Esame CISA 2006

D 1. Il Processo di Audit dei S.I. (10%)

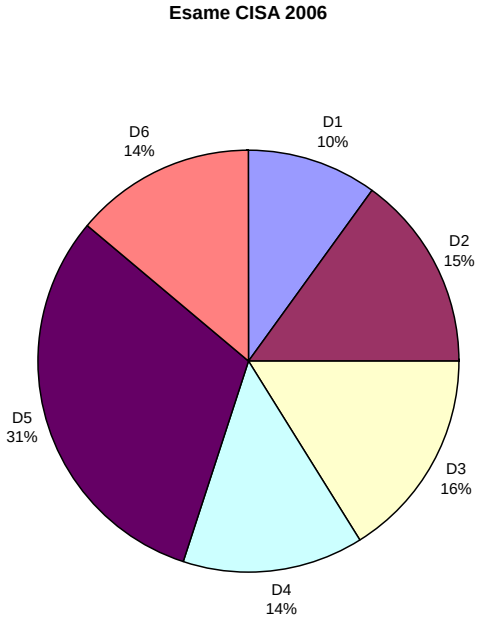
D 2. Il Governo dell'IT (15%)

D 3. Il Ciclo di Vita dei Sistemi Applicativi di Business e delle Infrastrutture IT (16%)

D 4. Erogazione e Supporto dei Servizi IT (14%)

D 5. La Protezione delle Informazioni (31%)

D 6. Ripristino dopo un evento catastrofico e Continuità Operativa (14%)



1 Il Processo di Audit dei S.I.

Argomenti del dominio:

- Organizzazione della funzione di Audit dei S.I.
- Gestione delle Risorse di Audit dei S.I.
- Pianificazione dell'Audit
- Leggi e Regolamenti
- Gli Standard e le Linee Guida ISACA per l'Audit dei S.I.
- Analisi dei Rischi
- Controlli Interni
- Effettuazione dell'Audit
- Autovalutazione dei Controlli (CSA)
- Cambiamenti nel processo di Audit dei S.I.

Obiettivo: L'obiettivo di questo dominio è garantire che il candidato CISA abbia le competenze necessarie per effettuare l'Audit dei S.I. in conformità con gli Standard, le Linee Guida e le Migliori Prassi di Auditing, per assistere l'organizzazione nell'assicurare che IT e Sistemi di Business siano protetti e controllati.

Attività:

1.1 Sviluppare ed implementare una strategia di Audit dei S.I. dell'organizzazione basata sul rischio, in conformità con gli Standard, le Linee Guida e le Migliori Prassi di Audit dei S.I.

1.2 Pianificare Audit specifici allo scopo di assicurare che IT e Sistemi di Business siano protetti e controllati.

1.3 Condurre gli Audit in accordo con gli Standard, le Linee Guida e le Migliori Prassi di Audit dei S.I. per raggiungere gli obiettivi di Audit pianificati.

1.4 Comunicare i problemi evidenti, i rischi potenziali ed i risultati dell'Audit ai principali interessati.

1.5 Consigliare nell'implementazione della Gestione dei Rischi e nelle pratiche di Controllo nell'organizzazione, mantenendo una posizione indipendente.

Elementi di conoscenza:

1.1 Conoscenza degli Standard, delle Linee Guida e delle Procedure di Audit dei S.I. e del Codice di Etica Professionale di ISACA.

1.2 Conoscenza di tecniche e prassi di Audit dei S.I.

1.3 Conoscenza di tecniche di acquisizione delle informazioni e di conservazione delle evidenze.

1.4 Conoscenza del Ciclo di Vita delle evidenze.

1.5 Conoscenza degli obiettivi di controllo e dei controlli relativi ai Sistemi Informativi.

1.6 Conoscenza dell'Analisi dei Rischi in un contesto di Audit.

1.7 Conoscenza delle tecniche di Pianificazione e Gestione dell'Audit.

1.8 Conoscenza delle tecniche di comunicazione e reporting.

1.9 Conoscenza dell'Autovalutazione dei Controlli (CSA).

1.10 Conoscenza delle tecniche di Audit continuo.

2 Il Governo dell'IT

Argomenti del dominio:

- Governo dell'Azienda
- Governo dell'IT
- Strategia dei Sistemi Informativi
- Politiche e Procedure
- Gestione dei Rischi
- Pratiche di Gestione dei Sistemi Informativi
- Struttura Organizzativa e Responsabilità nei S.I.
- Auditing della Gestione, Pianificazione ed Organizzazione dei S.I.

