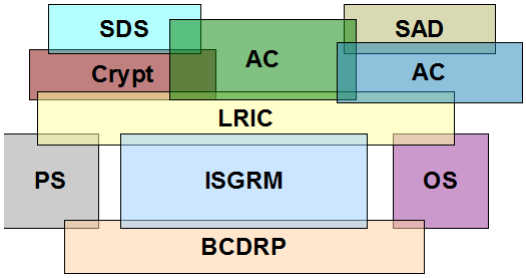
CISSP: Certified Information System SecurityProfessional

Appunti per l'Esame di Certificazione

1 agosto 2012



Paolo Ottolino (PMP CISSP-ISSAP CISA CISM OPST ITIL)

Prefazione
Questo manuale in Italiano fornisce appunti schematici per superare l'esame CISSP. Io ho superato l'esame nel 2004: alcuni aggiustamenti sono stati operati al CBK (Common Body of Knowledge) negli anni. Però nessun cambiamento sostanziale è stato adottato; questo testo riflette gli aggiornamenti necessari.

Indirizzamento
Il CISSP certifica le necessarie competenze nella progettazione, realizzazione e manutenzione di sistemi atti ad indirizzare la sicurezza delle informazioni. Cioé, esso è stato ideato per quei professionisti che realizzano nel campo IT infrastrutture e componenti di protezione, ovvero abilitano le funzioni di sicurezza nei sistemi esistenti.
Diversamente da altre certificazioni storiche del settore, il CISSP è stato pensato per chi opera fattivamente nella realizzazione di infrastrutture tecnologiche ad un livello intermedio, tattico. E' indirizzato a coloro i quali siano chiamati a comprendere le esigenze strategiche di business (es. certificazioni ISACA: CISM, etc) e del relativo auditing (es. ISACA: CISA) ma tuttavia sappiano interagire proficuamente a livello operativo con gli addetti specializzati (es. certificazioni SANS: GCUX, GCIH, etc).
Queste caratteristiche rendono l'esame CISSP altamente tecnico e di dimensioni ragguardevoli (difatti si compone di 10 domini). La preparazione all'esame risulta, quindi, più complessa di quella delle altre certificazioni rivolte ad altre figure professionali.

Esame di Certificazione
A partire dal 1° Settembre 2012 gli esami saranno nella forma CBT (Computer Based Test), la qual cosa comporta i seguenti vantaggi:

- sostenere l'esame non è più vincolato alle 2 dati annuali fissate da (ISC)2
- nel tempo verranno abilitate più sedi d'esame; attualmente i centri Pearson/Vue abilitati sono Roma (2) e Milano (1)
- non è più necessario allenarsi ad annerire i pallini con precisione e rapidità, come nell'esame PBT (Paper Based Text)

Indice

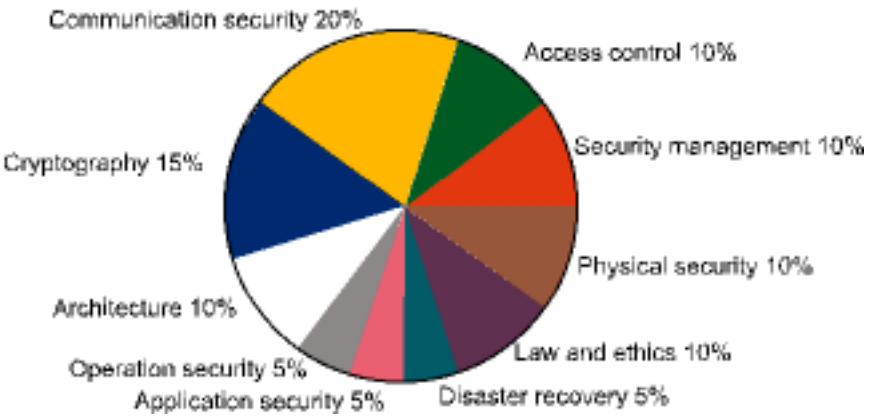
Introduzione

Domini CISSP

Come in tutte le certificazioni, il BoK è diviso in domini. Il CISSP è piuttosto corposo e ne annovera ben 10. Vediamoli nella tabella seguente:

Dominio	**Acronimo**	%
Access Control	AC	10
Telecommunication & Network Security	TNS	20
Information Security Governance & Risk Management	ISGRM	10
Software Development Security	SDS	5
Cryptography	Crypt	15
Security Architecture & Design	SAD	10
Operational Security	OS	5
Business Continuity & Disaster Recovery Planning	BCDRP	5
Legal, Regulation, Investigation and Compliance	LRIC	10
Physical (Environmental) Security	PS	10

La figura seguente illustra l'importanza relativa di ciascun dominio nei quiz d'esame:



Nel seguito sono sinteticamente indicati i contenuti di ciascun dominio, suddivisi per tipologia:

Information Security Governance & Risk Management: Gestione Strategica ed Organica della Sicurezza. Si tratta del dominio di più alto livello d'astrazione; esso rappresenta il cardine centrale sul quale sono imperniati tutti gli altri

Policy: indica un dominio che illustra il modo di indirizzare i requisiti mandatori cui si può essere soggetti:

Business Continuity & Disaster Recovery Planning: Meccanismi da adottare per garantire la Disponibilità dei Dati e della Infrastruttura IT

Legal, Regulation, Investigation & Compliance: Aspetti Legali legati al mondo IT, quali

- normative da rispettare
- modalità che devono essere abilitate per l'esecuzione delle investigazioni (anche con validità forense)
- metodi e meccanismi per eseguire il controllo di conformità

Approccio: indica un insieme di conoscenze che devono essere impiegate come linea guida tecnica nella progettazione e realizzazione delle infrastrutture di sicurezza, al fine di soddisfare i requisiti che provengono dai domini relativi alle Policy (BCDRP e LRIC)

