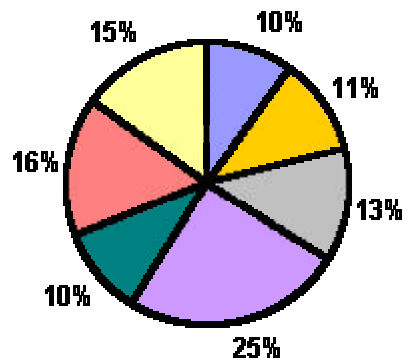


ESAME CISA 2003:

1. Gestione, pianificazione ed organizzazione SI (11%)
2. Infrastrutture tecniche e prassi operative (13%)
3. Protezione del patrimonio dati e degli asset aziendali (25%)
4. Ripristino in caso di calamità e continuità operativa (10%)
5. Sviluppo, acquisizione, attuazione e aggiornamento dei sistemi applicativi aziendali (16%)
6. Valutazione dei processi commerciali e gestione dei rischi (15%)
7. Procedure di revisione SI (10%)



1. Gestione, pianificazione ed organizzazione SI

Obiettivo: Valutazione della strategia, delle normative, degli standard, delle procedure e delle prassi in relazione alla gestione, alla pianificazione e all'organizzazione dei SI.

Attività:

- 1.1 Valutare la strategia dei Sistemi Informativi e dei suoi processi di sviluppo, attuazione e aggiornamento per garantire che supporti gli obiettivi di business dell'organizzazione.
- 1.2 Valutare le politiche dei Sistemi Informativi, gli standard, le procedure ed i processi per il loro sviluppo, attuazione e aggiornamento per assicurare che supportino la strategia dei Sistemi Informativi.
- 1.3 Verificare la conformità delle prassi di gestione dei Sistemi Informativi con le politiche dei Sistemi Informativi, gli standard e le procedure.
- 1.4 Valutare l'organizzazione e la struttura dei Sistemi Informativi per assicurare un adeguato supporto alle esigenze di business dell'organizzazione.
- 1.5 Valutare la scelta e la gestione dei servizi erogati da terze parti per garantire che supportino la strategia dei Sistemi Informativi.

Elementi di conoscenza:

- 1.01 Conoscenza degli elementi costitutivi delle strategie dei SI, politiche, standard e procedure

- 1.02 Conoscenza dei processi per lo sviluppo, l'attuazione e l'aggiornamento delle strategie dei SI, delle politiche, degli standard e delle procedure
- 1.03 Conoscenza delle strategie e delle politiche per la gestione dei progetti dei SI
- 1.04 Conoscenza dei quadri di riferimento per il governo dell'IT, per la gestione del rischio e per il controllo
- 1.05 Conoscenza delle strategie e delle politiche per la gestione dei problemi e del cambiamento
- 1.06 Conoscenza delle strategie e delle politiche per la gestione della qualità dei SI
- 1.07 Conoscenza delle strategie e delle politiche per la gestione della sicurezza dei SI
- 1.08 Conoscenza delle strategie e delle politiche per la gestione della continuità del business
- 1.09 Conoscenza delle strategie per la contrattualistica, i processi e la gestione dei contratti
- 1.10 Conoscenza dei ruoli e delle responsabilità delle funzioni dei SI (es. la separazione dei ruoli)
- 1.11 Conoscenza dei criteri di una struttura organizzativa dei SI e dei principi per la sua definizione
- 1.12 Conoscenza delle prassi di gestione dei SI, degli indicatori di prestazione e delle tecniche per la misurazione delle prestazioni
- 1.13 Conoscenza delle principali problematiche legislative e regolatorie (es. privacy, proprietà intellettuale)
- 1.14 Conoscenza degli standard e delle linee guida internazionali generalmente accettati

2. Infrastrutture tecniche e prassi operative

Obiettivo: Valutazione dell'efficacia e dell'efficienza nella realizzazione e gestione delle infrastrutture tecniche ed operative del sistema informatico aziendale, per assicurare che esso supporti adeguatamente gli obiettivi commerciali aziendali.