Obiettivo: L'obiettivo di questo dominio è di assicurare che l'organizzazione abbia in essere la struttura, le politiche, i meccanismi di accountability e le pratiche di monitoraggio per soddisfare i requisiti di governo aziendale dell'IT.

Attività:

2.1 Valutare l'efficacia della struttura di governo dell'IT per assicurare alla direzione un controllo adeguato sulle decisioni, direzioni e prestazioni dell'IT, in modo che supporti le strategie e gli obiettivi dell'organizzazione.

2.2 Valutare la struttura organizzativa dell'IT e la gestione del personale per assicurare che supportino le strategie e gli obiettivi dell'organizzazione.

2.3 Valutare la strategia IT ed i processi di sviluppo, approvazione, implementazione e manutenzione per assicurare che supportino le strategie e gli obiettivi dell'organizzazione.

2.4 Valutare le politiche, gli standard, e le procedure IT ed i processi per il loro sviluppo, approvazione, implementazione e manutenzione per assicurare che supportino la strategia IT e siano conformi con i requisiti legali e regolamentari.

2.5 Valutare le pratiche di gestione per assicurare la conformità con la strategia, le politiche, gli standard e le procedure IT dell'organizzazione.

2.6 Valutare gli investimenti di risorse nell' IT, l'uso, e le pratiche di assegnazione per assicurare l'allineamento con le strategie e gli obiettivi dell'organizzazione.

2.7 Valutare le strategie e le politiche contrattuali nell'IT e le pratiche di gestione dei contratti per assicurare che supportino le strategie e gli obiettivi dell'organizzazione.

2.8 Valutare le pratiche di gestione dei rischi per assicurare che i rischi relativi all'IT siano correttamente gestiti.

2.9 Valutare le pratiche di monitoraggio e garanzia per assicurare che la proprietà e la direzione ricevano sufficienti e tempestive informazioni sulle prestazioni dell'IT.

Elementi di conoscenza:

2.1 Conoscenza dello scopo delle strategie, delle politiche, degli standard e delle procedure IT per un'organizzazione e degli elementi essenziali di ciascuna.

2.2 Conoscenza dei framework di governo dell'IT.

2.3 Conoscenza dei processi per lo sviluppo, l'implementazione e la manutenzione delle strategie, delle politiche, degli standard e delle procedure IT (es. protezione delle informazioni, continuità operativa e ripristino dopo un evento catastrofico, gestione del ciclo di vita dei sistemi e delle infrastrutture, erogazione e supporto del servizio IT)

2.4 Conoscenza delle strategie e delle politiche di gestione della qualità.

2.5 Conoscenza della struttura organizzativa, dei ruoli e delle responsabilità relativi all'uso ed alla gestione dell'IT.

2.6 Conoscenza di standard e linee guida internazionali dell'IT, generalmente accettati.

2.7 Conoscenza dell'architettura IT aziendale e delle sue implicazioni per definire direzioni strategiche di lungo termine.

2.8 Conoscenza delle metodologie e degli strumenti di gestione dei rischi.

2.9 Conoscenza dell'utilizzo di framework di controllo (es. CobiT, COSO, ISO 17799).

2.10 Conoscenza dell'utilizzo dei modelli di maturità e di miglioramento dei processi (es. CMM, CobiT).

2.11 Conoscenza delle strategie contrattuali, dei processi e delle pratiche di gestione dei contratti.

2.12 Conoscenza delle pratiche per il monitoraggio ed il reporting delle prestazioni IT (es. balanced scorecard, key performance indicator [KPI]).

