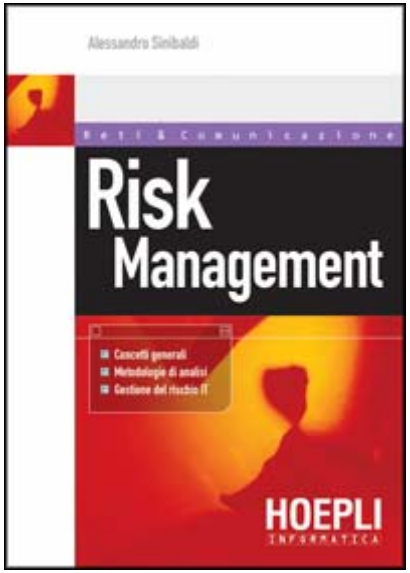


Risk management

Concetti e Metodologie

(a cura di **Alessandro Sinibaldi – CISSP, Assistente CC, MCSE: Security, CEH, OCP, CWSP, ...**)

INDICE DELLA PRESENTAZIONE :

Parte I

1. Cosa è il Rischio
2. Processi e Asset
3. Minacce
4. Vulnerabilità
5. Contromisure
6. Rischio

Parte II

7. Mehari
8. Octave
9. Cramm
10. Coras
11. Ebios

- Conclusioni
- Riferimenti bibliografici e sitografici
- Varie – Q&A

Cosa è il Rischio

Dato un obiettivo, inteso come opportunità, che vogliamo raggiungere, ci sono infinite variabili, nascoste o meno, che possono far sì che l'obiettivo sia solo parzialmente raggiunto o non sia raggiunto affatto.

Il mondo reale non è il mondo astratto modellizzato dai fisici, ma è un mondo stocastico, dominato dalla statistica e dalla complessità. E' il regno della probabilità.

Il Rischio è la possibilità che qualcosa non vada come previsto e che intervengano fattori che potrebbero portare alla diminuizione del Valore.

Cosa è il Rischio

Il raggiungimento di un obiettivo prevede l'esecuzione di un'attività, di cui generalmente, ci facciamo un modello.

Devo andare a comprare il pane…

Esco di casa e chiudo la porta a chiave

↓

Scendo le scale

↓

Vado al negozio più vicino

↓

Compro il pane

↓

Ritorno a casa

Ops..la chiave si rompe nella toppa!!

Ops..la portiera ha dato la cera. Scivolo e mi rompo una gamba!

Oggi è ferragosto! Tutti i negozi sono chiusi!

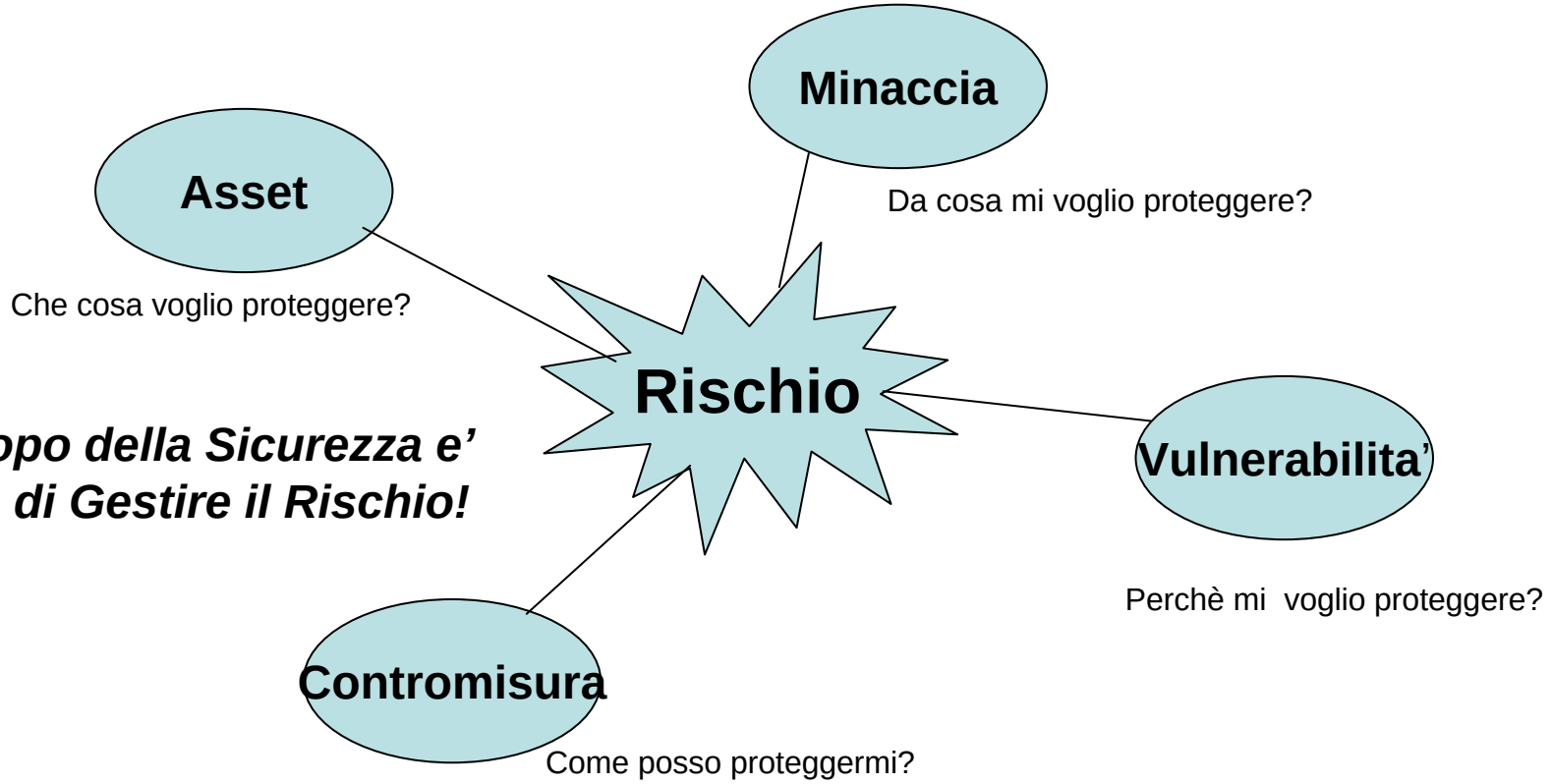
Ma che sbadato! Ho dimenticato il portafoglio a casa!!

Si rompe la busta del pane e finisce in una pozzanghera

Cosa è il Rischio

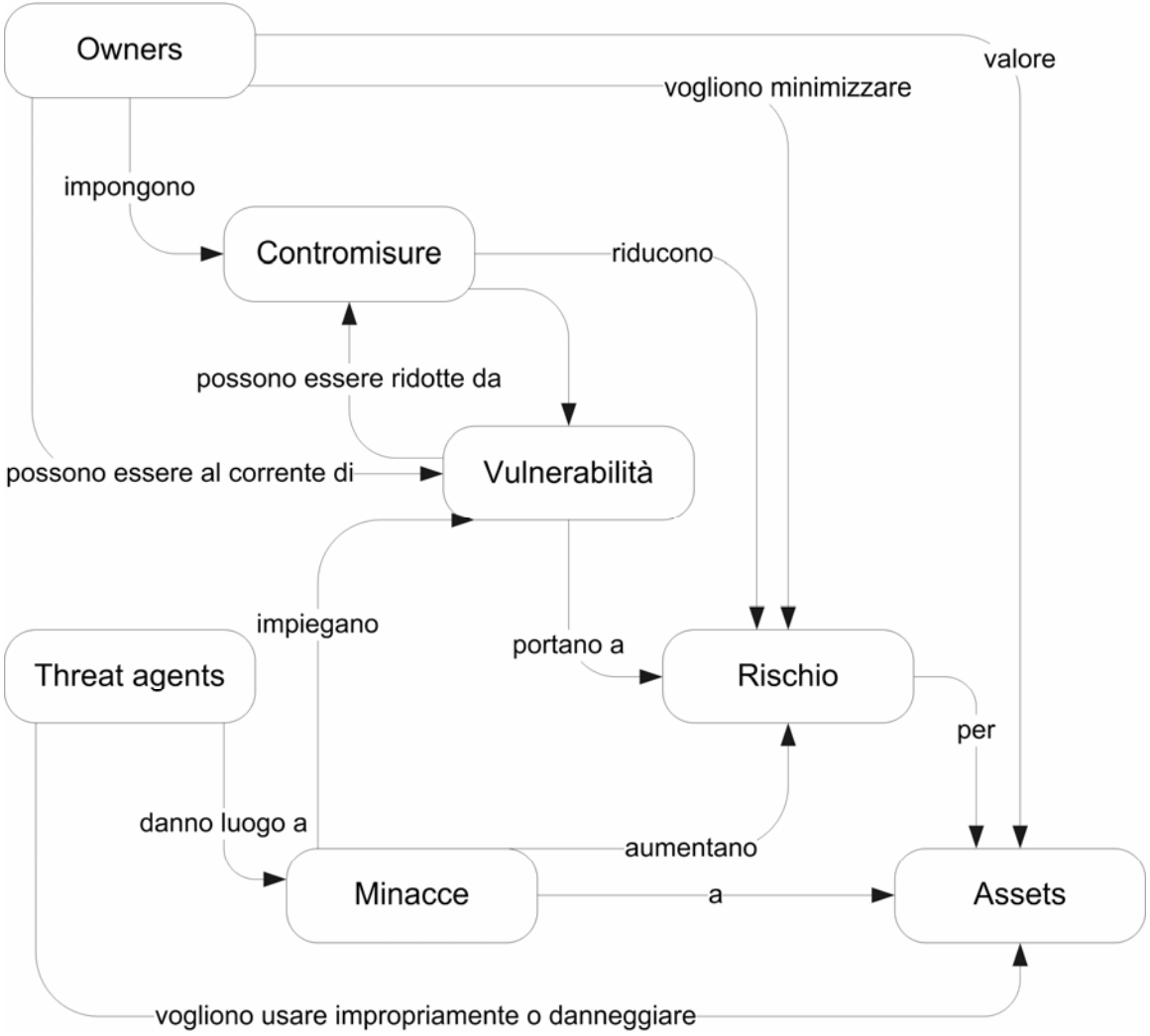
Il Rischio sta lì a ricordarci di tutte le cose che ci stiamo dimenticando di considerare…

Per questo, il Rischio non può essere evitato, può solo essere minimizzato! Dopo ciò, esistono solo due strade: accettarlo o trasferirlo (ad esempio con un'assicurazione).



