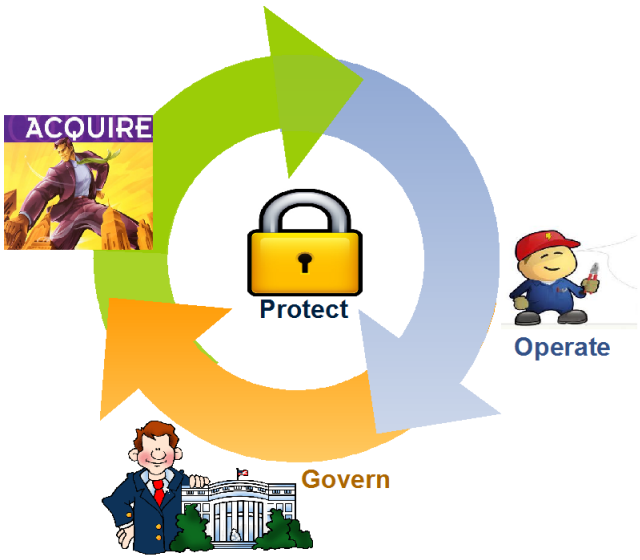
CISA: Certified Information System Auditor

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

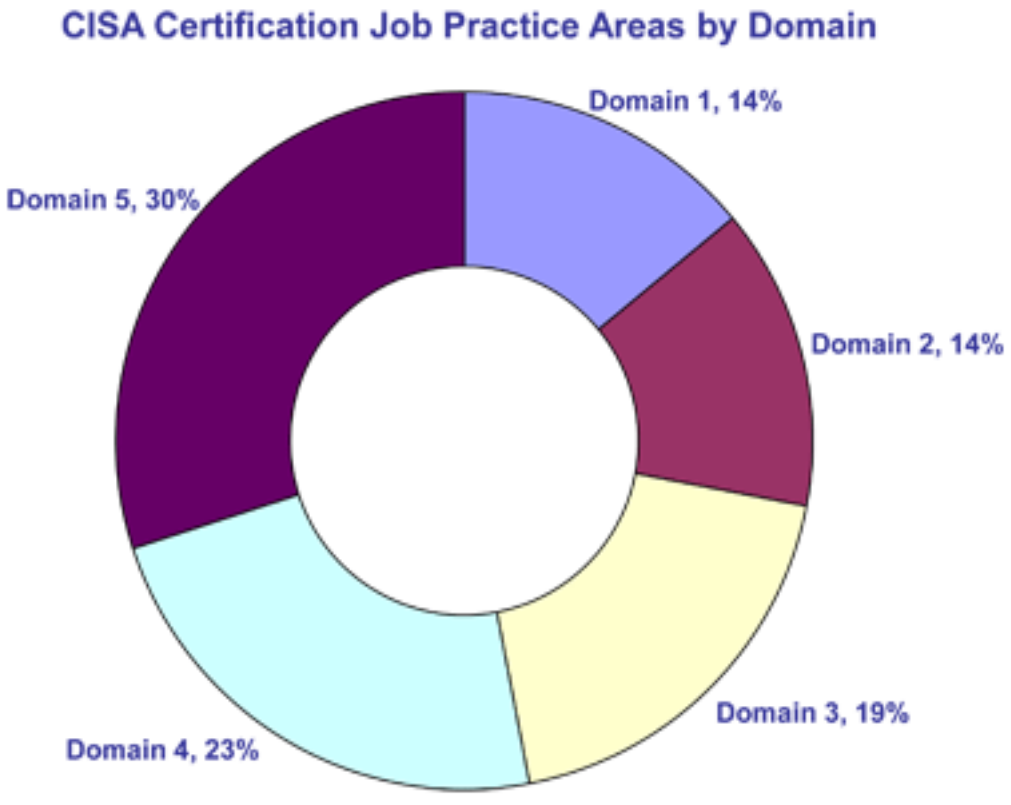
Introduzione

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

Chapter 1

Information System Audit Process

1.1 Audit

1.1.1 Concetti Generali

Audit: processo sistematico, indipendente e documentato per ottenere evidenze e valutarle con obiettività al fine di stabilire in quale misura siano stati soddisfatti determinati criteri

Criteri: insieme di politiche, procedure e requisiti utilizzati come riferimento

Audit Objective: obiettivo che delinea i goals specifici associati ad un particolare audit

Evidence: informazioni sufficienti, affidabili, rilevanti ed utili al fine di raggiungere gli audit objectives riguardanti l'area in esame

Engagement: atto di incarico per la esecuzione dell' audit, da formalizzarsi mediante engagement letter (Audit Charter)

Audit Trails: traccia della evidence che consente di ricostruire la catena degli eventi e delle informazioni fino all'origine

Auditor Responsabilities: un auditor ha la responsabilità di:

- determinare strenght ed effectiveness dei controlli
- assicurarsi che siano gli audit engagement siano:
  - pianificati
  - progettati
  - rivisti

  sulla scorta della valutazione preliminare del livello di rischio rappresentato da determinati atti irregolari o illegali
- riportare gli atti sospetti ai soggetti competenti

Materiality: significatività di un elemento informativo, espressione della importanza relativa

Control Objective: statement dei riusultati desiderati o degli scopi da perseguire nella implementazione delle procedure di controllo

1.1.2 Audit Types

1.1.2.1 Financial Statement Audit

Il Financial Audit è un esame approfondito dei registri e dei report finanziari di una compagnia, allo scopo di verificarne la relevance, accuracy e completeness. La funzione addetta all'espletamento del financial audit è detta "Attest Function". Lo scopo generale è quello di fare in modo che una azienda terza parte (CPA) fornisca una assicurazione scritta garantendo che il financial report sia "fairly

presented in conformity with generally accepted accounting principles" (ad esempio gli International Accounting Standard).
In dipendenza dagli scandali che vi sono stati (Enron, WorldCom, Arthur Andersen, etc) le procedure di assessment degli Internal Control sono aumentate di dimensione ed importanza all'interno del financial audit.
Gli Internal Auditors assistono gli auditor esterni, in modo coordinato.
Un financial Audit è condotto mediante tre step fondamentali:

Interim Review: il primo approccio alla compagnia, generalmente nella prima metà dell'anno fiscale. Lo scopo è:

- comprendere il business dell'azienda, l'ambiente in cui opera, le questioni di maggiore importanza
- prefigurarsi quali siano i rischi maggiori da un punto di vista dell'auditor, ovvero gli errori che possano occorrere
- analizzare le procedure di Internal Control

Hard Close: lavoro che si effettua prima della fine dell'anno fiscale, sui dati non definitivi (generalmente quelli raccolti fino ad un mese prima della fine dell'anno fiscale)

Final: lavoro finale, sui dati definitivi, generalmente compiuto qualche settimana dopo la fine dell'esercizio, beneficiando di tutto quanto elaborato durante la fase di Hard Close

1.1.2.2 Internal Audit Review

1.1.2.3 Control Self-Assessment

Processo formale in cui un team interno dell'azienda, di concerto con il Management, analizza l'efficacia dei controlli, allo scopo di identificare le aree più critiche, in modo da dedicarci maggior effort successivamente.

IS Auditor Role: in questa fase il ruolo dell'eventuale Auditor esterno, chiamato come consulente, è quello di "Facilitator"

1.1.2.4 Information Technology Audit

Raccolta ed analisi delle evidence relative al sistema informativo aziendale, allo scopo di determinare il grado di raggiungimento degli obiettivi imposti dalla strategia aziendale e dagli obblighi normativi, di legge e dei regolamenti di categoria. Verifica di:

- contromisure di sicurezza applicate agli assets
- mantenimento della integrità dei dati

1.2 Information Technology Audit

Review dei controlli della infrastruttura tecnologica di una compagnia, mediante un processo di raccolta ed analisi delle evidences relative all'Information System (inteso come l'insieme dei sistemi, pratiche ed esercizio per il trattamento dei dati) di una organizzazione.
L'obietto è quello di ottenere una reliable assurance di:

- assets safeguarding
- data integrity maintenance
- effectiveness
- efficient operations

1.2.1 IT Audit Types

Computerized System and Applications: verifica della adeguatezza di sistemi e applicazioni ai bisogni aziendali, in termini di:

- efficiency
- adequateness
- validity
- reliability
- timeliness

del processamento delle informazioni

Information Processing Facilities (Data Centers): verifica che le strutture fisiche siano controllate in termini di:

- timeliness
- accurateness
- efficientness

nel processamento delle informazioni

System Development: verifica che i sistemi in sviluppo raggiungano gli obiettivi dell'organizzazione

Management of IT and Enterprise Architecture: verifica che il Management abbia sviluppato una adeguata struttura aziendale e le relative procedure di controllo e misurazione delle performance dell'Information Processing

Network and Telecommunications: verifica che vi siano i necessari controlli sui clients come sui server e le infrastrutture di rete e collegamento

1.2.1.1 Evidence Scoring of Reliability

Le evidence possono essere le più affidabili possibili, si può stabilire una sorta di "scala" delle evidences milgiori:

1. Third Party: per questioni generali, una testimonianza (scritta) di terza parte è sempre più affidabile
2. Observation (and Interview): osservazione diretta dell'IS Auditor, in special modo per quanto riguarda personal e procedural controls ed il rispetto della segregation of duties
3. Automated System: trail derivanti dai sistemi, per le questioni meramente tecnologiche

1.2.2 IS Audit Regulation and Legislation

Varie Regulations sono state prodotte nei recenti anni, da diverse entità, per far fronte ai sempre maggior emergenti problemi relativi alla mancanza di controlli nelle organizzazioni. Fra queste:

HIPAA: Health Insurance Portability and Accountability Act

Gramm Leach Bliley Act:

Sarbanes Oxley Act:

COSO: Committe od Sponsoring Organization and Treadway Commission. Standard per il Financial Auditing consigliato da SEC per soddisfare i requisiti contenuti nella SOX. Definisce il concetto di "Internal Control". Trattato brevemente in un paragrafo successivo

ISACA: Information System Audit and Control Association. In un paragrafo successivo sono trattati:

- ISACA Code of Professional Ethic
- ISACA Standards
- ISACA Standards, Guidelines and Procedures

Statement of Audit Standard 70: "Service Oragnizations". Trattato brevemente in un paragrafo successivo

Statement of Audit Standard 94: "The Effect of Information Technology on the Audotor's Considerations of Internal Controls in a Financial Statement Audit". Trattato brevemente in un paragrafo successivo

CObIT Control Objective for Information and related Technology. Trattato brevemente in un paragrafo successivo

1.2.3 Controls

Dal CoSO proviene la definizione di Internal Control (che corrisponde, in pratica, al concetto di Countermeasure o Safeguard).

1.2.3.1 Types of Controls

Preventive Control: controllo inteso per fermare un errore dall'accadere

Detective Control: controllo inteso per rilevare un errore durante o immediatamente dopo il suo accadimento

Corrective Control: controllo inteso a ripristinare la situazione precedente l'accadimento dell'errore

Deterrent Control: controllo inteso per scoraggiare il compimento di un errore volontario

Mitigation Control: controllo inteso a mitigare il rischio collegato al funzionamento non perfetto di un controllo principale

Compensating Control: controllo utilizzato per mitigare la debolezza di un altro controllo. Esempi tipici sono:

- batch reconciliation
- transaction logs
- reasonableness test
- indipendent review
- audit trails

1.2.3.2 Classification of Controls

General Controls environmental controls

Pervasive Controls particolari controllo di tipo generale, focalizzati su:

- management
- monitoring

Detailed Controls controlli da applicare alle fasi di:

- Acquisition
- Implementation
- Delivery
- Support

Application Controls controlli specifici di una applicazione (Qualità dei Dati)

Integrity Controls: controlli d'integrità dei dati

- Referential Integrity (DB Foreign Key)
- Domain Integrity (Range Check)
- Relational Integrity (field value)

1.2.3.3 Scoring of Control

Nel consigliare i controlli da implementare, generalmente l'Auditor deve seguire questa scala di preferenze (almeno nelle domande d'esame):

1. Procedural/Personal
2. Detective
3. Preventive/Logical

1.2.4 Test Types

Compliance: valutazione iniziale della natura e della qualità dei controlli (controls risk < acceptable limits?)

Substantive: test di sostanza. Determina l'integrità dei processi in essere che forniscono evidenza dei risultati finali. Generalmente riguardano il ricalcolo, la conferma, la verifica dei risultati attraverso diverse (parallele) fonti informative ed osservazioni. Tipicamente eseguito qualora, nei precedenti test di compliance, si sia rilevata una sostanziale debolezza dei controlli in essere

Integrated:

1.2.5 Risk

Essenziale, nel mestiere di Auditor, è la cognizione del rischio. Di ogni entità deve essere valutato il rischio che viene corso.

Risk-Based Approach approccio in base al quale viene determinato il rischio ed ogni scelta viene compiuta nel senso di una riduzione dello stesso

Residual Risk rischio rimanente dopo la introduzione delle contromisure

1.2.5.1 Audit Related Risk Types

Business Risk: minacce che possono inficiare la capacità dell'organizzazione di raggiungere gli obiettivi di business

Inherent Risk rischio intrinseco, derivante dalla introduzione di un elemento o sistema nel IS, supposto che non vi siano internal controls ad esso correlati. Dipendono da Internal Controls di tipo General: Pervasive e Detailed

Control Risk rischio di (mancato) controllo, derivante dalla fallacità di un meccanismo di controllo, appunto, che non impedisce o rileva una debolezza. Il livello di Control Risk è determinato mediante compliance test (quali: user access right, exceptions follow-up, log review, software license audit) sulla struttura di controlli interni della organizzazione

Detection Risk rischio derivante dalla fallacità di un processo di controllo, ovvero che un substantive test non rilevi un errore. Il livello di Detection Risk è determinato dall'Inherent Risk e Control Risk mediante compliance tests

Audit Risk: rischio derivante dal raggiungimento di conclusioni errate a partire dai risultati dell'audit

1.2.5.2 Business Knowledge

Preliminarmente deve essere eseguita una analisi del business che viene svolto dall'azienda. In particolare devono svolte le seguenti attività:

- Business Issues and Risks Understanding
- Gain Confidence from the Management
- Audit Special Attention Item Identification
- Materiality of Risk and Control Weakness Understanding
- Management most Meaningful Risk Focus

1.2.6 Audit Types

Continuos Audit

1.2.7 Audit Software

1.2.7.1 Generalized Audit Software

Le funzionalità tipiche includono:

- mathematical computations
- stratification
- statistical analysis
- sequence checking
- duplicate checking
- recomputations

AFDS: Address Field Duplication Search

1.3 ISACA Ethic, Standard e Methodology

Information System Audit and Control Association.
Dal Documento "*IS Standard, Guidelines and Procedures for Auditing and Professional Standard*", pubblicato il 28 febbraio 2005 e reperibile all'url http://www.isaca.org/standards, si desumono i tre seguenti notevoli:

- Code of Professional Ethics
- IS Control Professional Standard
- IS Auditing Standard, Guidelines and Procedures

trattati nei paragrafi seguenti. Essi rappresentano i criteri secondo i quali devono essere condotti gli audit secondo ISACA. Inoltre costituiscono un valido strumento di ausilio per la progettazione e la conduzione di audit.

