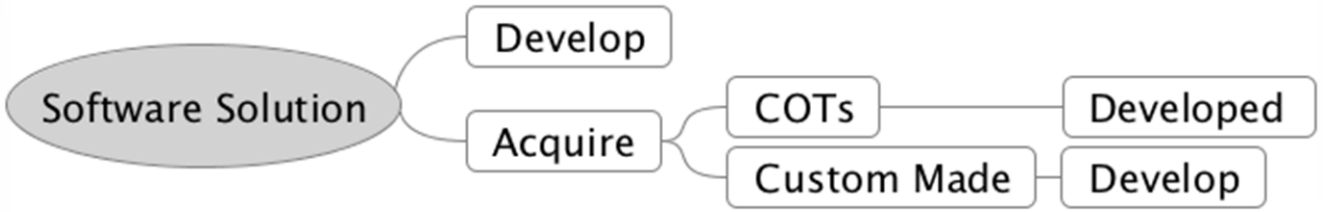
Context: Today's Landscape of SW Development & Acquisition

- Develop vs. acquire software
- Systems as a combination of acquired and developed components
- Open Source components
- The possibilities depend upon the acquisition type:
  - Commercial off-the-shelf (COTS)
  - Made-to-order
  - Forced upon due to merger/acquisition or reorganization
  - Obtained for free (normally open source)

Defining the Problem

Questions:

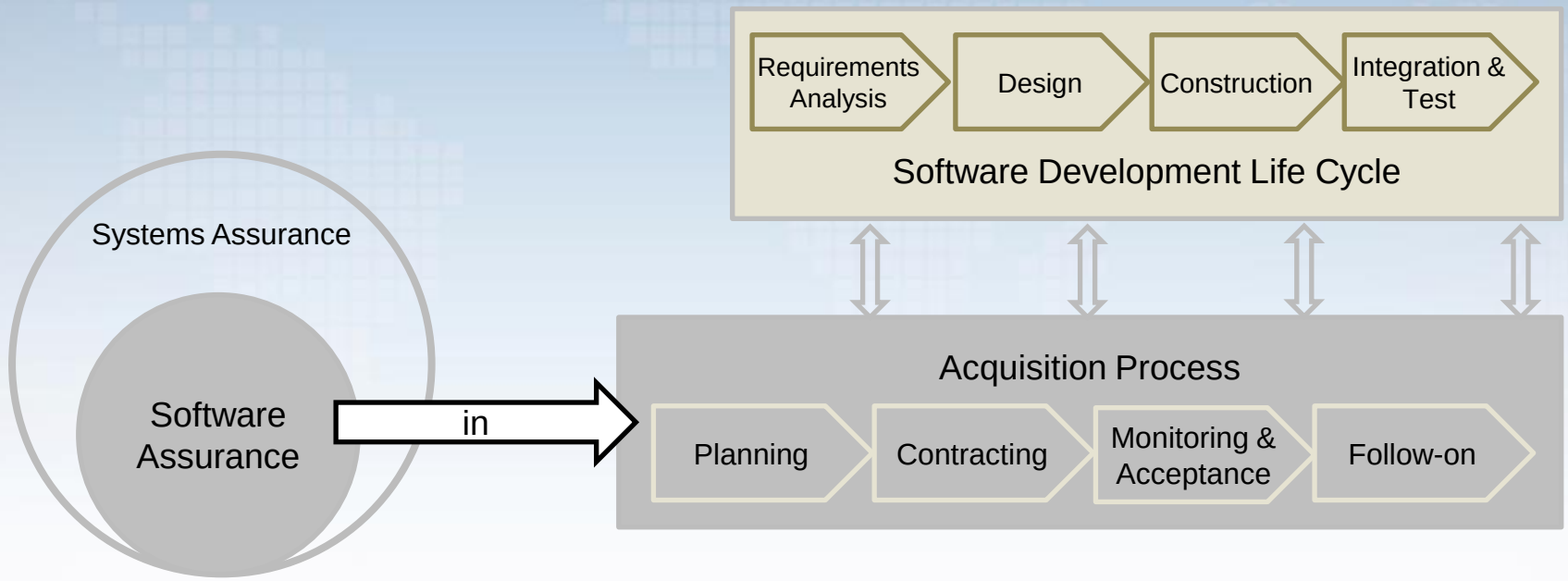
- Why are we acquiring software?
  - Address a business need
- Why don't we develop it?
  - Cost vs. Benefit
- How do we ensure that acquired software is secure?
  - Security Touchpoints when acquiring software