Lo scopo della Sicurezza e' quello di Gestire il Rischio!

Gli attori nella gestione del Rischio



Gli Asset

Sono ciò che vogliamo proteggere.

Nell'Era dell'Informazione, gli Asset sono l'**informazione** stessa, che viene creata, elaborata e distrutta dai processi organizzativi.

Di riflesso, un asset è qualsiasi cosa attraverso cui l'informazione transita, nasce o muore e quindi **Server**, **Reti**, **Persone**, **Documenti**….

Il primo passo è quello di capire che cosa è un Asset, cioè cos'è che porta Valore per l'azienda. è la mia Reputazione? E' il database dei clienti? Sono i servizi che erogo? Sono le persone con cui lavoro?

Ma per capire che cosa voglio proteggere, devo prima capire che cosa faccio, cioè i processi che costituiscono il modo in cui faccio Business…

I processi

I processi si dividono in:

- ***Processi strategici***
  - ***Processi competitivi:*** processi con cui l'organizzazione compete sul mercato e con i quali mira a superare la concorrenza (es. fidelizzazione del cliente, elaborazione strategie, individuazione delle esigenze del cliente)
  - ***Processi di innovazione e trasformazione:*** processi che forniscono le capacità richieste per il futuro (es. innovazione prodotti/servizi, investimenti strategici)
- ***Processi operativi:*** processi che realizzano i prodotti/servizi dell'organizzazione (es. gestione marketing e vendite, produzione/erogazione servizi, gestione della logistica)
- ***Processi di supporto:*** processi che aggiungono efficienza ed efficacia ai processi operativi (es. gestione risorse umane, gestione finanza e amministrazione, gestione servizi IT)

I processi

Nell'analisi dei processi aziendali è importante raccogliere le seguenti informazioni:

•definire lo ***scopo*** del processo;
•definire il ***responsabile*** del processo;
•stabilire inizio e fine del processo (***delimitazione*** del processo);
•identificare il ***cliente*** del processo;
•specificare l'***output*** del processo;
•definire gli ***input*** del processo;
•definire i ***fornitori*** degli input;
•verificare i ***vincoli, le leggi e i regolamenti***;
•stabilire i ***controll***i da effettuare;
•identificare le ***infrastrutture*** necessarie per produrre l'output;
•identificare le ***risorse umane*** necessarie e i livelli di competenza richiesti;
•identificare i ***sottoprocess***i;
•evidenziare se ***l'output del processo costituisce l'input*** per un altro processo.

I processi

Il passo successivo è la determinazione dei ***processi critici***. Definiremo come processi critici, quei processi tali che:

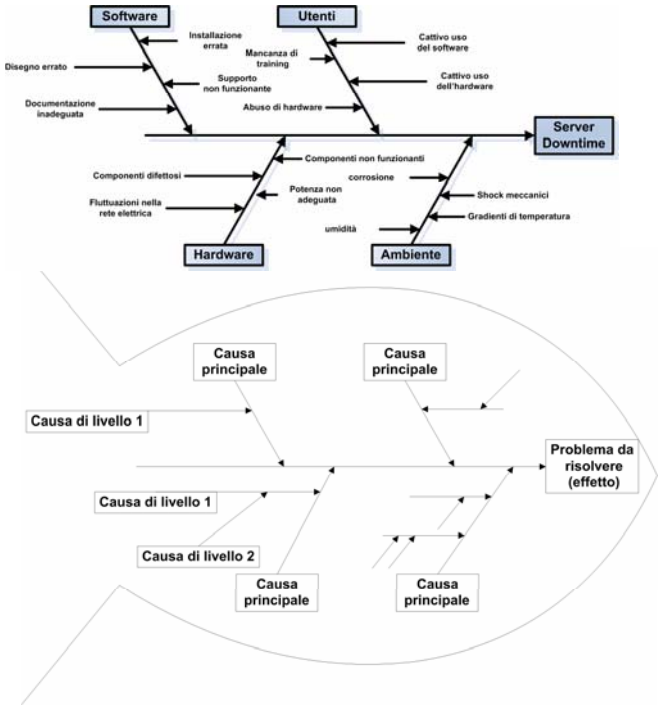
•l'output è utilizzato da più processi
•l'output ha valore per l'azienda.
•Il processo riceve molti input
•il numero di sottoprocessi che lo compongono è elevato

A queste definizioni, aggiungendo in più le variabili tempo, costo, qualità possiamo aggiungere le seguenti:

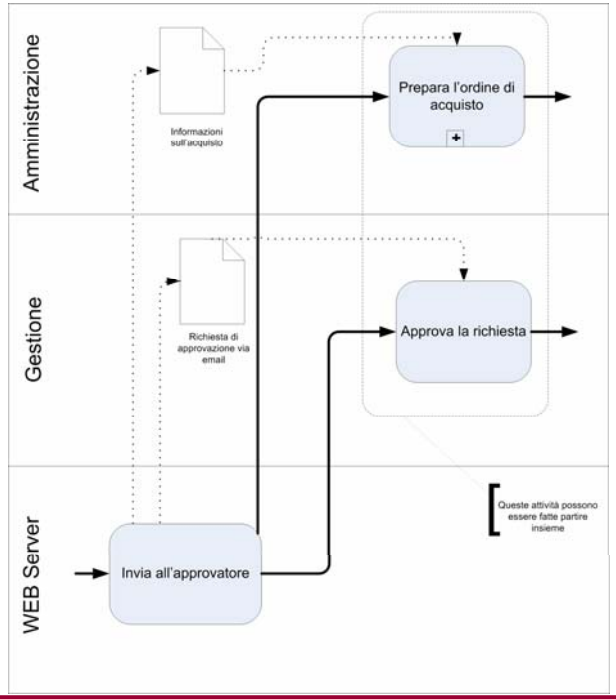
•l'output deve essere generato a partire dagli input in un tempo determinato
•l'output deve essere generato con una qualità determinata
•l'output deve essere generato con un costo massimo per l'azienda

Gli strumenti di analisi dei processi

- Business Process Diagrams
- Demo Diagrams
- Design Structure Matrix (analisi delle dipendenze tra processi)
- Diagrammi causa effetto o diagrammi di Ishikawa o diagrammi a lista di pesce

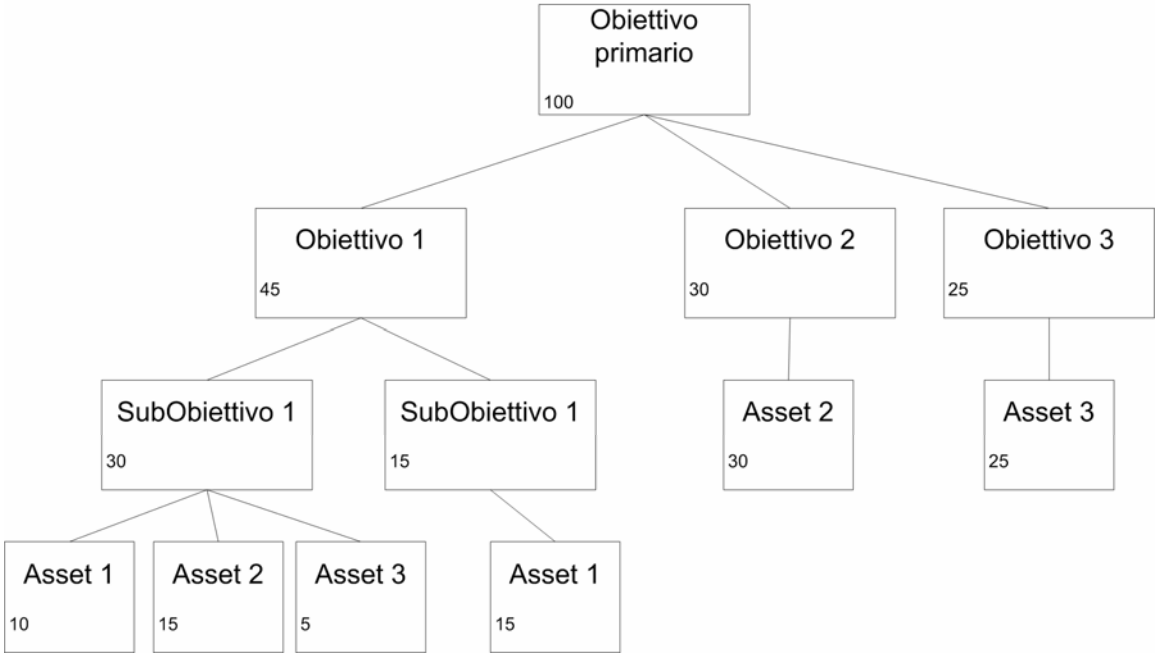


	P1	P2	P3	P4	P5	P6	P7	P8	P9	E1
P1										X
P2	X									
P3		X								
P4		X								
P5		X								
P6			X							
P7						X				
P8							X			
P9								X		



La dipendenza dei processi dagli asset

Una volta chiarita la differente importanza e priorità dei processi aziendali, il passo successivo è quello di capire da quali asset I processi dipendono in modo più o meno critico.
Un buono strumento da utilizzare per la documentazione sono i **Mission Trees**



Gli Asset

Abbiamo detto che gli Asset sono quelle entità entro le quali risiede il Valore per l'azienda.

Ma più precisamente…quali sono le caratteristiche/attributi dell'asset che portano valore?

