

Simulazione d'Esame - Risposte

Set di simulazione

Versione 1.0.1

ISTQB® Security Test Engineer Syllabus

Specialist Level

Compatibile con il Syllabus versione 1.0.1

International Software Testing Qualifications Board



Avviso di copyright

Avviso sul Copyright © International Software Testing Qualifications Board (di seguito chiamato ISTQB®).

ISTQB® è un marchio registrato di International Software Testing Qualifications Board.

Tutti i diritti riservati.

Gli autori dichiarano con la presente di trasferire il copyright a ISTQB®. Gli autori (come attuali titolari del copyright) e ISTQB® (come futuro titolare del copyright) hanno concordato le seguenti condizioni di utilizzo:

Possono essere copiati estratti di questo documento per un uso non commerciale se la fonte è riconosciuta.

Qualsiasi azienda Training Provider accreditata alla Formazione può utilizzare questa Simulazione d'Esame nei loro corsi di formazione se gli autori e ISTQB® sono riconosciuti come fonti e proprietari del copyright della Simulazione d'Esame, e a condizione che qualsiasi pubblicità di tale corso di formazione sia fatta dopo che l'accREDITAMENTO ufficiale dei materiali di formazione è stato ricevuto da un Member Board riconosciuto da ISTQB®.

Qualsiasi individuo o gruppo di individui può utilizzare questa Simulazione d'Esame negli articoli e nei libri, a condizione che gli autori e ISTQB® siano riconosciuti come fonti e possessori del copyright della Simulazione d'Esame.

È proibito qualsiasi altro utilizzo di questa Simulazione d'Esame senza prima avere ottenuto l'approvazione scritta di ISTQB®.

Qualsiasi Member Board riconosciuto da ISTQB® può tradurre questa Simulazione d'Esame a condizione di riprodurre il sopra menzionato Avviso di Copyright nella versione tradotta della Simulazione d'Esame.

Responsabilità del documento

Exam Working Group ISTQB® è responsabile di questo documento.

Questo documento è mantenuto da un team dedicato di ISTQB®, che consiste nei Syllabus Working Group e nell'Exam Working Group.

Riconoscimenti

Questo documento è stato prodotto da un core team di ISTQB®: Il core team ringrazia il team di review Exam Working Group, il Syllabus Working Group e i National Board per i loro suggerimenti e contributi.

Traduzione italiana a cura di ITA-STQB (www.ita-stqb.org) – info@ita-stqb.org

Revisione della traduzione italiana a cura di: Raffaele Bozzini, Salvatore Reale.

Cronologia delle revisioni

Simulazione d'esame - Modello di layout delle risposte utilizzato: Versione 2.6 Data: 29 settembre 2021

Versione	Data	Osservazioni
1.0	2024/09/10	Versione finale per l'approvazione GA
1.0	2025/01/31	Versione finale dopo revisione EWG

Indice dei contenuti

Avviso sul copyright	2
Responsabilità del documento	2
Ringraziamenti	2
Cronologia delle revisioni	4
Indice	5
Introduzione	6
Scopo del presente documento	6
Istruzioni	6
Risposte	7
1	8
2	8
3	8
4	9
5	9
6	9
7	10
8	10
9	10
10	10
11	11
12	11
13	11
14	12
15	12
16	12
17	13
18	13
19	13
20	14
21	14
22	15
23	16
24	16
25	17
26	17
27	17
28	18
29	18
30	18
31	18
32	19
33	20
34	20
35	21
36	21
37	21
38	22
39	22
40	22

Introduzione

Scopo del documento

Le domande di questa simulazione, le risposte e le relative giustificazioni associate alle domande di questa simulazione d'esame sono state create da un team di esperti in materia e da scrittori esperti di domande, con l'obiettivo di:

- Supportare i Member Board e l'Exam Board ISTQB® nelle loro attività di scrittura delle domande
- Fornire ai Training Provider e ai candidati all'esame esempi di domande d'esame

Queste domande non possono essere utilizzate senza essere modificate in nessun esame ufficiale.

