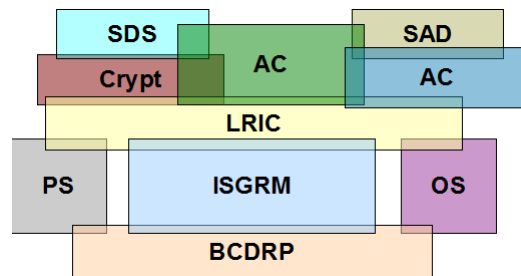


# CISSP: Certified Information System Security Professional

## 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 date 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

<b>1</b>	<b>Access Control</b>	<b>5</b>
1.1	Access Control Concepts	5
1.2	AAA	5
1.2.1	Definitions	5
1.2.2	Identification e Authentication	5
1.2.2.1	Authentication Factors	5
1.2.2.2	Biometrics	6
1.2.2.3	Password	6
1.2.2.4	Devices	7
1.2.3	Authorization	7
1.2.3.1	Access Criteria	7
1.2.3.2	Default to No Access	7
1.2.3.3	Need to Know (Least Privilege)	7
1.2.4	Single Sign On	7
1.2.4.1	Scripting	7
1.2.4.2	Kerberos	8
1.2.4.3	SESAME	8
1.2.4.4	Thin Clients (Dumb Terminal)	8
1.2.4.5	Directory Services	8
1.2.5	Accountability	8
1.2.5.1	Account Event Level	8
1.2.5.2	Audit Information Review	9
1.2.5.3	Intrusion Detection System	9
1.2.5.4	Honeypot	9
1.2.5.5	Network Sniffer	10
1.2.5.6	Protecting Audit Data	10
1.3	Access Control Model	10
1.3.1	Discretionary Access Control	10
1.3.2	Mandatory Access Control	10
1.3.3	Role Base (Nonmandatory) Access Control	10
1.3.3.1	Criteri di Accesso	11
1.4	Access Control Technique	11
1.5	Access Control Administration	11
1.5.1	Centralized Access Control	11
1.5.1.1	RADIUS	11
1.5.1.2	TACACS	11
1.5.1.3	Diameter	12
1.5.2	Decentralized Access Control	12
1.5.3	Hybrid	12
1.6	Access Control Methods	12
1.6.1	Access Control Functionality	12
1.6.2	Access Control Type	12
1.6.2.1	Administrative	13
1.6.2.2	Physical Controls	13
1.6.2.3	Technical Controls	13

1.7	Access Control Best Practices . . . . .	13
1.7.1	Task . . . . .	13
1.7.1.1	Unauthorized Disclosure of Information . . . . .	14
1.7.1.2	Penetration Test . . . . .	14
<b>2</b>	<b>Telecommunications and Network Security</b>	<b>15</b>
2.1	Introduction . . . . .	15
2.1.1	Telecommunications . . . . .	15
2.1.1.1	Standard Organization . . . . .	15
2.1.2	Networking . . . . .	15
2.1.3	Open System Interconnect . . . . .	15
2.1.3.1	Application (Layer 7) . . . . .	15
2.1.3.2	Presentation (Layer 6) . . . . .	15
2.1.3.3	Session (Layer 5) . . . . .	16
2.1.3.4	Transport (Layer 4) . . . . .	16
2.1.3.5	Network (Layer 3) . . . . .	16
2.1.3.6	Data Link (Layer2) . . . . .	17
2.1.3.7	Physical (Layer 1) . . . . .	17
2.2	Physical Layer . . . . .	17
2.2.1	Trasmission Definitions . . . . .	17
2.2.2	Network Topology . . . . .	17
2.2.3	Media Access Technology . . . . .	18
2.2.3.1	Token Passing . . . . .	18
2.2.3.2	Carrier Sense Multiple Access . . . . .	18
2.2.3.3	Polling . . . . .	18
2.2.4	Cabling . . . . .	18
2.2.4.1	Coaxial Cable . . . . .	18
2.2.4.2	Twisted Pair Cable . . . . .	18
2.2.4.3	Fiber-Optic Cable . . . . .	19
2.2.4.4	Cabling Problems . . . . .	19
2.3	Data Link Layer . . . . .	19
2.3.1	Local Area Network . . . . .	19
2.3.2	Metropolitan Area Network . . . . .	20
2.3.3	Wide Area Network . . . . .	20
2.3.3.1	Definitions . . . . .	20
2.3.3.2	WAN Technology . . . . .	20
2.3.3.3	MultiService Access Technology . . . . .	20
2.3.3.4	Remote Access . . . . .	21
2.3.4	Ethernet (IEEE 802.3) . . . . .	21
2.3.5	Token Ring (IEEE 802.5) . . . . .	21
2.3.6	FDDI (IEEE 802.8) . . . . .	22
2.3.7	Wireless . . . . .	22
2.3.7.1	Spread Spectrum . . . . .	22
2.3.7.2	WLAN Components . . . . .	22
2.3.7.3	Wireless Application Protocol . . . . .	22
2.3.7.4	WLAN IEEE Standards . . . . .	23
2.3.7.5	WLAN Best Practices Decalog . . . . .	23
2.3.7.6	New Wireless Standard 802.11i . . . . .	23
2.4	Network Layer . . . . .	24
2.4.1	Protocols . . . . .	24
2.4.2	Virtual Private Network . . . . .	24
2.4.2.1	Tunneling Protocol . . . . .	24
2.4.2.2	PPP Authentication Protocol . . . . .	25
2.5	Transport Layer . . . . .	25
2.6	Application Layer . . . . .	25
2.6.1	Network Operating System . . . . .	25
2.6.2	Domain Name System . . . . .	25