- Integrità
- Disponibilità
- Confidenzialità
- Privacy
- ……

Esempio: il file delle paghe dei dipendenti – è più importante che non venga alterato in modo improprio, che non venga letto da chi non dovrebbe o che sia sempre disponibile all'applicazione per la gestione degli stipendi? Che peso attribuireste agli attributi del file?

Classificazione degli Asset

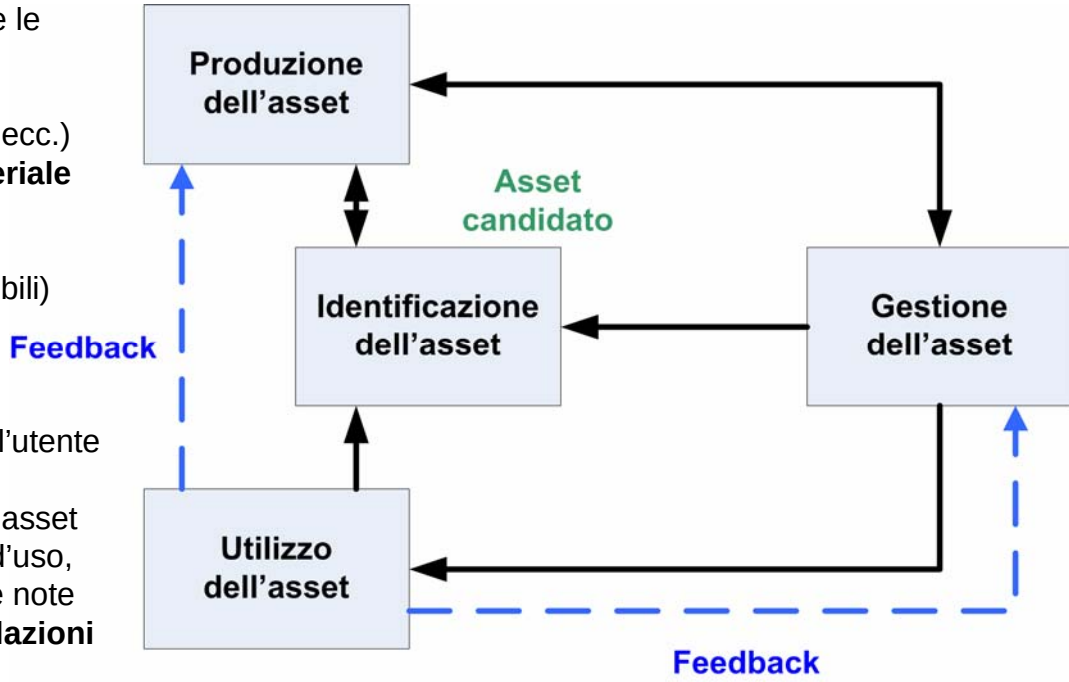
Dal momento che gli asset sono al centro delle strategie di sicurezza, la prima cosa da fare è conoscerli e catalogarli. Gli asset possono essere classificati in vari modi, usando uno o più attributi:

- per valore (economico e non)
- per dislocazione geografica
- per importanza e/o occorrenza nei processi
- per proprietario (ownership)
- per marca/produttore
- per capacità e/o prestazioni
- per data (ad es. di acquisto)

Asset Management

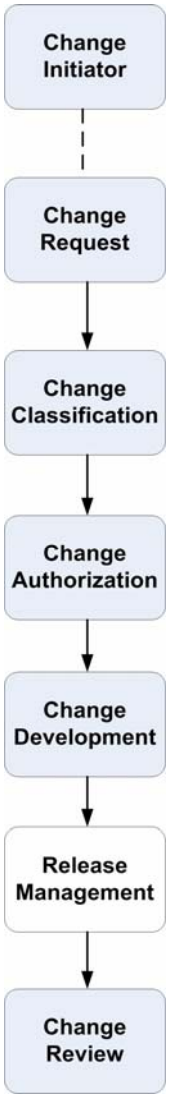
Un applicativo di asset management dovrebbe possedere le seguenti caratteristiche:

•Dare la possibilità all'utente di definire **campi/attributi personalizzati** (es. data di acquisto, numero di contratto ecc.)
•Generazione automatica o inserimento manuale di un **seriale** crescente di identificazione dell'asset
•**Viste configurabili** dall'utente (l'utente dovrebbe poter selezionare quali campi visualizzare tra tutti quelli disponibili)
•Deve gestire lo **storico** dell'asset
•Deve tener traccia della **posizione** dell'asset
•Deve tener traccia dello **stato** dell'asset
•Deve classificare l'asset in base a un **criterio scelto** dall'utente (ad es. per tipo, valore ecc.)
•Dovrebbe permettere di aggiungere alla descrizione dell'asset un'eventuale immagine, dei **documenti** (ad es. manuali d'uso, digitalizzazione di fatture di acquisto, schemi ecc.) e delle note
•Dovrebbe permettere di gestire/visualizzare eventuali **relazioni tra gli asset**
•Dovrebbe poter permettere di identificare i **proprietari/responsabili** dell'asset e l'eventuale unità/divisione di appartenenza
•Dovrebbe permettere di effettuare una **ricerca** sull'intera base dati tramite criteri specificati dall'utente, eventualmente anche sui documenti allegati all'asset
•Dovrebbe poter permettere di fare della **reportistica**.
•Dovrebbe specificare vari **ruoli** per gli utenti con privilegi diversi



IRM http://irm.stackworks.net
HYPERIC HQ http://www.hyperic.com/
Remedy Asset Management http://www.remedy.com
HP Openview Asset Center http://h20229.www2.hp.com/
Assyst http://www.axiossystems.com

Change Management

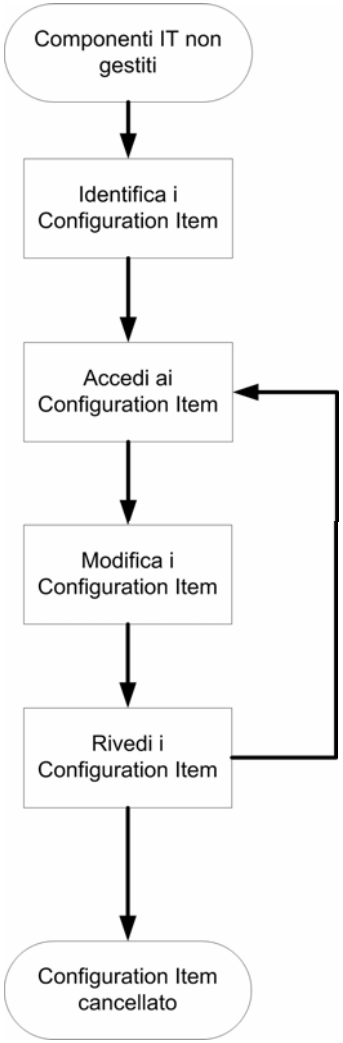


Tra le funzionalità previste dal sistema di change management ci dovrebbero essere:

- integrazione col sistema di asset management
- possibilità di gestire/modificare la priorità della RFC
- possibilità di modificare il tipo della RFC
- possibilità di gestire nell'applicativo varie tipologie di utenti
- realizzazione di workflow di approvazione ad hoc
- possibilità di allegare alla RFC la documentazione a corredo
- gestire lo storico dei cambiamenti (funzionalità che può essere condivisa/demandata al sistema di asset management)

Configuration Management

Configuration Management è il processo che deve identificare, controllare e tracciare tutte le versioni di hardware, software, documentazione, processi e procedure dell'organizzazione. Lo scopo è far sì che solo i componenti autorizzati siano usati e che tutti i cambiamenti vengano registrati e tracciati durante tutto il ciclo di vita del componente.



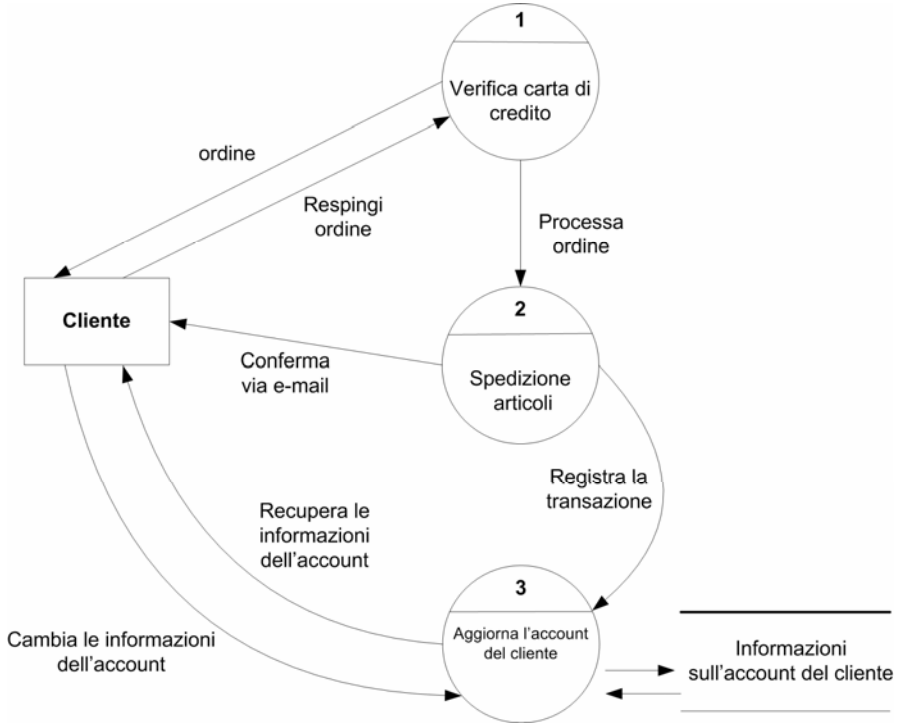
Cmdbuild http://www.cmdbuild.org
Netdirector http://www.netdirector.org
Controltier http://open.controltier.com
Lcfg http://www.lcfg.org
Microsoft SMS http://www.microsoft.com/italy/smserver

http://www.microsoft.com/italy/mom

Il Flusso dell'Informazione

Gli Asset danno l'informazione *statica*, ma ora ci serve anche l'informazione *dinamica*: coem si muove l'informazione all'interno dell'organizzazione?

