CISSP® 2015

Domain 6: Security Assessment & Testing

V1

Domain 6: Security Assessment & Testing

A. Design & validate assessment and test strategies

- The goal is to study security and identify **improvements** to secure the systems.
- An assessment for security is potentially the **most useful** of all security controls.
- Understand:
  - System Design should be validated with requirement to prevent design bug or vulnerability
  - Software is different from Hardware

Software vs. Hardware

	Software	Hardware
Quality depends on	Design & development	Design & development & manufacture
Cloning	Easy	Difficult
Complexity	Branching → complex	Low/Medium
Interface or interoperable	No standard	Highly standardization (USB)
Modification	Easier	Difficult
Performance vs. Aging	will not degrade	May degrade

B2. Penetration testing

- Simulating attack on network or system at **request of the owner or senior MGT**
- Perform periodically, use diff tools
- Senior Mgt be aware of risk and performance impact (authorization letter)
- Zero knowledge or Partial knowledge
- Internal or external
- **Blind test**: use public available data only, network staff is aware
- **Double-blind test**: similar to blind, network staff is not aware
- **Example tools:** Wireshark, w3af, Back Track

B3. Log reviews

- **Consideration**: store audit **securely**, keep right size
- **Review of Audit Information**
  - can be manual or automatic
  - event-oriented or periodical
  - **Audit-reduced tool**: reduce / filter the amount of information within audit log
  - **Security significant:** Privileged account activity, Exception, Configuration change, system startup / Shutdown, profile administration, abnormally high volume
- **Protecting Audit Data and Log information**
  - Most concern and Dangerous if intruder is able to delete or modify the audit log
  - Scrubbing: deleting incriminating data within audit log

B3. Log reviews

- **Log may come from:**
  - **Anti-malware, Anti-virus software**
  - **Intrusion Detection and Intrusion Prevention systems**
  - **Remote Access Software**
  - **Web Proxies**
  - **Patch Management Software**
  - **Authentication Servers**
  - **Routers**
  - **Firewalls**
  - **Network Access Control / Network Access Protection Servers**

B4. Synthetic transactions

- **Purpose**: To **track** availability, functionality and responsiveness of website; Enables a webmaster to **identify problems** (slow or down) before actually affecting customers.
- **Passive**: Real User Monitoring (RUM): capture and analyze real user transactions
- **Active**: Use external light-weight agent / script to simulate and measure user steps

B5. Code review & testing

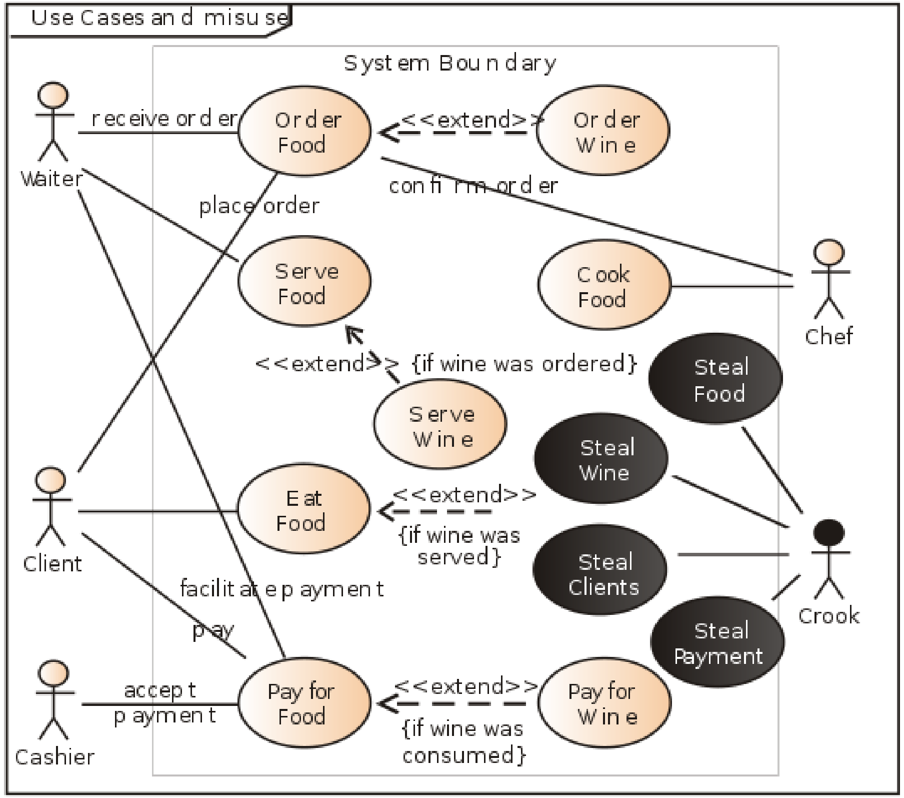
- **Bugs** discovered at **earlier** stage of development are **less expensive** to fix than later in the development cycle; normally can be identified earlier by **code review or testing**;
- **Code review (or Peer review)** is systematic examination of source code to find and fix mistakes overlooked in the initial development phase, improving both the overall quality of software and the developers' skills.
- **Examples of programming issues:**
  - Bad programming pattern causes SQL injections
  - Hardcoded plaintext password
- **Example of Controls:**
  - Such as Development checklist / guideline;
  - Pair Programming