2.6.3	Directory Services . . . . .	25
2.7	Network Devices . . . . .	25
2.7.1	Repeater (layer 1) . . . . .	25
2.7.2	Bridge (layer 2) . . . . .	26
2.7.2.1	Forwarding Tables . . . . .	26
2.7.3	Router (layer 3) . . . . .	26
2.7.3.1	Routing Tables . . . . .	26
2.7.4	Switch (layer 2+) . . . . .	27
2.7.5	Gateway (layer 4+) . . . . .	27
2.7.6	PBX . . . . .	27
2.7.7	Firewall . . . . .	27
2.7.7.1	Firewall Type . . . . .	27
2.7.7.2	Firewall Architecture . . . . .	27
2.7.7.3	Network Address Translation . . . . .	28
2.7.7.4	Honeypot . . . . .	28
<b>3</b>	<b>Information Security Governance &amp; Risk Management</b>	<b>29</b>
3.1	Security Management Concepts . . . . .	29
3.1.1	I 3 Principi Fondamentali della Sicurezza . . . . .	29
3.1.1.1	Availability . . . . .	29
3.1.1.2	Integrity . . . . .	29
3.1.1.3	Confidentiality . . . . .	29
3.1.2	Security Definitions . . . . .	29
3.1.3	Top-Down Approach . . . . .	30
3.2	Operational Security Model . . . . .	30
3.2.1	Layers . . . . .	30
3.2.2	Planning Horizon . . . . .	30
3.2.3	Business Requirement (Private vs. Military) . . . . .	30
3.3	Security Management Responsibilities . . . . .	30
3.3.1	Security Administration . . . . .	31
3.3.2	Supporting Controls . . . . .	31
3.3.2.1	Administrative Controls . . . . .	31
3.3.2.2	Technical (Logical) Controls . . . . .	31
3.3.2.3	Physical Controls . . . . .	31
3.3.3	Security Roles . . . . .	32
3.3.3.1	Information Owner . . . . .	32
3.3.3.2	Data Custodian . . . . .	32
3.3.3.3	User . . . . .	32
3.3.3.4	Senior Manager . . . . .	32
3.3.3.5	Security Professional . . . . .	32
3.3.3.6	Auditor . . . . .	32
3.3.4	Hiring Practices . . . . .	32
3.4	Risk Management . . . . .	33
3.4.1	Risk Analysis . . . . .	33
3.4.2	Quantitative Risk Analysis . . . . .	33
3.4.2.1	Asset and Information Evaluation . . . . .	33
3.4.2.2	Potential Loss per Risk Estimation . . . . .	34
3.4.2.3	Threat Analysis . . . . .	34
3.4.2.4	Loss Potential per Threat (Risk?) . . . . .	35
3.4.2.5	Recommendation, Safeguard, Countermeasures and Action . . . . .	35
3.4.3	Qualitative Risk Analysis . . . . .	36
3.4.3.1	Delphi Technique . . . . .	36
3.4.4	Handling Risk . . . . .	36
3.5	Security Documents . . . . .	36
3.5.1	Strategical Goals . . . . .	36
3.5.1.1	Policies . . . . .	36
3.5.2	Tactical Goals . . . . .	37