Lo strumento ideale sono i **Data Flow Diagrams**

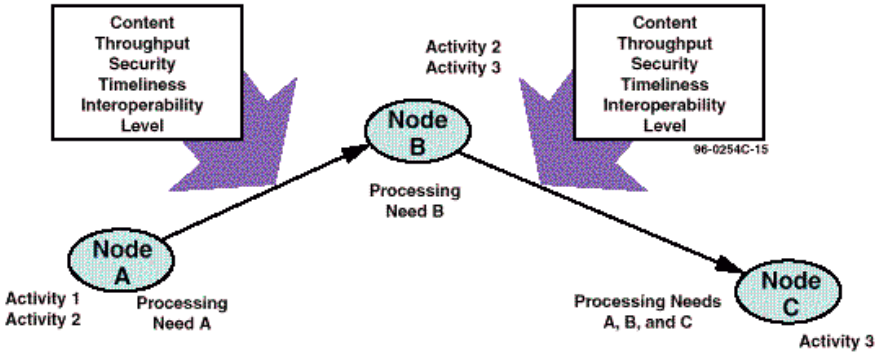


Il ***threat path*** viene definito come la sequenza dei nodi del processo che fanno un processamento dei dati critico per la sicurezza.

Il Flusso dell'Informazione

Ma ci servono anche altre due informazioni:

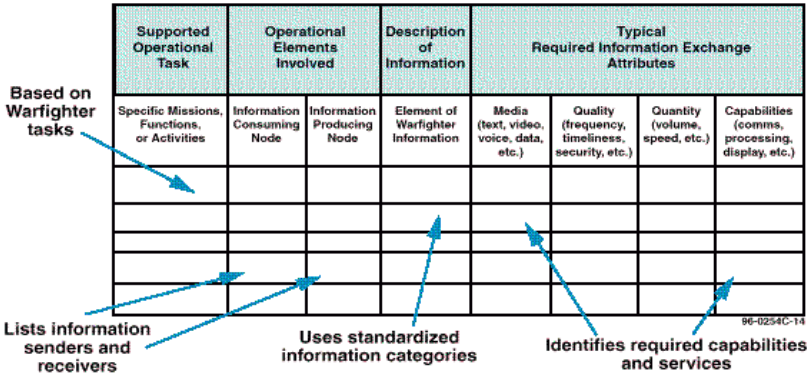
- ***Chi è connesso a chi?*** Node connectivity diagrams
- ***Chi scambia dati con chi?*** Information Exchange Matrix



Features:

- Provides graphic depiction of information exchanges and required capabilities
- Level of detail shown driven by purpose of particular architecture

Figure 4-6: Node Connectivity Diagram



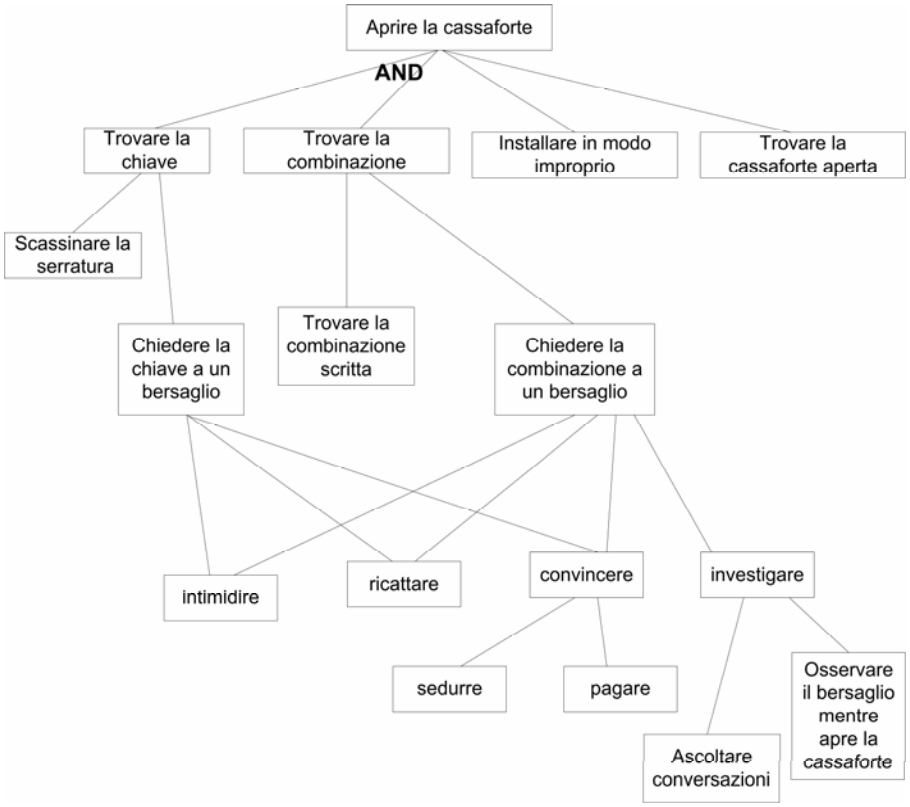
Features:

- Focuses on information content, flows, and supporting services required to accomplish operational tasks
- Level of detail shown depends on purpose of architecture

Figure 4-5: Information Exchange Matrix

Le minacce (threats)

Un pericolo, o minaccia, o *threat*, è la capacità da parte di un' entità (o ***Threat Agent***) di far leva su una vulnerabilità del sistema per esercitare un'azione con effetti potenzialmente negativi. Un buono strumento per descriverli è quello degli **Attack Trees**.



OpenFTA
(http://www.openfta.com/)

AttackTree+
(http://www.isograph-software.com/atpover.htm)

SecureiTree
(http://www.amenaza.com).

Alcuni di questi applicativi permettono di effettuare il ***pruning*** degli alberi di attacco. Questa procedura consiste nell'applicare un valore di soglia, ad esempio un valore per il costo necessario per effettuare l'attacco e nel lasciare nel diagramma solo quei cammini di attacco il cui costo totale è minore del valore indicato. Tale valore di soglia viene usato creando un ***Agent Profile***. Esso consiste, di fatto, in una descrizione sommaria dell'attaccante.

Le vulnerabilità

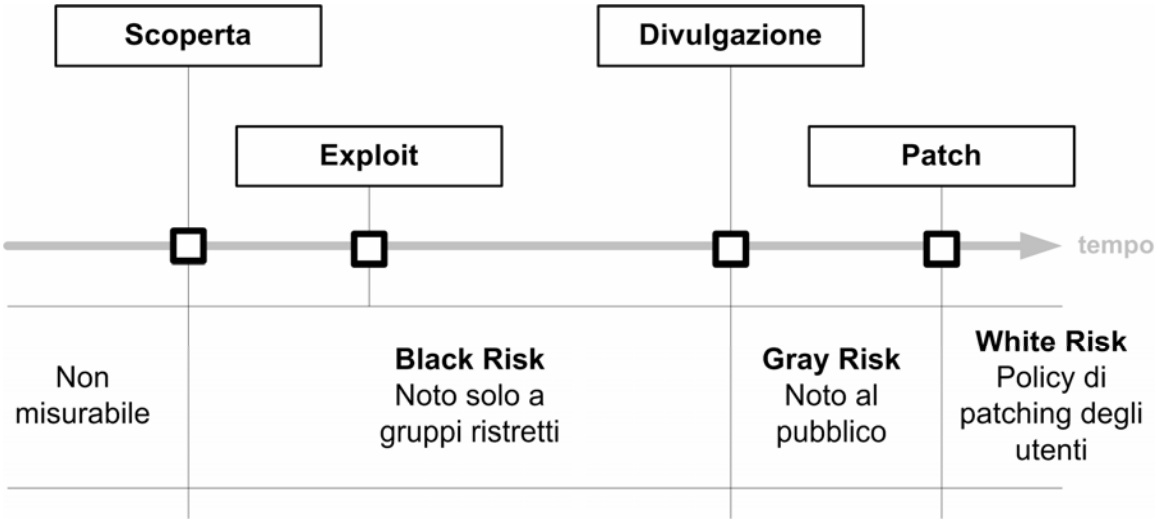
Una vulnerabilità è una debolezza in un asset che un Threat Agent può impiegare per modificare a suo vantaggio la posizione di sicurezza dell'asset, con impatto sugli attributi che ne costituiscono il valore, come la riservatezza, l'integrità, la disponibilità ecc.
Le vulnerabilità possono essere di tre tipi:

- ***Amministrative*** sono relative alle policies e alle procedure di sicurezza
- ***Fisiche*** sono le vulnerabilità relative alle persone, ai luoghi geografici e agli apparati fisici
- ***Tecniche*** sono relative all'aspetto tecnologico, cioè errori di configurazione di apparati, backdoor, password deboli ecc.