Si noti che gli esami reali possono includere un'ampia varietà di domande, e questa simulazione d'esame **non** intende includere esempi di tutti i possibili tipi, stili o lunghezze di domande; inoltre, questa simulazione d'esame può essere più difficile oppure meno difficile di qualsiasi esame ufficiale.

Istruzioni

In questo documento potete trovare:

- Tabella delle Risposte, includendo per ogni risposta corretta:
 - Livello di conoscenza (Livello K), obiettivo di apprendimento (LO) e valore del punteggio
- Insieme di risposte, includendo per tutte le domande:
 - Risposta corretta
 - Giustificazione per ogni opzione di risposta
 - Livello di conoscenza (Livello K), obiettivo di apprendimento (LO) e valore del punteggio
- Insieme di risposte aggiuntive, includendo per tutte le domande [non si applica a tutte le simulazioni d'esame]:
 - Risposta corretta
 - Giustificazione per ogni opzione di risposta
 - Livello di conoscenza (Livello K), obiettivo di apprendimento (LO) e valore del punteggio
- *Le domande sono contenute in un documento separato*

Tabella Riassuntiva delle Risposte

Numero domanda (#)	Risposta corretta	LO	Livello K	Punti
1	A	STE 1.1.1	K2	1
2	A	STE 1.1.2	K2	1
3	B	STE 1.2.1	K2	1
4	A	STE-1.3.1	K2	1
5	A, C	STE-1.3.2	K3	1
6	C	STE 1.4.1	K2	1
7	B, C	STE-2.1.1	K2	1
8	C	STE-2.1.2	K2	1
9	A	STE-2.2.1	K3	1
10	B, C	STE-2.2.2	K2	1
11	B	STE-2.2.3	K2	1
12	A	STE-2.2.4	K2	1
13	A	STE-2.2.5	K2	1
14	B	STE-3.1.1	K2	1
15	C	STE-3.1.2	K2	1
16	B	STE-3.2.1	K2	1
17	A	STE-3.2.2	K2	1
18	A	STE-3.2.3	K3	1
19	A	STE-4.1.1	K3	1
20	C, E	STE-4.2.1	K3	1

Numero domanda (#)	Risposta corretta	LO	Livello K	Punti
21	D	STE 4.3.1	K2	1
22	A	STE 4.3.2	K3	1
23	B, C	STE 5.1.1	K3	1
24	A	STE-5.2.1	K3	1
25	D	STE-5.3.1	K4	2
26	A	STE 5.3.1	K4	2
27	A	STE 6.1.1	K2	1
28	D, E	STE 6.1.2	K4	2
29	C	STE 6.2.1	K3	1
30	C	STE 6.2.2	K2	1
31	B, D	STE 7.1.1	K2	1
32	A, C	STE 7.2.1	K2	1
33	A	STE 7.3.1	K3	1
34	A	STE 7.3.2	K2	1
35	B	STE 8.1.1	K2	1
36	A, D	STE 8.2.1	K3	1
37	A, D	STE 8.3.1	K3	1
38	A	STE 9.1.1	K3	1
39	A	STE-9.2.1	K2	1
40	A	STE-9.2.2	K2	1