SDLC AND SECURITY TOUCHPOINTS

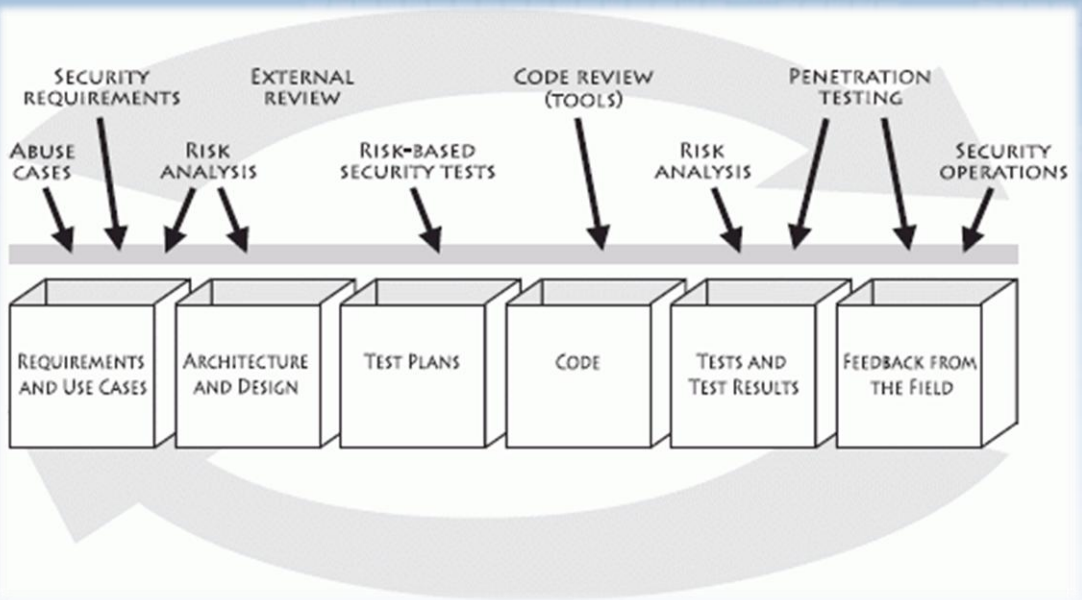
OWASP AppSecEU 15
Amsterdam, The Netherlands

How does security factor into the acquisition process?



Source: Software Assurance in Acquisition and Contract Language, U.S. Department of Homeland Security

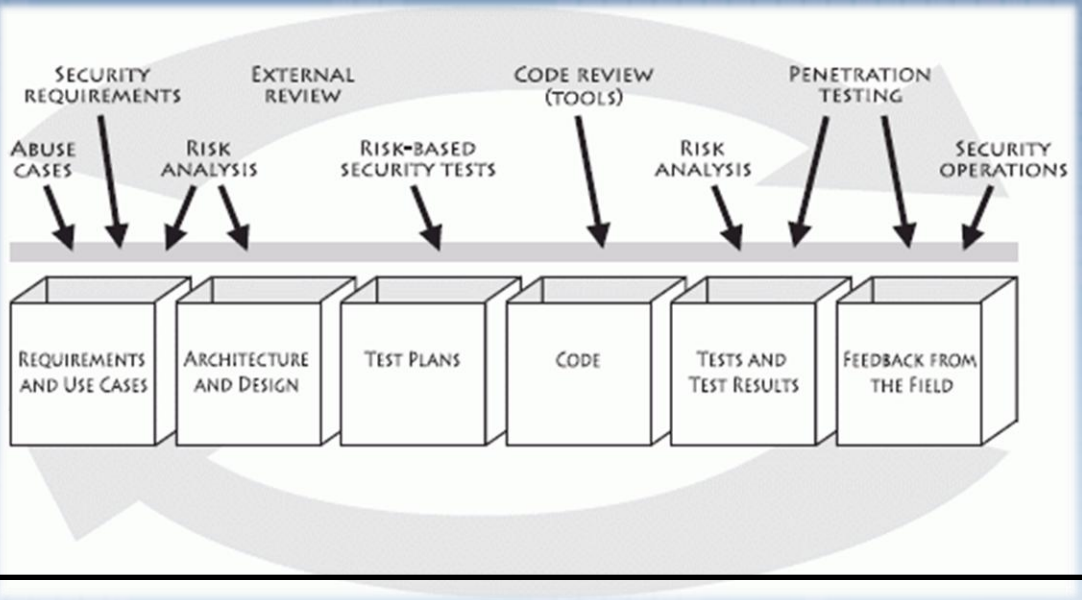
Context/Comparison:
What does it take to develop secure software?