Attività:

- 2.1 Verificare che l'acquisto, l'installazione e la manutenzione dell'hardware supportino efficacemente ed efficientemente sia le attività dei SI che le esigenze di business e che siano compatibili con le strategie aziendali
- 2.2 Valutare i processi di sviluppo/acquisizione, implementazione e manutenzione del software di sistema e dei programmi di utilità per assicurare il supporto alle attività IT dell'organizzazione ed alle esigenze di business e la compatibilità con le strategie dell'organizzazione.
- 2.3 Valutare i processi di acquisizione, installazione e manutenzione delle infrastrutture di rete per assicurare un supporto efficiente ed efficace alle attività IT dell'organizzazione ed alle esigenze di business.
- 2.4 Valutare le prassi operative dei SI per assicurare un utilizzo efficace ed efficiente delle risorse tecniche usate a supporto delle attività IT dell'organizzazione e delle esigenze di business.
- 2.5 Verificare i processi, strumenti e tecniche per la valutazione delle prestazioni ed il monitoraggio dei sistemi per assicurare che i sistemi elaborativi siano continuamente adeguati agli obiettivi di business aziendali.

Elementi di conoscenza:

- 2.01 Conoscenza dei rischi e dei controlli relativi alle piattaforme hardware, al software ed alle utility di sistema, alla infrastruttura di rete ed alle prassi operative dei SI.
- 2.02 Conoscenza delle prestazioni dei sistemi e di processi, strumenti e tecniche di monitoraggio (es. analizzatori di rete, messaggi di errore di sistema, report di utilizzo dei sistemi, bilanciamento dei carichi)

- 2.03 Conoscenza dei processi di acquisizione, sviluppo, implementazione e manutenzione dell'infrastruttura IT
- 2.04 Conoscenza dei principi di controllo dei cambiamenti e di gestione della configurazione per l'hardware ed il software di sistema
- 2.05 Conoscenza delle prassi relative alla gestione dell'infrastruttura tecnologica ed operativa (es. procedure di gestione dei problemi/delle risorse, help desk, schedulazione, accordi sui livelli di servizio)
- 2.06 Conoscenza delle funzionalità del software e delle utility di sistema (es DBMS, pacchetti di sicurezza)
- 2.07 Conoscenza delle funzionalità dei componenti di rete (es. firewall, router, server proxy, modem, concentratori di terminali, hub, switch)
- 2.08 Conoscenza delle architetture di rete (es. protocolli di rete, remote-computing, topologie di rete, Internet, Intranet, Extranet, client server)

3. Protezione del patrimonio dati e degli asset aziendali

Obiettivo: Valutazione della sicurezza logica, ambientale e infrastrutturale IT (informatica) per assicurarsi che soddisfino i requisiti commerciali dell'azienda per la tutela del patrimonio dati contro utilizzi, divulgazione o modifiche non autorizzati e per evitare rischi di danneggiamento o di perdita degli stessi.

Attività:

- 3.1 Valutare il disegno, l'implementazione e la verifica dei controlli di accesso logico allo scopo di assicurare integrità, riservatezza e disponibilità del patrimonio informativo
- 3.2 Valutare la sicurezza dell'infrastruttura di rete allo scopo di assicurare integrità, riservatezza, disponibilità ed utilizzo autorizzato della rete e delle informazioni
- 3.3 Valutare il disegno, l'implementazione e la verifica dei controlli ambientali per prevenire e/o minimizzare le potenziali perdite
- 3.4 Valutare il disegno, l'implementazione, e la verifica dei controlli di accesso fisico allo scopo di assicurare che il livello di protezione delle informazioni e dei beni aziendali sia sufficiente a soddisfare gli obiettivi aziendali

Elementi di conoscenza:

- 3.01 Conoscenza dei processi di disegno, implementazione e verifica della sicurezza (es.. gap-analysis, baseline, selezione dei prodotti)
- 3.02 Conoscenza delle tecniche di crittografia (es. DES, RSA)
- 3.03 Conoscenza dei componenti dell'infrastruttura (PKI) a chiave pubblica (es. certification authorities (CA), registration authorities)
- 3.04 Conoscenza delle tecniche di firma digitale
- 3.05 Conoscenza delle prassi di sicurezza fisica (es. dispositivi biometrici o logico-fisici)
- 3.06 Conoscenza delle tecniche di identificazione, autenticazione, e confinamento degli utenti alle sole funzioni ed ai dati autorizzati (es. password dinamiche, tecnologie a domanda e risposta, menu, profili)
- 3.07 Conoscenza del software di sicurezza (e.g. single sign-on, sistemi di rilevazione delle intrusioni (IDS), sistemi automatizzati di gestione dei permessi, NAT)
- 3.08 Conoscenza degli strumenti di test e valutazione della sicurezza (es. test di intrusione, scansione alla ricerca delle vulnerabilità)
- 3.09 Conoscenza della sicurezza di rete e Internet (es. SSL, SET, VPN, tunneling)
- 3.10 Conoscenza della sicurezza delle comunicazioni vocali