Audit Methodology

La metodologia completa (IS Auditing Standard, Guidelines and Procedures) è costituita dai componenti di seguito indicati, elencati in modo top-down (tra parentesi il numero totale):

Standards: Requisiti Obbligatori per Audit e Reporting (S1 - S8)

Guide Lines: Guida alla applicazione degli Auditing Standard (G1 - G31)

Procedures: ulteriori informazioni (esempi) sull'applicazione degli Audit Standard (P1 - P9)

dove ad ogni *Standards* corrispondono una o più *Guidelines*. Viceversa le *Procedures*, essendo di maggior dettaglio e comunque legate a particolari tecnologie, non sono direttamente connesse con le *Guidelines*. A questi debbono essere aggiunti gli *IS Control Professional Standard* (di emissione precedente) che contengono:

- 8 Standard
- 12 Guidelines

Codification

La codifica degli Standards e delle Guidelines è duplice. Infatti oltre alla numerazione S1 - S8, G1 - G31, indicata precedentemente, vi è una numerazione che tiene conto di:

- interconnessione fra *Standards* e *Guidelines* nell"'*IS Auditing Standards*"
- presenza degli *Standards* e *Guidelines* dell"'*IS Control Professional Standards*"

Gli Standards sono numerati nel seguente modo:

IS-Auditing-Standard-number: 0<digit>0

IS-Control-Professional-Standard-number: 5<digit>0

Le Guidelines sono numerate in base allo Standard cui fanno riferimento e con una numerazione a tre cifre simile a quella degli standard:

IS-Auditing-Guideline-number: IS-Auditing-Standard-number.<digit><digit>0

1.3.1 Code of Professional Ethics

1. Support the Implementation of, and encourage compliance with, appropriate standard, procedures and controls for IS
2. Perform duties with objectivity, due diligence and professional care, in accordance with professional standard and best practices
3. Serve in the interest of stakeholder and in a lawful and honest manner, while mainteining high standard of conduct and character, and do not engage in acts discreditable to the profession
4. Maintain the privacy and confidentiality of of information obtained in the course of their duties unless disclosure is required by legal authority.
5. Mantain competency in their respective fields and agree to undertake only those activities which can they resonably expect to complete with professional competence
6. Informa appropriate parties of the result of the work performed, revealing all relevant facts known to them
7. Support the professional education of stakeholderin enhancing their understanding of information system security and control

1.3.2 IS Control Professional Standard

Pubblicati nel maggio del 1999. I primi quattro (510 - 540) forniscono indicazioni di comportamento che devono essere tenuti dall'auditor nello svolgimento di ogni attività professionale. I secondi quattro (550 - 580) forniscono una guida operativa per la coduzione degli audit per la verifica dei controlli in essere:

510 Statement of Scope[1]

510.010 Responsability, Authority and Accountability: la Responsability, Authority e Accoutability della funzione di controllo delle infrastrutture IT deve essere propriamente documentata ed approvata da livello di management appropriato

520 Independence

520.010 Professional Independence: in ogni attività relativa al controllo delle infrastrutture IT, un atteggiamento professionale prevede un atteggiamento ed un'apparenza indipendente

520.020 Organizational Relashionship: la funzione (interna) di controllo delle infrastrutture IS deve essere sufficientemente indipendente dall'area sotto controllo da permettere uno svolgimento obiettivo dei compiti di controllo

530 Professional Ethic and Standards

530.010 Code of Professional Ethic: l'IS Control Professional deve aderire al "Code of Professional Ethic" emesso da ISACA

530.020 Due Professional Care: in ogni aspetto del lavoro l'IS Control Professional deve osservare:

- due professional care
- applicable professional standards

540 Competence

540.010 Skills and Knowledge: l'IS Control Professional deve essere competente tecnicamente, essendo in possesso delle competenze e delle conoscenze necessarie allo svolgimento del suo lavoro

540.020 Continuing Professional Education: l'IS Control Professional deve mantenere nel tempo le sue competenze attraverso i CPE

550 Planning

550.010 Control Planning: l'IS Control Professional deve usare le metodologie di Risk Assessment ed altre tecniche allo scopo di pianificare ed individuare le adeguate priorità nello svolgere le verifiche, in modo da raggiungere gli obiettivi

560 Performance of Work

560.010 Supervision: gli IS Control Professionals devono essere adeguatamente supervisionati e coordinati, allo scopo di assicurare il raggiungimento degli obiettivi e l'applicazione degli standard professionali (chi controlla i controllori)

560.020 Evidence: l'IS Control Professional deve assicurare evidences (prove) sufficienti, credibili, rilevanti e utili delle attività ed i compiti svolti allo scopo di raggiungere gli obiettivi. La valutazione dei controlli deve essere corroborata da appropriate analisi e interpretazioni di dette evidenze

[1] Lo "Stament of Scope" è un concetto successivamente espanso nell'Audit Charter (Engagement Letter)

560.030 Effectiveness: l'IS Control Professional, nello svolgimento del proprio lavoro, deve stabilire appriopriate misure delle effectiveness (efficienza) delle attività tese al raggiungimento degli obiettivi legate al suo ruolo e degli obiettivi definiti nello Statement of Scope

570 Reporting

570.010 Periodic Reporting: l'IS Control Professional deve riportare periodicamente ad un adeguato livello di management relativamente al grado di raggiungimento degli obiettivi raggiunto

580 Follow-up Activities

580.010 Follow-up: l'IS Control Professional deve:

- monitorare il rendimento delle procedure di controllo
- riesaminare i feedback sull'efficienza e la efficacia delle attività di controllo
- assicurarsi che siano predisposte le adeguate azioni correttive, se necessario

1.3.3 IS Audit Standard, Guidelines and Procedures

Corpus documentale più ampio, costituito da direttive emesse in più riprese. Gli Standards, che armonizzano e collegano la struttura, sono stati pubblicati nel gennaio 2005. Le Guidelines e le Procedures sono state realizzate precedentement, in genere.

Nella tabella seguente è presentata la organizzazione degli Standard e delle Guidelines relative ad ognuno di essi. Come già detto nel paragrafo introduttivo, le Procedures di esempio sono indipendenti dai particolari Standards o Guidelines.

No.	Standard	Number	Guideline
010	S1 Audit Charter See Also: 060.180	010.010	G5 Audit Charter
		010.020	G4 Outsourcing of IS Activities to Other Organizations
020	S2 Independence See Also: 060.090, 060.110	020.010	G17 Effect of Noaudit Role on the IS Auditor' Independence
		020.020	G12 Organizational Relationship and Independence
030	S3 Professional Ethic and Standard See Also: 020.020, 060.140, 060.070	030.010	G19 Irregularities and Illegal Acts
		030.020	G7 Due Professional Care
		030.030	G9 Audit Consideration for Irregularities
		030.040	G31 Privacy
040	S4 Competence. See Also:060.110, 060. 140, 060.180	040.010	G30 Competence
050	S5 Planning	050.010	G6 Materiality Concept for Auditing Information Systems
		050.020	G15 Planning
		050.030	G13 Use of Risk Assessment in Audit Planning
		050.040	G16 Effect of Third Parties on an Organization's IT Control
060	S6 Performance of Audit Work See Also: 010.020, 020.010, 030.010, 050.030, 050.040	060.010	G8 Audit Documentation
		060.020	G14 Application System Review
		060.030	G2 Audit Evidence Requirement
		060.040	G10 Audit Sampling
		060.050	G18 IT Governance
		060.060	G11 Effect of Pervasive IS Control
		060.070	G3 Use of Computer Assisted Audit Tecniques
		060.080	G1 Using the Work of Other Auditors
		060.090	G22 B2C E-commerce Review
		060.100	G23 System Development Life Cycle Review
		060.110	G24 Internet Banking
		060.120	G25 Review of VPN
		060.130	G26 Business Process Reenginering Project Review
		060.140	G28 Computer Forensic
		060.150	Business Continuity Planning Review (abrogato)
		060.160	G29 Post Implementation Review
		060.170	G21 Enterprise Resource Planning System Review
		060.180	G27 Mobile Computing
070	S7 Reporting See Also: 030.010, 060.010	070.010	G 20 Reporting
080	Follow-up Activities	-	-

1.3.4 IS Audit Standards

Gli 8 Standards sono stati emessi nel Gennaio del 2005.

S1 Audit Charter (010)

Audit Charter (Engagement Letter): purpose, responsibility, authority e accountability della funzione (interna) di Audit IS o dell'assegnazione (esterna) dell' Audit IS deve essere appropriatamente documentata in un "Audit Charter" o "Engagement Letter"

Agreement and Approvement: l'Audit Charter (Engagement Letter) deve essere concordata ed approvata da un adeguato livello dell'organizzazione

S2 Independence (020)

Professional Independence: in ogni attività relativa al controllo delle infrastrutture IT, l'IS Auditor deve essere indipendente nell'atteggiamento e nella apparenza

Organizational Independence: la funzione (interna) di controllo delle infrastrutture IS deve essere sufficientemente indipendente dall'area sotto controllo da permettere uno svolgimento obiettivo dei compiti di controllo

S3 Professional Ethic and Standard (030)

Code of Professional Ethic: l'IS Auditor deve aderire al "Code of Professional Ethics" allorquando conduce incarichi di audit

Due Professional Care: l'IS Auditor deve esercitare il due professional care, incluso l'osservanza degli applicable professional auditing standards, allorquando condice incariuchi di audit

S4 Competence (040)

Competence: l'IS Auditor deve essere professionalmmente competente, possedendo le necessarie competenze e conoscenze per condurre gli incarichi di audit

CPE: l'IS Auditor deve mantere nel tempo competenze professionali attraverso CPE e training

S5 Planning (050)

Coverage Plan: l'IS Auditor deve pianificare la copertura dell'IS auditing in modo da raggiungere gli obiettivi di audit e soddisfare le leggi cogenti ed iu professional auditing standards

Risk-Based Approach: l'IS Auditor deve sviluppare e documentare un Risk-based Approach

Audit Plan: l'IS Auditor deve sviluppare e documentare un piano di audit che annoveri i dettagli di verifica, la natura e gli obiettivi, le tempistiche ed il grado di approfondimento, gli obiettivi e le risorse necessarie

Audit Programme: l'IS Auditor deve sviluppare un adeguato programma di audit, dettagliando la natura, lee tempistiche, il grado di approfondimento delle procedure di audit richieste per completare la verifica

S6 Performance of Audit Work (060)

Supervision: lo staff di IS Auditors deve essere supervisionato in modo da garantire la ragionevole sicurezza che gli audit objectives siano raggiunti e gli applicable professional auditing standard siano utilizzati

Evidence: l'IS Auditor, durante lo svolgimento dell'audit, deve ottenere "sufficient, reliable and relevant evidences (prove)" allo scopo di raggiungere gli obiettivi. La valutazione dei controlli deve essere "supported by appropriate analysis" e "interpretazioni di dette evidenze

Documentation: l'intero processo di Audit dovrebbe essere documentato, descrivendo il lavoro di audit svolto e le evidences trovate, a supporto delle conclusioni e dei risultati dell'audit

S7 Reporting (070)

Report: l'IS Auditor deve presentare un report, in un formato opportuno, al comletamento dell'audit. Il report deve identificare l'organizzazione, i destinatari ed ogni restreizione nella diffusione

Scope Statement: l'Audit Report deve enunciare la finalità, gli obiettivi, il periodo di copertura, la natura, la durata, il grado di approfondimento del lavoro di Audit svolto

Finding Statement: L'Audit Report deve descrivere i risultati, le conclusioni, le raccomandazioni ed ogni riserva, precisazione, limitazione nella finalità che l'Auditor presenta nei confronti dell'audit stesso

Evidence: l'IS Auditor deve aver raccolto sufficienti Evidences per confortare i risultati contenuti nel report

Report Issuing: il Report dell'IS Auditor deve essere firmato, datato all'atto della emissione e distribuito in accordo con i termini stabiliti nell'Audit Charter (Engagement Letter)

S8 Follow-up Activities (080)

Follow-up: l'IS Auditor deve richiedere e valutare le informazioni rilevanti, dopo la comunicazione di risultati e raccomandazioni, allo scopo di indicare le appriopriate azioni che devono essere intraprese dal management in modo urgente

1.3.5 IS Audit Guidelines

Le 31 Guidelines sono state emesse tra il 1999 ed il 2005.

G1 Using the Works of Other Auditor and Expert (060.080)

Proprio in virtù della indipendenza (S2) di customers e suppliers, spesso l'IS Auditor trova che parte dell'ambiente sotto auditing sia controllato da una fuonzione od organizzazione indipendente.

G2 Audit Evidence Requirement (060.030)

Lo scopo di questa Guideline è la definizione del termine "evidence", come utilizzata nell'esecuzione degli audit allo scopo di mostrare "type and sufficiency os audit evidence"

G3 Use of Computer Assisted Audit Tecniques (060.070)

I CAAT sono molto utilizzati nei seguenti campi:

- test of details of transaction and balance
- analytical review procedures
- compliance test of IS general controls
- compliance test of IS application controls
- pentest

G4 Outsourcing of IS Activities to Other Organizations (010.020)

Una organizzazione (service user) può delegare (comprare) IS da un fornitore esterno (service provider). Le tipiche IS functions che possono essere fornite in outsourcing sono:

- data centre operations
- security
- application system development
- maintenance

G5 Audit Charter (010.010)

Tale Guideline aiuta l'IS Auditor nella stipula di una Audit Charter, in modo da definire:

- Responsability
- Authority
- Accountability

della funzione (interna) di Auditing

G6 Materiality Concepts for Auditing Information (050.010)

Cercando di riportare l'IS Audit ad un Financial Audit, tale Guideline fornisce all'IS Auditor condigli su come devono essere eseguiti materialmente gli assessment, in modo da:

- "focus their effort on high risk areas"
- "assess the severity of any errors or weakness found"

G7 Due Professional Care (030.020)

Tale Guideline chiarisce la locusione "Due Professional Care".

G8 Audit Documentation (060.010)

Tale Guideline fornisce indicazioni circa la documeentazione che deve essere preparata dall'IS Auditor. La documentazione rappresenta una registrazione di tutta l'attività svolta durante l'audit

G9 Audit Consideration for Irregularities (030.030)

Tale Guideline fornisce indicazioni su cosa debba essere considerato una irregolarity e sulle modalità di reporting. Alcune irregolarities possono essere considerate "fraudolent activities", in dipendenza dalla definizione legale di frode adottata dalla giurisdizione.

G10 Audit Sampling (060.040)

Tale Guideline fornisce indicazioni all'IS Auditor su come eseguire controlli a campione (progettando e scegliendo un audit sample). Gli Audit Sample devono soddisfare i requisiti di:

- reliable and relevant evidence
- supported by appropriate analysis

G11 Effect of Pervasive IS Controls (060.060)

Tale Guideline fornisce, analogamente al framework del CObIT, la differenziazione tra:

- gli IS Controls di dettaglio, rilevanti ai fini dell'IS Audit
- le caratterizzazioni dell'IS management and monitoring, che corroborano l'analisi dell'IS Auditor

G12 Organizational Relationship and Independence (020.020)

Tale Guideline espande il concetto di Indipendenza dell'IS Auditor

G13 Use of Risk Assessment in Audit Planning (050.030)

Tale Guideline fornisce suggerimenti circe i requisiti necessari nell'applicare il risk assessment nell'IS Audit, con riferimento a:

- Audit Risk: il rischio di raggiungere conclusioni incorrette
- Error Risk: il rischio che occorrano errori nell'area sotto audit

Entrambi sono valutati soggettivamente dall'IS Auditor

G14 Application System Review (060.020)

Tale Guideline descrive le "recommended practices" nell' effettuare l'Application System Review.

G15 Planning (050.020)

Tale Guideline definisce le componeenti del processo di planning, cercando di soddisfare i requisiti indicati nel CObIT.

G16 Effect of a Third Parties on an Organization' IT Control (050.040)

Tale Guideline fornisce una guida su come deve essere valutato l'effetto dell'usufruire dei servizi di una terza parte negli IS Controls

G17 Effect of Nonaudit Role on the IS Auditor's Independence (020.010)

Tale Guideline fornisce un framework per rendere l'IS Auditor in grado di:

- stabilire quando possa (sembrar) venire meno l'indipendence
- considerare possibili approcci alternativi quando possa (sembrar) venire meno l'indipendence
- determinare i requisiti di disclosure

G18 IT Governance (060.050)

Tale Guideline fornisce informazioni su come affrontare l'Audit dell'IT Governance, in modo da:

- considerare l'appopriata posizione nell'organizzazione dell'IS Auditor
- pianificare l'audit
- eseguire il corretto report e le attività di follow-up

G19 Irregularities and Illegal Acts (030.010)

Tale Guideline fornisce indicazioni all'IS Auditor sulla definizione di irregularity e illegal act (sovrapposizione con G9?).

G20 Reporting (070.010)

Tale Guideline stabilisce come l'IS Auditor deve eseguire il report in ottemperanza alle indicazioni ISACA e CObIT.

