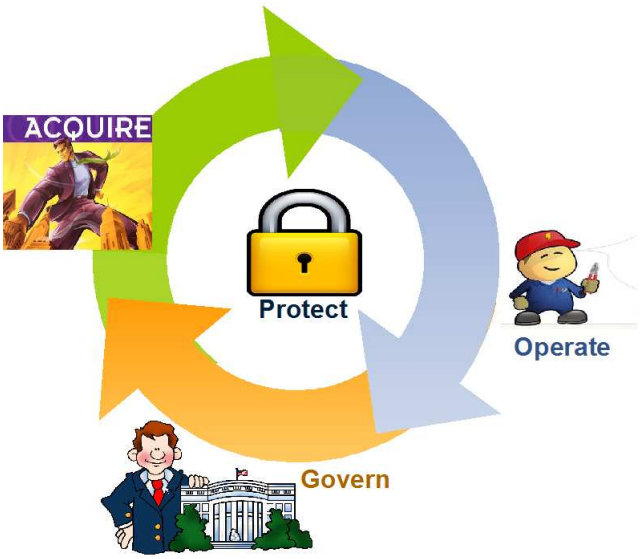
CISA: Certified Information System Auditor

Appunti per l'Esame di Certificazione

31 luglio 2012



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

Indirizzamento
Questo manuale in Italiano fornisce appunti schematici per superare l'esame del CISA nella versione del 2011. Io ho superato l'esame nel 2005 (CISA 2001); ho dunque provveduto a sistemare periodicamente il materiale concordemente con i cambiamenti operati nel BoK (Body of Knowledge). Difatti, ISACA provvede a rinnovare il BoK ogni 5 anni (2001-2005, 2006-2010, 2011-2015).
Vi sono 2 importanti variazioni nell'esame del 2001 rispetto a quello del 2011:

- maggiore enfasi sul concetto di Governance (divenuta maggiormente utilizzata), così come definita nel CObIT
- 5 domini anziché 7

Nella tabella seguente la mappatura puntuale:

Dominio 2011	**Dominio 2006**	**Dominio 2001**
Process of Auditing Information System	IS Audit Process	Information System Audit Process
Governance & Management of IT	IT Governance	Business Process Evaluation and Risk Management
	Business Continuity & Disaster Recovery	Business Continuity/Disaster Recovery
IS Acquisition, Development & Implementation	System and Infrastructure Life-Cycle Management	Business Application System Development, Implementation, Acquisition and Maintenance
IS Operations, Maintenance and Support	IT Service Delivery & Support	Technical Infrastructure and Organizational Practice
		Management, Planning and Organization of IS
Protection of Information Asset	Protection of Information Asset	Protection of Information Asset

Audit
Audit è un termine appartenente al lessico tecnico dell'economia e della finanza e indica:

Audit: "revisione contabile finalizzata alla certificazione del bilancio di un'azienda"

Deriva dal verbo latino AUDĪRE 'ascoltare'. Il termine fu poi acquisito dalla lingua inglese che ne fa uso a partire dal 1300 per indicare i pubblici ufficiali incaricati del controllo doganale. Ciononostante, come è successo per altre parole, il termine viene assunto in italiano, in questo particolare significato, non direttamente dal latino ma tramite la mediazione della lingua inglese, tanto è vero che i dizionari lo definiscono tuttora un esotismo.
La parola ha una storia relativamente recente nella nostra lingua ed è indicata come risalente ai primi anni '90 od ai tardi anni '80. Breve storia:

- **Attività Finanziaria**: verifica dei dati di bilancio e delle procedure di un'azienda per controllarne la correttezza
- **Gestione della Qualità** (UNI EN ISO 19011): processo sistematico, indipendente e documentato, finalizzato ad ottenere evidenze, in modo da valutare con obiettività i criteri di audit siano stati soddisfatti o meno
- **Organizzazione**: valutazione di un'organizzazione basata sul raffronto tra la sua realtà operativa e i requisiti richiesti