Access Control: Meccanismi di segregazione dell'infrastruttura, partizionamento delle risorse, ammissione d'ingresso e sorveglianza

Telecommunication & Network Security: Caratteristiche, Peculiarità e relativi Dispositivi per la sicurezza in ambito distribuito e di rete

Security Architecture & Design: Metodi, Architetture e Modelli da adottare per comporre la struttura IT in modo sicuro

Prassi: indicazioni operative, relative ai costumi, alle consuetudini ed alle usanze che devono essere introdotte nell'operatività quotidiana, al fine di aumentare il livello generale di sicurezza, in modo da non inficiare quanto realizzato da un buon Approccio (AC, TNS, SAD)

Operational Security: Prassi ed Istruzioni da adottare per operare nell'IT in modo sicuro

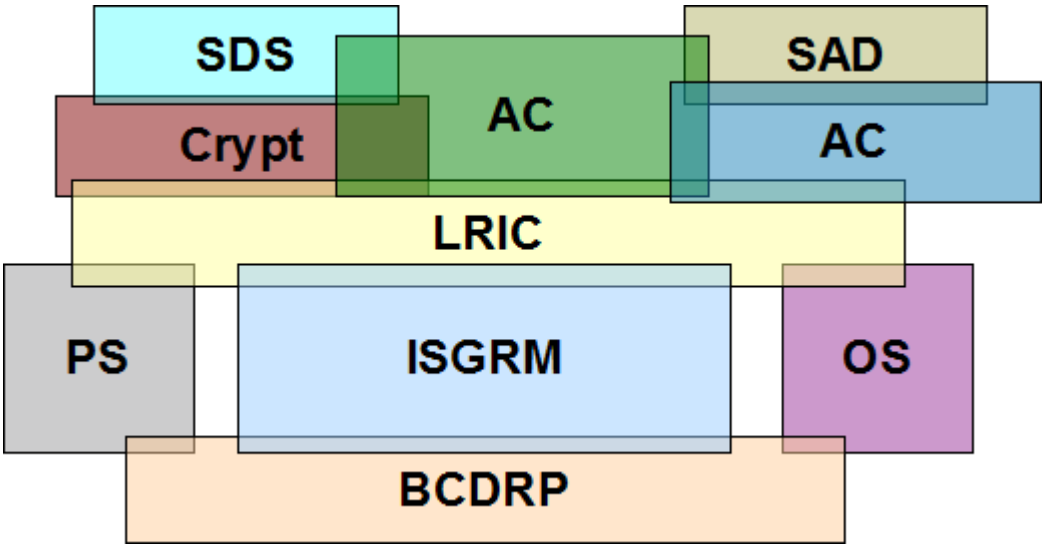
Software Development Security: Prassi e Metodi per lo sviluppo protetto di software. Modelli e Meccanismi per aumentare la sicurezza nel software

Tecniche: domini relativi a specifiche tecnologie, capacità e competenze da padroneggiare per poter essere impiegate nella sicurezza, soprattutto come ausilio per i domini di Approccio (AC, TNS, SAD)

Cryptography: Meccanismi ed algoritmi matematici di codifica dei dati, al fine di garantirne la Confidenzialità, l'Integrità

Physical (Environmental) Security: Aspetti di sicurezza dell'ambiente fisico: • anti-intrusione • fuoco ed esplosione • calamità naturali

La figura seguente mostra graficamente le interdipendenze logiche tra i diversi domini:



Strutturazione Quiz CISSP

Domande: 250 (225 in valutazione, 25 di esperimento)

Tempo: 6 ore

Passing Score: determianto dinamicamente. In generale, varia, intorno al 70%-75% (158 - 169)

Quiz Response Tips

Nel presente paragrafo vengono forniti dei suggerimenti di carattere generale allo scopo di determinare dei criteri per rispondere alle domande poste nei quiz, indipendentemente dall'argomento trattato.

Tipi di Quiz

Può essere utile capire la modalità con cui è stato ideato ogni quiz (domanda + le 4 possibili risposte), nel momento in cui ci si accinge a rispondere, allo scopo di determinare quale sia i processi mentali che ci si aspetti vengano seguiti, in funzione del livello di preparazione, e non cadere in facili trabocchetti. In questa ottica i quiz Le domande possono essere classificate in vari modi, in funzione di:

- formulazione della domanda
- scelta delle 4 risposte possibili

Formulazione della Domanda

What-is: domanda chiara e semplice, quale delle quattro seguenti possibili risposte è giusta

What-is-not: simile alla precedente ma con una o più negazioni, in modo da confondere

The-Best: domanda insidiosa, si chiede quale sia la migliore delle risposte sottoelencate

The-Most: domanda insidiosa,

Scelta delle 4 possibili Risposte

2-Bad: vi sono due risposte palesemente non corrette, occorre scegliere fra le restanti altre due

All-Valid: tutte le risposte corrispondono a concetti dell'esame ma solo una interessa la domanda posta

General Response Tips

Very Closer Choise

Letio Difficiliora

Acronyms

ATM: Automatic Teller Machine

CAAT: Computer Assisted Audit Tecniques

CobiT: Control Objectives for Information and related Technology

CORBA: Common Object Request Broker Architecture

CPA: Control Process Accounting (?)

CSA: Control Self-Assessment

EDI: Electronic Data Interchange

EFT: Electronic Found Transfer

FAR: False Acceptanse Rate

FRR: False Rejection Rate

ISACA: Information System Audit and Control Association

ITF: Integrating Test Facility

IPF: Integrated Processing Facility (CED)

PoS: Point of Sales

SOAP: Simple Object Access Protocol

SPOOL: Simultaneous Peripheral Operation On-Line