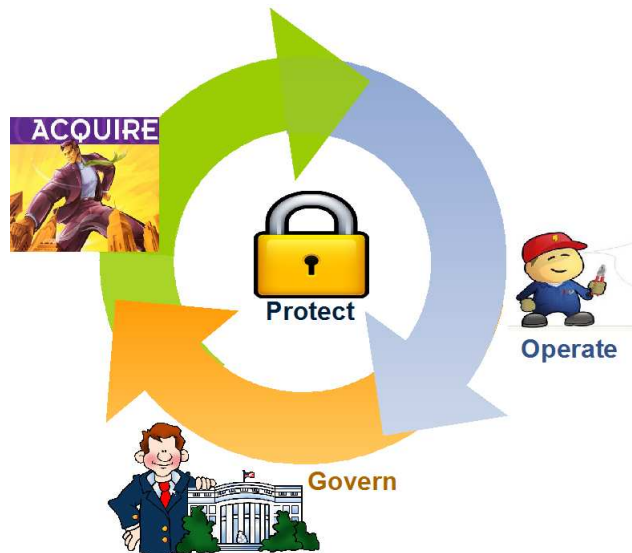


CISA: Certified Information System Auditor

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 AUDIRE '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

1	Information System Audit Process	5
1.1	Audit	5
1.1.1	Concetti Generali	5
1.1.2	Audit Types	5
1.1.2.1	Financial Statement Audit	5
1.1.2.2	Internal Audit Review	6
1.1.2.3	Control Self-Assessment	6
1.1.2.4	Information Technology Audit	6
1.2	Information Technology Audit	6
1.2.1	IT Audit Types	7
1.2.1.1	Evidence Scoring of Reliability	7
1.2.2	IS Audit Regulation and Legislation	7
1.2.3	Controls	8
1.2.3.1	Types of Controls	8
1.2.3.2	Classification of Controls	8
1.2.3.3	Scoring of Control	9
1.2.4	Test Types	9
1.2.5	Risk	9
1.2.5.1	Audit Related Risk Types	9
1.2.5.2	Business Knowledge	10
1.2.6	Audit Types	10
1.2.7	Audit Software	10
1.2.7.1	Generalized Audit Software	10
1.3	ISACA Ethic, Standard e Methodology	10
1.3.1	Code of Professional Ethics	11
1.3.2	IS Control Professional Standard	12
1.3.3	IS Audit Standard, Guidelines and Procedures	13
1.3.4	IS Audit Standards	14
1.3.5	IS Audit Guidelines	16
1.3.6	IS Audit Procedures	19
1.4	Audit Process	21
1.4.1	Establish the Terms of Engagement	21
1.4.2	Preliminary Review	21
1.4.3	Establish Materiality and Assess Risks	21
1.4.3.1	Materiality	21
1.4.3.2	Risk Assessment	22
1.4.4	Planning	22
1.4.5	Evaluation of Internal Controls	23
1.4.6	Audit Procedures	23
1.4.6.1	Evidences	23
1.4.6.2	Computer Assisted Audit Techniques	23
1.4.6.3	Audit Sampling	24
1.4.7	Completing the Audit	24
1.4.7.1	Reporting	24
1.4.7.2	Follow-up Activities	25

1.4.7.3	Assessing the Audit	25
1.5	Statement of Audit Standard	25
1.5.1	SAS 70	25
1.5.2	SAS 94	25
1.6	COBIT	26
1.6.1	Executive Summary	26
1.6.2	Framework	27
1.6.3	Control Objectives	28
1.6.4	Audit Guidelines	28
1.6.5	Implementation ToolSet	28
1.6.6	Management Guidelines	29
1.7	CoSO	29
1.7.1	Internal Controls	29
1.7.2	Framework	30
2	IT Governance & Management	31
2.1	Business Process Re-engineering	31
2.1.1	Benchmarking	31
2.1.1.1	ISACA Benchmarking Steps	31
2.1.2	BPR Steps	31
2.1.3	Business Performance Indicator	32
2.1.3.1	Key Performance Indicator	32
2.1.3.2	Balanced Scorecard	32
2.1.4	Evaluation of Controls	32
2.1.4.1	Input/Output Controls	32
2.1.4.2	Processing Controls	32
2.1.4.3	Output Controls	33
2.1.4.4	Integrity Controls	33
2.1.4.5	On-Line Auditing	33
2.1.4.6	Electronic Data Interchange	34
2.1.5	Business Process Change	35
2.1.5.1	Change-Management Team	35
2.1.5.2	Risk Indicators	35
2.2	Risk Management	35
2.2.1	Risk Management Phases	35
2.2.1.1	Program Development	35
2.2.1.2	Assets Identification	35
2.2.1.3	Threath and Vulnerability [Analysis]	36
2.2.1.4	Business Impact Analysis	36
2.2.1.5	Risk Level Evaluation	36
2.2.1.6	Control (Countermeasures) Design and Implementation	36
2.3	Business Continuity	36
2.3.1	Business Continuity Planning	36
2.3.1.1	Business Impact Analysis	37
2.3.1.2	System Classification	37
2.3.2	Insurance	37
2.3.2.1	Property Insurance	37
2.3.2.2	Liability Insurance	37
2.3.3	Human Resource (Response Team)	38
2.3.4	Alternative Sites	38
2.3.4.1	Hot Site	38
2.3.4.2	Warm Site	38
2.3.4.3	Cold Site	38
2.3.4.4	Duplicate Site	38
2.3.4.5	Reciprocal Agreement	39
2.3.5	BackUp and Storage	39
2.3.5.1	Backup Definitions	39