G21 Enterprise Resource Planning System Review (060.170)

Tale Guideline fornisce indicazioni circa l'Auditing dei sistemi ERP, durante i quali l'IS Auditor potrebbe esser coinvolto in attività "nonauditing".

G22 Business-to-Consumer E-commerce Review (060.090)

Tale Guideline fornisce indicazioni circa l'Auditing di infrastrutture e applicazioni B2C.

G23 System Development Life Cycle (060.100)

Tale Guideline è stata ideata per fornire indicazioni circa la revisione del SDLC.

G24 Internet Banking (060.0110)

Tale Guideline descrive le recommended practices per l'auditing delle infrastrutture, le applicazioni e le implementazioni di Internet Banking ed analizzarne il rischio.

G25 Review of Virtual Private Network (060.120)

Tale Guideline fornisce indicazioni circa l'ausit delle infrastrutture di VPN.

G26 Business Process Reenginering Project Review (060.130)

Tale Guideline fornisce:

- basic reenginering issues
- framework per l'assessment delle key activities
- framework per il risk assessment

relativi alle attività di Business Process Reenginering

G27 Mobile Computing (060.180)

Tale Giudeline fornisce indicazioni circa la sicurezza dei computer mobili

G28 Computer Forensic (060.140)

Tale Guideline fornisce indicazioni per l'audit del computer forensic

G29 Postimplementation Review (060.160)

Tale Guideline fornisce indicazioni circa le recommended practices per la postimplementation review. Solitamente le organizzazioni implementano soluzioni IT per soddisfare determinati requisiti di business. Solo dopo che le soluzioni sono state implementate se ne verifica l'efficacia e l'efficienza ed eventualmente si intraprendono azioni per il miglioramento delle implementazioni scelte.

G30 Competence (040.010)

Tale Guideline fornisce indicazioni all'IS Auditor in modo tale che acquisisca i necessari skill e conoscenze per rimanere competitivo nell'espletamento delle attività di auditing

G31 Privacy (030.020)

Tale Guideline assiste l'IS Auditor nel rispettare la privacy durante l'effettuazione delle attività di auditing. Può essere usata anche in altre circostanze.

1.3.6 IS Audit Procedures

Le 9 Procedures di esempio sono state emesse fra il 2002 ed il 2005. Riguardano dei casi di esempio notevoli

P1 IS Risk Assessment

Procedura in vigare dal 1 luglio 2002.
Fornisce:

- definizione dell'IS Audit Risk Assessment
- guida per l'utilizzo della metoddologia di IS Audit Risk Assessment da parte della funzione di Internal Audit
- guida alla scelta dei Risk Ranking e all'uso dei pesi

P2 Digital Signature

Procedura in vigore dal 1 lulgio 2002.
Fornisce un valido strumento per la valutazione delle Certification Authority, in termini di qualità del servizio e affidabilità

P3 Intrusion Detection

Procedura in vigore dal 1 agosto 2003.
Fornisce la descrizione dei passi che devono essere seguiti da un IS Auditor nell'esame di un IDS. In particolare sono descritti:

- definizione di IDS e funzionamento
- finalità e benefici derivanti dall'utilizzo dell'IDS
- principali tipi di IDS con vantaggi e svantaggi di ognuno
- guida alle condizioni necessarie per la corretta implementazione ed amministrazione di un iDS
- considerazioni nella pianificazione dell'esame di un IDS
- overview degli approcci di Audit
- probelamatiche inerenti il reporting
- tipi di procedures ed evidences nell'Audit

P4 Viruses and Other Malicious

Procedura in vigore dal 1 agosto 2003.
Fornisce una checklist delle procedure suggerite per prevenire e amministrare le infezioni derivanti da malware.

P5 Control Risk Self-Assessment

Procedura in vigore dal 1 agosto 2003.
Fornisce:

- definizione del Control Risk Self-Assessment (CRSA)
- guida all'uso delle metodologie di CRSA
- guida alla implementazione di un CRSA

P6 Firewalls

Procedura in vigore dal 1 agosto 2003.
Fornisce alcuni aspetti di guida per gli IS Auditor che sono coinvolti nella verifica i processi di interconnesione esterni ed interni delle varie entità (Internet, connessioni dirette, infrastrutture in affitto) e quindi anche la valutazione della robustezza delle barriere di protezione per fornire una ragionevole sicurezza dell'AIC triad

P7 Irregularities and Illegal Acts

Procedura in vigore dal 1 novembre 2003.
Fornisce una guida per determinare la natura, il grado di approfondimento e la tempistica delle procedure da intraprendere durante l'audit, in base ai risultati del risk assessment, volto alla riduzione del rischio di Irregularities and Illegal Acts

P8 Security Assessment-Penetration Testing and Vulnerability Analysis

Procedura in vigore dal 1 settembre 2004.
Fornisce una guida per gli IS Auditor che sono coinvolti in attività di verifica dei controlli perimetrali (e.g. Firewall) e Interni (e.g. Sistemi Operativi) in modo da garantire la ragionevole sicurezza che che tutte le minacce interne ed esterne compresa la compromissione dei sistemi, siano minimizzate mediantee identificazione e correzione delle vulnerabilità riscontrate in fase di PenTest e VA

P9 Evaluation of Management Controls over Encryption Methodologies

Procedura in vigore dal 1 gennaio 2005.
Fornisce un criterio di valutazione dei requisiti per le organizzazioni e le agenzie che non devono garantire un livello di classifica Top-Secret (SS). Non sono trattate le specifiche relative alla gestione delle chiavi mediante hardware (e.g. FIPS 140-2)

1.4 Audit Process

Il Processo di Audit costituisce un vero e proprio progetto, ed in quanto tale si compone di varie fasi, anche se definite in maniera leggermente differente rispetto a quanto avviene nel PMP, proprio per consentire di cogliere le peculiarità della attività di audit. In particolare la prima fase (Initiation) è qui esplicitamente suddivisa in più attività, per le altre fasi vi è un mapping quasi uno a uno rispetto alla definizione di progetto in PMP, come illustra la seguente Tabella:

PMP	IS Audit Process
Initiation	Establish the Terms of Engagement
	Preliminary Review
	Establish Materiality and Assess Risks
Planning	Planning
Execution	Evaluation of Internal Controls
Control	Audit Procedures
Closing	Completing the Audit (Report)

1.4.1 Establish the Terms of Engagement

Fase preliminare in cui vengono stabiliti la finalità e gli obiettivi del lavoro dell'auditor presso la organizzazione. Concordemente con 010.010, viene stipulato un Audit Charter allo scopo di definire:

Responsibility: scope, independences, deliverables

Authority: right of access to informations

Accoutnability: auditee' rights, agreed completion date

1.4.2 Preliminary Review

Fase in cui l'Auditor recepisce informazioni relative alla organizzazione. Vengono identificate la strategia e le responsabilità dell'amministrazione e del controllo delle strutture informatiche. L'Auditor può fornire un quadro di insieme del Business Environment, allo scopo di identificare le applicazioni maggiormente critiche nei confronti del business.

1.4.3 Establish Materiality and Assess Risks

Fase in cui l'Auditor di forma un giudizio preliminare riguardo:

Materiality: componenti essenziali

Business Risk: eventuali minacce che possono inficiare la capacità, da parte dell'organizzazione, di raggiungere gli obiettivi del business

Organization's Response to Risk: capacità dell'organizzazione di rispondere ai rischi

1.4.3.1 Materiality

Nella valutazione delle Materiality, l'auditor deve prendere in considerazione:

- il livello di errore accettato dal amangement
- l'effetto cumulativo di piccoli errori

Tipicamente sono valutati fattori "non finanziari" quali:

- Physical Access Control
- Logical Access Control
- System for Personnel Management
- Manufactoring Control
- Design
- Quality Control
- Password Generation

1.4.3.2 Risk Assessment

Il Risk è ogni evento o azione che non permette alla organizzazione di raggiungere i goals e gli objectives.
Devono essere valutati:

- Inherent Risk
- Control Risk
- Detection Risk

Sulla base del livello di rischio che si decide di accettare, sono decise la categorie di Evidences che saranno raccolte (cfr. paragrafo a seguire relativo alle "Audit Procedures").
Devono essere presentati documenti che attestino:

- tipo di Risk Analysis impiegato
- identificazione dei rischi significativi
- i rischi che l'audit studierà
- i tipi di evidenza che saranno usati a conforto della valustazione del rischio da parte dell'Auditor

1.4.4 Planning

Fase in cui l'Auditor pianifica lo svolgimento dell'audit. Da un punto di vista progettuale, viene stabilito il secondo dei tre parametri:

tempo: stabilito nella fase di Engagement, mediante l'Audit Charter

qualità: da stabilirsi mediante la misura dell'Audit Risk (funzione di Inherent Risk, Control Risk, Detection Risk). Tali fattori di rischio sono determinati durante la fase di Risk Assessment

costo: in dipendenza dai precedenti due

- Careful and Methodical Planning
- Determining the Scope and the Objectives of the Process
- Validate:
  - Plan
  - Scope
  - Objective

  with the StakeHolder
- Identify the Required Resources

1.4.5 Evaluation of Internal Controls

Fase in cui l'Auditor esamina gli Internal Controls, mediante la comprensione dei 5 componenti dei controlli:

Control Environment: fondamento degli altri cinque elementi (e.g. Management Philosophy, Operating Style)

Risk Assessment: Identificazione ed Analisi dei Rischi

Control Activities: policy, procedure redatte allo scopo di assicurare che il personale svolga le direttive del management

Information and Communications: assicura che l'organizzazione sia a conoscenza delle informazioni rilevanti e le comunichi in modo adeguato

Monitoring: disamina degli output degli Internal Controls

- Carrying out the Planned Tasks
- Document the Steps and Results along the way

1.4.6 Audit Procedures

Fase in cui l'Auditor raccoglie le Evidences.

1.4.6.1 Evidences

In base alla natura, alle modalità ed ai tempi necessari alla raccolta, le evidences sono classificate nelle seguenti categorie:

Observed Processes: osservazione diretta

Documentary Audit Evidences: log, records delle transazioni

Representations: documenti aziendali, quali: policy, procedures

Analysis: comparazione degli errori tra log, applicazioni ed utenti

I metodi di raccolta delle Evidences possono essere i seguenti:

Inquiry/Observation: osservazione diretta, interviste

Inspection: ispezione

Confirmation: ?

Reperformance: ?

Monitoring:

1.4.6.2 Computer Assisted Audit Techniques

I CAAT sono gli strumenti software di ausilio alla raccolta e l'analsi delle evidences.

Generalized Audit Software: software generico di analisi file e DB

Custom Audit Software: software di analisi file etc. appositamente sviluppati per il cliente

Test Data: dati di test, da inserire per provare i controlli di tipo application

Parallel Simulation: software che simulano l'attività umana (e.g. Compuware Quality Assurance) utilizzati prevamentemente per analisi di performance

Integrated Test Facility: analisi delle applicazioni mediante utilizzo diretto

1.4.6.3 Audit Sampling

L'Audit Sampling è l'applicazione dell'audit ad una popolazione inferiore al 100%, allo scopo di ridurre il numero di evidence da raccolgiere ed analizzare (ridurre i tempi di lavoro). I metodi di campionamento possono essere di tipo Statistico (Random, Systematic) o non-Statistico (Haphazard, Judgemental).

Sampling Risk: il rischio che le conclusioni cui l'Auditor giunge effettuando il sampling siano diverse rispetto a quelle cui sarebbe giunto se avesse analizzato tutta la popolazione

Attribute Sampling:

Variable Sampling:

- Validate or Test the Result of the Tasks

1.4.7 Completing the Audit

Report the Final Result (to StakeHolder or Management) for final Approval. Prima di scegliere il miglior tipo di report, l'Auditor deve verificare:

Subsequent Event

Final Evidential Evalutation Processes

Communication with Audit Committe and Management

Subsequent Discovery of Existing Fact at the Day of Audit Report

1.4.7.1 Reporting

In base allo standard ISACA 070, l'Auditor deve fornire un report in formato opportuno al termine dell'audit, in cui siano evidenziati:

- finalità
- objectives
- periodo di copertura
- natura
- tempistiche
- estensione

del lavoro svolto. I report possono essere di cinque tipi fondamentali:

Unqualified Audit Report: report nel quale l'Auditor afferma di aver potuto reperire sufficienti evidences, di aver agito in accordo con i GAAS, e di non aver avuto limitazioni sulle finalità del lavoro svolto

Unqualified Audit Report with Explanation: report nel quale l'Auditor afferma di aver riscontrato delle mancanze notevoli, per la quali occorre fare degli approfondimenti

Qualified Report: report nel quale l'Auditor afferma di non aver potuto formarsi una opinione piena in quanto vi sono state limitazioni sulle finalità dell'audit ovvero l'organizzazione si è discostata dalle GAAP

Qualified Report with Disclaimer: report nel quale l'Auditor afferma non essersi potuto formare una opinione siffuciente per via di evidences insufficienti o mancanza di indipendenza

Qualified Report with Adverse Opinion: report nel quale l'Auditor afferma che l'organizzazione non è conforme ai GAAP, ovvero non possiede dei report finanziari "puliti"

Altri documenti rilevanti sono:

- Auditor Notes
- Flowcharts
- Corrispondence
- Results of Observation
- Plans and Results
- Audit Plan
- Minutes of Meetings
- Computerized Records
- Data Files
- Application Results

1.4.7.2 Follow-up Activities

L'Auditor deve ottenere informazioni relativamente alla effettuazione delle necessarie azioni correttive a contrasto delle mancanze riscontrate durante l'audit.

1.4.7.3 Assessing the Audit

La documentazione relativa all'Audit può essere valutata da un senior manager od un partner, in base ai seguenti principi:

Completeness: l'audit deve aver coperto ogni elemento dell'audit subject

Pertinence: l'audit deve aver coperto solo elementi dell'audit subject

Accuracy: ogni elemento dell'audit deve essere preciso ed esente da errori

Appropriate Conclusions, Findings and Recommendations: l'audit deve presentare appropriate conclusioni e portare a soluzioni concrete, realizzabili in termini di tempo e costi

Follow-up to Findings and Recommendations: ci si deve essee assicurati della corretta comprensione delle raccomandazioni e dei risultati, nonchè delle possibili soluzioni da parte di chi di dovere

Audit Standard and Regulations

1.5 Statement of Audit Standard

1.5.1 SAS 70

"Service Oragnizations".

1.5.2 SAS 94

"The Effect of Information Technology on the Audotor's Considerations of Internal Controls in a Financial Statement Audit".

1.6 CObIT

Control Objective for Information and related Technology. Framework per la gestione del rischio informatico, ideata da:

- Information System Auditor and Control Association (ISACA)
- Information Technology Governance Institute (ITGI)

CObIT Mission: "research, develop, publicize and promote an auhoritative, up-to-date, international set of generally acceepted information technology control objectves for day-to-day use by business managers and auditors". Aiuta Managers, Auditors e Users nel comprendere il sistema IT in uso ed il conseguente livello di sicurezza e controllo necessario alla sua protezione

Fornisce un insieme di Control Objective per massimizzare i benefici e ridurre i rischi dovuti all'utilizzo della Information Technology, per:

- Managers
- Auditors
- IT Users

Il progetto fu intrapreso nel 1992 (lo stesso anno della pubblicazione del report "Internal Controls - Integrated Framework").