Indice

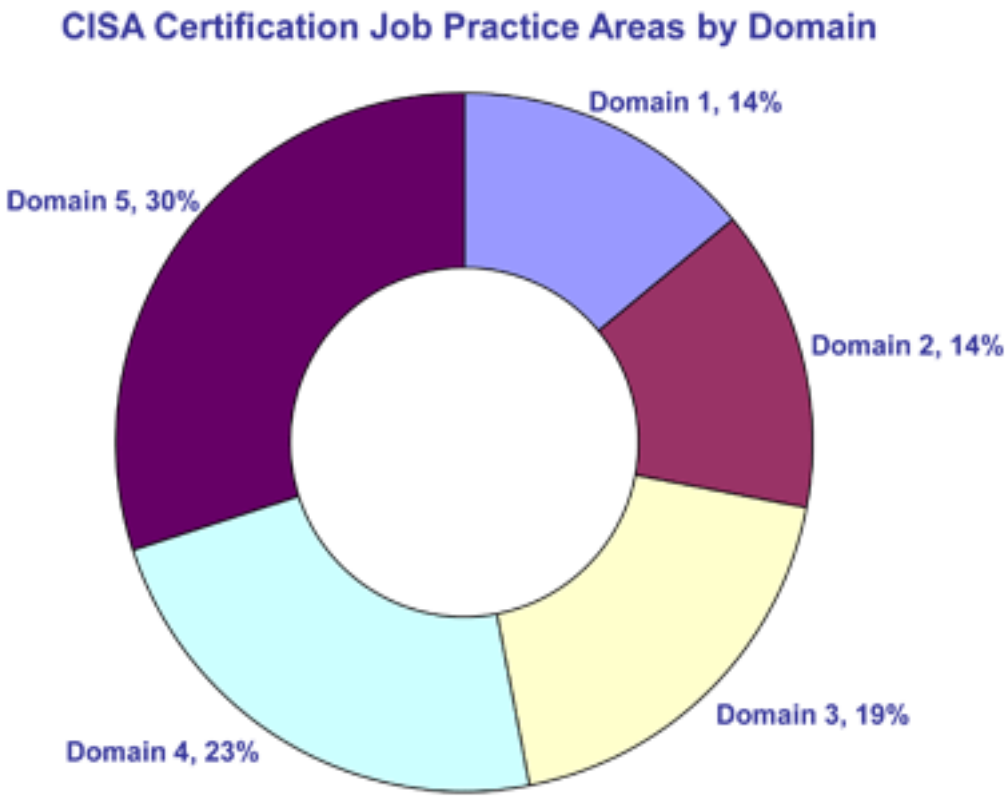
Introduzione

CISA Domains

La seguente tabella elenca i domini dell'esame CISA 2011:

#	Acronym	Nome	Note
1	ISAP	IS Audit Process	rimasto invariato
2	ITGM	IT Governance & Management	risultante da: - unione BPERM + BCDR - aggiunte Governance (CObIT)
3	ISADI	IS Acquisition, Development & Implementation	deriva da BASDAIM
4	ISOMS	IS Operation, Maintenance & Support	risultante da: - unione MPOIS + TIOP - introduzione Service (CObIT)
5	PIA	Protect Information Asset	invariato

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



CISA - CISSP mapping

Affrontando l'esame CISA, dopo aver sostenuto l'esame CISSP, esame i cui argomenti sono in molte parti coincidenti ancorchè affrontati da una prospettiva antitetica, ci si avvede di una certa sovrapposizione degli argomenti trattati nei vari domini.
Infatti mentre il CISSP[1] è più orientato alla realizzazione di sistemi sicuri, il CISA è orientato alla verifica dei controlli, tra cui anche quelli di sicurezza, facendo ricorso a concetti finanziari e di Project Management (ad esempio contenuti nell'esame PMP).
Nella seguente tabella sono evidenziate le corrispondenze tra i domini (indicati con acronimi, per brevità) dei differenti esami:

CISA	CISSP	Descrizione
ISAP	LIE, SMP	Le attività di Audit coinvolgono: - Legge (LIE) - Security Management (SMP)
ISOMS	SMP, TNS, OS	Le operazioni di manutenzione e supporto implicano la gestione (SMP), concetti di IT (TNS) e operativi (OS)
PIA	CRYPT, AC, SMA, PS	La protezione dei beni, implica concetti di crittografia (CRYPT), controllo d'accesso (AC), architetture (SMA) e fisici (PS)
ITGM	BCP, SMP	La Governance comporta pianificazioned della continuità (BCP) e gestione del rischio di alto livello (SMP)
ISADI	ASD	Le attività di acquisizione, sviluppo ed implementazione dei sistemi implicano concetti di sviluppo applicativo (ASD) principalmente

Come è evidente dalla tabella, rispetto al CISSP, alcuni domini (TNS, OS, CRYPT, AC, SMA, PS) sono contratti nella trattazione del CISA, altri (ASD, BCP) sono trattati con enfasi leggermente minore, infine SMP è sviscerato in molte sue parti e implicazioni.

Strutturazione Quiz CISA

Domande: 200 (175 in valutazione, 25 di esperimento)

Tempo: 4 ore

Passing Score: determianto dinamicamente. In generale, varia, intorno al 70%-75% (123 - 132)

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.

[1] I domini CISSP (Certified Information System Security Professional) sono i seguenti:

SMP: Security Management Practices

AC: Access Control

SMA: Security Models and Architecture

PS: Physical Security

TNS: Telecommunication and Network Security

CRYPT: Crytography

BCP: Business Continuity Planning

LIE: Law Investigation and Ethics

ASD: Application and System Development

OS: Operational Security

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

Argument Specific Response Tips

Auditor Responsibilities

L'auditor deve intraprendere le seguenti attività, elencate in ordine temporale:

1. report suspected acts to the appropriate parties
2. assess the strenght and effectiveness of controls
3. ensure audit engagement are planned, designed and rewieved

Auditor Tasks

1. understanding Business Objectives
2. Plan the Audit
3. Report to the intended parties

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