B5. Code review & testing

- **Testing**
  - **White-Box-Testing:** Testers know internal details, such as source code
  - **Black-Box-Testing:** no internal details of the system
  - **Dynamic Testing:** execute program and observe behavior
  - **Static testing**: Analyze requirement and structure, without executing program
  - **Manual Testing:** test scenario by human
  - **Automated Testing**: test by specialized application

B6. Misuse case testing

- **“Use case”** specifies required (or normal) behavior of software under development.
- **“Misuse Case”** is a business process modeling tool, which is the **inverse** of “Use Case”. Something should not happen;
- “Misuse Case” helps in defining new requirements, which are expressed as new Use Cases.



B7. Test coverage analysis

- to measuring how much a program has been tested.
- many kinds of test coverage:
  - Statement Coverage
  - Decision (Branch) Coverage
  - Condition Coverage
  - Multi-Condition Coverage
  - Loop Coverage
  - Path Coverage
  - Data Flow Coverage
- For example, in Statement coverage:
  - Has a particular statement ever been executed?
  - How many times has a statement been executed?
  - Have all the statements in a program been executed, at least once?

B8. Interface testing

- Determine data **transfer** among different programs or servers are working as **expected**, as designed.
- **What to check?**
  - All interactions among application are executed properly
  - Error handling, such as duplication or loss transaction
  - What about communication failed or reset
  - Compatibility of software, hardware, network connections

C. Collect security process data

C1. Account Management

- **Procedure** for account management is a **preventive** and proactive controls.
- However, there should be **detective** control (such as monitoring) to measure the **effectiveness** of these controls.
- For **example**, how long to create/change/remove a profile when the staff joins, transfers, promotes or leaves.
- Another **example**: the result of annual user recertification. If the gap is large, means the problem in design or operation of procedure.

C2. Management review

- A Software **management review**: management study into a **project's status** and allocation of resources.
- A **systematic evaluation** of a software acquisition, supply, development, operation, or maintenance process performed by or on behalf of management
- To monitor **progress**, determine the status of plans and schedules, confirm requirements
- To evaluate the **effectiveness** of management approaches used to achieve fitness for purpose.

C3. Key performance and risk indicators

- **Key Performance Indicator (KPI)** is a type of performance measurement.
  - right KPIs relies upon a good understanding of what is important to the organization.
  - For **example**: transaction throughput, helpdesk response time etc.
- **Key Risk Indicator (KRI)** is a measure to indicate how risky an activity is.
  - KRI give an early warning to identify potential event that may harm continuity of the activity/project.
  - For **example**, storage full %, traffic volume from a single IP, Packet with same source/destination IP etc.
- There are **too many** indicators, we must identify **Key** Indicators
  - High business impact
  - Easy to measure
  - With high correlation with the performance/risk
  - Sensitivity

C4. Backup verification data

- **Backup and Restoration Systems**
  - Policy / Procedure what gets backup, how often, how to backup….
  - Normally automatic backup
  - Full, differential and incremental backup
  - **Need to verify Backup integrity periodically**

C5. Training & awareness

- **Evaluating the training & awareness program**
  - Monitor and evaluated for effectiveness
  - By questionnaires and survey
  - By quiz
  - By comparing number of security incidents before/after training

C6. DRP & BCP

- There are many data in DRP & BCP, such as BIA result, drill result etc.
  - **BIA result**: RTO, RPO, Critical resource…
  - **Drill result**:
    - BCP coordinator should maintain historical drill result
    - These test problem should be documented, delegated, reviewed and followed up.
    - Evaluate thoroughness and accuracy to objectives

D. Analyze & report test outputs

- Common **problems** of test result
  - Too verbose
  - Too technical
  - Cannot link to business impact or risk rating
- The result format should be communicated and agreed in **advance**, especially work with 3rd parties.

E. Conduct or facilitate internal & third party audits

- **Auditing** is an alternative way to evaluate the **compliance of procedure and effectiveness.**
- Audit is more **independent** than internal expertise.
- **SAS70** (Statement on Auditing Standards): it is Service Organization Control (**SOC**) audit to provide **assurance** to Clients of service provider. Then no need to perform audit individually.