3.5.2.1	Standards . . . . .	37
3.5.2.2	Baselines . . . . .	37
3.5.2.3	Guidelines . . . . .	37
3.5.3	Operational Goals . . . . .	37
3.5.3.1	Procedures . . . . .	37
3.6	Information Classification . . . . .	37
3.6.1	Classes . . . . .	37
3.6.1.1	Commercial Business Classification . . . . .	37
3.6.1.2	Military Classification . . . . .	38
3.6.2	Data Classification Procedure . . . . .	38
3.7	Security Awareness . . . . .	38
3.7.1	Security Awareness Audiences . . . . .	38
3.7.1.1	Management . . . . .	38
3.7.1.2	Mid-Management . . . . .	38
3.7.1.3	Technical Department . . . . .	38
3.7.1.4	Staff . . . . .	38
<b>4</b>	<b>Software Development Security</b>	<b>39</b>
4.1	Introduction . . . . .	39
4.2	System Development . . . . .	39
4.2.1	Management and Development . . . . .	39
4.2.1.1	Risk Management . . . . .	39
4.2.1.2	Change Control . . . . .	39
4.2.1.3	Software Escrow . . . . .	39
4.2.2	Life Cycle Phases . . . . .	39
4.2.2.1	Project Initiation . . . . .	39
4.2.2.2	Functional Design, Analysis and Planning . . . . .	40
4.2.2.3	System Design Specification . . . . .	40
4.2.2.4	Software Development . . . . .	40
4.2.2.5	Implementation/Installation . . . . .	40
4.2.2.6	Operational/Maintenance . . . . .	41
4.2.2.7	Disposal . . . . .	41
4.2.3	Software Development Methods . . . . .	41
4.2.3.1	WaterFall . . . . .	41
4.2.3.2	Spiral Model . . . . .	41
4.2.3.3	Joint Analysis Developer . . . . .	41
4.2.3.4	Rapid Application Developer . . . . .	41
4.2.3.5	CleanRoom . . . . .	41
4.2.4	Capability Maturity Model . . . . .	41
4.3	DataBase Management . . . . .	42
4.3.1	Definizioni . . . . .	42
4.3.1.1	DataBase Models . . . . .	42
4.3.1.2	Relational DataBase Definitions . . . . .	42
4.3.1.3	Relational DB Components . . . . .	43
4.3.2	Security Issues . . . . .	43
4.3.2.1	Integrity . . . . .	43
4.3.2.2	Integrity Operation . . . . .	43
4.3.2.3	OnLine Transaction Processing . . . . .	43
4.3.2.4	Confidentiality . . . . .	43
4.3.2.5	Confidentiality Tricks . . . . .	44
4.4	Application Development Methodology . . . . .	44
4.4.1	General Definitions . . . . .	44
4.4.1.1	Data Structure . . . . .	44
4.4.2	Object Oriented Concepts . . . . .	44
4.4.3	Software Architecture . . . . .	45
4.4.4	Technology . . . . .	45
4.4.4.1	Object Request Broker e CORBA . . . . .	45