2.13 Conoscenza delle rilevanti questioni legislative e regolamentari (es. privacy, requisiti di governo aziendale).

2.14 Conoscenza della gestione del personale IT.

2.15 Conoscenza delle pratiche di investimento ed allocazione delle risorse IT (es. gestione del portafoglio, ritorno degli investimenti [ROI]).

3 Gestione del ciclo di vita dei sistemi e delle infrastrutture

Argomenti del dominio:

- Comprensione del Business
- Struttura di gestione dei progetti
- Pratiche di gestione dei progetti
- Sviluppo di applicazioni di business
- Approcci alternativi allo sviluppo applicativo
- Pratiche di sviluppo/acquisizione di infrastrutture
- Pratiche di manutenzione dei sistemi informativi
- Strumenti di sviluppo di sistemi e supporti alla produttività
- Pratiche di miglioramento dei processi
- Controlli applicativi
- Controlli di auditing delle applicazioni
- Sviluppo, acquisizione e manutenzione dei sistemi di auditing
- Sistemi applicativi di business

Obiettivo: L'obiettivo di questo dominio è di garantire che le pratiche di gestione per lo sviluppo/acquisizione, il test, l'implementazione, la manutenzione, e la dismissione dei sistemi e delle infrastrutture corrisponda agli obiettivi dell'organizzazione.

Attività:

3.1 Valutare il caso di business per il sistema proposto per l'acquisizione/sviluppo per assicurare che corrisponda ai traguardi di business dell'organizzazione.

3.2 Valutare il framework di gestione dei progetti e le pratiche di governo dei progetti per assicurare che gli obiettivi di business siano raggiunti in una maniera efficace sotto il profilo del costo, gestendo al contempo i rischi per l'organizzazione.

3.3 Effettuare revisioni per assicurare che un progetto stia progredendo come previsto dai piani di progetto, sia adeguatamente supportato dalla documentazione e il reporting degli stati di avanzamento sia accurato.

3.4 Valutare i meccanismi di controllo proposti per i sistemi e/o le infrastrutture durante le fasi di definizioni delle specifiche, di sviluppo/acquisizione, e test per assicurare che provvedano le misure di sicurezza e siano conformi con le politiche dell'organizzazione e con gli altri requisiti.

3.5 Valutare i processi attraverso i quali i sistemi e/o le infrastrutture sono sviluppati/acquisiti e testati per assicurare che i rilasci corrispondano con gli obiettivi dell'organizzazione.

3.6 Valutare la prontezza dei sistemi e/o delle infrastrutture in termini di implementazione e passaggio in produzione.

3.7 Effettuare la revisione post-implementazione dei sistemi e/o delle infrastrutture per assicurare che corrispondano agli obiettivi dell'organizzazione e siano soggetti ad efficaci controlli interni.

3.8 Effettuare revisioni periodiche dei sistemi e/o delle infrastrutture per assicurare che continuino a corrispondere agli obiettivi dell'organizzazione e siano soggetti ad efficaci controlli interni.

3.9 Valutare il processo attraverso il quale i sistemi e/o le infrastrutture sono mantenuti per assicurare il supporto continuato agli obiettivi dell'organizzazione e siano soggetti ad efficaci controlli interni.

3.10 Valutare il processo attraverso il quale i sistemi e/o le infrastrutture sono dismessi per assicurare la conformità con le politiche e le procedure dell'organizzazione.

Elementi di conoscenza:

3.1 Conoscenza delle pratiche di gestione dei benefici (es. studi di fattibilità, casi di business).

3.2 Conoscenza dei meccanismi di governo dei progetti (es. comitato direttivo, consiglio di sorveglianza del progetto).

3.3 Conoscenza delle pratiche, degli strumenti, dei framework di controllo nella gestione dei progetti.

3.4 Conoscenza delle pratiche di gestione dei rischi applicate ai progetti.

3.5 Conoscenza dei criteri di successo e dei rischi di progetto.

3.6 Conoscenza della gestione delle configurazioni, dei cambiamenti, e delle versioni, in relazione allo sviluppo ed alla manutenzione dei sistemi e/o delle infrastrutture.

