

# **Sample Exam Advanced Level Syllabus**

## **Security Testing**

Version GA – March 2016

---

International Software Testing Qualifications Board

---



Copyright Notice

This document may be copied in its entirety, or extracts made, if the source is acknowledged.

## Revision History

Version	Date	Remarks
1.0 – Beta	22 Sept 2015	Beta version of sample exam
1.0 – GA Candidate	04 March 2016	Updates after Exam WG review – question 18 and 29 changed to K3 level, typo in question 35 fixed, point allocations for #25 - #32 fixed.
1.0 – GA	15 March 2016	GA version with minor edits. LOs removed.

**Note: The LO for the question is highlighted. For some questions there were several LOs from which the question could be derived.**

AS-1.1.1 (K2) Understand the role of risk assessment in supplying information for security test planning and design and aligning security testing with business needs

AS-1.3.1 (K2) Understand the purpose of a security audit

**Question #1 (1 pt)**

Which of the following is a purpose of a security audit?

- a. To prevent users from using simple passwords
- b. To reveal insufficient patch updates provided by the vendor
- c. To halt unauthorized intruders from accessing the system
- d. To require users to change their password after a predetermined set of days

B is correct as keeping the patch updates current on the system is one of the purposes of a security audit. The others are good practices, but not the purpose of the security audit.

AS-1.1.2 (K4) Identify the significant assets to be protected, the value of each asset and the data required to assess the level of security needed for each asset

AS-1.1.3 (K4) Analyze a given situation to determine the proper risk assessment techniques to use to identify current and future security threats

**Question #2 (3 pts)**

You are responsible for ensuring that new vendors brought on externally for the project are fully compliant with government mandated guidelines as part of your risk assessment. On which stakeholders should you primarily focus to ensure these outside vendors continue to comply?

- a. Customers, users, and vendors to ensure there is good communication between them
- b. Public users and vendors who will follow the law as it applies to the source of information
- c. Federal and local agencies that communicate guidelines to follow
- d. Both internal and external sources that will use the information for further analyzing the risk

C is correct as this is the source of the guidelines. The guidelines may change so it's important to keep the communications channels open with these folks. A, B and D all need to be informed, but the information needs to come from the federal and local agencies.

AS-1.2.1 (K2) Understand the concept of security policies and procedures and how they are applied in information systems

**Question #3 (1 pt)**

Which of the following is a consequence of a policy that minimizes access to a system or device to acceptable levels?

- a. More devices are added to mitigate the impact
- b. Proper controls of self-provisioning devices such as routers are prohibited
- c. Devices that do not conform are removed from the wireless network
- d. Access to the VPN is severely restricted

C is correct. When this policy is implemented, non-conforming devices will be removed until they conform. A is not correct as this would not be an expected results. B is not correct because these controls will be encouraged. D is not correct because access will be controlled, not severely limited.

**AS-1.2.2 (K4) Analyze a given set of security policies and procedures along with security test results to determine effectiveness**

**Question #4 (3 pts)**

Your role as the Security Administrator is to help your organization understand the effectiveness of security policies and procedures across the enterprise. You will report your effectiveness findings to Senior Management after your analysis has been completed. Which of the following is the optimum strategy to accomplish this?

- a. Implement a static analysis evaluation independently for both policies and procedures
- b. Analyze the results from a security test to validate effectiveness
- c. Evaluate security test results that focus on current threats and attacks
- d. Evaluate the static test results for new and emerging software threats

B is correct. You should analyze the results of a security test to see if the policies and procedures have been followed and are effective. A is not correct because the static analysis should be over the code, if anything. C is not correct because the focus shouldn't just be on current threats and attacks, but also on configurations, etc. D is not correct because the focus is not just on the emerging threats.

**AS-2.2.1 (K2) Understand why security testing is needed in an organization, including benefits to the organization such as risk reduction and higher levels of confidence and trust**

**AS-2.3.1 (K2) Understand how project realities, business constraints, software development lifecycle, and other considerations affect the mission of the security testing team.**

**Question #5 (1 pt)**

If an organization experiences a security breach and legal action results, how does it help the organization to have done security testing?

- a. It can show that the organization has done due diligence to try to prevent such an incident
- b. The documentation from the security testing can be used to track down the perpetrator
- c. Since any important information would have been backed up before security testing, this backup can be used to restore any compromised information
- d. By tracing through the documented tests, the security testing team can discover how the breach was possible

A is correct per the syllabus. B is not correct because this information would probably not be helpful. C is not correct because the backup would likely be out of date and the information was not necessarily corrupted, but rather stolen or viewed. D is not correct because, although this may help point to areas where testing was not sufficient, it will not support the organization's defense of legal actions.

**AS-2.4.1 (K2) Explain why security testing goals and objectives must align with the organization's security policy and other test objectives in the organization**

**AS-2.4.3 (K2) Understand the relationship between information assurance and security testing**

**Question #6 (1 pt)**

Which of the following is a correct statement?

- a. Information assurance is a part of security testing
- b. Information assurance and security testing are two terms for the same thing
- c. Security testing is a part of information assurance
- d. The two terms refer to different areas of security

C is correct, security testing is a part of the larger area of information assurance.