4.4.4.2	Distributed Computing Environment . . . . .	45
4.4.4.3	COM e DCOM . . . . .	45
4.4.4.4	ODBC . . . . .	46
4.4.4.5	Object Linking and Embedding . . . . .	46
4.4.4.6	Dynamic Data Exchange . . . . .	46
4.4.4.7	Enterprise Java Beans . . . . .	46
4.4.4.8	Expert System and Knowledge Base Systems . . . . .	46
4.4.4.9	Artificial Neural Network . . . . .	46
4.4.4.10	Java . . . . .	46
4.4.4.11	ActiveX . . . . .	46
4.4.5	Attacks . . . . .	47
4.4.5.1	Malware . . . . .	47
4.4.5.2	Techniques . . . . .	47
4.4.5.3	Denial of Service . . . . .	47
4.4.5.4	Timing Attack . . . . .	48
<b>5</b>	<b>Cryptography</b>	<b>49</b>
5.1	Introduzione . . . . .	49
5.1.1	Breve Storia della Crittografia . . . . .	49
5.1.1.1	Antichità . . . . .	49
5.1.1.2	World War II . . . . .	49
5.1.2	Definizioni . . . . .	49
5.1.3	Obiettivi della Crittografia . . . . .	50
5.1.4	Ciphers Types . . . . .	50
5.1.4.1	Algorithm Based Ciphers . . . . .	50
5.1.4.2	Spy Ciphers . . . . .	50
5.1.4.3	Steganography . . . . .	50
5.1.5	Cryptography e Government . . . . .	50
5.1.5.1	Clipper Chip . . . . .	50
5.1.6	Cryptographic Principles . . . . .	50
5.1.6.1	Auguste Kerckhoff . . . . .	50
5.1.6.2	Claude Shannon . . . . .	51
5.1.7	Cryptographic Attack . . . . .	51
5.1.7.1	Key Discoverer (Cryptoanalysis) Attack . . . . .	51
5.1.7.2	Man-in-the-Middle Attack . . . . .	51
5.1.7.3	Dictionary Attack . . . . .	51
5.1.7.4	Replay Attack . . . . .	51
5.1.7.5	Birthday Attack . . . . .	52
5.1.7.6	Side Channel Attack . . . . .	52
5.2	Encryption Methods . . . . .	52
5.2.1	Symmetric . . . . .	52
5.2.1.1	Data Encryption Standard . . . . .	52
5.2.1.2	3DES . . . . .	53
5.2.1.3	Blowfish . . . . .	53
5.2.1.4	International Data Encryption Algorithm . . . . .	53
5.2.1.5	RC4, RC5, RC6 . . . . .	53
5.2.1.6	Advanced Encryption Standard . . . . .	53
5.2.1.7	Mode of Operation . . . . .	53
5.2.2	Asymmetric (Public Key Cryptography) . . . . .	54
5.2.2.1	Rivest Shamir Adleman . . . . .	54
5.2.2.2	Elliptic Curve Cryptosystem . . . . .	54
5.2.2.3	Diffie-Hellman . . . . .	54
5.2.2.4	El Gamal . . . . .	54
5.2.2.5	Digital Signature Algorithm . . . . .	54
5.2.2.6	Knapsack . . . . .	54
5.2.3	Hybrid . . . . .	54
5.2.4	One-Way-Hash . . . . .	54

5.2.4.1	Message Authentication Code . . . . .	54
5.2.4.2	Digital Signature . . . . .	54
5.2.4.3	Hash Algorithm . . . . .	55
5.2.4.4	Digital Signature Standard . . . . .	55
5.3	Public Key Infrastructure . . . . .	55
5.3.1	Objectives . . . . .	55
5.3.2	Components . . . . .	55
5.3.2.1	Certificate Authority . . . . .	55
5.3.2.2	Registration Authority . . . . .	55
5.3.2.3	Certificate Repository . . . . .	55
5.3.2.4	Certificate Revocation List . . . . .	55
5.3.2.5	Key backup e Recovery . . . . .	55
5.3.2.6	Key History Management . . . . .	55
5.3.2.7	Timestamping . . . . .	55
5.3.2.8	Client-side Software . . . . .	55
5.3.3	Key Management . . . . .	55
5.4	Internet Security . . . . .	56
5.4.1	E-Mail . . . . .	56
5.4.1.1	Multipurpose Internet Mail Extension . . . . .	56
5.4.1.2	Secure/MIME . . . . .	56
5.4.1.3	Pretty Good Privacy . . . . .	56
5.4.2	HTTP . . . . .	56
5.4.2.1	S-HTTP . . . . .	56
5.4.2.2	HTTPS . . . . .	56
5.4.2.3	Secure Electronic Transaction . . . . .	56
5.4.2.4	Cookie . . . . .	56
5.4.3	IPSec . . . . .	57
5.4.3.1	Internet Key Exchange . . . . .	57
<b>6</b>	<b>Security Architecture &amp; Design</b>	<b>59</b>
6.1	Introduzione . . . . .	59
6.1.1	BS 7799 . . . . .	59
6.1.2	Trust e Assurance . . . . .	60
6.2	Computer Architecture . . . . .	60
6.2.1	von Neumann . . . . .	60
6.2.1.1	Central Processing Unit . . . . .	60
6.2.1.2	Memory . . . . .	60
6.2.1.3	I/O Devices . . . . .	61
6.2.2	Processes . . . . .	61
6.2.2.1	Threats . . . . .	61
6.3	System Architecture . . . . .	62
6.3.1	Trusted Computing Base . . . . .	62
6.3.2	Best Practices . . . . .	63
6.4	Security Models . . . . .	63
6.4.1	Information Flow Model . . . . .	63
6.4.1.1	Information Flow Model . . . . .	63
6.4.1.2	Bell-LaPadula Model . . . . .	63
6.4.1.3	Biba Model . . . . .	63
6.4.2	Practical Model . . . . .	63
6.4.2.1	Graham-Denning Model . . . . .	63
6.4.2.2	Harrison-Russo-Ullman Model . . . . .	64
6.4.3	Misc Model . . . . .	64
6.4.3.1	Clark-Wilson Model . . . . .	64
6.4.3.2	Noninterference Model . . . . .	64
6.4.3.3	Brewer and Nash Model . . . . .	64
6.5	Security Modes of Operation . . . . .	64
6.6	System Evaluation Methods . . . . .	64