Il **potenziale d'attacco** rappresenta la "barriera" che un attaccante deve superare per poter sfruttare una vulnerabilità. Esso dipende tipicamente da alcuni fattori come:

- Il Tempo necessario per sfruttare la vulnerabilità
- L'Equipaggiamento necessario
- Le Capacità necessarie dell'attaccante
- La Conoscenza del sistema
- L'Accesso al sistema

Le vulnerabilità



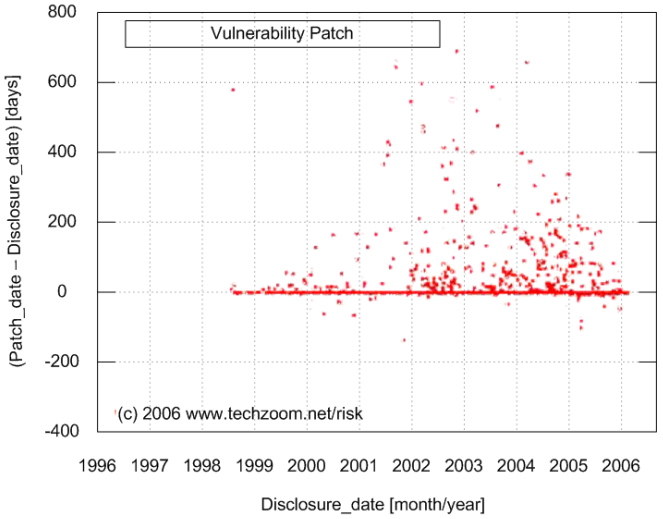
- La vulnerabilità viene scoperta (discovery)
- Il primo exploit viene rilasciato
- Il grande pubblico viene a conoscenza della vulnerabilità (disclosure)
- Viene sviluppata la patch che chiude la vulnerabilità

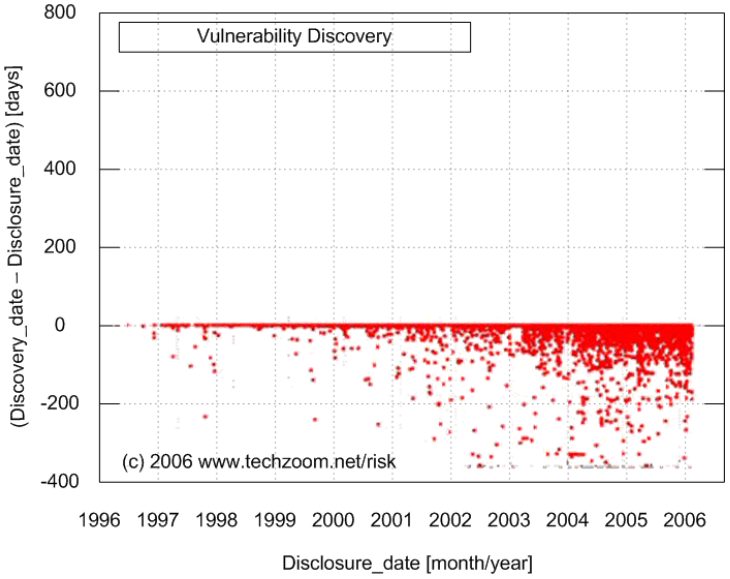
La disclosure è fatta ad opera di quelli che vengono chiamati ***Security Information Providers*** quali:
CERT (Computer Emergency Response Team, USA)
www.cert.org
Secunia (Secunia, Denmark)
www.secunia.com
FrSirt (French Security Incident Response Team, France)
www.frsirt.com
ISS X-Force (Internet Security Systems, USA)
www.iss.net
Securityfocus (Symantec, USA)
www.securityfocus.com
Mitre (Mitre, USA)
cve.mitre.org
OSVDB (Open Source Vulnerability Database, USA)
www.osvdb.org

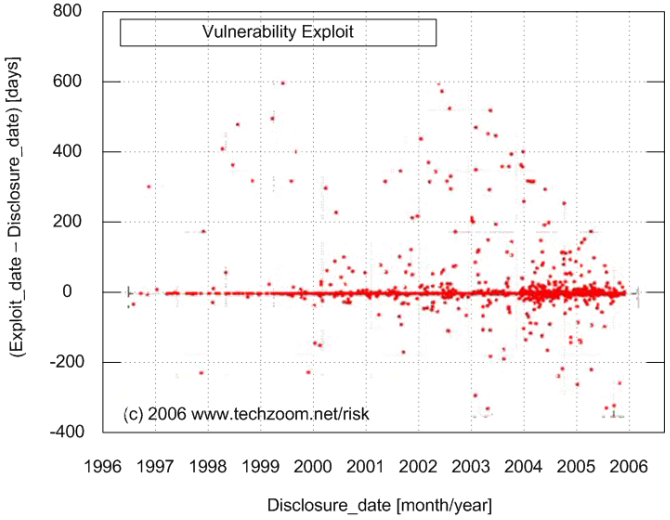
Le vulnerabilità

Questi emettono le cosidette ***Information Assurance Vulnerability*** (IAV) che possono essere di tre tipi:

- **IAV-A** o ***Information Assurance Vulnerability Alerts*** che sono considerate vulnerabilità ad alto rischio e devono essere chiuse entro 30 giorni
- **IAV-B** o ***Information Assurance Vulnerability Bulletins*** che sono cosiderate vulnerabilità a rischio medio
- **IAV-T** o ***Information Assurance VulnerabilityTechnical Advisories*** che sono cosiderate vulnerabilità a rischio basso







I trends delle vulnerabilità

Con il progredire delle tecnologie e l'aumento dell'attenzione in materia sicurezza i nuovi attacchi vanno molto concentrandosi su tre aspetti:

- sfruttano sempre di più ***porte tcp/ip lecite*** per penetrare nella rete e quindi possono essere fermati solo da firewall e contromisure di tipo applicativo (web application vulnerabilities)
- sono sempre più basati su tecniche di ***social engineering*** e sfruttano la complicità, spesso involontaria, di chi sta all'interno per far entrare programmi pericolosi
- ciò a cui tendono spesso è il ***furto dell'identità digitale*** dell'utente (carte di credito, dati personali e sensibili ecc.) oppure la creazione di migliaia di "zombie" (bot networks), cioè di computer infettati che possono agire in determinate circostanze secondo le volontà dell'attaccante e lanciare attacchi massicci contro una vittima determinata.

Le metriche della vulnerabilità

CVSS è nato come linguaggio universale per indicare la severità di una vulnerabilità e aiutare a determinare l'urgenza e la priorità della risposta.

Il punteggio Base rappresenta la ***severità*** della vulnerabilità, il punteggio Temporale la sua ***urgenza***, il punteggio Ambientale la ***priorità*** nella risposta entro l'ambiente dell'utente finale.

Le contromisure

Le Contromisure hanno lo scopo di ridurre il Rischio dovuto alla presenza di Vulnerabilità.
Possono avere vari obiettivi:

- ridurre la probabilità di occorrenza delle minacce
- ridurre le vulnerabilità
- ridurre gli impatti

e possono essere di vari tipi:

- **fisico** (ad es. un cancello, un badge, un estintore ecc.)
- **procedurale** (ad es. il fatto di mostrare un documento all'ingresso, un giro di sorveglianza fatto a orari diversi e non regolari, policies ecc.)
- **tecnico** (ad es. l'installazione di un RAID, un backup ecc.)
- **personale** (ad es. corsi di formazione sulla sicurezza, training specializzato ecc.)

Le contromisure possono essere anche:

- **preventive** (cioè atte a prevenire l'occorrenza del problema)
- **dissuasive** (cioè hanno lo scopo di dissuadere un eventuale attaccante, come una guardia armata, una legge, un cartello ecc.)
- **palliative** (cercano di diminuire l'impatto di un problema)
- **rivelatrici** (cercano di rivelare l'insorgere del problema prima possibile per limitarne l'impatto)
- **protettrici** (cercano di ridurre la vulnerabilità, ad es. dei sacchi di sabbia messi a protezione di una finestra al verificarsi di un uragano)

Livelli di Rischio dal Report di Assessment dei Rischi

Step 1.
Dare una priorità alle azioni

Le azioni vengono classificate con un punteggio che va da High a Low

Report di Assessment dei Rischi

Step 2.
Valutazione delle contromisure raccomandate
- Fattibilità
- Efficacia

Lista delle possibili contromisure

Step 3.
Analisi Costi-benefici
- Impatto dovuto all'implementazione
- Impatto dovuto alla non implementazione
- Costi associati

Analisi Costi-benefici

Step 4.
Selezione delle contromisure

Contromisure selezionate

Step 5.
Assegnazione delle responsabilità

Responsabilità assegnate

Step 6.
Sviluppo di un piano di implementazione delle Contromisure
- Rischi e livello di Rischio associato
- Prioritizzazione delle azioni
- Contromisure raccomandate
- Contromisure selezionate pianificate
- Persone responsabili
- Data di inizio
- Data di completamento degli obiettivi
- Requisiti di Maintenance

Valutazione degli impatti

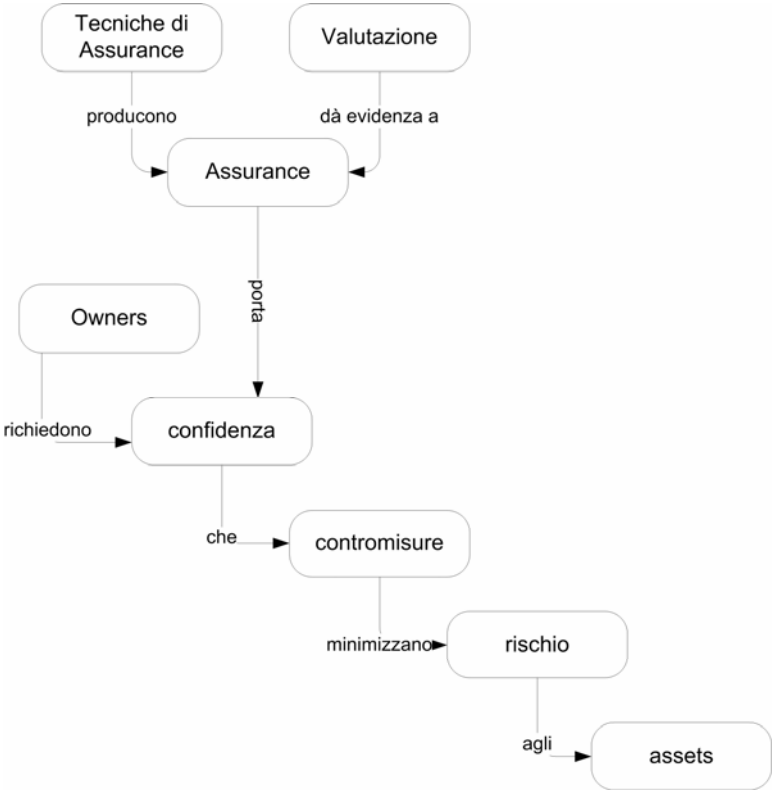
Step 7.
Contromisure selezionate implementate