Numero domanda (#)	Risposta corretta	Spiegazione / Motivazione	Obiettivo di apprendimento (LO)	Livello K	Numero di punti
1	a	a) È corretta: l'integrità mira a impedire la modifica o la cancellazione dei dati da parte di soggetti non autorizzati e viene misurata in base al grado in cui un asset consente solo l'accesso e la modifica autorizzati. b) Non è corretta: l'autorizzazione alla modifica dei dati non è riservata ai proprietari dei dati, ma è concessa solo agli utenti autorizzati. c) Non è corretta: la politica di conservazione dei dati è soggetta alla politica dell'organizzazione e ai requisiti giurisdizionali. d) Non è corretta: l'accesso degli utenti deve essere basato sull'autorizzazione e non ogni volta che un utente ne ha bisogno.	STE-1.1.1	K2	1
2	a	a) È corretta: la confidenzialità nel testing di sicurezza garantisce che i dati sensibili siano accessibili solo agli utenti autorizzati. Il testing di sicurezza verifica l'efficacia dei meccanismi di controllo degli accessi, impedendo così l'accesso non autorizzato alle informazioni riservate. b) Non è corretta: riguarda l'integrità. c) Non è corretta: riguarda la disponibilità e i meccanismi di ripristino rapido dopo un incidente. d) Non è corretta: riguarda la risposta dell'organizzazione agli incidenti	STE-1.1.2	K2	1
3	b	a) Non è corretta. È una descrizione del testing di sicurezza in generale. b) È corretta. L'audit di sicurezza valuta i processi e le infrastrutture di sicurezza di un'organizzazione ed è un tipo di tecnica di test statico. c) Non è corretta. Sebbene l'obiettivo sia corretto, l'audit si focalizza sui processi e sui controlli. d) Non è corretta. Gli audit si focalizzano sui processi e sui controlli.	STE-1.2.1	K2	1

4	a	a) È corretta: tutti gli utenti sono considerati non affidabili e devono autenticarsi e ricevere l'autorizzazione prima di poter accedere a qualsiasi risorsa. b) Non è corretta: una rete tradizionale è quella in cui tutti i dispositivi e gli utenti sono considerati affidabili a prescindere. c) Non è corretta: un'architettura Zero Trust si riferisce a un modello di sicurezza che non si fida intrinsecamente di nulla all'interno della rete. d) Non è corretta: un sistema Zero Trust garantisce che nessuno possa accedere ai dati senza le credenziali appropriate.	STE-1.3.1	K2	1
5	a, c	a) È corretta: Zero Trust verifica l'identità dell'utente, i privilegi, l'identità del dispositivo e la sicurezza per ogni accesso. I login e le connessioni scadono periodicamente, costringendo gli utenti e i dispositivi a essere continuamente riverificati. b) Non è corretta: anche gli account non umani devono essere monitorati. c) È corretta: l'accesso concesso alle risorse deve essere registrato in modo permanente e come record con timestamp. d) Non è corretta: la crittografia e la restrizione degli accessi agli asset si basano sulle politiche organizzative. e) Non è corretta: limitare i controlli di accesso ad applicazioni, risorse, dati e asset specifici, piuttosto che alla rete più ampia.	STE-1.3.2	K3	1
6	c	a) Non è corretta. L'allineamento OWASP e gli audit di sicurezza sono essenziali per garantire la sicurezza del software. b) Non è corretta. Patch e aggiornamenti regolari sono fondamentali per risolvere le vulnerabilità. c) È corretta. La personalizzazione del team è importante, ma non è direttamente collegata alle questioni di sicurezza. d) Non è corretta. La conformità delle licenze garantisce un utilizzo corretto, che può influire indirettamente sulla sicurezza.	STE-1.4.1	K2	1

7	b, c	a) Non è corretta perché il codice sorgente non è disponibile in un ambiente di pre-produzione e non è possibile individuare tutti i difetti. b) È corretta perché eseguire uno scanning delle vulnerabilità grey-box prima del deployment è una best practice. c) È corretta perché verificare che tutti i punti di ingresso non siano vulnerabili è una best practice. d) Non è corretta perché il codice sorgente non è disponibile in un ambiente di pre-produzione. e) Non è corretta perché il codice sorgente non è disponibile in un ambiente di pre-produzione.	STE 2.1.1	K2	1
8	c	a) Non è corretta perché la verifica delle regole di codifica di sicurezza deve essere effettuata <u>dopo</u> che il set di regole dei requisiti di sicurezza è completo. b) Non è corretta perché vengono eseguiti test dinamici. c) È corretta perché ci sono solo controlli statici e sono ben ordinati. d) Non è corretta perché vengono eseguiti test dinamici.	STE-2.1.2	K2	1
9	a	a) È corretta perché copre gli scenari principali per la sicurezza funzionale specificati nel requisito. b) Non è corretta perché testa solo i test validi. c) Non è corretta perché testa solo condizioni non valide. d) Non è corretta perché si espande nel penetration testing.	STE-2.2.1	K3	1
10	b, c	a) Non è corretta perché le modifiche dei ruoli e dei diritti devono essere revisionate. b) È corretta perché i diritti e i ruoli impostati o modificati devono essere revisionati. c) È corretta perché le modifiche dei ruoli e dei diritti devono essere verificate (correttezza) e validate (in linea con le esigenze della persona). d) Non è corretta perché non sappiamo quali modifiche vengono applicate ai diversi account. e) Non è corretta perché dobbiamo verificare anche la revoca dell'accesso all'applicazione.	STE-2.2.2	K2	1