1996: First Edition

1998: Second Edition

2000: Third Edition

1.6.1 Executive Summary

Executive Overview (pensata per il senior management) che fornisce una descrizione generale dei concetti e dei principi fondamentali del CObIT:

- sinossi del Framework
- i 4 Domains:
  - Planning and Organization
  - Acquisition and Implementation
  - Delivery and Support
  - Monitoring
- i 34 IT Processes (ad ognuno dei quali corrisponde un High Level Control Objective)

Il CObIT aiuta il management a prendere le decisioni relative alla infrastruttura IT, mediante:

- defining IT Strategic Plan
- Defining the Information Architecture
- Acquiring the Necessary Hardware and Software
- Ensuring Continous Services
- Monitoring the Performance of IT Systems

1.6.2 Framework

Spiega in che modo i processi dell'IT debbano fornire i servizi di informazione necessari agli obiettivi di business. definendo:

34 "High Level Control Objective": obiettivi di alto livello, uno per ogni macro-processo IT descritto nell'overview, divisi per domains

Planning and Organization: riguarda l'uso delle risorse IT e la sua infrastruttura, allo scopo di raggiungere i migliori risultati

PO1: Defining a Strategic IT Plan
PO2: Defining the Infoormation Architecture
PO3: Determine Technological Durection
PO4: Define the IT Organization and Relationship
PO5: Manage the IT Investment
PO6: Communicate Management Aims and Direction
PO7: Manage Human Resource
PO8: Ensure Compliance with External Requirements
PO9: Assess Risks
PO10: Manage Projects
PO11: Manage Quality

Acquisition and Implementation: riguarda la strategia aziendale nell'identificare i requisiti IT, acquisire le tecnologie ed implementarle

AI1: Identify Automated Solutions
AI2: Acquire and Maintain Application Software
AI3: Acquire and Maintain Technology Infrastructure
AI4: Develop and Maintain Procedures
AI5: Install and Accredit Systems
AI6: Manage Changes

Delivery and Support: riguarda il delivery delle soluzioni IT, l'esecuzione efficace ed efficiente delle applicazioni

DS1: Define and Manage Service Levels (SLA, SLM)
DS2: Manage Third Party Services
DS3: Manage Performance and Capacity
DS4: Ensure Continous Services
DS5: Ensure System Security
DS6: Indentify and Allocate Costs
DS7: Educate and Train Users
DS8: Assist and Advise Customers
DS9: Manage the Configuration
DS10: Manage Problems and Incident
DS11: Manage Data
DS12: Manage Facilities
DS13: Manage Operations

Monitoring: riguarda la strategia aziendale di continua verifica del ragguingimento degli obiettivi per i quali sono stati progettati ed implementati i controlli

M1: Monitor the Processes
M2: Assess Internal Control Adequacy
M3: Obtain Independent Assurance
M4: Provide for Independet Audit

7 Information Criterions: criteri secondo i quali sono valutati gli obiettivi (= i criteri del CoSO + AIC Triad):

Effectiveness:

Efficiency:

Confidentiality:

Integrity:

Availability:

Compliance:

Reliability:

5 IT Resources: risorse coinvolte in ogni obiettivo

- people
- application
- technology
- facilities
- data

1.6.3 Control Objectives

Approfondimento utile a delineare le necessarie policy e pratiche per il mondo IT. Definisce 318 control objectives di dettaglio, da inquadrarsi all'interno dei 34 High Level Control Objectives.

1.6.4 Audit Guidelines

Definisce le azioni che devono essere intraprese da un Auditor (nell'ottica Analize, Assess, Interpret, React, Implement), suddivise per ciascun High Level Control Objective, durante la valutazione del rischio derivante dalla mancanza di implentazione dei Control Objectives. Fornisce una guida su come:

- valutare i controlli
- verificare la compliance
- sostanziare il rischio derivante da controlli non implementati

1.6.5 Implementation ToolSet

Insieme di Tool con l'intento di agevolare la comprensione e l'utilizzo del framework:

- Management Awareness
- IT Control Diagnostic
- Implementation Guide
- FAQs
- Case Studies
- Presentation

1.6.6 Management Guidelines

Aiuta il Manager nella gestione dell'incontro tra Business Processes e Information Systems (Performance Measurement, IT Control Profiling, Awareness, Bencchmarking), mediante la definizione di:

Maturity Model: determina lo stato attuale e sperato del livello dei controlli e confrontarlo con il livello medio delle altre aziende dello stesso settore

Critical Success Factor: identifica le azioni più importanti per raggiungere gli obiettivi che rigaurdano il mondo IT

Key Goal Indicator: definisce i livelli di target delle performance

Key Performance Indicator: misura il grado di ragguingimento degli obiettivi di ogni controllo

1.7 CoSO

Committe of Sponsoring Organization and Treadway Commission, iniziativa privata degli USA, intrapresa nel 1985, allo scopo di:

- identificare i fattori che causano report finanziari fraudolenti
- stilare le raccomandazioni per ridurre l'incidenza dei report finanziari fraudolenti

L'importanza del CoSO sta nell'aver stabilito definzioni comuni per quanto riguarda:

- Internal Controls
- Standards
- Criteria

Nell'ottobre del 1985 fu fondata la Treadway Commission (National Commission on Fraudolent Financial Reporting), la quale consigliò che tutti i componenti lavorassero insieme per stendere una guida integrata agli Internal Controls. Successivamente, nel 1987, fu fondato il Committe of Sposoring Organization, il quale ingaggiò la Coopers & Librand (ancora non fusa con la PriceWotherhouse) per condurre un studio su un framework relativo agli Internal Controls e redarre il report "Internal Controls - Integrated Framework", rilasciato nel 1992, che costituisce lo standard che le compagnie degli USA utilizzano per valutare la propria compliance con l'FCPA (Foreign Corrupt Practices Act) e la SOX (Sarbanes Oxley).

1.7.1 Internal Controls

Process: gli Internal Controls sono dei processi ed in questo senso si inquadrano come mezzi

People: gli Internal Controls sono effettuati dalle persone, nei rispettivi livelli e ruoli aziendali

Reasonable Assurance: gli Internal Controls possono fornire solo una ragionevole sicurezza, non certo la sicurezza totale

Objectives: gli Internal Controls sono impiegati per il raggungimento di obiettivi, nelle seguenti categorie (non ortogonali):

- Effectivenes and Efficency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

1.7.2 Framework

Il framework proposto consta di 5 componenti interrelate, che costituiscono la metodologia di analisi degli internal controls

Control Environment: la comprensione dell'ambiente è essenziale per comprendere il "tone" dell'organizzazione, influenzando la coscienza che il personale ha degli Internal Controls. I Control Environment più importanti sono:

- Integrity
- Ethical Values
- Management's Operations Style
- Delegation of Authority
- Process of Management and Development of people

Risk Assessment: identificazione ed analisi dei rischi esterni ed interni, che interferiscono con il raggiungimento degli obiettivi

Control Activities: policy e procedure che assicurano l'adempimento delle direttive impartite dall'amministrazione:

- approvals
- authorization
- verification
- reconciliation
- reviews of operating performance
- security of assets
- segregation of duties

Information and Communications: i sistemi informativi giocano un ruolo molto importante in quanto sono di ausilio alla produzione dei report finanziari e di compliance ⇒Effective Communications

Monitoring: gli Internal Controls devono essere monitorati di continuo. Questo compito viene assolto mediante:

- ongoing monitoring activities
- separate evaluations

eventuali deficienze negli Internal Controls devono esser riportate e devono essere intraprese opportune azioni correttive

Chapter 2

IT Governance & Management

2.1 Business Process Re-enginering

La valutazione della efficacia ed efficienza della struttura IT rispetto agli obiettivi di business dell'organizzazionen coinvolge la struttura dell'IT Governance e l'allineamento rispetto rispetto agli obiettivi di business. Data la notevole concorrenza, occorre rivedere costantemente i processi legati al Business, allo scopo di renderli più efficienti. Questo generalmente porta ad un aumento dell'utilizzo delle infrastrutture informatiche e delle applicazioni.

IS Auditor task: identificare e quantificare l'impatto della eventuale eliminazione di controlli, nella reingegnerizzazione dei processi

2.1.1 Benchmarking

Benchmarking: processo continuo e sistematico di valutazione dei processi , prodotti e servizi forniti dalla organizzazione

2.1.1.1 ISACA Benchmarking Steps

ISACA ha identificato i seguenti steps nella esecuzione del Benchmark:

Plan: indiviaduare i processi più ciritici, da un punto di vista del benchmark, il modo in cui possono essere misurati, i tipi di dati necessari, i dati che devono essere raccolti

Research: identificazione del "Benchmarking Partner"

Observe: raccolta dei dati e condivisione con il partner

Analyze: riassunto ed analisi dei dati raccolti. Analisi del Gap tra l'attuale processo e quello proposto dal partner

Adapt: traduzione dei risultati in principi, strategie e piani di azione

Improve: milgioramento continuo, in ottemperanza agli obiettivi dell'organizzazione

2.1.2 BPR Steps

La reingengnerizzazione dei processi si compone delle seguenti fasi:

- Define the area to be reviewed
- Develop a Project Plan
- Gain an understanding of the business process re-engineering
- Redesign the Streamline of the Process
- Implement and Monitor the new Process
- Establish a Continous Improvement of the Process

2.1.3 Business Performance Indicator

Indicatori tramite i quali si decide se procedere o meno alla reingegnerizzazione del processo.

2.1.3.1 Key Performance Indicator

Rapporto del tipo $\frac{Servizio\,Fornito}{Risorse\,Impiegate}$. Per essere di facile utilizzo non devono superare le 3-5 unità.

2.1.3.2 Balanced Scorecard

Strumento per il management, che mette a confronto:

- Mission
- Strategy
- Measures

2.1.4 Evaluation of Controls

All'atto dell'avvenuta reingegnerizzazione, l'IS Auditor deve analizzare quali controlli siano stati implementati nelle nuove strutture informatiche, quali siano stati eliminati, quali modificati, quali siano rimasti invariati. Si tratta, perlopiù, di Application Controls.

2.1.4.1 Input/Output Controls

Controlli relativi alla fase di inserimento dei dati, ovvero, qualora la comunicazione tra un sistema e l'altro sia automatica, anche alla fase di output della applicazione che fornisce i dati.

Input Authorization: vi deve essere una autenticazione da parte di chi immette i dati. Un esempio notevole è

Second-Level Password: automated process che facilita l'approvazione di eccezioni nelle transazioni (e.g. autorizzazione ad un bonifico elevato)

Batch Controls: processo automatizzato mediante "programma" apposito per il controllo, da effettuarsi in un momento determinato. Vi sono due tipi fondamentali:

Hash Sequence: controllo della sequenza, numerazione consecutiva dei record in un lotto

Hash Total: scelta di campi specifici, in una serie di transazioni, allo scopo di rilevare perdite, perdita d'integrità o duplicazione dei dati

2.1.4.2 Processing Controls

Controlli relativi al processo di elaborazione, tesi ad assicurare che i dati siano accurati e completi. Si tratta perlopiù di controlli tesi a verificare l'integrità dei dati a monte (a volte anche a valle) della elaborazione. Alcuni controlli, come il Data Edit, dal momento che vengono eseguiti prima della elaborazione vera e propria, sono classificati come "preventative integrity controls".
I controlli possono essere automatici (Processing Controls) o eseguiti "a mano" (Edit Checks), quali:

Manual Recalculation: ricalcolo a mano di alcune transazioni scelte a caso

Run-to-Run Totals: quadratura di elaborazione. Verifica dei risultati ottenuti alla fine di ogni fase elaborativa

Base-Case: corpo di dati standard creato a scopo di test, generalmente definito dagli stessi utenti, per controllare che il modo di operare del sistema si mantenga corretto

Data-Validation Edit Alcuni controlli, come il Data Edit, dal momento che vengono eseguiti prima della elaborazione vera e propria, sono classificati come "preventative integrity controls".

Validation Edit	Description	Objective
Sequence Check	controllo che non vi siano "buchi"	Completeness
Limit Check	valore dei dati < max	
Range Check	min < data < max	
Validity Check	validità secondo criteri predeterminati	
Reasonableness Check	dati "ragionevoli"	Accuracy
Table look-ups	confronto con tabella di valori possibili	
Existence Check	esistenza dei dati	
Key Verification	reimmissione di parte dei dati da un altro impiegato	
Check Digit	somma dei dati inserita alla fine (trasposition, transcription error)	Accuracy
Parity Check		Completeness
Completeness Check	no null o blank in un determinato campo o non siano persi dei campi	Completeness
Duplicate Check	no data duplication	
Logical Relationship Check	valore dei dati in funzione di determinate condizioni	

2.1.4.3 Output Controls

Assicura che le informazioni appena elaborate siano comunicate in modo consistente e sicuro. ISACA indica i seguenti:

Logging: tracciamento delle transazioni relative a negoziazioni, dati sensibili, critici

Report Distribution: distribuzione autorizzata dei report

Balancing and Reconciling: tutti gli output relativi a transazioni devono essere loggati e poi confrontati nei totali

Output Error Handling: devono esistere delle procedure per la gestione degli errori

Output Error Retention: devono essere sviluppate delle apposite procedure per la retention delle informazioni, in accordo con la normativa vigente

2.1.4.4 Integrity Controls

Assicurano la completezza, accuratezza, consistenza e corretta autorizzazione ai dati, memorizzati in File System o DB (⇒controllo del corretto funzionamento del FS o del DB).

Referential Integrity Test: test della correttezza dei riferimenti contenuti nei dati immagazzinati

Relational Integrity Test: test della presenza di routine di validazione dei dati prima dell'inserimento nella base dati

2.1.4.5 On-Line Auditing

Audit continuo, volto alla riduzione dei documenti (Paperless Audit). L'Auditor verifica continuamente i controlli operanti senza interferire nella normale operatività aziendale, aumentando il livello di sicurezza. Vi sono 5 tecniche fondamentali:

SCARF/EAM: System Control Audit File and Embedded Audit Module, inserimento di soecifico software all'interno dei sistemi applicativi dell'azienda. Non comporta l'interruzione dei sistemi

Snapshot: rilavazione della fotografia del percorso della elaborazione delle transazioni (mediante opportuni marcatori). Rilascia un Audit Trail

Audit Hooks: collegamenti inseriti nei sistemi di elaborazione che attivano degli allarmi. Utile nel caso in cui solo alcuni processi debbano essere monitorati

Integrated Test Facilities: le transazioni di test sono calcolate insieme a quelle di esercizio. L'Auditor compara i risultati con i dati calcolati indipendentemente. Utile nel caso in cui non sia vantaggioso usare dati di test (data cleansing difficile)

Continuous and Intermittent Simulations: i sistemi simulano l'elaborazione delle transazioni, qualora esse corrispondano a determinati criteri predefiniti

2.1.4.6 Electronic Data Interchange

Lo scopo dell'EDI è quello di promuovere un più efficace ed efficiente metodo di interscambio dati, riducendo loscambio di carta, gli errori ed i ritardi. Un EDI si compone di:

Communication Handler: strato sottostante che fornisce le funzionalità per la comunicazione di documenti (Network/Transport)

EDI Interface: strato di comuicazione fra il "Communication Handler" e l"'Application System" (Session). Si occupa anche di inviare il "Functional Acknowlodgement", per implementare un Data Mapping più efficiente (costituisce un Audit Trail)

EDI Translator: strato di traduzione tra i vari formati dei documenti (Presentation)

Application Interface: strato di comunicazione verso la applicazione e di Data Mapping

Application System: strato di processamento dei dati

Functional Acknowledgement: acknowledgemetn della ricezione dei documenti

EDI Auditing Qualora si usino gli EDI verso enti esterni nalla propria organizzazione, vi deve essere un "Trading Partner Agreement", che definisce le responsabilità di entrambe le organizzazioni nell'utilizzo del sistema di transazioni. Devono altresì essere controllati:

Encryption: per le transazioni Inbound che utilizzino Internet

Transaction Logs: le transazioni evono essere tutte loggate allo scopo di poter determianrre eventuali errori

Message Count: devono essere logati e controllati periodicamente i dati relativi al conteggio delle informazioni scanbiate (send/receive)

Comparing: le transazioni Outbound, rispetto al master file

Segregation: dell'authority per autorizzare, iniziare e trasmettere le transazioni

FIPS In base alla FIPS 161-2 (29 aprile 1996) vi sono tre standard riconosciuti per l'EDI:

X12 Standard emesso dall' Accredited Standard Comittee (ASC) ed accreditato dall'ANSI. Può essere utilizzato per le applicazioni di tipo *domestic*.

UN/EDIFACT Standard emesso dalle United Nation (UN), Economic Commision for Europe. Può essere usato per le applicazioni di tipo *domestic* o *international*.