**AS-2.4.2 (K3) For a given project scenario, demonstrate the ability to identify security test objectives based on functionality, technology attributes and known vulnerabilities**

**Question #7 (2 pts)**

You are working at a bank as part of the security testing team. During a recent security audit it was noted that the user's passwords were not strong enough. Since that time, a new set of requirements has been issued to ensure password strength. Given this information, what would be a reasonable set of security objectives for general password rule testing?

- 1. Verify that passwords meet the requirements for length
  - 2. Verify that passwords meet the requirements for usage of characters, numbers, letters and capitalization
  - 3. Verify that passwords can be retried three times
  - 4. Verify that passwords cannot be re-used within a one year timeframe
  - 5. Verify that passwords must be reset every three months
  - 6. Verify that the user can request to have their password emailed to them
  - 7. Verify that the system administrator can reset a locked password
- 
- a. 1, 2, 3, 4
  - b. 1, 2, 4, 5
  - c. 3, 4, 6, 7
  - d. 4, 5, 6, 7

B is correct because all of these are valid security objectives. A is not correct because 3 is functional rather than security related (unless it locks them out, but we don't know that from this description). C is not correct because 6 and 7 are both functional rather than specific security requirements. D is not correct for the same reason as C.

**AS-2.5.1 (K3) For a given project, demonstrate the ability to define the relationship between security test objectives and the strength of integrity of sensitive digital and physical assets**

**Question #8 (2 pts)**

Your company recently made headlines after a security breach resulted in confidential customer information being stolen. Management has reacted with an edict that the scope of the security testing objectives needs to be expanded immediately. While you agree that something needs to be done, you are worried that this approach may be too reactive and may not result in the testing that is needed.

According to the syllabus, what is a reasonable concern if these initiatives are implemented?

- a. The testing will still miss issues because it will not be well-focused
- b. The testing will be outsourced so that it can be done more efficiently
- c. The testing scope may be too large and there may not be adequate resources to complete it
- d. The testing objectives are not clearly defined and may miss the same issues as previously escaped to production

C is correct per the syllabus as this is a common problem when the objectives are broadly defined. A and D are reasonable concerns, but we don't know when or how the test objectives will be defined, so this may be controllable. B is always a possibility and may be the right thing to do in this case, but there has been no indication that outsourcing will occur at this time.

AS-2.6.1 (K4) Analyze a given situation and determine which security testing approaches are most likely to succeed

AS-2.6.2 (K4) Analyze a situation in which a given security testing approach failed, identifying the likely causes of failure

AS-2.7.1 (K4) Analyze KPIs (key performance indicators) to identify security testing practices needing improvement and elements not needing improvement

### Question #9 (3 pts)

You have just accepted a job to create a security testing team for a company that handles sensitive medical information that is shared between doctors and hospitals. You have noticed that the security around this information is not sufficient to protect it from hackers or even accidental exposure. The person who had your job previously brought in a number of consultants to do testing, but the findings were not documented and no changes were implemented. In fact, you don't even know what the coverage was from the testing. You have presented your findings to the executive management team. While they have agreed in principle that they need security testing, they have not allocated the necessary budget or time to the project. It appears that while they think security is a good idea, they really have no understanding of what should be done or how it should be done. What should be your first step toward getting the executives aligned with the work that needs to be done?

- a. Create a detailed list of all the possible security holes and present these to the executives
- b. Provide a summary of the testing approach that you propose and give examples of how the testing will be conducted
- c. Bring in the legal team to explain what a security breach could cost the organization
- d. Create a security policy and security testing policy and demonstrate how that aligns with your proposed testing approach

D is correct. At this point, the organization needs a high level policy and plan to move forward. Without this policy, the testing may continue to be sporadic and high level support and funding will be difficult. A and C are not correct at this point although they might be useful if you have trouble getting funding when you work to implement the policy. B is not right because you need an overall policy before you define the approach.

AS-2.6.3 (K3) For a given scenario, demonstrate the ability to identify the various stakeholders and illustrate the benefits of security testing for each stakeholder group

### Question #10 (2 pts)

You have just come from a meeting where there was much discussion regarding the security approach of the organization. One of the points of emphasis was the importance of testing to ensure that data is protected from fraudulent access, particularly credit card information. You have been asked to prepare

a set of testing objectives that will help address this risk area. One of your tasks is to ensure that you are covering all the concerns of the stakeholders. Which stakeholder group is most likely to see the benefits from your efforts?

- a. Executive management
- b. Compliancy officers
- c. Business customers
- d. Regulatory officers

C is correct. The business customers will be most concerned with protection from fraudulent access as it is their data which is vulnerable. We would hope that A, B and D would also be involved, but this is not usually their primary benefit.

**AS-3.1.1 (K3) For a given project, demonstrate the ability to define the elements of an effective security test process**

**Question #11 (2 pts)**

As a Security Administrator you are responsible for all aspects of the security process, including testing. For this particular process you are to use conceptual tests as a basis for manual tests and execute these from an external vendor's perspective. Which security testing process does this most parallel?

- a. Security test creation of conditions and objectives
- b. Security test implementation
- c. Overall evaluating and reporting of security testing
- d. Security test analysis and design

B is correct. The use of the conceptual tests to create the manual tests and perform the execution is part of the security test implementation. A and D are not correct because this has already been done with the creation of the conceptual tests. C will occur after the tests have been executed.