11	b	a) Non è corretta perché descrive il monitoraggio delle risorse di sistema, non il testing di autenticazione. b) È corretta: si tratta di tecniche di testing di autenticazione valide menzionate nel syllabus per la verifica dei meccanismi di autenticazione. c) Non è corretta perché descrive il testing di autorizzazione, non il testing di autenticazione. d) Non è corretta perché descrive il testing delle prestazioni, non il testing di autenticazione.	STE-2.2.3	K2	1
12	a	a) È corretta perché descrive l'approccio completo al testing dei controlli di protezione dei dati. b) Non è corretta perché, sebbene le prestazioni del sistema siano un fattore da considerare, focalizzarsi esclusivamente sulla velocità e sull'efficienza fornisce una visione incompleta del testing di protezione dei dati. c) Non è corretta perché testare le interazioni degli utenti e gli elementi dello schermo affronta solo il livello superficiale delle funzionalità di sicurezza. d) Non è corretta perché rappresenta solo una piccola parte del testing di protezione dei dati.	STE-2.2.4	K2	1
13	a	a) È corretta perché esistono report e metriche sulle prestazioni di sicurezza che possono essere utilizzati per determinare se hai raggiunto il giusto livello di hardening. b) Non è corretta perché l'autenticazione forte è solo uno degli aspetti dell'hardenig. c) Non è corretta perché l'equilibrio non è necessario. Le aree più critiche potrebbero richiedere un hardening maggiore. d) Non è corretta perché esiste il pericolo che l'hacker non comunichi ciò che ha scoperto.	STE-2.2.5	K2	1

14	b	a) Non è corretta perché è già stato fatto con la creazione dei test di alto livello. b) È corretta perché l'uso dei test di alto livello per creare i test manuali ed eseguire l'esecuzione fa parte dell'implementazione dei test di sicurezza. c) Non è corretta perché avverrà dopo che i test sono già stati eseguiti. d) Non è corretta perché è già stato fatto con la creazione dei test di alto livello.	STE-3.1.1	K2	1
15	c	a) Non è corretta perché il sistema non ha bisogno di essere collegato e probabilmente non dovrebbe esserlo. b) Non è corretta perché potrebbe essere utile, ma non è una caratteristica principale. c) È corretta perché più l'ambiente di test imita la produzione, più valido sarà il testing. Ciò è particolarmente vero quando si tratta di diritti di accesso e impostazioni di delega. d) Non è corretta perché include plug-in che non sono in produzione, il che potrebbe causare sia falsi positivi che falsi negativi dal testing.	STE-3.1.2	K2	1
16	b	a) Non è corretta perché i warning non richiedono necessariamente una correzione. b) È corretta perché, dal punto di vista del testing di sicurezza, i warning del compilatore indicano potenziali problemi che potrebbero portare a vulnerabilità di sicurezza. c) Non è corretta perché potrebbe essere vero, ma non è correlato al testing di sicurezza. d) Non è corretta perché potrebbe essere vero, ma non è correlato al testing di sicurezza.	STE-3.2.1	K2	1