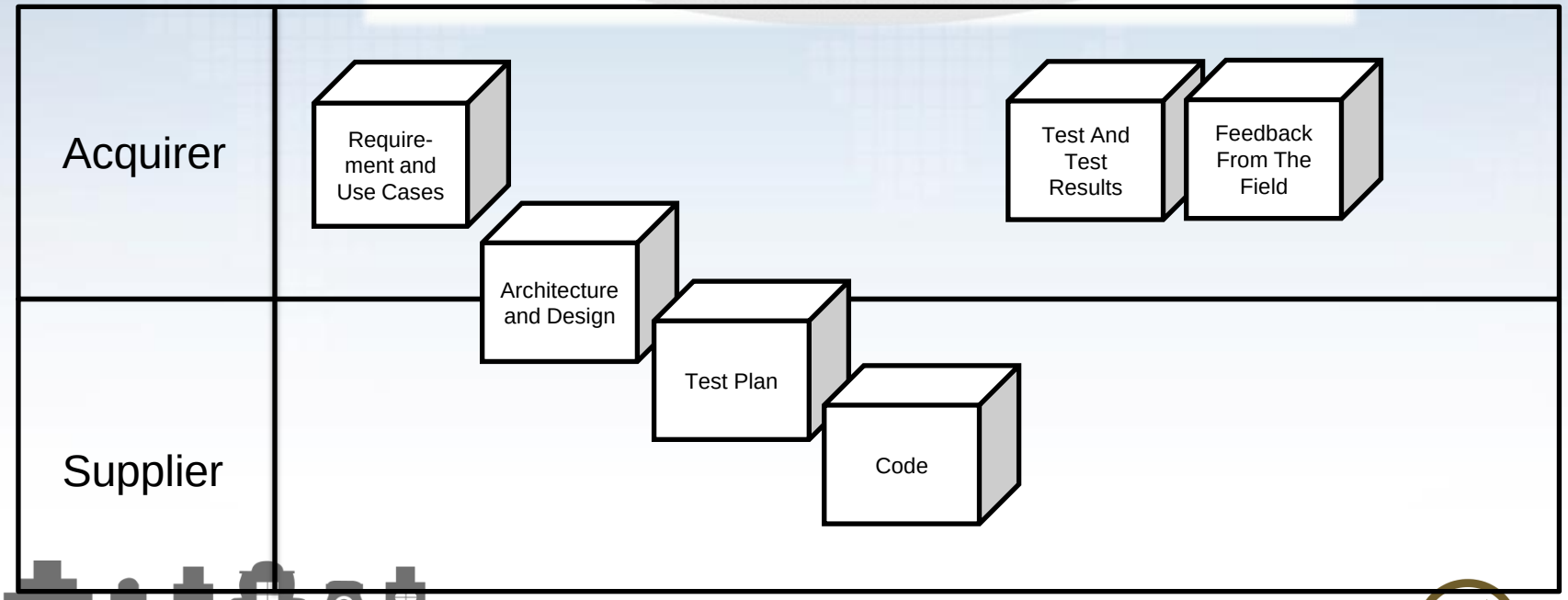


- Code review
- Architectural risk analysis
- Penetration testing
- Risk-based security tests

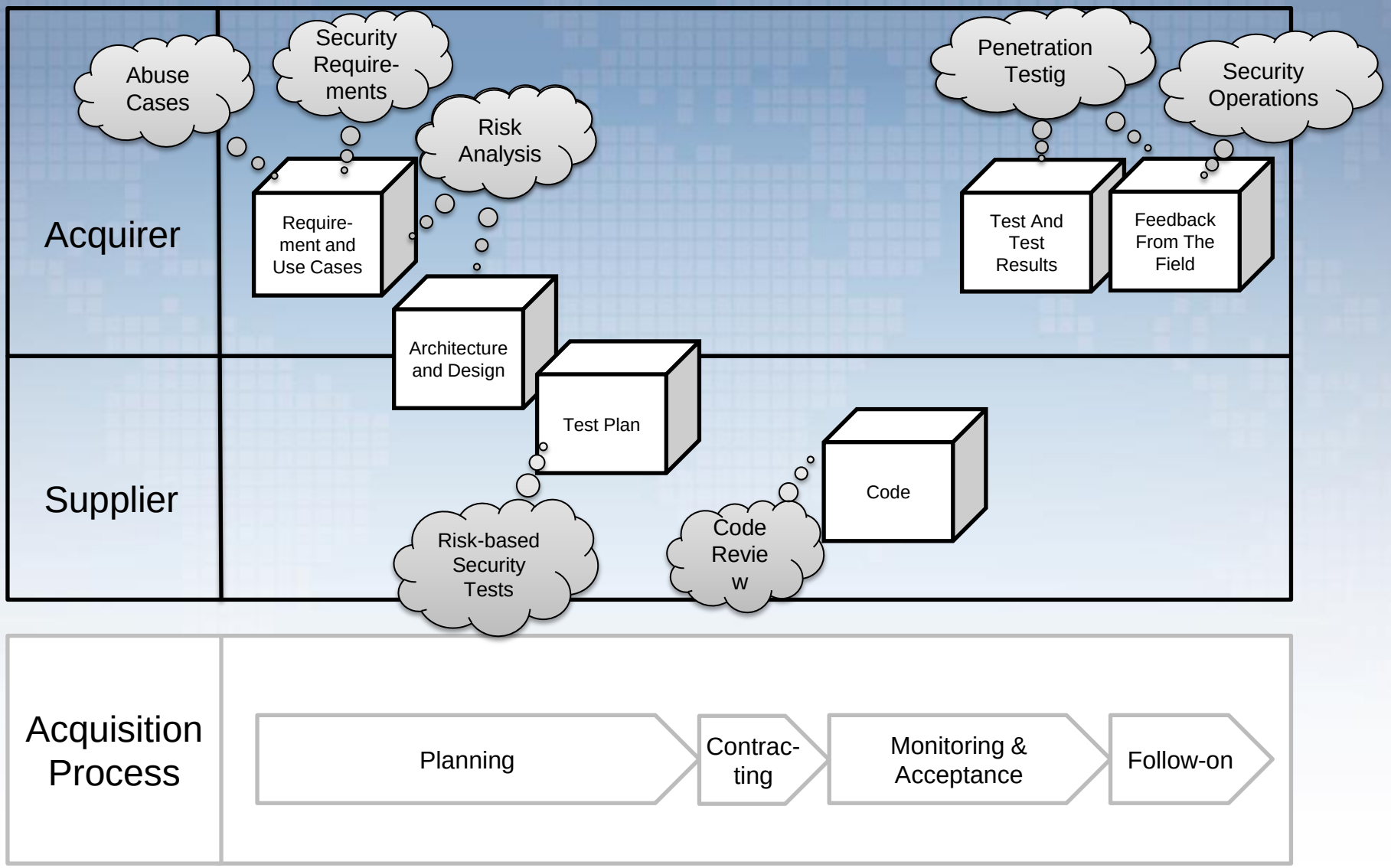
- Abuse cases
- Security requirements
- Security operations