HL7 Standard emesso da Health Level Seven, uno sviluppatore di standard accreditato ANSI. E' stato ideato come alternativa per le applicazioni sanitarie di un certo tipo, specificatamente per la trasmissione di:

- cartelle pazienti
- dati clinici
- dati epidemiologici
- dati di regolamentazione

2.1.5 Business Process Change

L'IS Auditor deve esaminare anche il progetto di reingegnerizzazione, per assicurare che gli obiettivi siano conformi con gli obiettivi aziendali.

2.1.5.1 Change-Management Team

Deve essere insediato un "Change-Management Team", allo scopo di valutare eventuali problematiche che dovessero emergere durante il roll-out verso il nuovo processo.

2.1.5.2 Risk Indicators

Vi possono essere dei rischi che potrebbero portare alla mancata implementazione del nuovo processo, tra cui:

- Insufficient Domain Expertise
- Unqualified to Handle Project Size/Complexity
- Dissatisfation
- High Staff Turn-over

2.2 Risk Management

Risk: possibilità che possa occorrere qualche cosa di avverso al raggiungimento degli obiettivi di business

Risk Mangement: processo che rende possibile, agli IT Managers, il bilanciamento tra i costi (operativi ed economici) e le misure di sicurezza proattive, per la difesa dei sistemi, acquisendo vantaggio nel raggiungimento degli obiettivi di protezione dei sistemi IT e dei dati di supporto al business. Il processo si compone delle fasi:

Risk Assessment: valutazione del livello di rischio

Mitigation: azioni necessarie alla riduzione del livello di rischio ad un valore accettabile

Maintenance: mantenimento del livello di rischio raggiunto

2.2.1 Risk Management Phases

2.2.1.1 Program Development

L'organizzazione deve sviluppare un Risk Management Program allo scopo di fissare gli obiettivi e le modalità della riduzione dei rischi che si intende operare. Devono essere indicati chiaramente, secondo ISACA:

Purpose: lo scopo che si prefigge il programma al fine di meglio usufruire e valutare i risultati conseguiti

Responsibility: deve essere chiaramente individuato una singola persona od un team responsabile per la esecuzione del programma, in modo tale che questo sia eseguito effettivamente

2.2.1.2 Assets Identification

Inventory degli assets che compongono l'area su cui si intende analizzare/ridurre il livello di rischio. Degli asset fanno parte:

- Systems
- Applications
- Data

2.2.1.3 Threath and Vulnerability [Analysis]

Analisi delle vulnerabilità e delle possibili minacce correlate agli asset ideintificati nella fase precedente. La minacce (e.g. facility in zona sismica), instanziate per mezzo di agenti di minaccia (e.g. terremoto), possono causare danni agendo (exploit) su determinate vulnerabilità (e.g. facility costruita senza i criteri anti-sismici e magari ideata per altri scopi).

2.2.1.4 Business Impact Analysis

Analisi dei possibili danni causati al business, delle diverse minacce (threaths) in azione (exploiting) sulle vulnerabilità (vulnerabilities). Gli impatti possono essere di due tipi diversi:

Quantitative Impacts: impatti direttamente quantificabili in termini di perdite economiche o mancato fatturato (e.g.)

Qualitative Impacts: impatti non direttamente quantificabili intermini di perdite economiche o mancato fatturato (e.g. danni di immagine)

ad essi corrispondono due diverse metodologie di analisi dei rischi:

Quantitative Risk Analysis: associa ad ogni minaccia (o combianzione di minacce) il valore della effettiva perdita in denaro

Qualitative Risk Analysis: utilizza metodi di classifica (Ranking Method) per valutare la minaccia, in funzione dell'importanza degli assets su cui potrebbe agire

Ovviamente non è possibile usare dei metodi quantitativi giudicando impatti qualitativi

2.2.1.5 Risk Level Evaluation

Valutazione del livello di rischio cui si l'organizzazione è esposta.

Residual Risk: rischio rimanente dopo l'implementazione delle contromisure

2.2.1.6 Control (Countermeasures) Design and Implementation

Qualora il livello di rischio sia superiore al valore massimo cui l'organizzazione ritiene di potersi tenere esposta, sono indicati, progettati ed implementati un insieme di Internal Controls (Countermeasures) aggiuntivi di contrasto alle minacce individuate.
Qualora, viceversa, il livello di rischio fosse inferiore al valore fissato, si potrebbe procedere alla dismissione di taluni Internal Control, laddove vi fosse un sollievo economico (e non vi fossero altre condizioni ostative come Law e Regulation Compliance).

2.3 Business Continuity

2.3.1 Business Continuity Planning

BCP: identificazione del personale, materiale e procedure necessarie al recovery, in modo da assicurare il minimo impatto sul business

DRP: parte del BCP che si occupa del Restore della operatività della organization. Un obiettivo fondamentale è la riduzione del tempo di ripristino e, se possibile, anche dei costi di riipristino

disaster:

disruption:

Il Business Continuity Planning Process si divide nelle seguenti fasi:

1. Business Impact Analysis
2. Business Recovery Strategy

3. Detailed Plan Development
4. Plan Implementation
5. Plan testing and Maintenance

2.3.1.1 Business Impact Analysis

1. Gather BIA Data
2. Review BIA Results
3. Establish Recovery Time
4. Define Recovery Alternative

Il coinvolgimento degli utenti è fondamentale durante la BIA

2.3.1.2 System Classification

I sistemi sono classificati in base alla sostituibilità con operazioni manuali (Manual) ed alla tolleranza alla interruzione (Tolerance), come nella tabella seguente:

Classification	Manual	Tolerance
Critical	No	Low
Vital	Brief	Yes
Sensitive	Yes	Yes
Noncritical	Yes	Yes

2.3.2 Insurance

In aggiunta al BCP e DR, possono essere stipulate delle polizze assicurative per la copertura parziale del rischio.

2.3.2.1 Property Insurance

Copertura delle perdite di:

- Building
- Personal Object (table, desk, chairs, etc)
- Loss of Income
- Earthquake
- Flood

2.3.2.2 Liability Insurance

Copertura delle perdite “indirette”, derivanti dall’esercizio o ricostruzione:

- Personal Injury
- Fire liability
- Medical Expenses
- Accident

2.3.3 Human Resource (Response Team)

Il BCP deve chiaramente definire il personale coinvolto nelle operazioni. Di seguito sono indicati i Response Team, il cui ruolo è palese dal nome che assumono, ovvero indicato fra parentesi:

- Emergency Action Team (primi ad intervenire)
- Damage-Assessment Team (quantificazione del disastro)
- Emergency-Management Team (coordinamento del recovery)
- Off-Site Storage Team (custodia e trasporto dei media verso il sito alternativo)
- Software Team (rispristino S.O.)
- Application Team (ripristino applicazioni)
- Security Team (monitoraggio della security)
- Emergency Operation Team ()
- Network Recovery Team (rerouting voice and data)
- Communication Team (recovery site)
- Transportation Team (ricerca e scelta di una locazione alternativa, qualora non sia già stata determinata)
- User Hardware Team (delivery e installazione dei terminali utente)
- Data Preparation and Record Team (preparazione dei dati nel sito di backup)
- Administrative Support Team (message center per il recovery site)
- Supplies Team (user hardware, contatto con i vendor e logistica)
- Salvage Team (relocation e valutazione più accurata dei danni)
- Relocation Team (spostamento di sede)

2.3.4 Alternative Sites

Le risorse necessarie per il recovery sono:

- people
- place
- things

2.3.4.1 Hot Site

E' una copia esatta della situazione in esercizio. Soluzione buona per il recovery delle funzioni critiche.

2.3.4.2 Warm Site

Contiene solo gli apparati meno costosi.

2.3.4.3 Cold Site

Non contiene alcun apparato informatico, solo HVAC e corrente. Soluzione valida per il recovery di sistemi non critici.

2.3.4.4 Duplicate Site

Soluzione valida solo nel caso che l'organizzazione abbia più di un sito

2.3.4.5 Reciprocal Agreement

Soluzione non buona nel caso in cui l'organizzaziona abbia grossi DB o transazioni on-line

2.3.5 BackUp and Storage

Recovery Point Objective: dimensione dei dati da salvare

Recovery Time Objective: tempo massimo per il ripristino

2.3.5.1 Backup Definitions

Full

Differential

Incremental

GFS: Grandfather, Father and Son

2.3.5.2 Tape Storage

On-Site Storage

Off-Site Storage

Electronic Vaulting

2.4 Evaluation of Business Continuity

2.4.1 Testing Approach

2.4.1.1 Paper Test

Test che riguarda la semplice analisi e revisione della documentazione riguardante il BCP

2.4.1.2 Walk-Through Test

Estensione del Paper Test, in cui si richiede la partecipazione dei rappresentati di ogni area operativa nella revisione del piano.

2.4.1.3 Preparedness Test

Test di simulazione di una emergenza, in cui vengono coinvolte le risorse effettive, ristretto ad una area di business

2.4.1.4 Full Operational Test

Test di simulazione completa di tutto il piano di Business Continuity per tutta la organizzazione. Deve comprendere i seguenti task:

- verificare completezza e precision del BCP
- valutare la performance delle persone coinvolte, il livello di conoscenza delle persone dell'esercizio e delle persone non direttamente coinvolte nel BCP
- valutare la capacità di coordinamento, la capacità del sito di backup, la capacità di recupero dei dati vitali
- valutare lo stato e la quantità degli equipaggiammenti presenti nel sito di Backup
- Misurare le performance di tutta l'operazione

Durante i test devono essere prese delle vere e proprie misure, in termini di risorse utilizzate e qualità prodotta:

- Time: elapsed time
- Amount: lavoro svolto
- Count: ammontare di dati vitali recuperati
- Accuracy: rapporto tra l'accuratezza dei dati del sito di recovery verso quello originale

2.4.2 Evaluating the Capability to Continue

L'IS Auditor deve cercare le evidence dell'implementazione di un processo strutturato di BCP. Il senior Management è responsabile di assicurarsi della effettiva riduzione dei rischi derivante dalla corretta implementazione del piano.
Nel piano deve essere specificato:

- key personnel
- personnel task

2.4.2.1 Business Disruption

L'IS dovrebbe:

- partecipare ai test ed alla revisione del BCP
- assicurarsi della efficacia dei backup
- controllare il personale: gli effettivi skills ed i corrispondenti task, ruoli e responsabilità

Il processo di Audit prevede:

- Ottenere una copia del BCP
- Verificare a campione le copie del BCP
- Valutare l'efficacia del BCP
- Rivedere le priorità indicate nel BCP
- Controllare che tutte le applicazioni presenti siano menzionate nel BCP (comprese quelle presenti nei PC)
- Determinare lo stato di aggornamentoe manutenzione degli Off-Site (soprattutto l'Hot Site)
- Verificare i contatti indiicati
- Intervistare le persone indicate
- Valutare le procedure di aggiornamenti e report dei test

2.4.2.2 Short-term Disruption

La disruption non comporta, di contro al disaster, la impossibilità di proseguire tutte le attività di business. Viceversa è causata da malfunzionamenti localizzati, con conseguenti blocchi di una sola area o applicazione. Generalmente si recupera sostituendo l'HW e proseguendo con un recovery.
L'IS Auditor dovrebbe controllare:

Backup Procedure: procedure relative alla esecuzione dei backup ed alle prove di recovery

Onsite Storage: i media contenenti dovrebbero essere conservati in luoghi sicuri: armadi ignifughi o sale Lampertz. Dovrebbe esistere un inventario dei media utilizzati

OffSite Storage: la facility che ospita i media con il backup dovrebbe avere sistemi di sicurezza almeno equivalenti a quelli in vigore nelle sedi di esercizio. I dati devono essere tenuti sincronizzati qualora ci si prepari ad un recovery di dati time-sensitive

Restoration: procedure per la riparazione/sostituzione degli apparati e dei software in essi contenuti

2.4.2.3 Primary Facility Disruption

L'OffSite Facility devve avere le stesse misure di sicurezza che occorrono nella sede fondamentale. Inoltre non devono essere presenti loghi o insegne che facciano presagire la società di appartenenza della facility, in modo da evitare sabotaggi.
L'IS Auditor deve verificare le seguenti notevoli all'interno del BCP:

- piano di movimentazione delle persone e delle cose (punti di incontro, organizzazione dei gruppi, relocation)
- ricostruzione dell'insieme dell' Information System
- Recovery
- caratteristiche del Off-Site (contratto, compatibilità con le esigenze)
- Shared Site agreement

Chapter 3

IS Acquisition, Development & Implementation

Le Organizations spendono molti soldi nello sviluppo, acquisizione, implementazione e manutenzione delle applicazioni. E' necessaria una chiara ed efficiente IT Management Methodology che includa:

- System Development Life Cycle
- Project Management Techniques
- IT Organizational Policy
- Change Management Process

3.1 System Development Life Cycle

Processo logico che deve essere usato da parte dei System Analysts e dei System Developers, durante lo sviluppo dei sistemi, allo scopo di:

- produrre high-quality software
- raggiungere le necessità del business e degli utenti
- stimare correttamente tempi e costi
- agire in modo efficient e effective
- cost-effective maintenance

Gli SDLC più comuni sono quelli che vanno sotto il nome di: Classic Life Cycle Model, ovvero:

- Linear Sequential Model
- Waterfall Model

Nel prosieguo sarà descritto ed utilizzato il Waterfall Model.

3.1.1 Feasibility

Studio di fattibilità. Identifica:

- Strategic Benefit (productivity gain, future cost avoidance)
- Cost Saving
- PayBack

Deve essere anche prodotto un Business Case allo scopo di "giustificare" il progetto.

3.1.2 Requirement Definition

Definisce e determina:

- il problema o la necessità per i quali è stato ideato il progetto
- requisiti di qualità e funzionali
- approccio: make or buy

Devono essere resi partecipi tutti gli stakeholder: Management, Users, in modo da assicurarsi l'effettiva aderenza del progetto alle necessità di business:

- gli utenti specificano i requisiti necessari (access control, regulatory restriction, interface requirement)
- l'IS Auditor deve verificare che i requisiti siano corretti e completi
- l'IS Auditor deve verificare che siano stati inseriti i requisiti relativi alla sicurezza

3.1.2.1 Acquisition

Qualora sia stata scelta la via del "buy", non si applica più l'SDLC ma occorre ugualmente seguire un processo rigoroso, in particolare:

- stilare una Request For Proposal (RFP)ed inviarla a molte società
- scegliere le migliori offerte
- limitare il numero delle società a 2-3, qualora ciò non sia già stato fatto precedentemente
- negoziare e siglare il contratto

L'IS Auditor deve controllare che si esegua un processo rigoroso nella scelta del fornitore (come illustrato nel capitolo relativo alla Technical Infrastructure and Operational Practices)

3.1.3 Design

Sulla base dei requisiti individuati nella fase precedente vengono definite le Specification (specifiche) ed i Test Plan (piani di test), in particolare:

- Baseline dell'applicazione da implementare (in modo da evitare lo scope creep)
- Specifiche del sistema e dei sottosistemi
- dettagli di implenetazione, in funzione delle scelte di hardware, software, network
- specifiche di programma e dei DB
- security plan
- Test Plan riguardanti le diverse componenti: Unit, Subsystem, Integration, Interface, Files, Security, Backup, Recovery

L'IS Auditor deve controllare che siano stati considerati ed inclusi i controlli di sicurezza necessari.