17	a	a) È corretta perché la progettazione dei test di sicurezza a livello di integrazione dei componenti deve includere test di sicurezza delle API integrate e dei flussi integrati configurati, focalizzandosi sulla confidenzialità e l'integrità tra i componenti. b) Non è corretta perché si tratta di un test di integrazione funzionale che verifica solo la connettività dell'API. Secondo il syllabus, i test di sicurezza a livello di integrazione dovrebbero focalizzarsi su aspetti di sicurezza quali l'autorizzazione, la confidenzialità e l'integrità dei flussi integrati, non solo sulla capacità di connessione. c) Non è corretta perché, sebbene l'affidabilità del fornitore sia importante, si tratta di un'attività di audit. Il syllabus richiede specificamente un testing di sicurezza effettivo dei componenti integrati per verificare che siano privi di vulnerabilità, non solo la verifica delle credenziali del fornitore. d) Non è corretta perché si tratta di un test delle prestazioni a livello di integrazione, non di un test di sicurezza. Secondo il syllabus, i test di sicurezza dovrebbero focalizzarsi sulle potenziali vulnerabilità e sui vettori di attacco che derivano dalle interazioni tra i componenti, non sulle loro caratteristiche prestazionali.	STE-3.2.2	K2	1
18	a	a) È corretta. È la migliore pratica di sicurezza rispetto alle altre. b) Non è corretta perché il numero di tentativi non è quantificato. c) Non è corretta perché riutilizzare una vecchia password non è una buona pratica, in quanto può compromettere la sicurezza e la privacy online. d) Non è corretta perché non sarebbe sicuramente una buona pratica di sicurezza memorizzare password non crittografate in un blocco note.	STE-3.2.3	K3	1
19	a	a) È corretta, perché gli standard sono approvati da un organismo di riferimento riconosciuto. b) Non è corretta, perché gli standard industriali e gli standard de facto non sono obbligatori. c) Non è corretta, poiché gli standard non sono obbligatori. d) Non è corretta, poiché non esiste alcuna correlazione tra il livello di dettaglio e le best practice, ovvero esistono best practice molto dettagliate.	STE-4.1.1	K3	1

20	c, e	a) Non è corretta poiché i CWE non contengono alcun test case (manca il livello di astrazione CVE). b) Non è corretta poiché i CWE non contengono exploit (manca il livello di astrazione CVE). c) È corretta poiché CWE raggruppa diversi tipi di attacco, CWSS li prioritizza e i CVE sono vulnerabilità specifiche per un determinato CWE. d) Non è corretta poiché i CWSS non contengono test case (manca il livello di astrazione CVE). e) È corretta poiché il CVE lascia al security tester il compito di derivare test case specifici.	STE-4.2.1	K3	1
21	d	a) Non è corretta, poiché i parametri di contesto potrebbero influire sul comportamento dell'app. b) Non è corretta, poiché gli oracoli del test per le app senza un contesto specifico possono essere utilizzati in modo efficiente per il testing di sicurezza. c) Non è corretta, poiché gli oracoli del test per le app senza un contesto specifico possono essere utilizzati in modo efficiente per il testing di sicurezza. d) È corretta: se tutti i parametri di un'app sono standard, gli oracoli del test possono essere riutilizzati direttamente per il testing di sicurezza.	STE-4.3.1	K2	1