Source: Gary McGraw: Building Security In Seven Touchpoints for Software Security

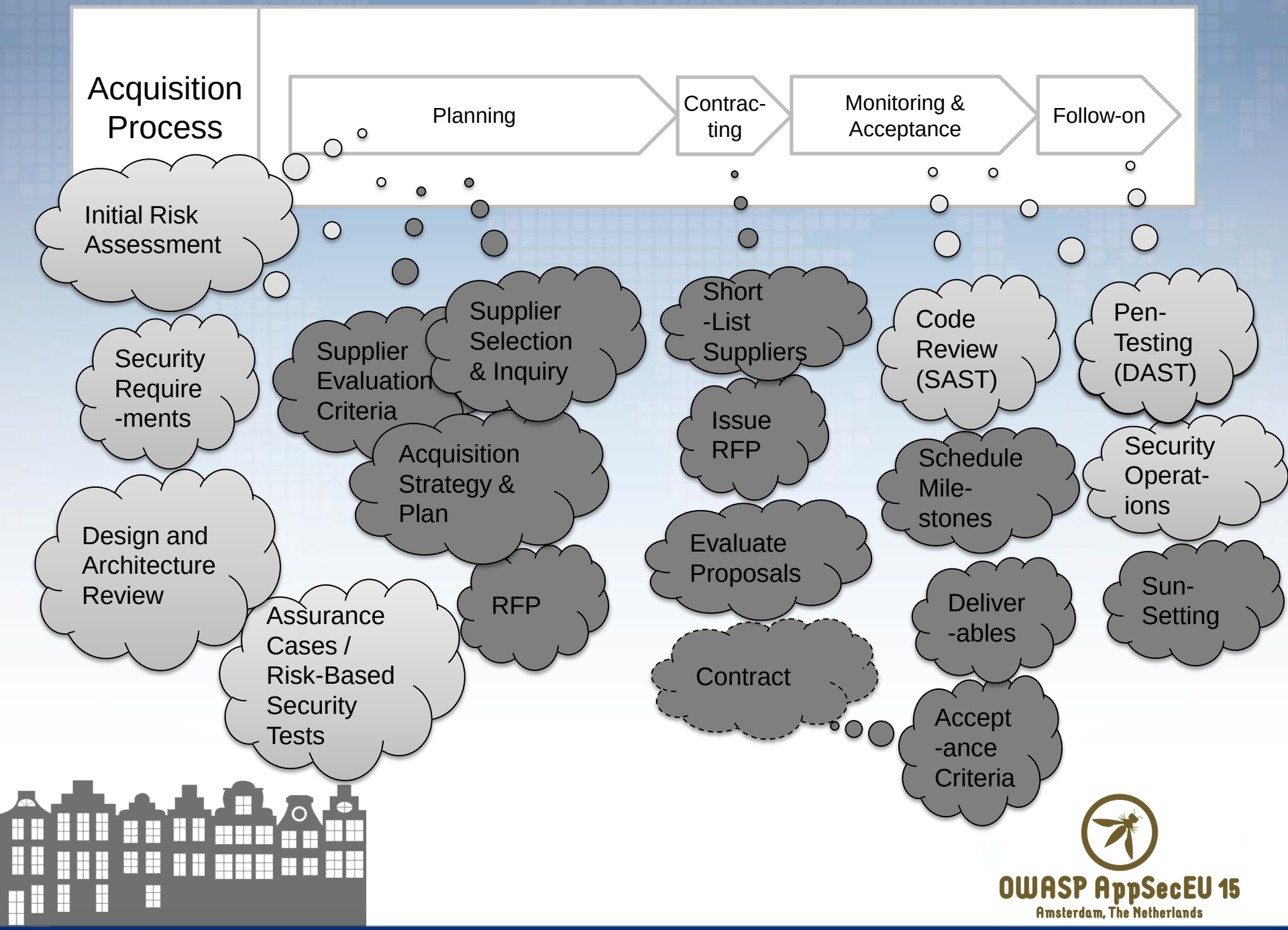




Source: Gary McGraw: Building Security In Seven Touchpoints for Software Security



Source: Gary McGraw: Building Security In Seven Touchpoints for Software Security