2.3.5.2	Tape Storage	39
2.4	Evaluation of Business Continuity	39
2.4.1	Testing Approach	39
2.4.1.1	Paper Test	39
2.4.1.2	Walk-Through Test	39
2.4.1.3	Preparedness Test	39
2.4.1.4	Full Operational Test	39
2.4.2	Evaluating the Capability to Continue	40
2.4.2.1	Business Disruption	40
2.4.2.2	Short-term Disruption	40
2.4.2.3	Primary Facility Disruption	41
3	IS Acquisition, Development & Implementation	43
3.1	System Development Life Cycle	43
3.1.1	Feasibility	43
3.1.2	Requirement Definition	44
3.1.2.1	Acquisition	44
3.1.3	Design	44
3.1.4	Development	44
3.1.5	Implementation	45
3.2	Project Management Techniques	45
3.2.1	Function Point Analysis	45
3.2.2	Gantt Chart	46
3.2.3	Program Evaluation Review Technique	46
3.2.4	Critical Path Methodology	46
3.2.5	Decision Support System	46
3.3	IT Organizational Policy	46
3.3.1	Capability Maturity Model	46
3.3.2	Programming Methods and Techniques	46
3.3.2.1	Formal Coding Standard	46
3.3.2.2	Prototyping	47
3.3.2.3	Rapid Application Development	47
3.3.2.4	Computer Aided Software Engineering	47
3.3.2.5	ACID	47
3.3.2.6	Cohesion and Coupling	47
3.3.2.7	On-line Programming	48
3.3.3	Languages	48
3.3.3.1	Strumenti	48
3.3.4	Personnel	48
3.4	Change Management Process	48
3.4.1	Change Control Process	48
3.4.1.1	Emergency Change	49
3.4.2	Quality Management	49
3.4.2.1	Testing Approach	49
3.4.2.2	Testing Levels	49
3.4.2.3	Testing Types	50
3.4.3	Application Definition	50
4	IS Operation, Maintenance & Support	51
4.1	Technical Infrastructure	51
4.1.1	IT Functions	51
4.1.1.1	Project Management	51
4.1.1.2	Line Management	51
4.1.2	Cobit Controls	51
4.1.2.1	Acquisition	51
4.1.2.2	Standards	52
4.1.2.3	Performance	52

4.1.2.4	Configuration	52
4.1.2.5	Service Providers	52
4.1.3	Evaluating Hardware	52
4.1.3.1	Hardware Components and Attributes	52
4.1.3.2	Computer Category	52
4.1.3.3	Risk and Control	53
4.1.3.4	Change and Configuration	53
4.1.4	Evaluating Software	53
4.1.4.1	Firmware	53
4.1.4.2	Operating Systems	53
4.1.4.3	Middleware	54
4.1.4.4	DataBase	54
4.1.4.5	Risk and Controls	54
4.1.4.6	Change and Configuration	55
4.1.5	Evaluating Network	55
4.1.5.1	ISO/OSI	55
4.1.5.2	Network Types	55
4.1.5.3	Type of Transmission	55
4.1.5.4	Network Topology	55
4.1.5.5	Network Devices	56
4.1.5.6	Risk and Controls	56
4.1.5.7	Test Types	57
4.2	Operational Practices	57
4.2.1	CobiT	57
4.2.2	Risk and Controls	57
4.2.3	Performance and Monitoring Process	57
4.3	Business Plan	58
4.3.1	Strategies	58
4.3.1.1	IT Steering Committee	58
4.3.1.2	Change Control Process	58
4.3.2	Policy	58
4.3.2.1	Policy Development Approach	58
4.3.2.2	Policy Types	58
4.3.2.3	Area of Policy Development	59
4.3.3	Procedure	59
4.3.4	Organizational Chart	59
4.4	IT Organization	59
4.4.1	IS Strategy	59
4.4.1.1	IS Assessment	59
4.4.2	IS Function	60
4.4.2.1	On-going Operation	60
4.4.2.2	Project	60
4.4.3	IS Strategy Components	60
4.4.4	IS Department Organization	60
4.4.4.1	Evaluation	60
4.4.5	Third Party Auditing	60
4.4.5.1	Audit	60
4.4.6	Contract Management	61
4.4.6.1	Tipologie di Contratti	61
4.5	IS Strategy and Policy	61
4.5.1	Project Management	61
4.5.1.1	Project Management Phases	61
4.5.2	Problem Management	62
4.5.3	Change Management	62
4.5.3.1	Change Request	62
4.5.4	Quality Management	62
4.5.4.1	Capability Maturity Model	62