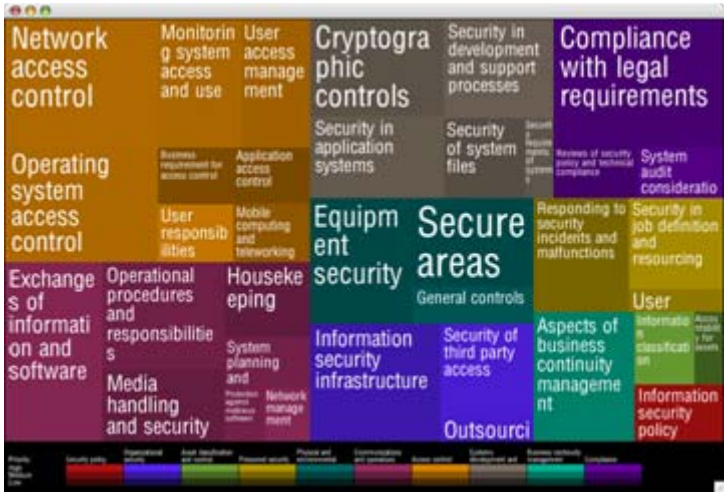
Rischio residuo

Le contromisure

Utilizzo delle best practices

Common Criteria
ISO 17799
ITIL





Le contromisure

Leggi e normative

- **Legge sulla Privacy**
- **Sarbanes-Oxley Act**
- **HIPAA**
- **Basilea 2**

Norme: Legge sulla Privacy

Il Testo Unico della Privacy, o D. Lgs. 196/2003, ha come oggetto il Trattamento dei dati.
In particolare, per ***Trattamento*** si intende qualunque operazione o complesso di operazioni effettuata anche senza l'ausilio di strumenti elettronici, su dati, anche se non registrati in una banca dati (raccolta, conservazione, organizzazione, estrazione, raffronto, utilizzo ecc.).
Per quanto riguarda i dati, essi sono suddivisi nelle seguenti categorie:

- ***dati personali*** qualunque informazione relativa a persona fisica o giuridica, ente o associazione, identificati e identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
- ***dati identificativi*** dati personali che permettono l'identificazione diretta dell'interessato
- ***dati sensibili*** dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ***dati giudiziari*** dati personali idonei a rivelare provvedimenti [..] in materia di casellario giudiziario, di anagrafe delel sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- ***dati anonimi*** dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

La legge individua quattro tipologie di soggetti:

- ***l'interessato*** la persona fisica o giuridica, l'ente o l'associazione cui si riferiscono i dati personali
- ***il titolare*** la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
- ***il responsabile*** la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali
- ***gli incaricati*** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Norme: Sarbanes-Oxley act

Il Sarbanes-Oxley Act è stato approvato dal Congresso degli Stati Uniti nel 2002, in risposta al numero sempre crescente di frodi finanziarie.
Lo scopo della legge è quello di proteggere gli investitori richiedendo l'accuratezza, l'affidabilità e la tracciabilità del materiale (documentazione, bilanci ecc.) pubblicamente emesso dall'azienda.
Questo Atto ha stabilito una maggiore indipendenza degli Audits (allo scopo di evitare intimidazioni e inganni nei confronti degli Auditors) e una responsabilità personale penale del Management dell'Azienda.
Pur partendo da un ambito prettamente finanziario, la legge ha ricadute pure sulla Gestione dell'ambito IT (sezione 404) ed è concentrata sui controlli interni. Da questo punto di vista, essa trova una naturale partnership in metodologie come COBIT e COSO.
Un controllo interno è visto come un processo, sotto la responsabilità del Management, volto ad assicurare:

- efficienza ed efficacia dei processi operativi
- affidabilità dei reports finanziari
- conformità alle leggi e regolamenti applicabili

I dati finanziari, in quanto parte dei dati informativi dell'azienda, si trovano sui server aziendali. In questo senso, è cruciale garantirne l'integrità. Così, l'ambiente IT deve essere protetto e oggetto di controlli e monitoraggio.

Norme: HIPAA

La Health Insurance Portability and Accountability Act del 1996 (HIPAA) comprende una serie di regole per standardizzare la comunicazione dell'informazione sulla salute in formato elettronico tra medici e assicuratori. Oltre a ciò, vengono espresse regole per proteggere la privacy e la sicurezza di informazioni sulla salute che portino all'identificazione dell'individuo.
La natura dell'informazione (Protected Health Information) trattata da HIPAA è tale che:
permette l'identificazione dell'individuo

- si riferisce allo stato di salute presente, passato o futuro
- si riferisce alla fornitura di cure mediche all'individuo
- si riferisce al pagamento delle cure mediche presenti, passate e future prestate all'individuo

La legge copre tutti coloro che generano o trattano informazioni legate alla salute dell'individuo.

Norme: Basilea 2

Basilea 2 è un sistema di regole volte ad assicurare la stabilità patrimoniale delle banche, a garanzia del risparmiatore. È un accordo firmato dai governatori delle Banche centrali dei G10 nel 2004 e che entrerà in vigore il 1 gennaio 2007. Di fatto esso stabilisce le condizioni per cui una banca possa essere considerata patrimonialmente solida. Basilea 2 nasce sulle basi di un precedente accordo, Basilea 1, firmato nel 1988.
I tre concetti fondamentali sono:
le Banche, nel corso della loro attività si assumono dei rischi, che possono essere di tre tipi:

- ***Rischio di credito*** è il rischio a cui si espone la Banca a fronte della sua attività creditizia ed è funzione dell'eventuale insolvibilità dei suoi clienti
- ***Rischio di mercato*** è il rischio di perdita, a cui è esposta la Banca, per effetto di congiunture sfavorevoli di mercato, investimenti poco redditizi, tassi di interesse crescenti e così via
- ***Rischio operativo*** è il rischio di perdite, a cui la Banca è esposta, per effetto dell'ineguatezza e del malfunzionamento di procedure, risorse umane e sistemi interni o per l'accadimento di eventuali eventi esterni

Ogni Banca, in funzione del Rischio a cui è esposta, deve mettere da parte un capitale minimo definito
Patrimonio di Vigilanza
Il Patrimonio di Vigilanza deve almeno essere superiore all'8% del valore ponderato per il Rischio.

Il Rischio

Il Rischio è una funzione di:

- il valore monetario dei suoi assets (A)
- le vulnerabilità (V)
- le minacce potenziali e la loro natura (T)
- la natura e l'intenzione dell'impatto (I)

Quindi R=f(A,T,V,I).

Una semplice espressione per la funzione f è data dal seguente ragionamento.

I due ingredienti fondamentali sono la **probabilità** e l'**impatto** che sono rispettivamente espressi dalle quantità

ARO Annualized Rate of Occurrence

che rappresenta la probabilità che il rischio si verifichi in un anno

SLE Single Loss Expectancy

che rappresenta la perdita di valore di un asset in seguito alla realizzazione di una minaccia

A questo punto possiamo calcolare

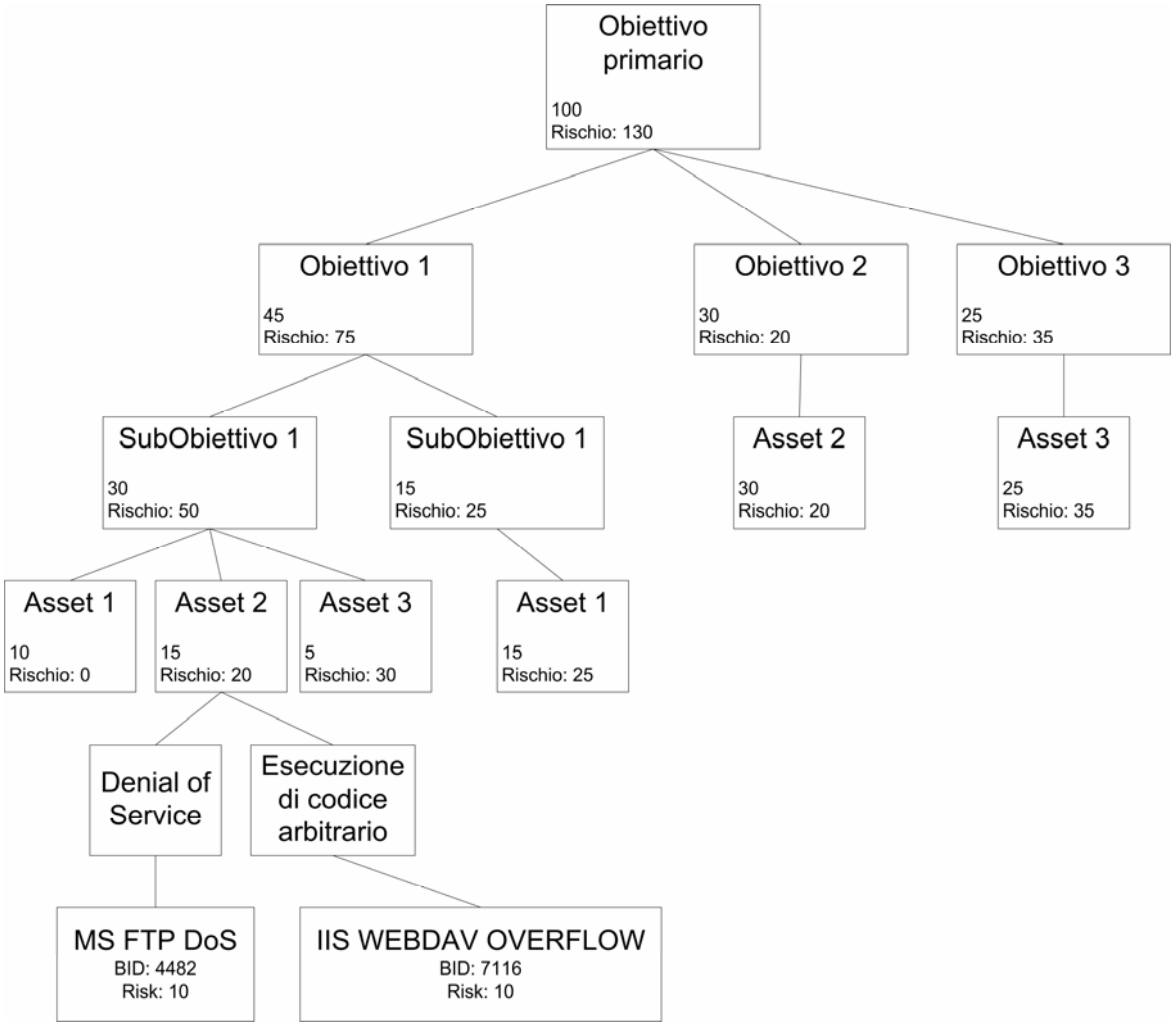
ALE Annual Loss Expectancy = **ARO x SLE**

che rappresenta la perdita monetaria attesa in un anno per effetto del verificarsi della minaccia

L'ALE è il valore che va confrontato con la spesa annua per la sicurezza per calcolare il ROSI (Return of Security Investment)

Relazione tra Rischio, Asset e Processi

Nel **Risk Tree** si associano gli assets con i possibili Threats e questi alle vulnerabilità. In base all'importanza delle vulnerabilità, si associano quindi i valori, in modo analogo a quanto si fa con i Mission Trees.