Acquisition Process
Planning
Contrac-ting
Monitoring & Acceptance
Follow-on
Initial Risk Assessment
Security Require-ments
Supplier Evaluation Criteria
Supplier Selection & Inquiry
Acquisition Strategy & Plan
Design and Architecture Review
Assurance Cases / Risk-Based Security Tests
RFP
Short-List Suppliers
Issue RFP
Evaluate Proposals
Contract
Code Review (SAST)
Schedule Mile-stones
Deliver-ables
Accept-ance Criteria
Pen-Testing (DAST)
Security Operat-ions
Sun-Setting

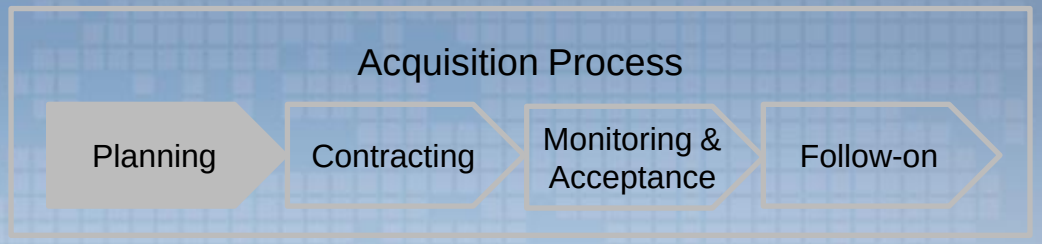
Security Touchpoints for Acquiring Software

Acquisition Type: / Touchpoint:	COTS	Made to order / custom software
Security Requirements	- Define security requirements (function and non-functional) - May not find exact fit of features → Largely similar to Software Development	Largely Similar to software Development
Abuse Cases	- Acquirer can develop abuse cases → Vendor can be requested to cooperate and include abuse cases in test case scenarios	
Architectural Risk Analysis	- Acquirer may only have limited view of internal architecture of the software → Vendor can be requested to submit security design and architecture documents for review	- **Acquirer may be involved in SDLC and given option to request architectural change as needed** → Vendor can be requested to submit security design and architecture documents for review
Security Tests	Potentially security tests can be run on an evaluation version of the software. Otherwise the vendor can be requested to provide evidence of such testing	
Code Review	Consider requesting to provide results of 3rd party code review	Possibly negotiate access to source code for direct assessment
Penetration Testing	Depends on type of software: - Web client, fat client, service, mobile device, … - Hosting: Hosted by Vendor or Acquirer? - Example 1: web client, hosted by Acquirer: If Acquirer has access to an evaluation version of the software, a penetration test can and should be performed - Example 2: Service, hosted by Vendor: Pen testing can only be done in agreement with Vendor, evidence of pen testing can be shared with Acquirer, or pen testing can be carried by a trusted third party	
Security Operations	Characteristic: Acquirer cannot make changes to the software. Therefore security vulnerabilities need patch management. - Bound to the mitigation schedule followed by the vendor. (Patch management, Service Level Agreements (SLAs))	- Defined support terms - Service Level Agreement (SLA)

ACQUISITION PROCESS – PLANNING

OWASP AppSecEU 15
Amsterdam, The Netherlands

Acquisition Process: Planning



- Determine the need for a new software solution
- Develop the security requirements of the system
- Set an acquisition strategy or plan
- Define evaluation criteria and plan
- Inquire about suppliers

Needs Determination and System Profiling

- What is the purpose of the software, what will it serve?
- How does the acquired software treat the problem?
- How much will it be exposed to threats?
- How widespread will it be?
- Who is liable in case of an exploit causing damage?

Identify Security Category

Typical questions for a risk analysis:

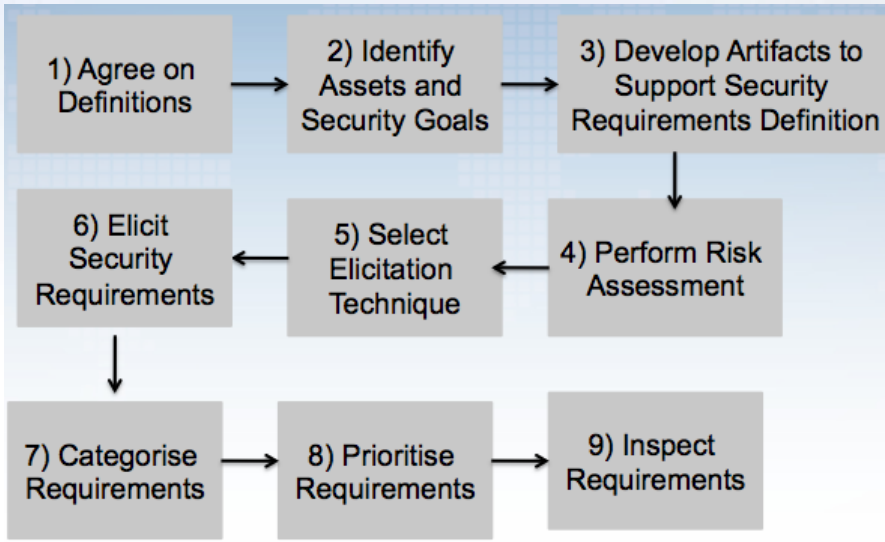
- What is the value of the system?
- **What software/data assets need to be protected to sustain the system?**
- **What are the potential adverse conditions to be prevented and managed?**
- What is the impact of software unpredictability?
- **How do security controls mitigate identified risks?**
- How is residual risk determined and managed?