4.5.4.2	ISO	63
4.5.5	Security Management	63
4.5.5.1	Physical Controls	63
4.5.5.2	Logical Controls	63
4.5.6	Business Continuity	63
4.6	Jobs and Responsibilities	63
4.6.1	Segregation of Duties	63
4.6.1.1	Figure Professionali	63
4.6.1.2	Segregationa Ares	64
4.6.2	Observation Process	64
5	Protection of Information Asset	65
5.1	Information Security Management	65
5.2	Logical Access Control	66
5.2.1	Access Control Components	66
5.2.2	Access Control Types	66
5.2.2.1	Discretionary Access Control	66
5.2.2.2	Mandatory Access Control	66
5.2.2.3	Non-Discretionary Access Control	67
5.2.3	Access Control Tips	67
5.2.4	Identification and Authentication Techniques	67
5.2.4.1	Authentication Form	67
5.2.4.2	Password	67
5.3	Network Security	68
5.3.1	Network Controls	68
5.3.2	Network Security Devices	68
5.3.2.1	Firewall	68
5.3.2.2	Virtual Private Network	68
5.3.2.3	Intrusion Detection Systems	68
5.3.2.4	Single Sign On	68
5.3.2.5	Privacy Branch eXchange	68
5.3.3	Intrusion Methods and Techniques	69
5.3.3.1	Passive Attack	69
5.3.3.2	Active Attack	69
5.3.3.3	Indirect Attack	69
5.3.3.4	Security Scanning	69
5.3.3.5	Information Security Source	69
5.4	Cryptography	69
5.4.1	Definizioni Fondamentali	70
5.4.2	Altre Definizioni	70
5.4.3	CypherSuite	71
5.4.3.1	Asymmetric Mechanism	71
5.4.3.2	Symmetric Mechanisms	72
5.4.3.3	Mode of Operation	72
5.4.3.4	Hash	72
5.4.4	Public Key Infrastructure	72
5.5	Physical Security	73
5.5.1	Power	73
5.5.1.1	Power Threats	73
5.5.1.2	Rimedi	73
5.5.2	Environmental	73
5.5.3	Fire	73
5.5.3.1	Sensori	73
5.5.3.2	Fire Suppression System	74
5.5.4	Physical Access	74
5.5.4.1	Access Control	74
5.5.4.2	Biometric	74

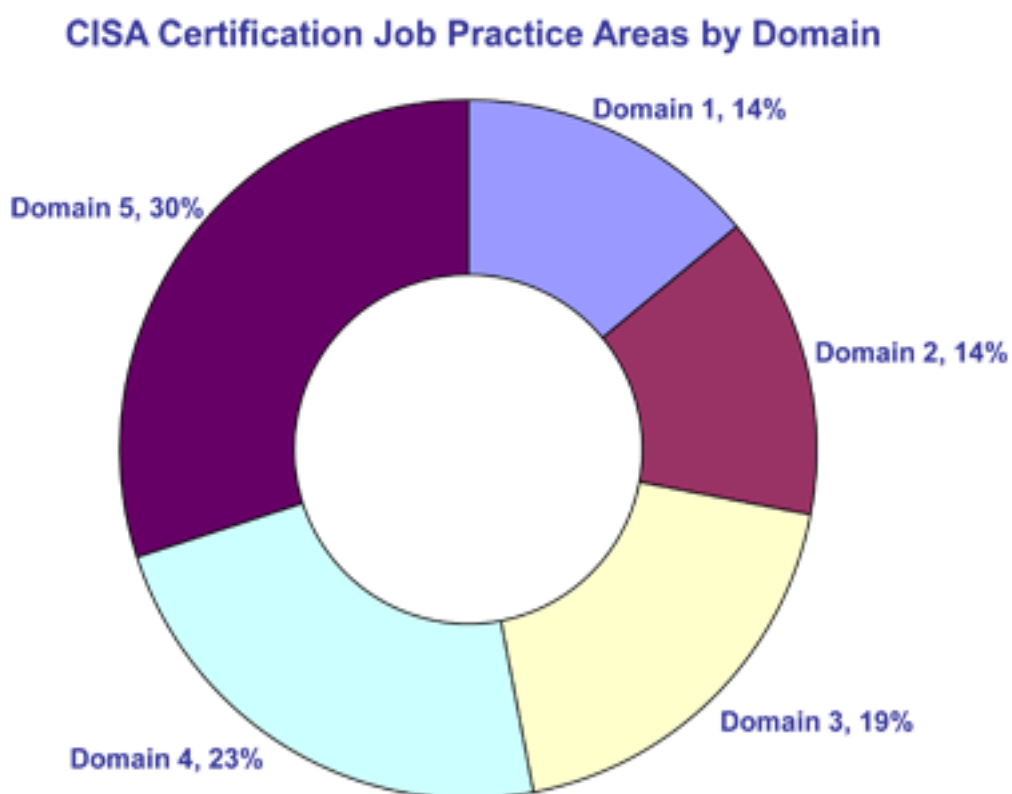
Introduzione

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 CISSP¹ 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 pianificazione 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: determinato 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.

¹I 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: Cryptography

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 Techniques

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