**AS-3.2.1 (K4) Analyze a given security test plan, giving feedback on strengths and weaknesses of the plan.**

**Question #12 (3 pts)**

You have been developing a security test plan for a system that will store medical information for patients and will transfer that data to specialist doctors. You have covered the following areas in your plan:

- Scope (what's in scope and out of scope)
- Roles and assignments
- Responsibilities (vendors vs. internal)
- High level schedule
- Environment requirements and setup
- List of necessary authorizations and approvals

What information do you still need to supply in this test plan to meet the minimum requirements as noted in the syllabus?

- a. A list of the necessary credentials and training for the personnel who will be conducting the testing
- b. A schedule showing the time that will be required to design, run and evaluate the security tests

- c. A copy of the regulatory standards that must be met by this system
- d. A list of the individuals who will be doing the testing and their contact information in the event of a security breach

B is correct per the syllabus. A might be needed but that is not one of the minimum requirements and may already be understood in the roles and responsibilities section. C is not correct because the standards might be referenced but not included in the plan. D is not correct because this level of detail does not belong in the plan and the individual testers should not be contacted during a breach.

AS-3.3.1 (K3) For a given project, implement conceptual (abstract) security tests, based on a given security test approach, along with identified functional and structural security risks

AS-3.3.2 (K3) Implement test cases to validate security policies and procedures.

### Question #13 (2 pts)

Which of the following test cases would best test a system's security procedure?

- a. Three unsuccessful login attempts will generate a lock-out message. Contact your manager or the System Administrator so they can give you a temporary password over the phone. You must then change the temporary password upon logging in. You log out then log back in using your newly created password.
- b. You receive a lock-out message after several attempts to log in. You call IT support to obtain a new password. You log in with the temporary password, log back out, then log in again and enter a new password.
- c. After several attempts you are locked out of the system. You use a password that worked previously. However, it no longer works. You attempt to create a new password but you are now locked out. A complete reboot of the machine is the next step to take you to the prompt to re-enter the password.
- d. After the first attempt to use an invalid password you immediately pull up a list of passwords on your notepad on your PC to ensure you are using the correct one. You try another password from the list and it works.

A is correct. B and C are not correct because of the word "several". D is not correct because this would definitely not be a good security practice.

AS-3.4.1 (K2) Understand the key elements and characteristics of an effective security test environment

AS-3.6.1 (K2) Understand the importance of maintaining security testing processes given the evolving nature of technology and threats

### Question #14 (1 pt)

Which of the following are main characteristics of an effective security test environment?

- a. Closely tied to production systems to enhance security at all points
- b. Isolates different old versions of the operating systems for use in the environment
- c. Mimics the production environment in terms of access rights
- d. Includes all production environment plug-ins as well as other plug-ins not in the production environment in order to ensure the most comprehensive setup

C is correct because the closer the test environment mimics production, the more valid the testing will be. This is particularly true when it comes to access rights and delegation settings. A is not correct

because the system don't need to be and probably shouldn't be connected. B may be useful, but is not a main characteristic. D is not correct because it includes plug-ins that are not in production which could result in both false positives and false negatives from the testing.

**AS-3.4.2 (K2) Understand the importance of planning and obtaining approvals before performing any security test**

**Question #15 (1 pt)**

What is a significant concern when seeking approval for the security testing tools?

- a. Some countries prohibit the use of certain security testing tools
- b. Ensure the approval process for security testing tools can be bypassed on an exception basis in cases where a malicious event is in progress
- c. The risks of the tool are rarely known before it is procured and are better discovered when the tools is in use
- d. Because security testing tool risks are usually known, there is no need for a mitigating strategy

A is correct. While some tools are quite good and effective for testing, they may be prohibited by some countries and some organizations. B is not correct because there is always a danger of deploying a sub-optimal tool to deal with a crisis. A fast-track approval process makes sense, but a complete bypass is risky. C and D are not correct because there may be unknown risks from tools and it's better to do the due diligence in tool selection rather than deal with the consequences of a poorly selected tool.

**AS-3.5.1 (K4) Analyze security test results to determine the following:**

- Nature of security vulnerability
- Extent of security vulnerability
- Potential impact of security vulnerability
- Suggested remediation course of action
- Optimal test reporting methods

**Question #16 (3 pts)**

You are reviewing a set of security test results run on a product that is going through final testing before release to production. This is an update of a version that is currently in production. The application just tested was your e-commerce site, and it has a defect that allows cross-site scripting. Which of the following is the proper set of steps you should take?

- a. Report the problem to the developer, add it to the stakeholder report, and continue testing for other types of defects
- b. Test if the problem exists in the current production version, document the defect in a secure system, notify the developer, continue testing for other XSS defects
- c. Investigate the extent of the problem by conducting further tests on the planned release with particular concentration on other XSS issues, conduct static analysis on the code
- d. Inform management, document the defect and include it in your weekly status report to stakeholders, continue testing for other security defects to determine the extent of the security issues

B is correct. The first priority is to see if the problem exists in the production version. The defect should be documented only in a secure defect tracking system since the problem may exist in production. Since one XSS issue was found, there may be others so continued testing is warranted. A is not

correct because the defect should not be publicized in the stakeholder report. C is not correct because while further testing is needed, notification is critical. D is not correct because of the stakeholder reporting.

**AS-4.1.1 (K2) Explain why security is best achieved within a lifecycle process**

**Question #17 (1 pt)**

At what point in the SDLC should there be checking to ensure that proper secure coding practices have been followed?