Le metriche del Rischio

Le metriche sono strumenti disegnati per facilitare il processo decisionale. Esse sono normalmente basate sulla raccolta e l'analisi di dati relativi alle performance.

Il loro scopo è quello di:

- confrontare la stessa situazione in momenti diversi e quindi di definire il concetto di ***Degradazione della Sicurezza****;*
- ***Confrontare*** realtà diverse e quindi anche di capire l'importanza di scelte diverse in ambito sicurezza che varie organizzazioni possono fare
- facilitare il compito di ***Procurement***, cioè di acquisire le risorse necessarie per migliorare la propria posizione di sicurezza
- seguire meglio l'***Evoluzione*** della sicurezza in azienda e di capire se si sta andando nella direzione voluta

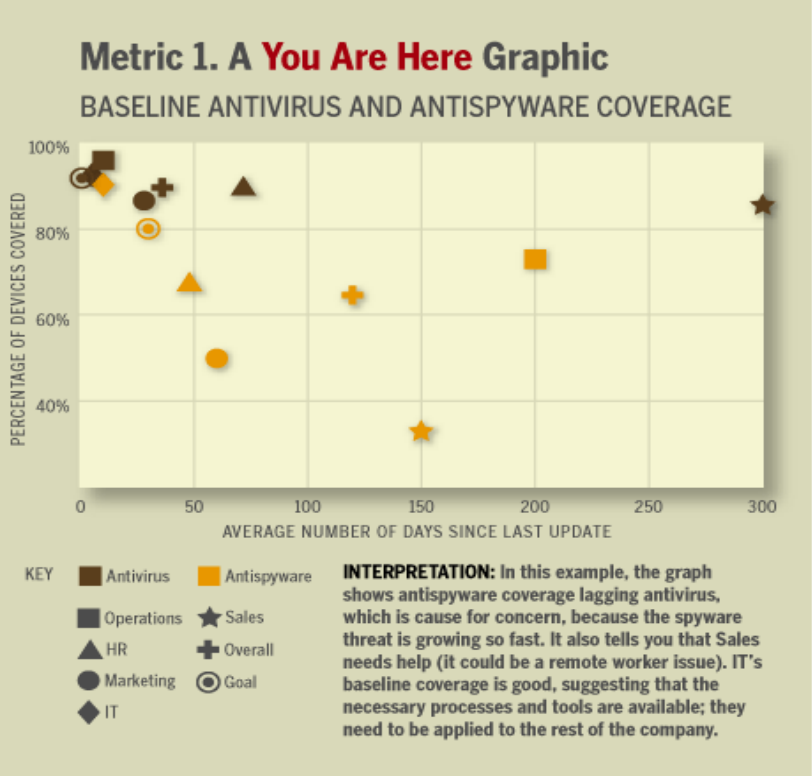
Le metriche del Rischio

Una buona metrica dovrebbe avere queste caratteristiche:

- i ***criteri*** che la definiscono devono essere ***oggettivi e ripetibili***
- deve essere ***facile*** da raccogliere (possibilmente con strumenti automatizzati)
- deve contenere ***unità di misura*** e scale numeriche
- essere espressa con un ***numero***
- un plus è che possa essere facilmente ***comprensibile***

Alcune metriche suggerite sono:

- protezione da virus e spyware, espressa come percentuale di sistemi protetti
- latenza delle patch, cioè tempo che intercorre tra il rilascio di una patch e la sua installazione
- complicazione delle password, espressa come tempo richiesto per indovinare una password con strumenti adeguati
- rispetto delle best practice espresso come percentuale dei sistemi contenuti in varie fasce di compliance
- monitoraggio del traffico di email in funzione del tempo
- monitoraggio del rapporto tra email legittime e spam in funzione del tempo
- numero di tentativi di login falliti in funzione del tempo

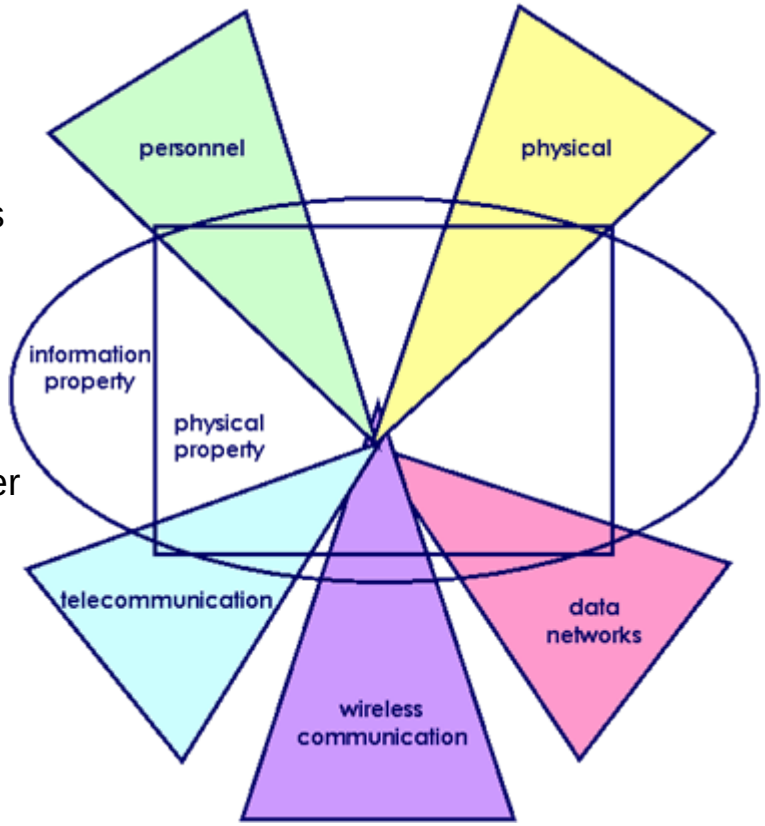


Il controllo del Rischio

- Audit (es. test con OSSTMM)
- Governance (COBIT)

OSSTMM è una metodologia technology-oriented, basata su metriche, per fare tests di sicurezza.
Un test dovrebbe essere:
- **quantificabile**
- **consistente e ripetibile**
- **valido nel tempo**
- basato sull'**abilità** dell'analista e del tester e non sui tools utilizzati
- **rispettoso** delle leggi e dei regolamenti
- **completo**

Un sistema, oggetto di valutazione di sicurezza, è visto come un blocco con dei punti di accesso attraverso cui interagisce con l'esterno.



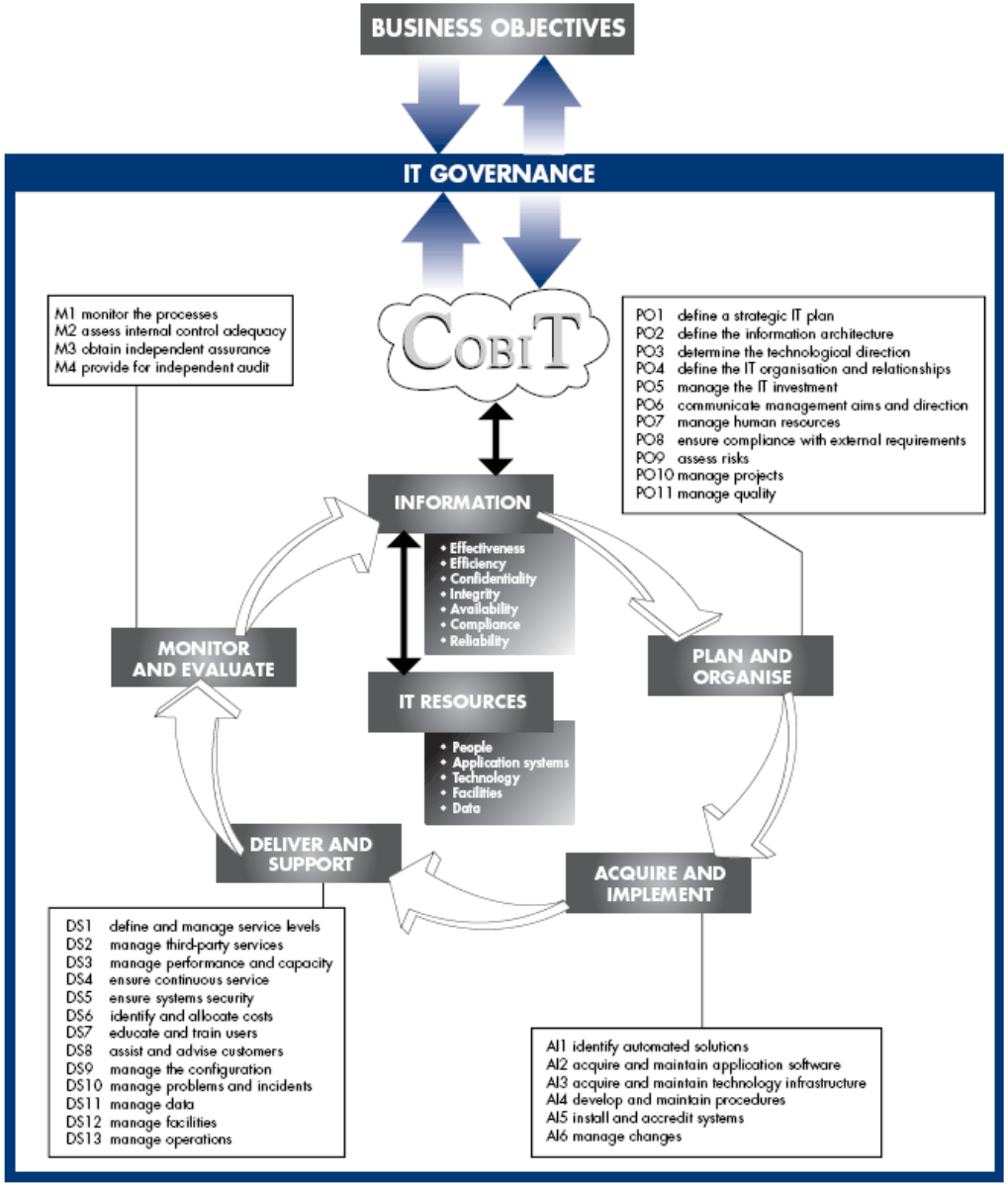
I tests sono raggruppati in 6 canali o sezioni, che si sovrappongono parzialmente. Ogni canale rappresenta un modo di accedere al sistema. Ogni sezione contiene moduli e i moduli contengono tasks. Questi ultimi sono i singoli tests.