6.6.1	Orange Book . . . . .	64
6.6.1.1	D: Minimal Protection . . . . .	65
6.6.1.2	C: Discretionary Protection . . . . .	65
6.6.1.3	B: Mandatory Protection . . . . .	65
6.6.1.4	A: Verified Protection . . . . .	65
6.6.1.5	Rainbow Series . . . . .	65
6.6.2	ITSEC . . . . .	65
6.6.3	Common Criteria . . . . .	66
<b>7</b>	<b>Operational Security</b>	<b>67</b>
7.1	Operational Security Concepts . . . . .	67
7.1.1	Administrative Management . . . . .	67
7.1.2	Accountability . . . . .	67
7.1.3	Product Evaluation . . . . .	67
7.1.3.1	Operational Assurance . . . . .	67
7.1.3.2	Life Cycle Assurance . . . . .	68
7.1.4	Input/Output Control . . . . .	68
7.2	Internet Security . . . . .	69
7.2.1	E-Mail . . . . .	69
7.2.1.1	Simple Mail Transfer Protocol . . . . .	69
7.2.1.2	Post Office Protocol 3 . . . . .	69
7.2.1.3	Internet Message Access Protocol . . . . .	69
7.2.1.4	SMTP Relaying . . . . .	69
7.2.2	Fax . . . . .	69
7.3	Hack and Attack . . . . .	69
7.3.1	Network Map and Fingerprint . . . . .	69
7.3.2	Techniques . . . . .	69
7.3.3	Attacks . . . . .	69
7.3.3.1	Penetration Test . . . . .	70
7.3.4	Operation Department . . . . .	70
7.3.4.1	Unusual and Unexplained Occurrences . . . . .	70
7.3.4.2	Deviation from Standard . . . . .	70
7.3.4.3	Unscheduled Initial Program Load . . . . .	70
<b>8</b>	<b>Business Continuity &amp; Disaster Recovery Planning</b>	<b>71</b>
8.1	Introduction . . . . .	71
8.1.1	Business World Characteristics . . . . .	71
8.1.1.1	AIC Triad . . . . .	71
8.1.2	Definitions . . . . .	71
8.1.2.1	Threats Types . . . . .	71
8.1.2.2	Disruption Types . . . . .	72
8.1.2.3	Business Continuity Plan Goals . . . . .	72
8.2	Business Continuity Plan . . . . .	72
8.2.1	Basilar Steps . . . . .	72
8.2.1.1	Project Initiation . . . . .	72
8.2.1.2	Business Impact Analysis . . . . .	72
8.2.1.3	Recovery Strategy Development . . . . .	72
8.2.1.4	Recovery Plan Development . . . . .	73
8.2.1.5	Implementation . . . . .	73
8.2.1.6	Testing (Maintenance) . . . . .	73
8.3	Provided Procedures . . . . .	74
8.3.1	Extended Backup . . . . .	74
8.3.1.1	OffSite Hardware BackUp . . . . .	74
8.3.1.2	Software BackUp . . . . .	74
8.3.1.3	BackUp Types . . . . .	75
8.3.1.4	Backup Technologies . . . . .	75
8.3.1.5	Human Resources . . . . .	75