22	a	a) È corretta in quanto una terminologia coerente facilita la comunicazione (1a), le conoscenze di esperti riutilizzano le conoscenze di esperti in materia di sicurezza (2b), il benchmarking dimostra facilmente l'efficacia delle attività di testing di sicurezza applicate (3d) e una panoramica olistica della sicurezza da parte di un gruppo di esperti può verificare la completezza delle attività di testing di sicurezza (4c). b) 3c non è corretto (il benchmarking non fornisce necessariamente alcuna evidenza di completezza), 4d non è corretto (la panoramica olistica della sicurezza non fornisce alcuna evidenza dell'efficacia). c) 1d non è corretto (la terminologia non fornisce alcuna evidenza dell'efficacia), 2a non è corretto (le conoscenze di esperti non implicano necessariamente una comunicazione più semplice), 3b non è corretto (il benchmarking non consente necessariamente il riutilizzo delle conoscenze di esperti). d) 1b non è corretto (la terminologia non riutilizza le conoscenze di esperti in materia di sicurezza), 2d non è corretto (le conoscenze di esperti non forniscono necessariamente alcuna evidenza dell'efficacia), 3a non è corretto (il benchmarking non consente una comunicazione più semplice).	STE-4.3.2	K3	1
----	---	--	-----------	----	---

23	b, c	a) Non è corretta: portare a termine le attività di test di sicurezza in modo che i test possano essere mantenuti ed eseguiti regolarmente per supportare eventuali nuovi requisiti di sicurezza e/o rilevare nuove minacce. b) È corretta, poiché l'azienda dipende fortemente dai propri fornitori, vi è una maggiore possibilità di successo falsificando l'id di un fornitore. c) È corretta, poiché l'azienda dipende fortemente dai propri fornitori, le fatture di un fornitore potrebbero essere più importanti per la contabilità rispetto ad altre. d) Non è corretta, perché non trae vantaggio dal contesto organizzativo. e) Non è corretta, perché non trae vantaggio dal contesto organizzativo.	STE-5.1.1	K3	1
24	a	a) È corretta, il settore dell'aeronautica è fortemente regolamentato e questo deve essere tenuto in considerazione dal security tester. b) Non è corretta. Anche se questo aspetto deve essere testato, il test mira più a un requisito funzionale e non rientra nell'ambito del testing di sicurezza. Se potrebbero esserci effetti collaterali negativi, questi devono essere testati invece di essere ignorati. c) Non è corretta, poiché il tempo e il budget non costituiscono un vincolo in nessun contesto regolamentato. d) Non è corretta, perché non trae vantaggio dal contesto organizzativo e non fornisce alcuna guida quando ci si focalizza sulle attività di test.	STE-5.2.1	K3	1

25	d	a) Non è corretta, poiché il proseguimento delle attività di testing può offuscare le tracce di un incidente di sicurezza effettivo. Inoltre, segnalare solo dopo aver completato tutte le attività di testing potrebbe essere troppo tardi in caso di incidente grave. b) Non è corretta, poiché un attacker potrebbe anche essere un insider. Vedere anche a) perché continuare il testing non è una soluzione valida. c) Non è corretta, poiché l'arresto di un sistema potrebbe causare la perdita di tracce in caso di incidente. Sebbene questa possa essere una soluzione valida in alcuni casi, un security tester non ha l'autorità per decidere autonomamente. d) È corretta, poiché un'azienda dovrebbe disporre di meccanismi di risposta agli incidenti funzionanti e, dopo la segnalazione di un incidente, dovrebbero essere avviati dei processi per indagare sull'incidente segnalato.	STE-5.3.1	K4	2
26	a	a) È corretta, come indicato nel syllabus. b) Non è corretta, non tutti gli attacchi iniziano con il social engineering. c) Non è corretta, lo sfruttamento/ottenimento dell'accesso avviene dopo la raccolta di informazioni (ad esempio tramite social engineering). d) Non è corretta, manca la fase di ottenimento dell'accesso, quindi non viene effettuato alcun attacco.	STE-5.3.1	K4	2
27	a	a) È corretta, come indicato nel syllabus. b) Non è corretta, le sole attività di testing di sicurezza statico non saranno in grado di individuare tutte le vulnerabilità. c) Non è corretta, è possibile eseguire SAST e DAST, ma è necessario integrarli con ulteriori attività di test di sicurezza e verifiche. d) Non è corretta, non vi è alcuna necessità documentata di mantenere il testing di sicurezza sincronizzato con il testing manuale.	STE-6.1.1	K2	1