- Determine impact of a breach of
  - Confidentiality
  - Integrity
  - Availability
- Determine the Security Category / Risk Rating of the system

Develop Security Requirements

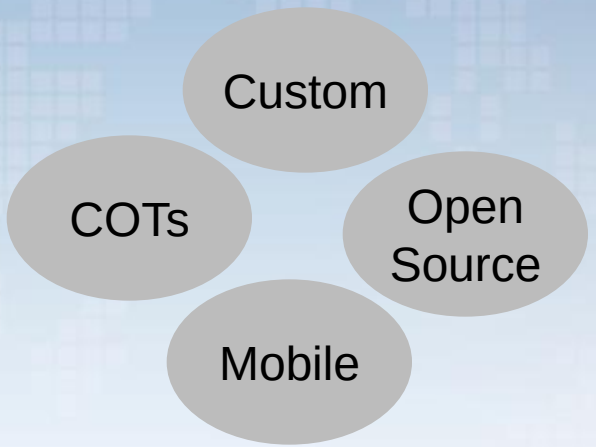
- Security Category will guide security requirements identification
- Define terminology to provide for common understanding
- Define levels of confidentiality, integrity and availability
- Establish a criteria to identify criticality of security concerns
- Build assurance cases
- Identify acceptance criteria
- Identify and review system architecture
- Refer to regulations and organizational policies

SQUARE Methodology



Identify Software Alternatives

- **Risk treatment:**
  - Accept
  - Mitigate
  - Avoid
  - Transfer or share



- **Tradeoffs when mitigating risk**
  - Risk reduction vs.
    Increased costs vs.
    Decreased operational effectiveness

Create Acquisition Plan

- **Roles and responsibilities**
  - Involve personnel with significant software security experience in all acquisition stages
  - State the expertise required and the specific involvement
- **Roadmap for completing actions and milestones**
  - Allow for the time needed to complete security tests
- **Special considerations in the purchase and implementation of software**
  - Define required qualifications of vendor or supplier
  - Plan for independent testing, instead of relying too much on existing certifications or attestations, which possibly resulted from security testing a different version or configuration

Request For Proposal Considerations

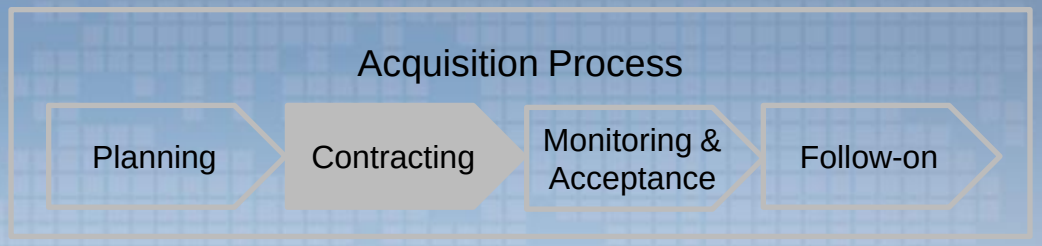
Identify:

- Request for Proposal content and format
- Statement of Work expectations and attachments
- Technical evaluation criteria and plan
- Incentives and penalties
- Deliverables
- Contractor monitoring and project indicators
- Risks pertaining to selected vendor strategy
  - e.g. vendor unfamiliar with legacy interface

Plan process for evaluating responses to RFP

ACQUISITION PROCESS – CONTRACTING

Acquisition Process: Contracting



- Issue Solicitation/RFP
- Evaluate Proposals
- Finalize Contract

Issue Solicitation/RFP and Evaluate Proposals

- **The Request for Proposals should include the following:**
  - Work statement
  - Terms and conditions
  - Instructions to suppliers
  - Certifications
  - Prequalification
- **Subject Matter Experts (SMEs) should evaluate each proposal along with the evidence provided to support answers to the due diligence questionnaire**
- **Sample questionnaire:**

No.	Question	COTS Proprietary	COTS Open-Source	GOTS	Custom
1	Can the pedigree of the software be established? Briefly explain what is known of the people and processes that created the software.	✓	✓	✓	✓
2	Explain the change management procedure that identifies the type and extent of changes conducted on the software throughout its life cycle.	✓		✓	✓
3	What type of license(s) are available for the open source software? Is it compatible with other software components in use? Is indemnification provided, and will the supplier indemnify the purchasing organization from any issues in the license agreement? Explain.	✓	✓		✓

Software Assurance Due Dilligence Questionnaires:

https://buildsecurityin.us-cert.gov/sites/default/files/DueDiligenceMWV12_01AM090909.pdf