3.1.4 Development

Sulla base delle specifiche precedentemente indiividuate, si dà inizio a:

- programmazione di dettaglio
- formalizzazione dei processi organizzativi di supporto al sistema
- test

3.1.5 Implementation

Fase in cui si procede al Final User Acceptance Test. Possono essere incluse anche le attività di certification a accreditation. Devono essere stabiliti i piani di implementazione e migrazione.
Prima della definitiva entrata in esercizio, si deve:

- eseguire dei penetration test sulla applicazione allo scopo di verificarne l'implementazione dei controlli di sicurezza
- stilate le procedure relative (backup, recovery, patch upgrade)

3.2 Project Management Techniques

Le tecniche di project management (le cui fasi sono state spiegate precedentemente nel capitolo dedicato al Management Planning and Organization) qui descritte si rivolgono al calcolo delle risorse stimate per eseguire il progetto. Devono essere evitati i seguenti Risk Indicators:

- assenza di una formal project-management methodology
- insufficiente esperienza del project-manager
- mancanza dell'approvazione da parte dello Steering Commitee
- evidenza della mancanza di aderenza al business da parte dei precedenti progetti

3.2.1 Function Point Analysis

Tecnica per la stima della dimensione del lavoro che deve essere svolto. ISACA prevede un modello di stima di massima basato sulla complessità (Simple, Average, Complex) della macro azioni da implementare, divise in categorie (User Input, User Output, User Inquiries, Files, External Interfaces).
In pratica occorre:

- catalogare le macro-azioni secondo uno dei 5 tipi di appartenenza
- catalogare ogni azioni inn base alla scala di complessità
- eseguire la somma pesata secondo i parametri riportati nella tabella seguente:

Parameter	Weight		
	Simple	Average	Complex
User Input	3	4	6
User Output	4	5	7
User Inquiries	3	4	6
Files	7	10	15
External Interfaces	5	7	10

In base al numero FP calcolato, che costituisce una stima della dimensione del progetto, possono essere stabiliti i seguenti parametri:

- $Productivity = FP/Person - mounth$
- $Quality = Defects/FP$
- $Unitary Cost = Money/FP$

Function Point Analysis è un valido ausilio per la determinazione delle necessità in termini di risorse e tempo, che comunque resta una delle attività più difficili durante la fase iniziale.

3.2.2 Gantt Chart

Diagramma sviluppato durante la fase di Work BreakDown Structure, allo scopo di illustrare graficamente:

- Timelines
- Milestones
- Dependecies

3.2.3 Program Evaluation Review Technique

PERT è una tecnica che permette di avere una misura più accurata dei tempi di durata del progetto, in quanto prende in considerazione, oltre al Likely Case, anche il Worst Case ed il Best Case, sulla base della esperienza del personale incaricato del planning.
Per ogni task, il tempo desunto dal PERT deriva dal seguente calcolo:
$PERT\,Time = (Best\,Time + (4 * Likely\,Time) + Worst\,Time)/6$

3.2.4 Critical Path Methodology

CPM analizza i differenti task da portare avanti con lo scopo di determinare se vi sono attività bloccanti rispetto ad altre. Qualora si riscontrino attività necessarie per lo svolgimento di altre attività successive esse sono critiche in quanto:

- un ritardo nello svolgimento porterebbe ad un ritardo di tutto il progetto
- non possono essere eseguite in parallelo

3.2.5 Decision Support System

DSS aiuta ad enfatizzare la flessibilità nell'approccio alle decisioni dell'utente. Presenta le seguenti caratteristiche:

- Management Control
- Semistructured Dimension
- Change in Decision process

3.3 IT Organizational Policy

3.3.1 Capability Maturity Model

Deve essere utilizzato un modello che consenta la misura dello stato di sviluppo, quale il CMM, proposto dalla Carnegie Mellon University, illustrato nel capitolo relativo al Management Planning and Organization.
Il raggiungimento del livello 3 (Defined) assicura l'utilizzo di un processo standard di software-development.

3.3.2 Programming Methods and Techniques

3.3.2.1 Formal Coding Standard

Utilizzo di metodologie di comunicazione chiara fra i membri del team di sviluppo e con gli utenti finali. Inoltre l'utilizzo di standard nella naming-convention aiuta la manutenzione e modifica siccessiva del software.

3.3.2.2 Prototyping

Metodologia di sviluppo del software facente uso di sviluppo rapido del codice e test integrati. In questo modo gli utenti possono vedere i risultati dello sviluppo ancor prima che venga sviluppato tutto il codice e sono possibili correzioni e modifiche rapide (da sottoporre comunque all'approvazione del CCB). Occorre tenere presente i seguenti fattori, nell'uso del prototyping:

- optimistic expectation of project timelines
- more complicated change control
- definition of extra-requirements function

3.3.2.3 Rapid Application Development

RAD è usato per sviluppare rapidamente applicativi di importanza strategica, ridurre i costi di sviluppo, mantenere un'elevata qualità. Devono essere impiegate una tecnica di sviluppo comprovata, assieme ad una well-defined methodology:

- Small development team
- Very-Trained Development team
- Evolutionary Prototyping (in modo da poter essere facilmente adattato alle esigenze diverse nel tempo)
- Integrated Power Tools (modeling, prototyping, reusability)
- Central Repository (CVS)
- Interactive Design
- Rigid Development Time Frame

3.3.2.4 Computer Aided Software Engineering

Prodotti software di supporto, in tutte le fasi dello sviluppo delle applicazioni. Sono supportate:

- Analisi
- Programmazione nella fase di Design
- Documentazione

3.3.2.5 ACID

Atomicity: DB commit solo a transazione completata

Completeness (Consistency?): integrità

Isolation: ogni transazione separata delle altre

Durability: DB sopravvive al failure

3.3.2.6 Cohesion and Coupling

Più cohesion (atomicità logica delle funzioni) e meno coupling (interdipendenza dei moduli e classi)

3.3.2.7 On-line Programming

On-Line programming è la programmazione effettuata tramite l'ausilio di strumenti come il Concurrent Version System (CVS) che permette di far lavorare diverse persone direttamente sugli stessi sorgenti. Si ottengono i seguenti vantaggi:

- minor costo di sviluppo
- minor tempo di risposta
- risorse di programmazione più ampie

D'altronde presenta anche i seguenti svantaggi:

- integrità ridotta
- controllo della versione sovrascrivibile

3.3.3 Languages

I tipi di linguaggi maggiormente in uso sono i seguenti:

High-Level: linguaggi di alto livello di utilità generale, tipicamente di tipo imperativo (e.g. CoBOL, C)

Object-Oriented: linguaggi orientati agli oggetti (e.g. C++, Java)

Script: linguaggi interpretati, generalmente utili per il Web o per utilità sistemistiche (e.g. SHell, PERL, JavaScript, VBScript)

Fourth-Generation: linguaggi utili alla implementazione rapida delle interfacce utente, ma non della logica di calcolo (e.g. 4GL)

3.3.3.1 Strumenti

Link Editor: in pratica ld(1)

Compiler:

3.3.4 Personnel

Control Group: componenti dell'area di esercizio, responsabili per la raccolta, protocollazione ed elaborazione dei dati in ingresso per vari gruppi di utenti. Sottopongono i nuovi sorgenti nell'ambiente di esercizio per la compilazione

Data Base Administrator:

System Analyst:

Librarian: archivista, responsabile della conservazione e manutenzione di tutti gli archivi di dati e programmi

3.4 Change Management Process

3.4.1 Change Control Process

Ogni modifica deve essere sottoposta al processo di CCP, come descritto nel capitolo relativo al Management, Planning and Organization.
La modifica può essere richiesta anche da un utente. Gli utenti devono partecipare al processo di approval.

3.4.1.1 Emergency Change

Nell'esercizio si può incorrere nella emergenza della modifica di una applicazione. In questo caso la procedura deve seguire un iter diverso, allo scopo di sveltire la modifica. Si incorre nell'Emergency Change qualora la correzione avvenga prima del completamento della Change Request. Deve essere posta particolare attenzione in queste occasioni: i programmatori devono accedere ed essere tracciati, sulla base della autorizzazione legata all'ID dell'emergenza. Il codice deve essere conservato in una apposita emergency library, fino alla approvazione del Control Board. (de sta ceppa)

3.4.2 Quality Management

Gli sviluppatori devono eseguire test completi (unit, module, full, regression) ad ogni modifica del software. Devono essere testati i seguenti elementi:

- Unit (singoli moduli)
- Interface e Integration (interfacce dei protocolli utilizzati per la integrazione con gli altri sistemi)
- System (applicazione nel suo intero)
- Recovery
- Security (insieme dei controlli di sicurezza)
- Stress/Volume
- Performance
- Final Acceptance (da parte degli utenti)

3.4.2.1 Testing Approach

I test possono, al solito,seguire due differenti approcci:

- Top-Down (generalmente per i RAD)
- Bottom-Up (in modo da testare i singolo componenti, permette un early detection)

Le fasi per il test devono essere le seguenti:

Test Plan: sviluppo del piano di test, definizione dei risultati attesi (I/O, lenght, expected result)

Testing: utilizzo degli strumenti di test e confronto con i risultati attesi

Defects Management: i difetti devono essere loggati e corretti

3.4.2.2 Testing Levels

Unit Test: test dei singoli moduli

Interface/Integration Testing: test delle interfacce di comunicazione verso altri sitemi e dell'interscambio dati

System Testing: test di tutti i componenti del sistema

Final Acceptance Test: test di due aree della Quality Assurance

Quality Assurance: test delle funzioni tecniche del sistema (da parte di personale specializzato)

User Acceptance: test del sistema da parte degli utenti. Non eseguire tale tipo di test potrebbe portare un impatto molto negativo nella implementazione della applicazione, in quanto influirebbe sulla operatività

3.4.2.3 Testing Types

Questi sono alcuni dei tipi di test che possono essere svolti in funzione del testing level:

WhiteBox Test: test del funzionamento di un modulo, tipicamente, mediante controllo della corretta esecuzione delle istruzioni in esso contenute (test del corretta implementazione del protocollo), eventualmente tramite ispezione del codice ("aprendo la scatola")

BlackBox Test: test a scatola chiusa del modulo, sistema o più propriamente delle interazioni fra i vari moduli che compongono il sistema

Regression Test: riesecuzione di test, su una piattaforma parzialmente rimaneggiata, allo scopo di rivelare eventuali errori che possano essere venuti a verificarsi sulle componenti non soggette a modifica

Parallel Test: processo di test su due sistemi, quello modificato ed uno alternativo, generalmente l'originale, allo scopo di confrontare i risultati e le funzionalità

Sociability Test:

Incremental Test: test eseguito solo sulle componenti aggiuntive di un software già funzionante

3.4.3 Application Definition

Abend: terminazione irregolare di una elaborazione (prima della fine del job) causata da una condizione di errore che non è gestita dalle funzionalità di recovery attivabili a job attivo

Application Tracing and Mapping: utility di tracciamento e mappatura della applicazione, che può essere usata per analizzare il flusso dei dati attraverso la logica elaborativa e per documentare:

- percorso logico
- condizioni di controllo
- sequenze di elaborazione

Resilience: capacità di un programma di recuperare da un errore

Chapter 4

IS Operation, Maintenance & Support

4.1 Technical Infrastructure

4.1.1 IT Functions

4.1.1.1 Project Management

4.1.1.2 Line Management

Control Group: responsabile per il logging

Data Management: responsabile per la definizione delle architetture dati

Database Administrator: responsabile per l'amministrazione del DB. Esegue, di norma, le seguenti funzioni:

- definition of conceptual schema
- definition of integrity and security check
- development of data model (with users)

Systems Administrator: responsabile per l'amministrazione dei sistemi

Network Manger/Administrator: responsabile per il planning, implementation, maintenance della infrastruttura di telecomunicazioni

Quality Manager: responsabile per il controllo della qualità di ogni attività eseguita nell'area della infromation technology

4.1.2 Cobit Controls

Il CobiT frnisce una serie una serie di policy per le funzioni IT, suddivise nelle seguenti aree

4.1.2.1 Acquisition

1. Definition of Information Requirements
2. Formulation of Alternative Course of Action
3. Formulation of Acquisition Strategy
4. Third-Party Service Requirements
5. Technological Feasibility Study
6. Economic Feasibility Study

7. Information Architecture
8. Risk Analysis Report
9. Cost-Effective Security Control
10. Audit Trails Design
11. Ergonomics
12. Procurement Control
13. Software Product Acquisition
14. Third-Party Software Maintenance
15. Contract Application Programming
16. Acceptance of Facilities
17. Acceptance of Technology

4.1.2.2 Standards

4.1.2.3 Performance

4.1.2.4 Configuration

4.1.2.5 Service Providers

4.1.3 Evaluating Hardware

4.1.3.1 Hardware Components and Attributes

I componenti di un hardware sono, schematicamente, i seguenti:

CPU:

Input/Output Devices:

Gli attributi che si richiede un computer abbia sono i seguenti

Multitasking: capacità di eseguire più di un tack alla volta

Multiprocessing: presenza di più di una CPU ed utilizzo in contemporanea delle stesse

Multithreading: possibilità di eseguire più di un task alla volta, in un singolo programma

4.1.3.2 Computer Category

Derivata dalla tassonomia di Flynn

Supercomputer: i computer più potenti che ci siano. Non possono eseguire diversi programmi concorrenti

Mainframes: molti controlli di accesso ed autorizzazione ai programmi. L'elaborazione è solo sul Mainframe

Minicomputer: piccoli Mainframes

Microcomputer: praticamente i personal computer. Sono usati in ambienti Client/Server

Notebook: come i PC. Possono essere rubati (e con essi i dati ivi contenuti!)

PDA: Personal Digital Assistant. Sono dei mini PC che consentono di fare tutte le operazioni possibili su un PC

4.1.3.3 Risk and Control

Request for Proposal: specifiche per i vendor, detta anche Invitation To Tender. Deve contenere i seguenti parametri:

- Information Processing Requirements (application, performance, processing approach)
- Hardware Requirements (CPU, Input/Output Devices)
- Software System Application (S.O., librerie, compilatori, etc)
- Support Requirements (Maintenance, Training)
- Constraints (Staffing, Capacity, Delivery Dates)
- Conversion Requirements

L'IT organization deve:

- implementare le policy per l'SDLC
- sottomettere i grandi progetti allo Steering Commitee

L'IS Auditor deve:

- verificare l'esistenza di un approccio strutturato all'Acquisition, Implementation, Maintenance

4.1.3.4 Change and Configuration

L'IT Organization deve:

- sottoporre agni richiesta di cambiamento al processo di Change Control (CCP)

L'IS Auditor deve verificare:

- Hardware Performance Monitoring Plan
- Problem Log Review
- Hardware Availability and Performance Reports

4.1.4 Evaluating Software

L'IT organization deve:

- gestire una mappa dei software utilizzati, insieme alle licenze ed al supporto
- assicurarsi che il software soddisfi gli standards
- creare policy and procedure per il rispetto delle leggi sul copyright

4.1.4.1 Firmware

Software che è contenuto in un chip (e.g. Boot PROM)

4.1.4.2 Operating Systems

I S.O. sono stati ideati per fornire le seguenti funzionalità di base:

- Definire le Interfacce
- Abilitare l'Accesso alle Risorse
- Amministrare lo Scheduling delle Risorse (tra cui la CPU)

I S.O. sono configurati (tuning) per addivenire alle esigenze della organizzazione

Network Operating System: S.O. (dei thin client?) con le segueti features:

- disponibilità di documentazione in linea
- accesso utente a varie risorse di rete
- autorizzazione per l'utente ad accedere a particolari risorse
- computer host da adoperare senza particolari comandi o azioni

4.1.4.3 Middleware

Il Middleware fornisce la integrazione fra applicazioni distinte. Le funzionalità che fornisce di solito sono le seguenti:

Transaction Processing (TP) Monitor: monitoraggio e processamento delle transazioni su DB

Remote Procedure Calls (RPC): richiesta di esecuzione di funzioni su unn computer remoto (CORBA, RFC di SAP, RPC Unix e Microsoft)

Messaging Services: Messagin Queue remoto (e.g. BEA Messaging Queue,)

4.1.4.4 DataBase

Hierarchical: relazione padre-figlio tra le tabelle (no relazioni multiple, no flessibilità)

Network: relazione padre-figlio multipla tra le tabelle (complesso da gestire)

Relational: separa i dati dalla struttura del DB. I database oggi sono quasi tutti cosi' (eccezioni notevoli sono i file di configurazione dei S.O.)