8.3.2	Disaster Recovery . . . . .	75
8.3.2.1	Disaster Recovery Team . . . . .	75
8.3.3	Emergency Response . . . . .	75
<b>9</b>	<b>Law, Regulation, Investigation &amp; Compliance</b>	<b>77</b>
9.1	Ethics and Hackers . . . . .	77
9.1.1	Principles . . . . .	77
9.1.1.1	(ISC) <sup>2</sup> Code of Ethics . . . . .	77
9.1.1.2	Computer Ethics Institute . . . . .	77
9.1.1.3	Internet Architecture Board . . . . .	77
9.1.1.4	Generally Accepted System Security Principles . . . . .	78
9.1.2	MOM . . . . .	78
9.1.2.1	Motive . . . . .	78
9.1.2.2	Opportunity . . . . .	78
9.1.2.3	Means . . . . .	78
9.1.3	Attacks . . . . .	78
9.1.3.1	Internal Attacks . . . . .	78
9.1.3.2	External Attacks . . . . .	78
9.1.3.3	Phreaking . . . . .	79
9.2	Law . . . . .	79
9.2.1	Liability . . . . .	79
9.2.2	Types of Laws . . . . .	79
9.2.2.1	Categories of Laws . . . . .	79
9.2.2.2	Intellectual Property Laws . . . . .	79
9.2.2.3	Software Piracy . . . . .	80
9.2.3	Law, Directives, Regulations . . . . .	80
9.2.3.1	Health Insurance Portability and Accountability Act (HIPAA) . . . . .	80
9.2.3.2	Gramm-Leach-Bliley Act . . . . .	80
9.2.3.3	Computer Fraud and Abuse Act . . . . .	80
9.2.3.4	Federal Privacy Act . . . . .	80
9.2.3.5	European Union Principles on Privacy . . . . .	81
9.2.3.6	Computer Security Act . . . . .	81
9.2.3.7	Security and Freedom From Encryption . . . . .	81
9.2.3.8	Federal Sentencing Guidelines . . . . .	81
9.2.3.9	Economic Espionage Act . . . . .	81
9.2.4	International Cooperation Effort . . . . .	81
9.2.4.1	G8 . . . . .	81
9.2.4.2	Interpol . . . . .	81
9.2.4.3	European Commission . . . . .	81
9.3	Investigation . . . . .	81
9.3.1	Computer Forensic . . . . .	81
9.3.1.1	Crime Scene . . . . .	81
9.3.1.2	Incident Response Team . . . . .	82
9.3.1.3	Chain of Custody . . . . .	82
9.3.2	Incident Handling . . . . .	82
9.3.3	Evidence . . . . .	82
9.3.3.1	Evidence Life Cycle . . . . .	82
9.3.3.2	Admissible Evidence Characteristics . . . . .	82
9.3.3.3	Evidence Categories . . . . .	82
9.3.4	Surveillance, Search, Seizure . . . . .	82
9.3.4.1	Surveillance . . . . .	83
9.3.4.2	Search . . . . .	83
9.3.4.3	Seizure . . . . .	83
9.3.4.4	Interrogating . . . . .	83

<b>10 Physical (Environmental) Security</b>	<b>85</b>
10.1 Introduction . . . . .	85
10.1.1 Physical Security Risks . . . . .	85
10.1.1.1 Physical Theft . . . . .	85
10.1.1.2 Service Interruption . . . . .	85
10.1.1.3 Physical Damage . . . . .	85
10.1.1.4 Compromised System Integrity . . . . .	85
10.1.1.5 Unauthorized Disclosure . . . . .	85
10.1.2 Physical Security Components Selection Process . . . . .	85
10.1.2.1 Hardware . . . . .	85
10.1.3 Planing Process . . . . .	85
10.2 Administrative Controls . . . . .	85
10.2.1 Facility Selection . . . . .	86
10.2.2 Facility Construction . . . . .	86
10.2.2.1 Building Issues . . . . .	86
10.2.3 Facility Management . . . . .	87
10.2.3.1 Facility Components . . . . .	87
10.2.3.2 Computer and Equipment Rooms . . . . .	87
10.2.4 Personnel Controls . . . . .	87
10.2.4.1 Pre-employment Screening . . . . .	87
10.2.4.2 Employee Maintenance . . . . .	88
10.2.4.3 Post-Employment . . . . .	88
10.2.5 Training . . . . .	88
10.2.6 Emergency Response and Procedures . . . . .	88
10.3 Technical Controls . . . . .	88
10.3.1 Access Controls . . . . .	88
10.3.1.1 Personnel Access Control . . . . .	88
10.3.1.2 Card Badge . . . . .	89
10.3.2 Intrusion Detection . . . . .	89
10.3.3 Alarms . . . . .	89
10.3.4 Monitoring (CCTV) . . . . .	89
10.3.5 Heating, Ventilation, Air Conditioning (HVAC) . . . . .	89
10.3.6 Power Supply . . . . .	90
10.3.6.1 Power Protection . . . . .	90
10.3.6.2 Electrical Power Distrurbs . . . . .	90
10.3.7 Fire . . . . .	90
10.3.7.1 Placemnt of Sensors and Detection . . . . .	90
10.3.7.2 Placement of Sprinklers . . . . .	91
10.3.7.3 Fire Protection . . . . .	91
10.3.7.4 Type of Detection . . . . .	91
10.3.7.5 Type of Suppression . . . . .	91
10.3.8 Backups . . . . .	92
10.4 Physical Controls . . . . .	92
10.4.1 Fencing . . . . .	92
10.4.2 Gates . . . . .	93
10.4.3 Bollards . . . . .	93
10.4.4 Locks . . . . .	93
10.4.5 Lighting . . . . .	93
10.4.6 Surveillance . . . . .	94
10.4.7 Facility Construction Materials . . . . .	94