3.7 Conoscenza degli obiettivi di controllo e delle tecniche che assicurano la completezza, l'accuratezza, la validità, e l'autorizzazione delle transazioni e dei dati nei sistemi applicativi IT.

3.8 Conoscenza delle architetture aziendali relativamente ai dati, alle applicazioni ed alle tecnologie (es. applicazioni distribuite, applicazioni basate sul web, servizi web, applicazioni ad n-livelli).

3.9 Conoscenza delle pratiche di analisi e gestione dei requisiti (verifica dei requisiti, tracciabilità, gap analysis).

3.10 Conoscenza dei processi di acquisto e di gestione dei contratti (es. valutazione dei fornitori, preparazione dei contratti, gestione dei fornitori, garanzia).

3.11 Conoscenza delle metodologie e degli strumenti di sviluppo applicativo e comprensione dei loro punti di forza e di debolezza (es. pratiche di agile development, prototipazione, sviluppo applicativo rapido [RAD], tecniche di progetto orientate agli oggetti.).

3.12 Conoscenza dei metodi di controllo della qualità.

3.13 Conoscenza dei processi di gestione dei test (es. strategie di test, piani di test, ambienti di test, criteri di entrata ed uscita).

3.14 Conoscenza degli strumenti, delle tecniche e delle procedure di conversione dei dati.

3.15 Conoscenza delle procedure di dismissione dei sistemi e/o delle infrastrutture.

3.16 Conoscenza delle pratiche di certificazione ed accreditamento del software e dell'hardware.

3.17 Conoscenza dei metodi e degli obiettiv di revisione post-implemetazione (es. chiusura di progetto, comprensione dei benefici, misurazione delle prestazioni).

3.18 Conoscenza delle pratiche di migrazione dei sistemi e di dispiegamento delle infrastrutture.

4 Erogazione e Supporto dei Servizi IT

Argomenti del dominio:

- Sistemi Informativi: Esercizio
- Sistemi Informativi: Hardware
- Sistemi Informativi: Architetture e Software
- Sistemi Informativi: Infrastrutture di rete
- Auditing delle Infrastrutture e dell'Esercizio

Obiettivo: L'obiettivo di questo dominio è di garantire che le pratiche di gestione del servizio IT che assicurino l'erogazione dei livelli di servizio richiesti per soddisfare gli obiettivi dell'organizzazione.

Attività:

4.1 Valutare le pratiche di gestione dei livelli di servizio per assicurare che il livello di servizio da parte dei fornitori di servizio interni ed esterni sia definito e gestito.

4.2 Valutare la gestione dell'esercizio per assicurare che le funzioni di supporto IT corrispondano efficacemente alle necessità del business.

4.3 Valutare le pratiche di amministrazione dei dati per assicurare l'integrità e l'ottimizzazione dei database.

4.4 Valutare l'uso di strumenti e tecniche di monitoraggio di capacità e prestazioni per assicurare che i servizi IT corrispondano agli obiettivi dell'organizzazione.

4.5 Valutare le pratiche di gestione dei cambiamenti, delle configurazioni e delle versioni per assicurare che i cambiamenti fatti all'ambiente di produzione dell'organizzazione siano adeguatamente controllati e documentati.

4.6 Valutare le pratiche di gestione degli incidenti e dei problemi per assicurare che incidenti, problemi o errori siano registrati, analizzati, e risolti in maniera tempestiva.

4.7 Valutare la funzionalità dell'infrastruttura IT (es. componenti di rete, hardware, sistemi, software) per assicurare che supporti gli obiettivi dell'organizzazione.