Normalization: stritturazione dei dati allo scopo di ridurre duplicazioni ed inconsistenze:

- Ogni campo in una tabella rappresenta una unica informazione
- Ogni tabella deve avere un campo di chiave primaria
- E' possibile modificare i dati (diversi dalla chiave primaria) senza toccare gli altri campi

Data Dictionary: descrive tutti gli item contenuti nel DB

Meta Data: data elements necessari a definire un sistema DBMS valido in tutta la azienda

Directory System: definisce la locazione dei dati ed il metodo di accesso

Hashing: tecnica per il partizionamento degli indici, in modo da farli risiedere su dischi diversi (scelti in base all'hash)

Internal Schema: definzione dello storaging fisico fisico dei dati (funzionamento interno del DBMS, su cui non si interviene)

4.1.4.5 Risk and Controls

l'IT organization deve:

- essere aggiornato sulle nuove features dei software, in modo da favorire il miglioramento dei processi di business
- manutenere le applicazioni in esercizio (update, licensing, support)
- supportare un capacitiy-management plan
- sollecitare commenti da parte di utenti e management durante lo sviluppo dei programmi

Configuration Management Audit: audit che comprende sempre anche la verifica delle licenze del software utilizzato

4.1.4.6 Change and Configuration

Il Software deve seguire il CCP, in modo che soddisfi:

- le esigenze di business
- internal comaptibility standards

L'IT deve:

- mantenere separati gli ambienti (development, test, production libraries)
- assicurarsi che le library sia concistenti rispetto alla segregation of duties

L'auditor può:

- effettuare un source code comparison, alo scopo di tracciare i cambiamenti

4.1.5 Evaluating Network

4.1.5.1 ISO/OSI

Data Encapsulation: inserimento dei dati in un formato pronto per la connnessione

SSL: definito a livello 5 (Session)

PDU: Protocol Data Unit

TCP: connection-oriented (reliable)

UDP: best-effort

4.1.5.2 Network Types

LAN: Local Area Network

WAN: Wide Area Network

MAN: Metropolitan Area Network

VPN: Virtual Private Network

4.1.5.3 Type of Transmission

Unicast:

Multicast:

Broadcast:

4.1.5.4 Network Topology

Bus:

Star:

Ring:

Mesh:

4.1.5.5 Network Devices

Firewall

Firewall: apparato che restringe l'accesso a determinati settori della rete

Vi sono vari tipi e tecnologie di firewall, fra cui:

Packet-Filtering: analisi fino al livello 4

Stateful-Inspection: analisi su tutti i livelli

Proxy: analisi approfondita su tutti i livelli (lui dice che sia il più sicuro)

Da un punto di vista topologico, i firewall possono essere configurati in varie maniere:

Bastion Host: macchina propriamente hardenizzata allo scopo di ospitare un firewall

Screened Host: firewall di difesa ad una rete

Screened Subnet: confinamento di una rete fra due firewall, allo scopo di creare un livellamento della difesa

Router Apparati che consentono l'instradamento dei pacchetti da una rete all'altra, mediante implementazione del livello 3 OSI.

Modem

Bridge

Switch

Hub

4.1.5.6 Risk and Controls

Ci sono i seguenti Critical Success Factors:

Interoperability: capacità di integrazione dei vari devices

Availability: tolleranza ai guasti ed agli errori

Flexibility: facilità di adeguamento alle nuove esigenze (scalabilità)

L' IS Auditor deve identificare:

- LAN topology
- Network component
- Network topology
- Network uses
- Documentation
- Administrator Functions

Physical Controls

- Physical Access Control
- Hardware, Software e Manuali in una locazione sicura
- Accesso Ristretto agli armadi contenenti seerver ed apparati di rete
- UPS (Uninterruptable Power Supply)

Logical Access Controls

- Unique Password
- Written Authoritzation to Application Access
- Logging Login Attempts
- Documentation

4.1.5.7 Test Types

Performance of Flow and Error Control: Transport Layer Protocol Analyzer

4.2 Operational Practices

4.2.1 CobiT

Il Cobit stabilisce 11 processi per il management e deployment dei sistemi IT:

- Develop a Strategic Plan
- Articulate the Information Architecture
- Find an Optimal Fit between IT and Organization Strategy
- Design IT Function to mathc the Organization Needs
- Maximize the Return On IT Investment
- Communicate IT Policy to Users
- Manage the IT WorkForce
- Comply with external Regulations, Laws and Contracts
- Conduct IT Risk Assessment
- Maintain an High-Quality System-Development Process
- Incorporate Sound Project-Management Techniques

4.2.2 Risk and Controls

Segregation of Duties:

Organizational Chart: Responsibility and Authority

Job Description: Responsability and Accountability

4.2.3 Performance and Monitoring Process

Devono essere aggiornati i dati relativi alle performance ed ai guasti che occorrono alle apparecchiature. In particolare devono esser presenti (ed analizzati dall'IS Auditor) i log relativi a:

- System Logs
- Abnormal Job Termination
- Operator Problem Report
- Capacity Monitoring
- Network Monitoring
- System Downtime

4.3 Business Plan

4.3.1 Strategies

Deve essere prevista, ed analizzata dall'Auditor, una chiara strategia di business aziendale, di tipo:

Long-Term (3 anni): Strategical

Short-Term (1 anno): Tactical. deve esserci una corretta integrazione tra personale IT e Business nei progetti

Tali strategie devono essere continuamente riviste, sulla base delle richiesta di mercato e dei clienti. La strategia deve essere approvata, rivista, etc dal senior management.

4.3.1.1 IT Steering Commitee

Lo steering Commitee assicura che la strategia del dipartimento IT sia allineata (allign) e di supporto alla strategia di business della organizzazione. Esso è composto da senior manager. Il Comitato deve:

- mantains detailed meeting minutes
- review of major IT projects
- ensure efficient use od data processing resources

Il Comitato non deve:

- providing guidance in day-to-day operations

La strategia deve essere continuamente rivista, in base alla evoluzione della strategia di business aziendale, alla evoluzione della tecnologia, etc.

4.3.1.2 Change Control Process

Processo con il quale sono costantemente modificate le strategie, le policy, le procedure di supporto al Business

Change Control Board: comitato preposto alla valutazione di ogni richiesta di modifica a sistemi e documentazione, rivedendo ed eventualmente suggerendo modifiche. E' costituito da senior manager

4.3.2 Policy

Security Policy Implementation: assimilazione del Framework e degli intenti da tutte le parti coinvolte

4.3.2.1 Policy Development Approach

Top Down: metodo più naturale di sviluppo delle policy, che eredita direttamente quanto ideato nelle strategie. Presenta il difetto di poter richiedere maggior tempo per lo sviluppo e non coprire determinate esigenze operative particolari

Bottom Up: metodo meno naturale ma più veloce ed efficiente. Deve essere eseguito dopo una Risk Analysis. Può presentare il difetto di essere meno aderente alla strategia individuata

4.3.2.2 Policy Types

Regulatory: policy che descrivono l'obbligatorietà di determinati comportamenti, in determinate situazioni, allo scopo di soddisfare i requisiti di legge

Advisory: policy che hanno lo scopo di consigliare determinati comportamenti

Informative: policy che hanno lo scopo di descrivere determinate circostanze

4.3.2.3 Area of Policy Development

Planning:

Organization:

Hardware:

Network:

Security: Triade AIC. Deve essere previste le policy di:

- Basic Access Authorization
- Response Program (to handle intrusion)

Operations: ongoing operations

Contingency: BCP e DRP

Financial and Accounting:

4.3.3 Procedure

Le procedure sono documenti di dettaglio che raccolgono i dettami delle policy e descrivono i processi amministrativi ed operativi. Sono i documenti più fluidi, in quanto contengono maggiori dettagli, e quindi devono essere sottoposte a revisione continua per assicurarne l'aderenza alla realtà.

4.3.4 Organizational Chart

Deve essere rivisto dall'Auditor per identificare responsabilità e ruoli.

4.4 IT Organization

4.4.1 IS Strategy

Il dipartimento IT deve avere un valido processo di elaborazione e modifica della propria strategia che preveda:

- development
- communication
- implementation

La IT Strategy deve:

1. essere allineata con la strategia di business
2. permettere l'utilizzo efficiente delle risorse di calcolo
3. servire come base per la definizione delle policy e procedure

4.4.1.1 IS Assessment

L'IS Assessment prevede dei meccanismio per calcolare quanto abbiano deviato dai livelli pianificati es attesi le attività. Questi metodi includono:

- IS Budget
- capacity and growth planning
- industry standards/benchmarking
- financial management practices
- goal accomplishment

4.4.2 IS Function

4.4.2.1 On-going Operation

System maintenance:

User Support:

Problem (Incident) Management:

Change Management:

Quality Assurance:

4.4.2.2 Project

4.4.3 IS Strategy Components

- Policy
- Procedure

4.4.4 IS Department Organization

4.4.4.1 Evaluation

Un Auditor deve considerare le seguanti questioni:

- Segregation of Incomaptible Duties
- Vesting in Different People
- Accomplish Judicious Choice

4.4.5 Third Party Auditing

Outsourcing: contratto fra una organizzazione ed una terza parte, per la fornitura di servizi relativi ai sistemi informativi, sviluppo, processamento ed hosting

Service Level Agreeement: descrizione del livello di servizio fornito (con le relative penali)

4.4.5.1 Audit

Il client epuò richiedere che il fornitore si sia sottoposto ad un Audit (come il SAS70) allo scopo di verificare eventuali vulnerabilità della struttura che potrebbe inficiare la qualità dei servizi erogati. Un tipico audit dovrebbe portare le seguenti informazioni:

1. Report of Independent Auditor
2. Descrizione delle Policy e Procedure importanti
3. Control Objectives
4. Client Control Considerations

Le questioni di particolare interesse, da sottoporre ad accurata analisi sono:

- program and file properties
- due care and confidentiality
- continued service, in the event of disaster

Audit Client's Business Plan reviewed prior to Organization IT Strategic Plan

4.4.6 Contract Management

Contract: accordo fra due o più persone per la fornitura di beni o servizi. In esso devono essere specificati:

- Offer (bene oggetto della offerta)
- Consideration (prezzo corrisposto)
- Acceptance (colui che presterà il servizio)
- Legal Purpose
- Capacity

4.4.6.1 Tipologie di Contratti

Employee Contract: contratto di assunzione

Confidentiality Agreement:

Trade Secret Agreement:

Discovery Agreement:

Noncompete Agreement:

4.5 IS Strategy and Policy

4.5.1 Project Management

I progetti maggiori devono essere approvati dall'IS Steering Commiteee, per assicurarne la compliance con le strategie aziendali.

4.5.1.1 Project Management Phases

Planning: fase in cui vengono identificati il team, il PM, la dimmensione del progetto, le risorse in termini di costi, tempi e qualità attesa. Quindi viene determinata la Work BreakDown Structure[1]

Scheduling: fase in cui viene prodotto il Gantt ed eseguita la Critical Path Analysis

Monitoring: monitoraggio continuo della deviazione rispetto al plan

Controlling: "No good plan survive the contact with the enemy", modifiche che vengono eseguite sul progetto, in modo da adattarsi ai ambiamenti che sono intercorsi dalla ideazione del pln

Closing: fase conclusiva in cui si ottiene la "acceptance" scritta da parte del cliente e viene gestita il rilascio della documentazione

[1] Un Work BreakDown Structure si compone delle seguenti informazioni:

- Project Milestone
- Resource Required (Persone e Soldi)
- Amount of Time
- Back Out (in caso di sostituzioni di piattaforme in essere)
- User Acceptance Testing

4.5.2 Problem Management

Problem Management: minimizzazione degli effetti negativi, sulla organizzazione, di un incidente causato da un errore e prevenirne l'accadimento

Devono essere sviluppate apposite policy e procedure che descrivano:

- recognition
- logging
- resolution
- escalation
- tracking
- reporting

4.5.3 Change Management

La presenza di una adeguata procedura di Change Mangement, assicura che tutte le attività (analisi dei rischi, analisi di compatibilità, etc) siano eseguite.

4.5.3.1 Change Request

Una CR contiene tutte le informazioni necessarie per la valutazione della "bontà" della modifica richiesta, in particolare:

- Originator
- Reasons
- Work BreakDown Structure
- Documentation
- Risk Assessment

Subject Matter Expert: colui che revisiona la CR, prima che venga sottoposta al CCB

4.5.4 Quality Management

Quality Assurance: assicura che il personale segua i processi di qualità determinati e ampiamenti descritti

Quality Control: conduce test in modo tale da verificare l'assenza di difetti e verificare il gradimento degli utenti

Certification: valutazione tecnica del livello di sicurezza di un sistema

Accreditation: autorizzazione all'uso di un sistema, a fronte di una certificazione

4.5.4.1 Capability Maturity Model

Sebbene sia uscito il CMMI, ISACA si basa sul CMM. Esso è stato sviluppato dalla Università Carnegie Mellon, allo scopo di fornire uno strumento per l'analisi della maturità dello sviluppo dei software. Prevede 5 livelli:

Optimizing (5): si ricerca continuamente il miglioramento (Continous Process Improvement)

Managed (4): vi sono dei criteri per misurare la qualità del prodotto (Quantitative Quality Goals)

Defined (3): l'intero processo è stato documentato. Tutti i progetti seguono tale standard (Documented Project)

Repeteable (2): sono tracciati costi, schedulazioni e funzionalità. Può essere garantito il successo di progetti simili (Basic Project Management)

Initial (1): non vi è un processo delineato. Il successo dipende dalle capacità personali

4.5.4.2 ISO

ISO 9001:

ISO 9126:

4.5.5 Security Management

Confidentiality:

Availability:

Integrity:

4.5.5.1 Physical Controls

I controlli fisici servono per difendersi da questi tipici attacchi:

- Social Engineering
- Shoulder Surfing
- Piggy Backing

4.5.5.2 Logical Controls

- Segregation of Duties
- Logging od Accesses
- Transaction Log Monitoring
- Penetration Test

4.5.6 Business Continuity

Business Continuity Planning: piano ideato per ridurre il rischio di blocco dell'attività produttiva in concomitanza dell'occorrimento di una catastrofe. Il BCP deve essere rivisto con cadenza annuale

Disaster Recovery: piano sviluppato dall'IT per il recupero, nel tempo più rapido possibile, del funzionamento della infrastruttura

L'implementazione dei BCP e DRP, dipende dall'avallo e dal coinvolgimento del Management.

4.6 Jobs and Responsabilities

4.6.1 Segregation of Duties

4.6.1.1 Figure Professionali

Quality Assurance

System Analyst

Quality Control Administrator

Change Control

Problem Management

4.6.1.2 Segregationa Ares

- Authorization
- Custody
- Record Keeping
- Reconciliation

4.6.2 Observation Process

Un Auditor deve osservare il personale, durante lo svolgimento del proprio lavoro, allo scopo di determinare:

Organizational Function: la funzione svolta ll'interno della organizzazione

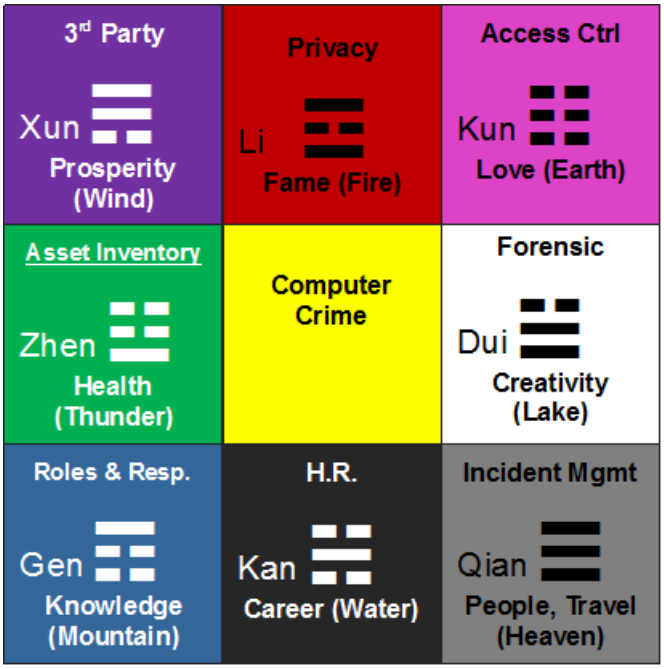
Process: i processi esistenti, la presenza di eventuali procedure, il rispetto delle stesse

Chapter 5

Protection of Information Asset

5.1 Information Security Management

I 9 aspetti della gestione della sicurezza delle informazioni possono essere facilmente messe in analogia con il Ba Gua (8 trigrammi) nella conformazione dell'Later Heaven Sky (Cielo Posteriore), nella forma del quadrato 3x3 (Lucky Quadrant), illustrato nella figura seguente (modello "Information Feng Shui"):



Vediamo nella seguente tabella il significato di ciascuno di essi e la applicazione alle aree della sicurezza:

Trigramma	Descrizione	Security Area
Xun	Gentle Penetration, Wealth & Prosperity (Wind)	3rd Party
Li	Rapid Movement, Radiance, Fame & Reputation (Fire)	Privacy
Kun	Receptive Energy, Love, Marriage (Earth)	Access Control
Zhen	Excitation, Health, Family (Thunder)	Asset Inventory
-	the Center	Computer Crime
Dui	Joy, Satisfaction, Creativity (Lake)	Forensic
Qian	Expansive Energy, Helpfull People & Travel (Heaven)	Incident Mgmt
Kan	Danger, Rapid Rivers, the Moon (Water)	H.R.
Gen	Stillness, Immovability, Knowledge (Mountain)	Roles & Resp.