- 3.11 Conoscenza delle tecniche e dei metodi di attacco/frode (e.g. hacking, spoofing, Trojan horse, DOS, spamming)
- 3.12 Conoscenza delle fonti di informazione relativamente a minacce, standard, criteri e prassi di valutazione, relative alla sicurezza delle informazioni
- 3.13 Conoscenza delle tecniche di monitoraggio della sicurezza, dei processi e tecniche di rilevazione e di escalation (es. tracce di audit, rilevazione delle intrusioni, gruppi di gestione delle emergenze informatiche)
- 3.14 Conoscenza dei virus e dei meccanismi di rilevazione, prevenzione e correzione
- 3.15 Conoscenza delle prassi e dei dispositivi di protezione ambientale (es. antincendi, sistemi refrigeranti)

4. Ripristino in caso di calamità e continuità operativa

Obiettivo: Valutazione del processo volto allo sviluppo e al mantenimento di piani documentati, comunicati e testati, a garanzia della continuità operativa e informatica dell'azienda in caso di calamità o interruzioni straordinarie.

Attività:

- 4.1 Valutare l'adeguatezza delle strategie di backup e restore per assicurare il ripristino del normale flusso elaborativo in caso di interruzioni di breve durata e/o la necessità di rielaborare o di far ripartire un processo.
- 4.2 Valutare la capacità dell'organizzazione di continuare a fornire capacità elaborativa per i processi ICT in caso di indisponibilità delle risorse elaborative primarie.
- 4.3 Valutare la capacità dell'organizzazione di assicurare la continuità operativa in caso di calamità.

Elementi di conoscenza:

- 4.01 Conoscenza delle tecniche di gestione delle crisi e di analisi di impatto operativo.
- 4.02 Conoscenza delle tecniche di ripristino in caso di calamità (DR) e di continuità (BC) operativa (es. sito caldo, freddo, architettura di rete fail-safe, accordi reciproci).
- 4.03 Conoscenza delle tecniche di pianificazione e dei processi di ripristino in caso di calamità e di continuità operativa.
- 4.04 Conoscenza delle metodologie e delle prassi di salvataggio ed archiviazione
- 4.05 Conoscenza delle metodologie di testing dei processi di ripristino in caso di calamità e di continuità operativa.
- 4.06 Conoscenza delle prassi assicurative concernenti processi di ripristino in caso di calamità e di continuità operativa.
- 4.07 Conoscenza delle problematiche relative alle risorse umane (es. pianificazione dell'evacuazione, gruppi di intervento).

5. Sviluppo, acquisizione, attuazione e aggiornamento dei sistemi applicativi aziendali

Obiettivo: Valutazione delle metodologie e dei procedimenti applicati per lo sviluppo, l'acquisizione, l'attuazione e l'aggiornamento dei sistemi applicativi aziendali al fine di assicurarne la coerenza con gli obiettivi commerciali dell'azienda.

Attività:

- 5.1 Valutare i processi mediante i quali sono sviluppati ed implementati i sistemi applicativi, allo scopo di assicurare che contribuiscano al raggiungimento degli obiettivi aziendali.
- 5.2 Valutare i processi mediante i quali sono acquisiti ed implementati i sistemi applicativi, allo scopo di assicurare che contribuiscano al raggiungimento degli obiettivi aziendali.
- 5.3 Valutare i processi mediante i quali sono mantenuti i sistemi applicativi, allo scopo di assicurare la continuità del loro supporto agli obiettivi aziendali.

Elementi di conoscenza:

- 5.01 Conoscenza delle metodologie e degli strumenti di sviluppo dei sistemi (es. prototyping, RAD, SDLC, tecniche di disegno object-oriented)
- 5.02 Conoscenza delle metodologie di documentazione e di rappresentazione grafica
- 5.03 Conoscenza delle prassi di implementazione applicativa (es. test pilota, parallelo)
- 5.04 Conoscenza delle metodologie di assicurazione della qualità del software
- 5.05 Conoscenza delle architetture applicative (es. applicazioni client server, object-oriented, data warehousing, applicazioni web-based , interfacce)
- 5.06 Conoscenza di principi, metodi e prassi di testing
- 5.07 Conoscenza di principi, metodi e prassi di gestione dei progetti (es. PERT, CPM, tecniche di stima)
- 5.08 Conoscenza dei processi di acquisizione dei sistemi applicativi (es. valutazione dei fornitori, preparazione dei contratti, gestione dei fornitori, garanzie)
- 5.09 Conoscenza dei principi di manutenzione applicativa (es. versioning, packaging, richieste di modifica)
- 5.10 Conoscenza di strumenti, tecniche e procedure di migrazione dei sistemi e di conversione dei dati
- 5.11 Conoscenza delle procedure di controllo dei cambiamenti e di gestione di cambiamenti di emergenza.
- 5.12 Conoscenza delle tecniche di revisione post-implementazione

6. Valutazione dei processi commerciali e gestione dei rischi

Obiettivo: Valutazione dei sistemi e dei processi commerciali al fine di assicurare che i rischi vengano gestiti in conformità con gli obiettivi commerciali dell'azienda.