Due Diligence Questionnaires

- **Help evaluate criteria**
  - Evidence should be requested or on-site follow-up reviews should verify the answers
- **Help address following concerns:**
  - Organizational history
  - Foreign interests and influences
  - **Security track record**
  - Financial history and status
  - Individual malicious behavior
  - **Software security training and awareness**
  - Software history and licensing
  - Development process management
  - Software development facility
  - Concept and planning
  - Design
  - Software development
  - Component assembly
  - Testing (supply-side)
  - Installation and acceptance
  - Software change management
  - Build-in software defenses
  - Assurance claims and evidence
  - Software manufacture and packaging
  - Support
  - Operating environment for services
  - Security monitoring
  - **Timeliness of vulnerability mitigation**
  - Service confidentiality policies

Perform for short listed suppliers

Software Supply Chain Risk Management & Due-Diligence - https://buildsecurityin.us-cert.gov/sites/default/files/DueDiligenceMWV12_01AM090909.pdf

Software Assurance Risks – Evaluating Suppliers

SwA Concern Categories	Risks	Purpose for Questions
Individual Malicious Behavior	A developer purposely inserts malicious code, and the supplier lacks procedures to mitigate risks from insider threats within the supply chain.	To determine whether the supplier has and enforces policies to minimize individual malicious behavior.
Security "Track Record"	A software supplier that is unresponsive to known software vulnerabilities may not mitigate/patch vulnerabilities in a timely manner.	To establish insight into whether the supplier places a high priority on security issues and will be responsive to vulnerabilities they will need to mitigate.
Financial History and Status	A software supplier that goes out of business will be unable to provide support or mitigate product defects and vulnerabilities.	To identify documented financial conditions or actions of the supplier that may impact its viability and stability, such as mergers, sell-offs, lawsuits, and financial losses.
Organizational History	There may be conflicting circumstances or competing interests within the organization that may lead to increased risk in the software development.	To understand the supplier's organizational background, roles, and relationships that might have an impact on supporting the software.

Source: Software Assurance in Acquisition: Mitigating Risks to the Enterprise - https://buildsecurityin.us-cert.gov/sites/default/files/publications/SwAinAcquisition%20MitigatingRisks%20to%20Enterprise.pdf

Contracting Touchpoints

- Vendor to deliver appropriate documentation
  - **Secure defaults and configurations**
- Terms for updates and new releases
  - Conditions for requested modifications and functional changes
  - **Security vulnerabilities resolution (0-days) and turn-around**
  - **Access to source code (agreement)**
  - **Modification of source code and willingness of vendor to participate**
  - Agree on possible future migration to other platforms
    - Vendor must support migration effort even if to another product
    - Vendor to grant access to new supplier for migration effort
- Warranties
  - Software performs according to requirements
  - **Software does not contain undisclosed features or security holes**
  - Expedited response in case of failure

Example: OWASP Secure Software Contract Annex

The OWASP has developed a contract annex for custom made software

Sample paragraphs:

(c) Design
Developer agrees to provide documentation that clearly explains the design for achieving each of the security requirements. In most cases, this documentation will describe security mechanisms, where the mechanisms fit into the architecture, and all relevant design patterns to ensure their proper use. The design should clearly specify whether the support comes from custom software, third party software, or the platform.

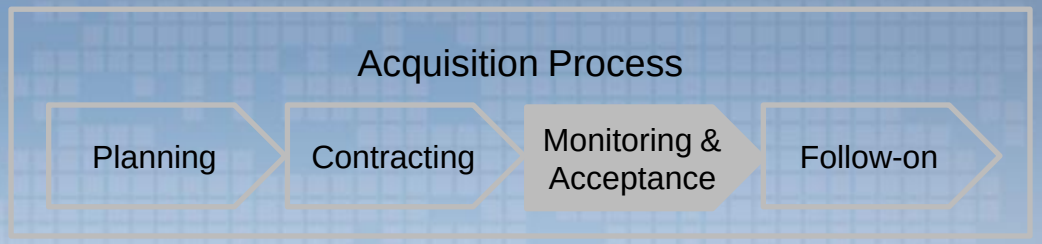
(e) Security Analysis and Testing
Developer will perform application security analysis and testing (also called "verification") according to the verification requirements of an agreed-upon standard (such as the OWASP Application Security Verification Standard (ASVS)). The Developer shall document verification findings according to the reporting requirements of the standard. The Developer shall provide the verification findings to Client.

(f) Secure Deployment
Developer agrees to provide secure configuration guidelines that fully describe all security relevant configuration options and their implications for the overall security of the software. The guideline shall include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured for security. The default configuration of the software shall be secure.

Source:
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

ACQUISITION PROCESS – MONITORING AND ACCEPTANCE

Acquisition Process: Monitoring & Acceptance



- Establish work schedule
- Implement change control
- Review and accept deliverables

Establish Work Schedule & Implement Change Control

- Schedule should include specific timelines for meeting or delivering the security requirements

- The change control procedures should ensure that security requirements are not compromised when changes are made

Review and Accept Deliverables

- **Deliverables other than the software can be:**
  - documentation
  - test cases and results
- **Acceptance criteria should be:**
  - explicit
  - measurable
  - included in the terms and conditions
- **Examples of acceptance criteria:**

"The Supplier shall demonstrate that all application software is fully functional when residing on the operating system and on middleware platforms used by the Acquirer in its production environment, configured as noted above."