28	d, e	a) Non è corretta, come indicato nel syllabus. b) Non è corretta: le attività del modello Waterfall devono essere pianificate in anticipo, il che può causare modifiche necessarie durante l'esecuzione. c) Non è corretta: la maggior parte delle organizzazioni che utilizzano DevOps dispone di un team di sicurezza che verifica la produzione durante le operazioni. Non è scontato che il team DevOps sia coinvolto. d) È corretta: entrambi i modelli di sviluppo software consentono modifiche ad hoc nelle attività e l'utilizzo di enabling team quando necessario. e) È corretta: il modello di sviluppo Agile consente modifiche ad hoc al piano quando necessario.	STE-6.1.2	K4	2
29	c	a) Non è corretta, come indicato nel glossario. b) Non è corretta, non vi è alcuna prova a sostegno di tale affermazione. c) È corretta, come indicato nel syllabus. d) Non è corretta.	STE-6.2.1	K3	1
30	c	a) Non è corretta, come indicato nel glossario. b) Non è corretta, non ci è alcuna prova a sostegno di tale affermazione. c) È corretta, come indicato nel syllabus. d) Non è corretta.	STE-6.2.2	K2	1
31	b, d	a) Non è corretta, poiché un test report deve contenere tutte le informazioni necessarie per comprendere i risultati. Non è necessario fornire alcuna informazione sul tester specifico. b) È corretta in quanto i criteri di accettazione specifici del progetto non fanno necessariamente parte dell'OWASP Top-10. c) Non è corretta in quanto OWASP elenca le vulnerabilità delle best practice, ma i criteri di accettazione dipendono da un contesto di business specifico. d) È corretta, poiché un penetration test ha una visione black-box di quel sistema e non può testare alcun aspetto white-box. e) Non è corretta, poiché esistono molte guide per lo stile del codice di sicurezza specifiche per diversi contesti, che non possono essere riflesse da un unico OWASP generico.	STE-7.1.1	K2	1

32	a, c	a) È corretta, poiché il testing di sicurezza senza un framework di riferimento e iterazioni regolari non genera alcun valore aggiunto sistematico. b) Non è corretta, poiché una frequenza annuale può essere troppo bassa per sistemi molto critici e troppo alta per uno strumento utile ma non indispensabile. c) È corretta in quanto il testing di sicurezza aiuta a identificare le vulnerabilità il prima possibile. d) Non è corretta, poiché le vulnerabilità comunicate quotidianamente potrebbero essere irrilevanti per un contesto specifico (ad esempio, nessuna connessione a Internet). e) Non è corretta, poiché potrebbero esistere vulnerabilità identificate che sono irrilevanti per un contesto specifico o che non necessitano di alcun rimedio in quanto esistono altri sistemi di mitigazione (ad esempio un firewall specifico). D'altra parte, potrebbero esistere vulnerabilità per le quali il periodo di 6 mesi potrebbe essere troppo lungo per vulnerabilità identificate e sfruttabili con gravità elevata o critica.	STE-7.2.1	K2	1
----	------	--	-----------	----	---

33	a	a) È corretta, poiché l'aggiunta di ulteriori oggetti di test a un test plan può essere utilizzata per identificare ulteriori debolezze (1c), l'aggiunta di ulteriori approcci di test può essere utilizzata per ottenere ulteriori approfondimenti su un determinato sistema (2a) e una migliore copertura dei test, mentre mantenere gli oggetti di test e gli approcci di test esistenti può essere utilizzato per identificare ulteriori debolezze (3b). b) Non è corretta, poiché 1b non è corretto (gli oggetti di test aggiuntivi non sono noti all'ISMS) e 2d non è corretto (gli approcci di test aggiuntivi non rendono più sicuro alcun sistema IT). c) Non è corretta, poiché 4b non è corretto (aumentare l'automazione dell'esecuzione dei test di sicurezza non migliora in alcun modo un ISMS, né identifica ulteriori debolezze). d) Non è corretta, poiché 1d non è corretto (ulteriori oggetti di test non rendono più sicuro alcun sistema IT), 2c non è corretto (ulteriori approcci di test non identificano nuovi componenti) e 4a non è corretto (aumentare l'automazione dell'esecuzione dei test di sicurezza non migliora in alcun modo un ISMS, né genera nuovi approfondimenti su un determinato sistema).	STE-7.3.1	K3	1
34	a	a) La risposta corretta è A (spiegata nel syllabus). b) Non è corretta, tutti i test di sicurezza generano informazioni quantificabili sulla sicurezza di un sistema che possono essere utilizzate per misurare l'efficacia dell'ISMS. c) Non è corretta, il numero di test di sicurezza non è correlato alla qualità della sicurezza. d) Non è corretta, l'efficacia di un ISMS è tanto migliore quanto più vengono utilizzate tecniche di testing di sicurezza.	STE-7.3.2	K2	1