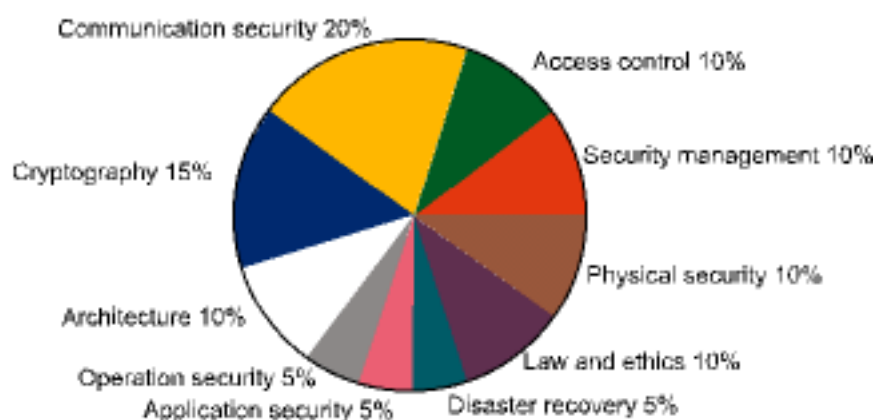
# Introduzione

## 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 inciappare quanto realizzato da un buon Approccio (AC, TNS, SAD)

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

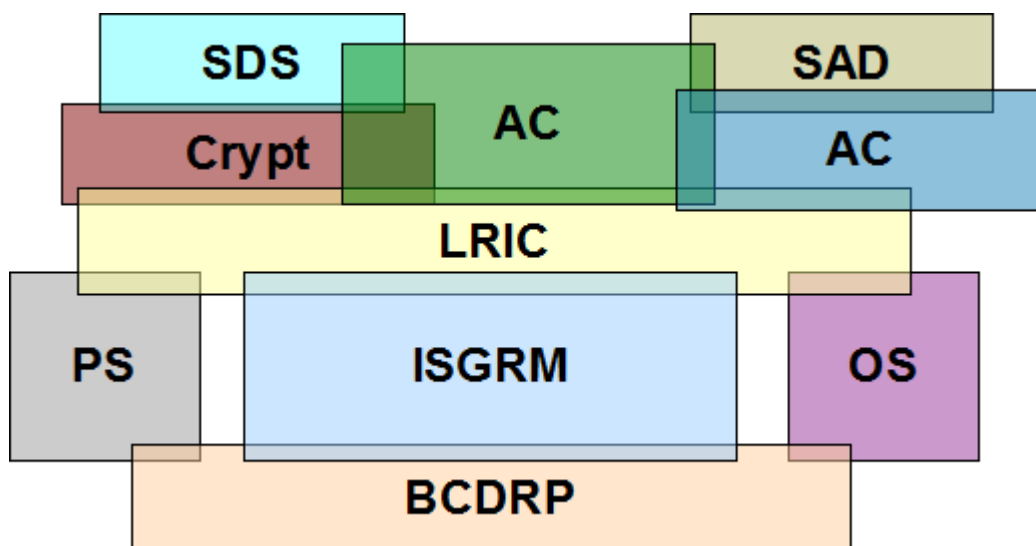
**Software Development Security:** Prassi e Metodi per lo sviluppo protetto di software. Modelli e Meccanismi per aumentare la sicurezza nel software

**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:** determinato 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 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