- a. Component testing
- b. Integration testing
- c. System testing
- d. Security acceptance testing

A is correct. The checking should be done as soon as the code is written.

**AS-4.1.2 (K3) Implement the appropriate security-related activities for a given SDLC (e.g., iterative, sequential)**

**Question #18 (2 pts)**

You have been asked by the business analyst to help with defining the requirements for the security aspects of a system. This is a safety-critical system that stores medical information for patients and supplies this information to health professionals at hospitals, doctors' offices and ambulances. At what point in the lifecycle should the security requirements be documented and at what level of detail?

- a. They should not be documented formally because of the need to protect the security implementation within the code from outsiders
- b. They should be documented in a detailed and unambiguous way in the requirements documents during the requirements phase
- c. They should be documented during the design phase when the code approach is known rather than at the requirements phase when the approach is not known
- d. They should be restricted to the functional access and availability requirements from the user's perspective and should be documented during the requirements phase

B is correct. A is not correct, although it is important that the documented requirements be protected from those who do not need to know. C is not correct because although they may be refined at the design level, they should be initially captured during the requirements definition phase. D is not correct because security requirements also need to include secure coding practices, etc.

**AS-4.2.1 (K4) Analyze a given set of requirements from the security perspective to identify deficiencies**

AS-4.3.1 (K4) Analyze a given design document from the security perspective to identify deficiencies

**Question #19 (3 pts)**

A deficiency has been discovered in production. If an unauthorized user copies a URL from a session of an authorized user, the unauthorized user can paste the URL into their session and continue to process with the authorized user's rights. In the case that was reported, the unauthorized user was

able to use the authorized user's URL to change the system administration password. In order to close this gap, the developers will check the session ID and the user ID anytime a URL is used.

What is a realistic concern for this fix?

- a. It will not fix the problem and session hijacking will still be possible
- b. It will fix the problem, but the usability may be adversely affected
- c. It will fix the problem, but performance may be adversely affected
- d. It will not fix the problem and will expose a new vulnerability with session IDs

C is correct. It is likely that this level of checking will slow down the system because it will have to check on each screen change. A and D are not correct because the fix should fix the problem. B is not correct because there should be no impact to usability (unless you are the hacker!).

**AS-4.4.1 (K2) Understand the role of security testing during component testing**

AS-4.4.4 (K2) Understand the role of security testing during component integration testing

**Question #20 (1 pt)**

During component level testing, why should the security tester review compiler warnings?

- a. Because these indicate security problems that must be fixed
- b. Because these indicate potential issues that should be investigated
- c. Because these indicate coding issues that will cause functional defects
- d. Because these indicate poor programming practices that will increase maintainability

B is correct. From a security testing standpoint, compiler warnings indicate potential issues that could lead to security gaps. A is not correct because warnings do not necessarily require a fix. C and D may be true, but are not related to security testing.

AS-4.4.2 (K3) Implement component level security tests (abstract) given a defined coding specification

**AS-4.4.5 (K3) Implement component integration security tests (abstract) given a defined system specification**

**Question #21 (2 pts)**

You have been testing a system that has 20 defined components. You have done extensive security testing on each of the components. The system is now ready to move into component integration security testing. How should you approach this testing?

- a. Since component integration testing is concerned with the summation of the vulnerabilities of the individual components, conducting the same tests on the integrated components is the best approach.
- b. The main risk is now in the integration of the components themselves, so testing should cover each interface and verify that there are no vulnerabilities in the interfaces and the components should also be retested.
- c. It is likely that new vulnerabilities are present with the integrated components as well as with the larger system and infrastructure that is now testable, so testing should expand to include these new areas.
- d. Since the components are now integrated, the security risks will be reduced because the possible interactions are now limited so only the integration points should be tested and no component re-testing is needed.

C is correct. New vulnerabilities may be present with the integrated components and new testing areas are likely to be available. A is not correct because component integration testing is not the sum of the individual components. B is not correct because the testing should not be limited to just the interfaces and the original components. D is not correct because security risks are likely to be increased, not decreased.

**AS-4.4.3 (K4) Analyze the results from a given component level test to determine the adequacy of code from the security perspective**

**Question #22 (3 pts)**

You are creating security test cases to check for SQL injection on an input field that allows up to 5 alphanumeric characters. You are planning to apply equivalence partitioning to reduce the number of test cases you will need to execute. Given this information, which of the following is the minimum set of inputs you would need to use to test this field?

- a. bbbbb, 12345, '
- b. %, ', @, ab123
- c. ', ab123
- d. '

C is correct as this has one test for SQL injection and one for a valid input. This is the minimum number of tests. A and B have more than the minimum number and D doesn't have enough tests because it doesn't test the valid input. It would be advisable to do more testing on the various characters that can support SQL injection, but this question is asking to apply EP and get the minimum number of test cases.

**AS-4.5.1 (K3) Implement an end-to-end test scenario for security testing which verifies one or more given security requirements and tests a described functional process**

**AS-4.6.1 (K3) Implement an end-to-end security retest / regression test approach based on a given scenario**

**Question #23 (2 pts)**

You have been given the following requirement for security testing.