Elementi di conoscenza:

4.1 Conoscenza delle pratiche di gestione del livello di servizio.

4.2 Conoscenza delle migliori prassi di gestione dell'esercizio (es. schedulazione del carico di lavoro, gestione dei servizi di rete, manutenzione preventiva).

4.3 Conoscenza dei processi, degli strumenti e delle tecniche di monitoraggio delle prestazioni dei sistemi (es. analizzatori di rete, report di utilizzo dei sistemi, bilanciamento del carico).

4.4 Conoscenza delle funzionalità dell'hardware e dei componenti di rete (es. router, switch, firewall, periferiche).

4.5 Conoscenza delle pratiche di amministrazione dei database.

4.6 Conoscenza della funzionalità del software di sistema, inclusi sistemi operativi, programmi di utilità, e sistemi di gestione dei database.

4.7 Conoscenza delle tecniche di pianificazione e di monitoraggio della capacità.

4.8 Conoscenza dei processi per gestire i cambiamenti schedulati e quelli di emergenza ai sistemi di produzione e/o all'infrastruttura, incluse le pratiche di gestione dei cambiamenti, delle configurazioni, delle versioni, e delle correzioni.

4.9 Conoscenza delle pratiche di gestione degli incidenti/problemi (es. help desk, procedure di escalation, tracciabilità).

4.10 Conoscenza delle pratiche di licenze software e di inventario.

4.11 Conoscenza degli strumenti e delle tecniche di resilienza di sistema (es. hardware fault-tolerant, eliminazione dei singoli punti di guasto, clustering).

5 La Protezione delle Informazioni

Argomenti del dominio:

- Importanza della Gestione della Sicurezza delle Informationi
- Esposizioni degli Accessi Logici e Controlli
- Sicurezza dell'Infrastruttura di Rete
- Auditing del Framework di Sicurezza delle Informazioni
- Auditing della Sicurezza dell'Infrastruttura di Rete
- Esposizioni Ambientali e Controlli
- Esposizioni degli Accessi Fisici e Controlli
- Mobile Computing

Obiettivo: L'obiettivo di questo dominio è di garantire che l'architettura di sicurezza (politiche, standard, procedure e controlli) assicurino la confidenzialità, l'integrità e la disponibilità delle informazioni.

Attività:

5.1 Valutare il progetto, l'implementazione, ed il monitoraggio dei controlli di accesso logico per assicurare la confidenzialità, l'integrità, la disponibilità e l'uso autorizzato delle informazioni.

5.2 Valutare la sicurezza dell'infrastruttura di rete per assicurare la confidenzialità, l'integrità, la disponibilità e l'uso autorizzato della rete e delle informazioni trasmesse.

5.3 Valutare il progetto, l'implementazione, ed il monitoraggio dei controlli ambientali per prevenire o minimizzare le perdite.

5.4 Valutare il progetto, l'implementazione, ed il monitoraggio dei controlli di accesso fisico per assicurare che le informazioni siano adeguatamente salvaguardate.

5.5 Valutare i processi e le procedure usate per memorizzare, richiamare, trasportare e dismettere le informazioni confidenziali.

Elementi di conoscenza:

5.1 Conoscenza delle tecniche per il progetto, l'implementazione ed il monitoraggio della sicurezza (es. accertamento delle minacce e dei rischi, analisi della sensibilità, accertamento dell'impatto per la privacy).

5.2 Conoscenza dei controlli di accesso logico per l'identificazione, l'autenticazione, e la restrizione degli utenti a funzioni e dati autorizzati (es. password dinamiche, tecniche challenge/response, menù, profili).

5.3 Conoscenza delle architetture di sicurezza di accesso logico (es. single sign-on, strategie di identificazione degli utenti, gestione delle identità).

5.4 Conoscenza di metodi e tecniche di attacco (es. hacking, spoofing, cavalli di troia, negazione del servizio, spamming)

5.5 Conoscenza dei processi relativi al monitoraggio ed alla risposta agli incidenti di sicurezza (es. procedure di escalation, squadre di emergenza per la risposta agli incidenti).