"The Supplier shall NOT change any configuration settings when providing software updates unless specifically authorized in writing by the Acquirer."

- **SMEs to review each software deliverable and analyze test results produced by the supplier or independent tester to ensure that security requirements are met**

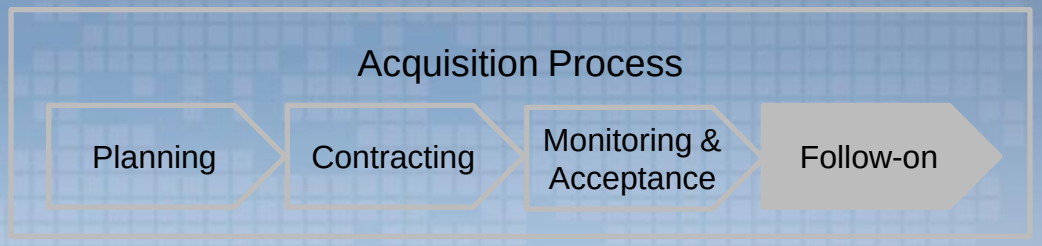
This can be DAST or manual penetration of testing of the application

3rd party Certifications for Security Testing

- **Industry reputation** – is supplier known for this type of testing?
- **Methodology** – how does supplier propose to perform the required tests?
- **Relevance** – is the supplier able to collect and digest the security requirements relevant for your systems and identify relevant security issues?
- **References** – Can supplier furnish references of other clients in your industry?
- **Competence** – is the supplier able to securely process and maintain information about our system? Reports? Results? Do they practice due diligence?
- **Common services**
  - Static Application Security Testing
  - Dynamic Application Security Testing
  - Security Architecture and Design Reviews

ACQUISITION PROCESS – FOLLOW-ON

Acquisition Process: Follow-on



- Maintain the software
- Dispose of or decommission the software

Maintain the Software

- Prepare for the long run: changes of the software, its configuration or its context may invalidate assumptions made for security requirements
- Configuration control
- Upgrades and patches
- Support

- Operational security
- Security vulnerabilities found in operation
- Identify severity of vulnerabilities
- SLA terms for handling critical issues

Dispose of or Decommission the Software

- Safe and secure retirement of software
- Related data should also be securely
  - destroyed
  - migrated
  - archived

RECAP AND CONCLUSIONS

Recap

- Acquisition or develop is a business driven cost benefit decision.
  - The Acquisition process includes business criteria (performance, stability) as well as security criteria
  - This presentation outlines the security touch points in the acquisition process to highlight where security expertise is required in the acquisition process and where security practices should be applied

- Acquisition process is very much a part of the System Development Lifecycle
- Software Development Lifecycle Security Touch Points apply according to strategy
- Acquisition Phases include: Planning, Contracting, Monitoring & Acceptance and Follow-on
- For each of the above phases contract is key document to ensure vendor commitment before, during and after acquisition

Conclusions

- Apply touchpoints for building secure software to the software acquisition process (e.g. abuse cases, architectural risk analysis, security requirements, …)
- Use risk-driven process in selecting software suppliers
  - Questionnaire for COTS and custom software
- Require security testing (SAST, DAST) of software to be acquired
  - Ensure security reports are periodically submitted for review and that identified risks are treated
- Introduce security-focused terms and conditions into acquisition contract
  - Consider contracting touchpoints and OWASP Secure Software Contract Annex

How much have we developed this topic?

- Fragments/parts of the process exist but no best practice recommendation for the whole process of security touchpoints
- Recognised the overlaps in acquisition and development with regards to security
- Hope to build a gauge system that can help easily identify aspects to consider for the different system development scenarios

Sources

1. Software Assurance in Acquisition: Mitigating risks to the Enterprise - Mary Linda Polydys and Stan Wisseman
2. An Investigation of ‘Build vs. Buy’ Decision for Software Acquisition by Small to Medium Enterprises - Farhad Daneshgar, Lugkana Worasinchai and Graham Low
3. Development and Acqusition – Federal Financial Institutions Examination Council
4. Arguing Security - Creating Security Assurance Cases - Charles B. Weinstock, Howard F. Lipson, and John Goodenough
5. Software Acquisition Planning Guidelines – Software Engineering Institute (SEI)
6. Software Supply Chain Risk Management & Due-Diligence (Software Assurance Pocket Guide Series: Acquisition & Outsourcing, Volume II Version 1.2, June 16, 2009)
7. Adapting the SQUARE Method for Security Requirements Engineering to Acquisition- Nancy R. Mead - SEI
8. Security Quality Requirements Engineering (SQUARE) Methodology - Nancy R. Mead et. Al Carnegie Melon - SEI
9. Developing a Product Line Acquisition Strategy for a DoD Organization: A Case Study - John K. Bergey et al
10. The DoD Acquisition Environment and Software Product Lines - John K. Bergey et al

Thank you! Questions?

- Carsten Huth: Carsten.Huth@hp.com
- Nadim Barsoum: Nadim.Barsoum@hp.com
- Dawid Sroka: Dawid.Sroka@hp.com