A user will be allowed to request their password. If they make this request, they must answer two of their three security questions correctly. If they answer correctly, a link will be sent to their email. The link will take them to a page where they can reset their password. Once reset, they can login with the new password. The link must be disabled 1 hour after it is sent. The user is allowed only two password requests without a reset, after which they will have to call the help desk. For any other errors, the user ID is locked and must be unlocked by the help desk.

Which of the following is the minimum list of test conditions to adequately test the functional security covered by this requirement?

- a. Invalid user; valid user; 2 correct answers; 2 incorrect answers; good email; bad email; reset with good password; reset with bad password; link good; link expired; two requests without reset; three requests without reset
- b. Valid user; 2 correct answers; good email; reset with good password; link good; two requests without reset

- c. Invalid user; 2 incorrect answers; bad email; reset with bad password; link expired; three requests without reset
- d. Buffer overflow on each input field; SQL injection on each input field; XSS on the login page and reset password page, invalid user; valid user; 2 correct answers; 2 incorrect answers; good email; bad email; reset with good password; reset with bad password; link good; link expired; two requests without reset; three requests without reset

A is correct as it covers the main scenarios for the functional security specified in the requirement. B tests only on the valid tests. C tests only the error conditions. D expands into attack testing as well as functional testing.

**AS-4.5.2 (K3) Demonstrate the ability to define a set of acceptance criteria for the security aspects of a given acceptance test**

**Question #24 (2 pts)**

A user will be allowed to request their password. If they make this request, they must answer two of their three security questions correctly. If they answer correctly, a link will be sent to their email address. The link will take them to a page where they can reset their password. Once reset, they can login with the new password. The link must be disabled one hour after it is sent. The user is allowed only two password requests without a reset, after which he will have to call the helpdesk. For any other errors, the user ID is locked and must be unlocked by the help desk.

Which of the following is a valid set of acceptance criteria for this requirement?

1. User can reset password if less than three requests have been made since last reset, and two security questions are answered correctly, and the link is used to reset and a valid password is entered at the reset prompt.
  2. More than two requests results in user ID locked.
  3. More than two requests without a reset results in user ID locked.
  4. More than two security questions missed results in error.
  5. More than two security questions missed, user ID is locked.
  6. If email error is received by the system, user ID is locked.
  7. If invalid password is entered on reset, the user is prompted with the proper rules.
  8. Reset password can be used to log into the system.
- a. 1, 2, 4, 6, 7, 8
  - b. 1, 2, 3, 4, 5, 6, 7, 8
  - c. 3, 5, 6, 7, 8
  - d. 1, 3, 5, 6, 8

D is correct because it provides the acceptance criteria based on the requirement. 7 is tempting and would be logical, but it is not specified in the requirement. The others are not correct because they do not contain the proper criteria. 2 is incorrect where 3 is correct. 4 is incorrect where 5 is correct.

**AS-5.1.1 (K2) Understand the concept of system hardening and its role in enhancing security**

**AS-5.1.2 (K3) Demonstrate how to test the effectiveness of common system hardening mechanisms**

**Question #25 (2 pts)**

You are implementing procedures for evaluating system hardening in an effort to test the system's security effectiveness. What procedure might you follow to ensure the hardening mechanisms put in place are working as expected?

- a. Closely monitor various security performance reports and metrics to determine if the correct level of access and authentication is achieved
- b. Frequently audit strong authentication to ensure a high level of intrusion protection is maintained at all times
- c. Evaluate the hardware components that have been hardened and compare these to other hardened software components to ensure equilibrium is being achieved
- d. Enlist a known hacker to conduct an independent assessment of the hardening effectiveness

A is correct. There are security performance reports and metrics available that can be used to determine if you have achieved the right level of hardening. B is not correct because strong authentication is just one aspect of hardening. C is not correct because equilibrium is not needed. The more critical areas may warrant better hardening. D is not correct because there is the danger of the hacker not telling you what is found.

**AS-5.2.1 (K2) Understand the relationship between authorization and authentication and how they are applied in securing information systems**

AS-5.2.2 (K3) Demonstrate how to test the effectiveness of common authorization and authentication mechanisms

**Question #26 (1 pt)**

What are key attributes of security authentication of a medium complexity IT system?

- a. It verifies that the user has the correct profile and corresponding rights to access limited parts of the system
- b. It is key in identifying the amount of system resources the user can utilize
- c. It verifies that user entering the system is legitimate
- d. It uses common credentials among users to gain entry into the system

C is correct. It verifies that the user is legitimate and authorized. A is not correct because it is not looking at access rights. B is not correct because system resource utilization is not a consideration. D is not correct because common credential verification should not be used – each individual should have unique credentials.

AS-5.3.1 (K2) Understand the concept of encryption and how it is applied in securing information systems

**AS-5.3.2 (K3) Demonstrate how to test the effectiveness of common encryption mechanisms**

**Question #27 (2 pts)**

Typical encryption mechanisms are vulnerable to threats which makes it important to understand their effectiveness at any given time. Identify which of the following you should implement to gain confidence in your encryption mechanisms?

- a. Evaluate cryptographic keys to ensure they are at least 256 bits in size
- b. Ensure you are applying random algorithms to generate random numbers where possible
- c. Develop tests that ensure symmetric encryption is used in the right modes
- d. Remove all WEP protocols to see how the system performs

C is correct per the syllabus. A is not correct because a minimum of 768 bits should be used. B is not correct because the random algorithm is easy to crack. D is not correct because WEP protocols should be left in place, not removed.