5.6 Conoscenza di dispositivi, protocolli, e tecniche di sicurezza di rete ed internet (es. SSL, SET, VPN, NAT).

5.7 Conoscenza dei sistemi di rilevamento delle intrusioni e configurazione, implementazione, esercizio e manutenzione dei firewall.

5.8 Conoscenza delle tecniche e degli algoritmi di crittografia (es. AES, RSA)

5.9 Conoscenza delle componenti delle infrastrutture a chiavi pubbliche (PKI) (es. autorità di certificazione, autorità di registrazione) e tecniche di firma digitale.

5.10 Conoscenza degli strumenti di rilevazione e delle tecniche di controllo dei virus.

5.11 Conoscenza degli strumenti di test e di accertamento di sicurezza (es. penetration test, scansione di vulnerabilità).

5.12 Conoscenza delle pratiche e dei dispositivi di protezione ambientale (es. estintori, sistemi di climatizzazione, sensori di umidità).

5.13 Conoscenza dei sistemi e delle pratiche di sicurezza fisica (es. biometria, carte d'accesso, lucchetti numerici, token).

5.14 Conoscenza degli schemi di classificazione dei dati (es. dato pubblico, confidenziale, privato, sensibile).

5.15 Conoscenza della sicurezza delle comunicazioni vocali (es. Voice Over IP).

5.16 Conoscenza dei processi e delle procedure usati per memorizzare, richiamare, trasportare e dismettere le informazioni confidenziali).

5.17 Conoscenza dei controlli e dei rischi associati con l'uso di dispositivi portatili e wireless (es. PDA, dispositivi USB, dispositivi Bluetooth).

6 Ripristino dopo un evento catastrofico e Continuità Operativa

Argomenti del dominio:

- Processo di pianificazione di Continuità/Ripristino dei SI
- Eventi Disastrosi
- Processo di Pianificazione della Continuità Operativa
- Organizzazione ed Assegnazione delle Responsabilità
- Componenti di un Piano di Continuità Operativa
- Test del Piano
- Backup e Restore
- Auditing dei Piani di Continuità/Ripristino

Obiettivo: L'obiettivo di questo dominio è di garantire che nell'eventualità di una interruzione della continuità operativa e che i processi di ripristino dopo un evento catastrofico, assicurino la tempestiva riattivazione dei servizi IT, minimizzando l'impatto sull'operatività.

Attività:

6.1 Valutare l'adeguatezza delle misure di backup e restore per assicurare la disponibilità delle informazioni richieste per riprendere le elaborazioni.

6.2 Valutare il piano dell'organizzazione, di ripristino dopo un evento catastrofico, per assicurare che abiliti il recupero delle capacità di elaborazione IT in caso di disastro.

6.3 Valutare il piano di continuità operativa dell'organizzazione per assicurare la sua capacità di continuare con le operazioni aziendali essenziali durante il periodo di interruzione dell'IT.

Elementi di conoscenza:

6.1 Conoscenza dei processi e delle pratiche di backup dei dati, di memorizzazione, manutenzione, ritenzione, e ripristino.

6.2 Conoscenza dei regolamenti, delle leggi, dei contratti, e delle questioni assicurative relative alla continuità operativa ed al ripristino dai disastri.

6.3 Conoscenza dell'analisi di impatto sul business (BIA).

6.4 Conoscenza dello sviluppo e manutenzione dei piani di continuità operativa e di ripristino dai disastri.

6.5 Conoscenza degli approcci e dei metodi di test della continuità operativa e del ripristino dai disastri.

6.6 Conoscenza delle pratiche di gestione delle risorse umane in relazione alla continuità operativa e al ripristino dai disastri (es. piani di evacuazione, squadre di emergenza).

6.7 Conoscenza dei processi usati per invocare i piani di continuità operativa e di ripristino dai disastri.

6.8 Conoscenza delle tipologie di siti alternativi di elaborazione e metodi usati per monitorare gli accordi contrattuali (es. siti caldi, siti tiepidi, siti freddi).