Ognuna di queste 9 aree necessita di una gestione idonea. Alcune di esse sottendono concetti più complessi (5). Questi possono essere inquadrati all'interno del modello dei 5 elementi:

Elemento	Concetto	Area
Wood	Network Security	Asset Inventory
		3rd Party
Fire	Cryptography	Privacy
Earth	Logical Access Control	Access Control
		Computer Crime
		Roles & Resp.
Metal	Detection	Forensic
		Incident Mgmt
Water	Physical Security	H.R. Security

Questo permette di ricreare i corrispondenti cicli:

Generazione: normale successione dei concetti, così come dovrebbero scaturire l'uno dall'altro, producendo una normale consecuzione logica:

- Nework Security fa sorgere necessità di Crypt
- Crypt consente il Logical-Access-Control
- Logical-Access-Control abilita la possibilità di Detection
- Detection deve essere effettuata anche su Physical
- Physical determina la possibilità di Network Security

Dominazione: illustrazione dei legami indiretti ma indissolubili tra le fasi:

Riduzione: illustrazione ...:

Mitigazione: illustrazione ...:

Nei paragrafi seguenti, la trattazione è organizzata secondo questi 5 concetti più complessi.

5.2 Logical Access Control

5.2.1 Access Control Components

Subject: colui che richiede di accedere alle informazioni

Object: entità che contiene le informazioni

Access: flusso di informazioni dall'oggetto al soggetto

5.2.2 Access Control Types

5.2.2.1 Discretionary Access Control

L'accesso alle informazioni contenute nell'oggetto è a completa discrezione del data owner

5.2.2.2 Mandatory Access Control

L'accesso alle informazioni è legato ad una classificazione delle stesse ed ad un livello di NOS posseduto dal soggetto (per ambienti Miitari)

5.2.2.3 Non-Discretionary Access Control

L'accesso alle informazioni è stabilito in modo centrale e comunque in accordo alle policy dell'organizzazione. I criteri di controllo di accesso di tipo non discretional più diffusi sono:

Rule-Based: basato sul ruolo ricoperto dal personale

Task-Based: basato su una particolare attività

Lattice-Based: simile al Mandatory, ma per ambienti civili

Rule-Based: basato su delle regole, derivanti dalle policy aziendali (e.g. Firewall)

Restricted User Interface: controlla al contempo l'accesso ai dati ed alle funzioni

5.2.3 Access Control Tips

I permessi di accesso possono essere espressi in vari modi, fra cui:

Access Control Matrix

Capability Table

Access Control List

L'amministrazione (Provisioning) degli accessi può essere:

Decentralized: gestito sito per sito

Centralized: gestito centralmente, ad esempio tramite un sistema di Identity ed Access Management

5.2.4 Identification and Authentication Techniques

Identification:

Authentication:

Authorization:

5.2.4.1 Authentication Form

- Something you Know
- Something you Have
- Something you Are

Strong Authentication: two Factor Authentication

5.2.4.2 Password

Le password sono il metodo più diffuso per la autenticazione, il più economico ed anche il più debole. Possono essere configurati alcuni parametri per fornire un irrobustimento del meccanismo:

- Alert Threshold
- Account Disabilitation
- Passwrod Lenght
- Password Complexity

Cognitive Password: password basate sulla risposta ad una domanda personale

One Time Password: password che hanno una valenza "una tantum", generalmente associate all'utilizzo di un Token

5.3 Network Security

5.3.1 Network Controls

Per ISACA, i seguenti sono i controlli da eseguire relativamente alla network:

- i controlli devono essere eseguiti da operatori tecnicamente qualificati
- i controlli dovrebbero essere separati
- il software dovrebbe restringere l'accesso consentito agli operatori
- audit trails review
- documentation
- access monitoring
- analisi relativa alle performance (workload balance, fast response, system efficiency)
- terminal identification
- data encryption

5.3.2 Network Security Devices

5.3.2.1 Firewall

DoS: Denial of Service (occorre filtrare opportunamente il traffico in uscita)

FTP: chiudere l'accesso allo scaricamento dei file via FTP

CallBack: tecnica usata per le connessioni RAS, può essere raggirata mediante call forwarding

5.3.2.2 Virtual Private Network

PPTP

IPSec

5.3.2.3 Intrusion Detection Systems

Sono di due tipi fondamentali:

- Signature Based
- Anomaly Detection Based (molti falsi positivi)

5.3.2.4 Single Sign On

Sistemi soggetti a vulnerabilità derivanti dall'avere un single point of failure per l'autenticazione

5.3.2.5 Privacy Branch eXchange

Centralini telefonici privati. Sono soggetti alle seguenti vulnerabilità:

- Theft of Service
- Disclosure of Information
- Information Modification
- Unauhtorized Access
- Denial of Services
- Traffic Analysis

5.3.3 Intrusion Methods and Techniques

5.3.3.1 Passive Attack

- Scanning
- Eavesdropping (packet analysis)
- Traffic Analysis

5.3.3.2 Active Attack

- BruteForce
- DoS
- Spamming
- Trojan Horse
- Social Engineering

5.3.3.3 Indirect Attack

- Virus
- Worms
- RootKit (Integrity Check)

5.3.3.4 Security Scanning

- Vulnerability Assessment (Nessus)
- Penetration Test
- Honey Pots

5.3.3.5 Information Security Source

- CERT (www.cert.org)
- CVE (cve.mitre.org)
- Forum of Incident Response and Security Team (www.first.org)
- SANS Insitute (www.sans.org)
- Computer Crime and Intellectual Property Section (www.ccips.org)
- Insecure (www.insecure.org)
- Information System Security (www.infosyssec.com)

5.4 Cryptography

La crittografia ha l'obiettivo di nascondere (dal greco κρυπτω) determinate informazioni, rendendole rivelabili solo a coloro cui sono destinate, per mezzo di una chiave (cui i destinatari propri sono in possesso): cioé Confidenzialità. Ovvero, qualora qualcuno, cui le informazioni non erano indirizzate, dovesse venire in possesso di una copia dei dati crittografati, non potrebbe risalire alle informazioni contenutevi[1].
Questo può essere applicato a dati:

[1] Ovviamente, ciò ha una importanza basilare in guerra e nelle azioni militari. In base ad essa (vedi Enigma, Alan M. Turing, Colossus, Bletchley Park, etc) l'informatica ha avuto l'evoluzione vertiginosa che conosciamo dalla fine della II Guerra Mondiale.

- Archiviati: At-Rest
- in Movimento: Communication

Successivamente, con il progredire della potenza di calcolo degli elaboratori, sono state aggiunte altre finalità alla crittografia, di cui alla tabella seguente:

Obiettivo	Applicazione	Definizione	Meccanismo	Dispositivo
Confidentiality	At-Rest Communication	nascondere le informazioni	Symmetric	SSL-TLS, PKI
Integrity	Communication	garantire la non manomissione (involontaria o per dolo) dei dati	Hash + Sign Hash-Chain	SSL-TLS
Authenticity	Communication	assicurare l'identità del mittente	Asymmetric	SSL-TLS, PKI
Non-Repudians	Comunication	assicurare che non vi sia ripudio postumo	Asymmetric	PKI

5.4.1 Definizioni Fondamentali

Algorithm: insieme di regole matematiche per la definizione dei vari standard di encryption e decryption

PlainText: testo in chiaro

Cyphertext: testo dopo essere stato sottoposto a cifratura $Cyphertext = Crypt_{Key}(PlainTest)$

Encipher: cifratore

Decipher: decifratore

Key: chiave

5.4.2 Altre Definizioni

KeySpace: spazio delle chiavi (di tutti i possibili valori assumibili dalle chiavi) per un determinato algoritmo

Key Clustering: isyanza in cui due distinte chiavi, applicate allo stesso plaintext, generano il medesimo cyphertext

Cryptosystem: implementazione hardware e software delle critpografia

Work Factor (Strenght): stima del tempo, risorse e sforzo necessario alla rottura di un criptosystem

Collision: circostanza in cui due differenti plaintext danno luogo allo stesso ciphertext

Link Encryption: cifratura del collegamento (dal Data Link in sù)

End to End Encryption: cifratura a livello applicativo

Cryptography: scienza che studia le metodologie per conservare e trasmettere i dati in modo tale che solo chi di dovere possa averne accesso

Cryptoanalysis: scienza che studia il modo con cui rompere i segreti degli algoritmi di cifratura ed i loro componenti

Cryptology: unione di Cryptography e Cryptoanalysis

Working Factor: computazione necessaria alla ricerca della chiave di cifratura, mediante ricerca per key combination

Strenght: robustezza data da:

- key lenght
- Initial Vector Number
- Algorithm Complexity

5.4.3 CypherSuite

Le tecniche di crittografia sono state standardizzate. Nelle comunicazioni a Trasporto (TCP), si fa spesso uso del protocollo SSL (Secure Socket Layer) o TLS (Transport Layer Security) che creano uno strato di sessione superiore, sopra quello di trasporto che garantisce l'uso di crittografia. Ovviamente il massimo beneficio si ha quando viene usato insieme ad una PKI, per una corretta gestione della delega di responsabilità nell'assegnazione del Certficato (e della chiave corrispondente, quindi) all'utente.
Tramite SSL-TLS è possibile indirizzare tutti gli obiettivi della crittografia su menzionati. La cypher-suite è quella stringa che descrive quali algoritmo crittografici vengono utilizzati in quella particolare sessione ed in che modo (cfr. RFC 5246) ed assume questa forma generale:

Cypher-Suite Example: TLS_RSA_WITH_3DES_EDE_CBC_SHA

La tabella seguente fornisce una semplificazione:

Stringa	Significato	Valori
Protocollo	protocollo usato	SSL TLS
Asymmetric Mechanism	algoritmo asimmetrico usato (authentication & session-key negotiation)	NULL RSA DH DHE_DSS KRB5
WITH	separatore algoritmi	N/A
Symmetric Mechanism	algoritmo simmetrico utilizzato (payload chypherment)	NULL DES 3DES RC4 AES Camellia
crypto sequence	solo 3DES: sequenza di utilizzo	EDE
Mode of Operation	modalità con cui concatenare i segmenti di plaintext da (de)cifrare	_ (NULL) CBC GCM
Hash	algoritmo di hash utilizzato	NULL SHA SHA256 SHA128 MD5

Dove abbiamo i seguenti:

5.4.3.1 Asymmetric Mechanism

Algoritmi asimmetrici possibili:

NULL: nessuno, di prova

RSA: Rivest, Shamir, Adlemann

DH: Diffie-Hellman puro

DHE_DSS: Diffie-Hellman per Data Signature Standard

KRS5: Kerberos 5

5.4.3.2 Symmetric Mechanisms

Algoritmi simmetrici possibili:

NULL: nessuno, di prova

DES: Data Encryption Standard (vecchio, usato solo per retro-compatibilità)

3DES: anch'esso ormai data. Viene usato nella seqienza

RC4: Algoritmi ideati da Ron Rivest, analizzati e brevettati dalla RSA Data Security Inc. RC5 presenta: 32, 64, 128 data bit

Camellia: algoritmo ideato nel 2000 in NTT e Mitsubishi Electronic Corporation a 128 bit. Stesso livello di sicurezza e performance di AES

AES: Nel Gennaio 1997 il NIST ha indetto il bando per scegliere il sostituto del DES. Fu scelto l'algoritmo Rijndael, ideato da Joan Daemon e Vincent Rijmen. 128, 192 e 256 bit

5.4.3.3 Mode of Operation

Modi di utilizzo definiti dal NIST per i cifratori a blocchi approvati dal FIPS, per criptare messaggi più lunghi del blocco trattato da ogni algoritmo. Alcuni di essi emulano esplicitamente uno stream cipher mediante l'utilizzo di un keystream generator.

Galois/Counter Mode: nuovo, efficiente e performante (vedi http://en.wikipedia.org/wiki/Galois/Counter_Mode)

Cipher Block Chaining: la chiave $K_i$usata per cifrare il blocco B_iè il risultato C_{i-1}della cifratura del blocco B_{i-1}

5.4.3.4 Hash

Questi algoritmi funzionano senza chiave di cifratura, semplicemente creano un fingerprint (hash) del messaggio sulla base di regole predefinite. Lo scopo è quello di combinare tali hash con altri metodi crittografici per garantire la integrità anche in occasione di modificazioni intenzionali

MD5: miglioramento di MD4, 128 bit

SHA: progettato da NIST e NSA per essere usato nel DSS. Originariamente 160 bit, ora anche 256 e 384

In generale:

Message Authentication Code: $MAC = Hash(Message, SecretKey)$

Digital Signature: $DS = Crypt_{Priv}(Hash(Message))$

5.4.4 Public Key Infrastructure

Come detto in precedenza, le PKI occorrono per operare la giusta delega di responsabilità, nell'atto della consegna delle chiavi crittografiche. L'utilizzo di queste deve poi essere svolto tramite SSL-TLS, tipicamente. Devono essere presenti i seguenti componenti:

Componente	Sigla	Utilizzo
Certification Authority	CA	responsabile dell'intero ciclo di vita dei certificati
Registration Authority	RA	cui può essere delegata l'identificazione del richiedente ed il conseguente "link" alla chiave pubblica
Certificate Revocation List	CRL	
Certification Practice Stetement	CPS	elenco delle regole che governano l'emissione dei certificati
Certificate Repository	CR	archivio dei certificati
Key History Managment		
Key BackUp & Recovery		
TimeStamping		

5.5 Physical Security

5.5.1 Power

5.5.1.1 Power Threats

Total Failure: mancanza totale di corrente

BrownOut: diminuzione duratura del livello di tensione

Sag: diminuzione rapida e temporanea della tensione

Spike:

Surge:

ElectroMagnetic Interference:

5.5.1.2 Rimedi

UPS: Uninterrutable Power Supply

PCS: Power Conditioning System (per Sag, Spike, Surge)

Generator: generatore autogeno

5.5.2 Environmental

Umidità: tra il 40% ed il 60%

Temperatura: tra i 70°F ed i 74°F

5.5.3 Fire

5.5.3.1 Sensori

Smoke Detector:

Heat-Activated Detector:

Flame-Activated Detector:

5.5.3.2 Fire Suppression System

Water Sprinklers:

Water Dry Pipe: sono considerati i migliori sistemi (purchè accompagnati da un meccanismo di distacco della corrente elettrica)

Halon: interferisce con la reazione chimica. Sostituito con altri gas: FM-200, NAF SIII, NAF PIII

CO2: elimina l'ossigeno presente (dannoso per l'uomo: provoca soffocamento)

5.5.4 Physical Access

5.5.4.1 Access Control

Access Policy: identificazione delle persone

Visitor Logging: tracciamento degli individui che accedono

Escorting Visitor: gli individui che accedono sono accompagnati ed osservati di continuo

5.5.4.2 Biometric

False Rejection Rate: percentuale di mancato riconoscimento di individui che hanno diritto ad accedere

False Acceptance Rate: percentuale di riconoscimmenti di individui che non hanno diritto ad accedere

Equal Error Rate: percentuale in cui FRR e FAR sono uguali