Attività:

- 6.1 Valutare l'efficacia e l'efficienza dei sistemi informativi nel supportare i processi aziendali, mediante tecniche di benchmarking, analisi delle best practice o reingegnerizzazione dei processi aziendali (BPR), per assicurare l'ottimizzazione dei risultati.
- 6.2 Valutare il disegno e l'implementazione dei controlli automatizzati e manuali, allo scopo di assicurare che i rischi identificati per i processi aziendali siano ad un livello accettabile.
- 6.3 Valutare i progetti di modifica dei processi aziendali, allo scopo di assicurare che siano adeguatamente controllati, gestiti, organizzati e dotati di personale.
- 6.4 Valutare l'implementazione aziendale della gestione del rischio e dei controlli.

Elementi di conoscenza:

- 6.01 Conoscenza di metodologie e prassi di disegno ed ottimizzazione dei processi aziendali (es. e-Business, B2B, BPR).

- 6.02 Conoscenza dei controlli sui processi aziendali (es. gestione, controlli manuali ed automatizzati)
- 6.03 Conoscenza degli indicatori di prestazione dei processi aziendali (es. balanced scorecard, key performance indicators (KPI))
- 6.04 Conoscenza delle prassi di controllo, gestione ed organizzazione dei progetti aziendali.
- 6.05 Conoscenza dei meccanismi di visualizzazione e reporting dello stato di avanzamento dei progetti.
- 6.06 Conoscenza dei criteri e delle insidie relative al successo dei progetti.
- 6.07 Conoscenza di rischi e modelli di controllo aziendale (Corporate Governance).

7. Procedure di revisione SI

Obiettivo: Svolgere le attività di revisione SI in conformità agli standard e ai principi di verifica SI professionalmente in uso per assicurarsi che i sistemi informatici e amministrativi siano adeguatamente controllati, monitorati e vagliati.

Attività:

- 7.1 Sviluppare e/o implementare obiettivi e strategie di audit dei sistemi informativi basate sul rischio, in accordo con gli standard di audit comunemente accettati, allo scopo di assicurare che l'IT ed i processi aziendali siano adeguatamente controllati, verificati, valutati, e che siano in linea con gli obiettivi aziendali.
- 7.2 Pianificare verifiche specifiche allo scopo di assicurare che gli obiettivi e le strategie IT siano soddisfatti.
- 7.3 Ottenere evidenze utili, rilevanti, affidabili e sufficienti per raggiungere gli obiettivi di audit.
- 7.4 Analizzare le informazioni acquisite per identificare le circostanze da rapportare ed ottenere le conclusioni.
- 7.5 Rivedere il lavoro effettuato allo scopo di fornire ragionevole assicurazione che gli obiettivi siano stati raggiunti.
- 7.6 Comunicare i risultati di audit ai principali attori
- 7.7 Facilitare l'implementazione di prassi di controllo e di gestione dei rischi all'interno dell'azienda

Elementi di conoscenza:

- 7.01 Conoscenza degli Standard e delle Linee Guida ISACA per l'Auditing IT e del Codice di Etica Professionale.
- 7.02 Conoscenza di tecniche e prassi di auditing IT.
- 7.03 Conoscenza di tecniche di acquisizione delle informazioni e di conservazione delle evidenze (es. osservazione, questionari, interviste, supporti elettronici)
- 7.04 Conoscenza degli obiettivi di controllo e dei controlli relativi ai sistemi informativi (es. preventivi, rivelatori).
- 7.05 Conoscenza dei rischi di business e di audit correlati all'IT (es. minacce, impatti).
- 7.06 Conoscenza di criteri, principi, e metodologie di analisi dei rischi.
- 7.07 Conoscenza delle tecniche di pianificazione e gestione dell'audit (es. finanziarie, qualità, organizzazione dell'audit)
- 7.08 Conoscenza delle tecniche di comunicazione (es. reporting, presentazioni, facilitazioni, negoziazioni, risoluzione dei conflitti)
- 7.09 Conoscenza delle tecniche di gestione del personale (es. staffing, formazione)