AS-5.4.1 (K2) Understand the concept of firewalls and the use of network zones and how they are applied in securing information systems

AS-5.4.2 (K3) Demonstrate how to test the effectiveness of existing firewall implementations and network zones

**Question #28 (1 pt)**

Which is true of the relationship between a firewall and a network zone?

- a. Both a network zone and firewall focus on the size of data that is being passed through
- b. A network zone communicates through safe protocol options while a firewall ensures those protocols are safe
- c. A sub-network can be considered a network zone and a firewall can be traffic monitoring software
- d. A network zone blocks malicious traffic from an untrusted zone which the firewall does not filter

C is correct per the syllabus. A is incorrect because network zones do not focus on size of data. B is not correct. Network zones are parts of the configuration of the firewall and define the authorized flow of data between networks. D is not correct because the firewall blocks the traffic, not the network zone.

AS-5.5.1 (K2) Understand the concept of intrusion detection tools and how they are applied in securing information systems

AS-5.5.2 (K3) Demonstrate how to test the effectiveness of existing intrusion detection tool implementations

**Question #29 (2 pts)**

You are working at an organization which has an intrusion detection tool deployed. You are concerned that traffic is getting through that should be considered unauthorized. Which of the following should you apply to most effectively test the abilities of the intrusion detection tool and provide input to update the intrusion specifications?

- a. Develop a series of scenarios based on past experience
- b. Use tests that generate malicious traffic to add new intrusion specifications
- c. Apply it to situations of known malicious traffic
- d. Use it in conjunction with other IDS products when possible

B is correct because these tests can be used to add new intrusion specifications which were formerly considered to be authorized traffic. A and C might be useful, but will not be as effective as B in making sure the tool will work for the future as well as the present. D is true for the usage, but not for the testing.

AS-5.6.1 (K2) Understand the concept of malware scanning tools and how they are applied in securing information systems

AS-5.6.2 (K3) Demonstrate how to test the effectiveness of existing malware scanning tool implementations

**Question #30 (1 pt)**

Which of the following is a main disadvantage to malware scanning tools?

- a. They only detect certain levels of malware
- b. They can only detect malware that is known to the tool
- c. They tend to be overly complex to run
- d. They do not provide updating and reporting capabilities

B is correct. The malware tool can only detect malware that it already knows about. B may be correct depending on the particular focus of the tool, but is not a main disadvantage. C is generally not true – the tools are normally easy to run. D is not correct because the tools provide the ability to update themselves with new findings and to produce reports.

AS-5.7.1 (K2) Understand the concept of data obfuscation tools and how they are applied in securing information systems

AS-5.7.2 (K3) Demonstrate how to test the effectiveness of data obfuscation approaches

**Question #31 (2 pts)**

You need to remove personal identification numbers from a legacy system in order to reduce risk during testing. Part of your data obfuscation plan includes verifying how effectively the data is masked. Which of the following is the most effective approach to use?

- a. Manually verify in the database that the data targeted for obfuscation is no longer understandable for logical human interpretation
- b. Design a brute force attack on the obfuscated data
- c. Substitute the sensitive data with random data of varying string lengths
- d. Enlist the development teams to generate a program to stress the database for vulnerabilities

B is correct per the syllabus. A brute force or dictionary attack can be used to see if personal information is still accessible. A is not correct because it is generally not feasible because of the amount of data and time it would take. C is not correct because this is more of an anonymizing exercise. Also, the field length might be limited so this may corrupt the data. D is not correct because we are not trying to stress test the database itself.

AS-5.8.1 (K2) Understand the concept of security training as an SDLC activity and why it is needed in securing information systems

AS-5.8.2 (K3) Demonstrate how to test the effectiveness of security training

**Question #32 (1 pt)**

What is often considered the weakest link in software security?

- a. The lack of a consistent and comprehensive security training plan
- b. The effort necessary to maintain document and procedure updates in order to keep up with continuing security threats
- c. The behavior of humans
- d. The constant advancement in malicious techniques

C is correct. It's the humans and their behavior that is the weakest link. A, B and D are concerns, but C is the weakest link in the security chain.

AS-6.1.1 (K2) Explain how human behavior can lead to security risks and how it impacts the effectiveness of security testing

AS-6.3.1 (K2) Understand the importance of security awareness throughout the organization

**Question #33 (1 pt)**

Which of the following is a potential security risk?

- a. Publishing an accounting department's organization chart on the company's web site
- b. Posting birthday wishes for a co-worker on Facebook
- c. Posting the company phone directory on the company Intranet
- d. Posting professional experience in a Linked In profile

A is correct. This information could be used to determine approval chains for invoice approvals which could then be used to create and approve fake invoices if the accounting system can be hacked. B is incorrect because the birth date should not be used in any employee information such as a password (we hope!). C is incorrect because the company intranet should be behind the firewall with other protected information. D is not correct because this information is unlikely to be useful to a hacker.

AS-6.1.2 (K3) For a given scenario, demonstrate the ability to identify ways in which an attacker could discover key information about a target and apply measures to protect the environment

**Question #34 (2 pts)**

You are responsible for security testing your company's financial application. You have recently received email from a person who claims to have hacked into the system using Shodan and has discovered that you are running an out-of-date and vulnerable OS on one of your servers. You have checked and the hacker is correct. You have made sure the server has been updated. Your preliminary check has shown no trace of how the hacker got into your system. Should you be concerned?