35	b	a) Non è corretta, poiché il nome del security tester e la tempistica di esecuzione dei test sono irrilevanti. b) È corretta, poiché l'ambiente di test, le precondizioni preimpostate dei test eseguiti, i dati di test utilizzati, la procedura di esecuzione dei test e il comportamento rilevato possono rappresentare dati riservati. c) Non è corretta, poiché l'elenco dei nomi degli sviluppatori, il metodo di sviluppo software identificato e gli strumenti di sviluppo sono irrilevanti. d) Non è corretta, in quanto le funzioni di codifica e la copertura dei test funzionali sono irrilevanti.	STE 8.1.1	K2	1
36	a, d	a) È corretta, poiché una vulnerabilità identificata potrebbe comunque tralasciare alcune informazioni prima della mitigazione. b) Non è corretta, in quanto non è compito del security tester stimare l'effort necessario per una vulnerabilità identificata. c) Non è corretta, in quanto non è compito del security tester creare un progetto su come mitigare una vulnerabilità identificata. d) È corretta, poiché è importante ricontrollare che la vulnerabilità identificata possa essere sfruttata in produzione. e) Non è corretta, poiché non è compito del security engineer riparare immediatamente qualsiasi problema riscontrato	STE 8.2.1	K3	1
37	a, d	a) È corretta, poiché la disattivazione di una funzionalità specifica può mitigare un rischio identificato. b) Non è corretta, poiché il successo di questa tecnica dipende dal tipo di vulnerabilità. c) Non è corretta, poiché non è possibile aspettarsi che tutte le vulnerabilità vengano automaticamente bloccate in un Web Application Firewall. d) È corretta, poiché l'aggiunta di controlli di sicurezza può ridurre il rischio. e) Non è corretta, poiché l'eliminazione delle vulnerabilità può essere molto costosa e richiedere molto tempo, quindi è necessario analizzare in anticipo altre opportunità per mitigare il rischio molto prima.	STE 8.3.1	K3	1

38	a	a) È corretta. SCA è un controllo molto veloce sui componenti in uso e dovrebbe essere eseguito prima di qualsiasi altro controllo. b) Non è corretta. Sebbene SAST garantisca che non rimangano vulnerabilità di sicurezza sconosciute, si focalizza sul codice dell'applicazione. c) Non è corretta. Richiede che l'applicazione sia in esecuzione. d) Non è corretta. Richiede che lo sviluppo dell'applicazione sia in una fase avanzata.	STE 9.1.1	K3	1
39	a	a) È corretta. DAST è uno scanner dinamico. b) Non è corretta. L'analisi statica non è dinamica. c) Non è corretta. SCA è un metodo di testing statico. d) Non è corretta. SAST è un metodo di testing statico.	STE 9.2.1	K2	1
40	a	a) È corretta, poiché il codice può essere analizzato. b) Non è corretta. Un progetto può essere sottoposto a review manualmente. c) Non è corretta. Il codice può essere analizzato, ma il servizio no. d) Non è corretta. I processi possono essere monitorati ma non analizzati staticamente.	STE 9.2.2	K2	1