- a. No, this is a "white hat" hacker and means no harm to your company
- b. No, you have fixed the vulnerability so the system is now safe
- c. Yes, your security testing is not sufficient and you need to re-run your tests to see what was missed
- d. Yes, since the hacker didn't admit how he got in the system, he can still access it and may decide to exploit the vulnerability next time

D is correct and that is your biggest point of concern. A is not correct and could be a dangerous assumption. B is not correct because the hacker still has access to the system. C may be true, but re-running the same tests is not going to help with this issue.

AS-6.1.3 (K2) Explain the common motivations and sources for performing computer system attacks

AS-6.2.1 (K2) Explain how security measures can be compromised by social engineering

**Question #35 (1 pt)**

Why is an attack from inside the organization particularly worrisome?

- a. The attacker is likely driven by curiosity and will be unrelenting

- b. The attacker is likely bored at work and will continue hacking the system for entertainment
- c. The attacker is already inside the firewall and is an authorized system user
- d. The attacker is likely to launch a DOS attack which will cripple the servers

C is correct. The biggest threat here is that the external protections are useless because the attacker is already inside the system. A and B are more likely to occur with an external attacker. D is not the most likely attack – generally internal users are after information they can sell or can use to embarrass the company.

**AS-6.1.4 (K4) Analyze an attack scenario (attack performed and discovered) and identify possible sources and motivation for the attack**

### Question #36 (3 pts)

You are working in an organization where system administration access to the servers is highly restricted. Only three long-term and trusted employees know the root passwords. Recently though, there have been several odd occurrences. An unknown program, called “IKnowYourBirthday” was found to be running and was emailing birthday greetings to staff members. The birth dates were correct and the greetings were all signed “From your favorite server”. This program was killed and no one could figure out where it came from. A second problem occurred when the corporate phone list was hacked and all the phone numbers were changed to 867-5309 (apparently taken from the song by the same name). The correct list was restored and again no one could figure out how it had been done, although the new file had been created by “root”. You’ve just received a phone call from the lead system administrator telling you that the root password has been changed. It has been determined that the password was set to the lead system administrator’s dog’s name.

Further investigation has discovered that the problems started shortly after a series of virus-infected emails were detected. When the first one was found, safeguards were immediately put in place to stop any further spread of the virus, but now you are wondering if someone managed to get into the system via code that was introduced into the system by the virus.

What should you do now as your next step of investigation?

- a. Look to see if the HR birthdate information was accessed from outside the system, and if so, trace the IP address
- b. Verify if the lead system administrator’s dog’s name is posted somewhere in social media
- c. Check the suspicious email that was sent and try to trace the IP address
- d. Check the personnel files of the other two system administrators to see if there is an indication that they are unhappy

C is correct. It’s the best place to start because it appears that this might have been where the problem originated. If C doesn’t find anything, then A and D would be the next likely paths to pursue since it’s possible this is an internal attack (D) or that the attacks are separate and the birthdate information might provide some information as to who has been near it. B might be pursued, but it would be easier to just ask the sys admin who would know the dog’s name.

**AS-6.3.2 (K3) Given certain test outcomes, apply appropriate actions that can be taken to increase security awareness**

### Question #37 (2 pts)

During testing of an upgrade, you have discovered that it is possible to create a man-in-the-middle attack that can change the amount charged to customers on your e-commerce web site. Your tester successfully changed the amount so that customers were all getting a 10% discount. What should you do first?

- a. The tester should be discouraged from creating these types of attacks as they are not realistic in the production environment
- b. Immediately inform management that the attack was created by the test team as part of testing, in case it is detected
- c. Work with the developers to implement checks such as SSL-trip to ensure certificates are valid and not self-signed
- d. Check production to see if the vulnerability is also in the production code

D is correct. The first priority is to see if the vulnerability is in the production code and get the problem fixed immediately. C should be the next step to ensure the developers are coding correctly and using all available tools to check for this type of issue. A is incorrect because this is exactly what security testers should be doing. B is incorrect because management permission should always be obtained prior to testing, not afterward.

**AS-7.1.1 (K2) Understand the need to revise security expectations and acceptance criteria as the scope and goals of a project evolve**

**Question #38 (1 pt)**

Why is it important to reassess security risk expectations on a frequent basis?

- a. Stakeholders have to be educated on all security risks at all times
- b. Stakeholders will make business decisions based on associated security risk levels
- c. Users must develop a manual-based risk mitigation plan
- d. Both user and stakeholder expectations regarding security should be kept from changing

B is correct. Stakeholders often have to make business decisions regarding the security risk level that is acceptable and any necessary mitigation plans. A is not correct because everyone doesn't need to know everything. C is not correct because a manual-based risk mitigation plan is not feasible and the users probably wouldn't be implementing this anyway. D is not correct because expectations should change.

**AS-7.2.1 (K2) Understand the importance of keeping security test results confidential and secure**

**AS-7.2.2 (K2) Understand the need to create proper controls and data-gathering mechanisms to provide the source data for the security test status reports in a timely, accurate, and precise fashion (e.g., a security test dashboard)**

**Question #39 (1 pt)**

Which of the following is an important aspect of security test results?

- a. They are published for users and stakeholders to access in order to help them better understand risk
- b. They should be shared with developers across the enterprise in order to mitigate risk for future development projects
- c. The fewer people that know the better
- d. Results should always be classified by criticality

C is correct. The results from security tests should be kept confidential and access to the results should be tightly controlled. This is because the outcome of the tests often identify weaknesses in the current system under test and often the same issues with the production system. A is not correct because of the need to tightly control access to the results. B is not correct because only limited parts of the report should be made available to the developers to improve their coding. Likewise, limited parts should be made available to infrastructure people to fix any infrastructure issues that may have been found. D is true, but is not the most important aspect.

**AS-7.2.3 (K4) Analyze a given interim security test status report to determine the level of accuracy, understandability, and stakeholder appropriateness**

**Question #40 (3 pts)**

You are finalizing your security test status report for a project that is ready for deployment into production. There is a high degree of risk for this project due to the nature of the system. As a result, you want to place particular emphasis on risk. Based on this, what is the best way to articulate risk on your report?

- a. A descriptive risk assessment included in the summary
- b. Overall risk included in the last section of the report
- c. Risk impact described in the summary and later detailed in terms of specific vulnerabilities
- d. Risk impact is not part of the summary of the report

C is correct. The risk impact should be described in the summary and detailed later in the report by discussing specific vulnerabilities. A is not correct because the details should not be in the summary. B is not correct because the information should not be recorded only at the end of the report. D is not correct because this is an important part of the report.

**8.1.1 (K2) Explain the role of static and dynamic analysis tools in security testing**

**Question #41 (1 pt)**

In what way are dynamic security analysis tools different from general dynamic analysis tools?

- a. The security tools probe the system rather than just the application under test
- b. The security tools work the same in dynamic or static mode
- c. The security tools are better suited to detect problems such as memory leaks
- d. The security tools need to be tailored to the language in which the application is implemented

A is correct. B is incorrect because there are both dynamic and static analysis security tools. C is incorrect because memory leaks are detected by the general dynamic analysis tools, not the security specific ones. D is incorrect because this is true of all static analysis tools.

**8.2.1 (K4) Analyze and document security testing needs to be addressed by one or more tools**

**Question #42 (3 pts)**

You have been given the job of testing the organization's firewall. You have reviewed the implementation plan and steps, verified that the configuration has been set up as instructed by the firewall vendor and have conducted port scanning. Your organization is particularly concerned about

denial of service (DOS) attacks, particularly since they had one when the old firewall was in place. What type of testing should you conduct to help detect unexpected behavior that could be exploited by a DOS attack?

- a. Create tests that will send malformed network packets or fuzzed data and see if they are detected and rejected by the firewall
- b. Implement automated tests to stress test the servers to test the failover capabilities
- c. Test the encryption and decryption algorithms to determine if they are fast enough to deal with the load of a DOS attack
- d. Conduct software component hardening to ensure the attack surface is reduced as much as possible

A is correct as both of these techniques are used to test firewalls. B and C are incorrect because the goal is to prevent the attack rather than let it get through the firewall. D is incorrect because software component hardening will help the individual software components, but not the firewall and its implementation.

### 8.2.2 (K2) Understand the issues with open source tools

8.2.3 (K2) Understand the need to evaluate the vendor's capabilities to update tools on a frequent basis to stay current with security threats

#### Question #43 (1 pt)

If you have acquired a tool that is used under the GNU General Public License, which of the following is an important consideration for tool maintenance?

- a. Reliability of the vendor and ability to provide support
- b. Frequency and availability of updates from the vendor
- c. Technical capabilities of your team to support and customize the tool for your environment
- d. License cost and support contract cost

C is correct. The GNU license is free and it is an open source community so there is no vendor. A and B are incorrect because there is no vendor. D is incorrect because the tool is free although you may have development costs in customizing the tool for your needs.

### 9.1.1 (K2) Understand the benefits of using security testing standards and where to find them

9.3.1 (K2) Understand where to learn of industry trends in information security

#### Question #44 (1 pt)

Which of the following is a benefit of conforming to security testing standards?

- a. They are consistent and easy to follow as they are separate and independent from project goals and objectives
- b. They are the building blocks for future security testing, eliminating the need to start from scratch
- c. They outline an effective offense to meet threats before they enter the system
- d. They allow for latitude in security practices since threats are always changing dynamically

B is correct. A is not correct because security standards may be mentioned in the project goals and objectives. C is not correct because they are defensive in nature. D is not correct because they define

certain standards that help define practices – the standards should be responsive to changes in the threats.

**9.1.2 (K2) Understand the difference in applicability of standards in regulatory versus contractual situations**

9.2.1 (K2) Understand the difference between mandatory (normative) and optional (informative) clauses within any standard

**Question #45 (1 pt)**

What are advantages to imposing security standards in contracts?

- a. They provide each party a legal exit when an unforeseen security issue adversely affects the product
- b. They provide a starting place for both parties to begin their negotiations
- c. They are a convenient way to make public the agreement between parties
- d. They can change as standards change, even when the contract is finalized

B is correct. By defining the security standards, each party can then determine what is required and further specify those requirements. A is not correct because it's too late then! C is not correct because the security agreements are likely to be kept private. D is not correct because contracts don't usually change in this way.