Il controllo del Rischio

COBIT (Control Objectives for Information and related Technology) è un framework per sviluppare e gestire controlli interni e livelli di sicurezza appropriati in Information technology.

Un ***Controllo*** è definito come l'insieme delle policies, delle procedure, delle pratiche e delle strutture organizzative che hanno lo scopo di fornire una ragionevole confidenza che gli obiettivi di business saranno raggiunti e gli eventi indesiderati saranno prevenuti o rivelati e corretti.

L'***IT governance*** è definita come la struttura di relazioni e processi per dirigere e controllare l'organizzazione allo scopo di raggiungere gli obiettivi di business.



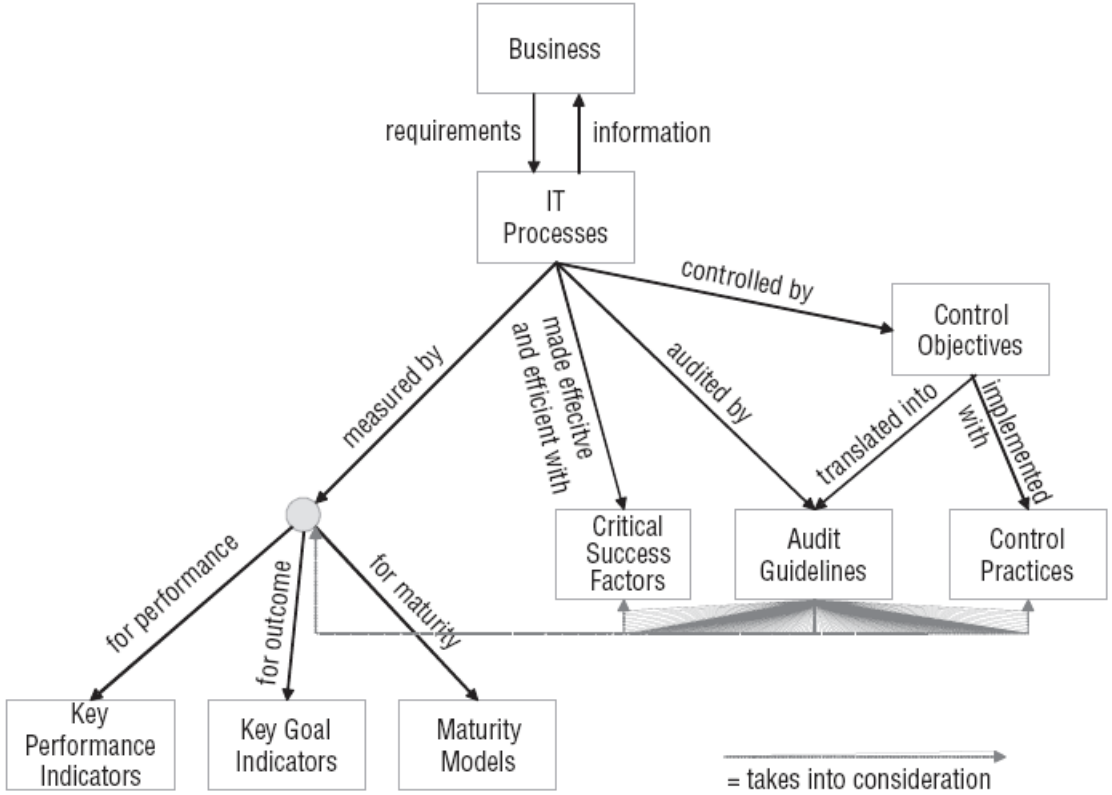
Il controllo del Rischio

Maturity Models – è un modo di dare un punteggio, da 0 a 5, alla maturità dei processi IT di un'organizzazione. I cinque livelli sono: Non esistente (0), Iniziale (1), Ripetibile (2), Definito (3), Gestito (4), Ottimizzato (5).

Critical Success factors (CSFs) – definiscono le azioni più importanti che il management deve intraprendere per avere il controllo sui processi IT.

Key Goal Indicators (KGIs) – sono misure che dicono al management se un processo IT ha ottenuto i suoi requisiti di business.

Key Performance Indicators (KPIs) – sono misure che indicano quanto bene un processo IT sta raggiungendo il suo scopo.



INDICE DELLA PRESENTAZIONE :

Parte I

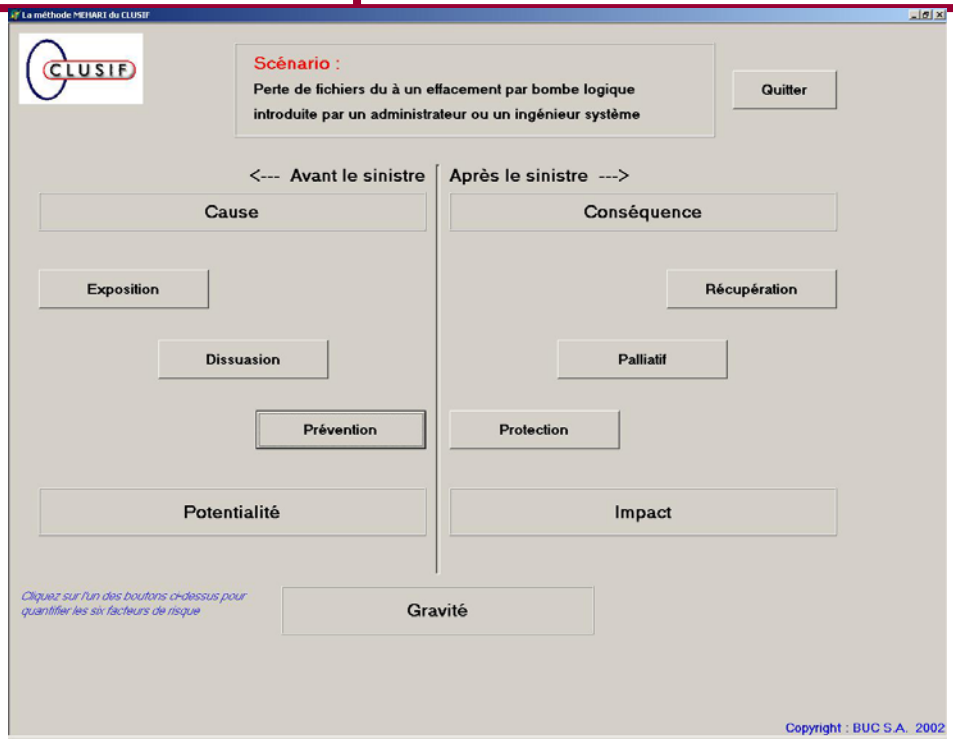
1. Cosa è il Rischio
2. Processi e Asset
3. Minacce
4. Vulnerabilità
5. Contromisure
6. Rischio

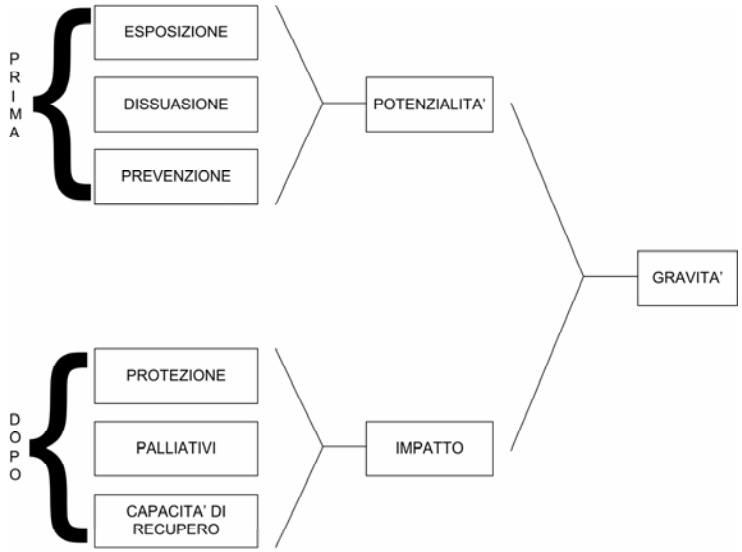
Parte II

7. Mehari
8. Octave
9. Cramm
10. Coras
11. Ebios

- Riferimenti bibliografici e sitografici
- Varie – Q&A

Mehari



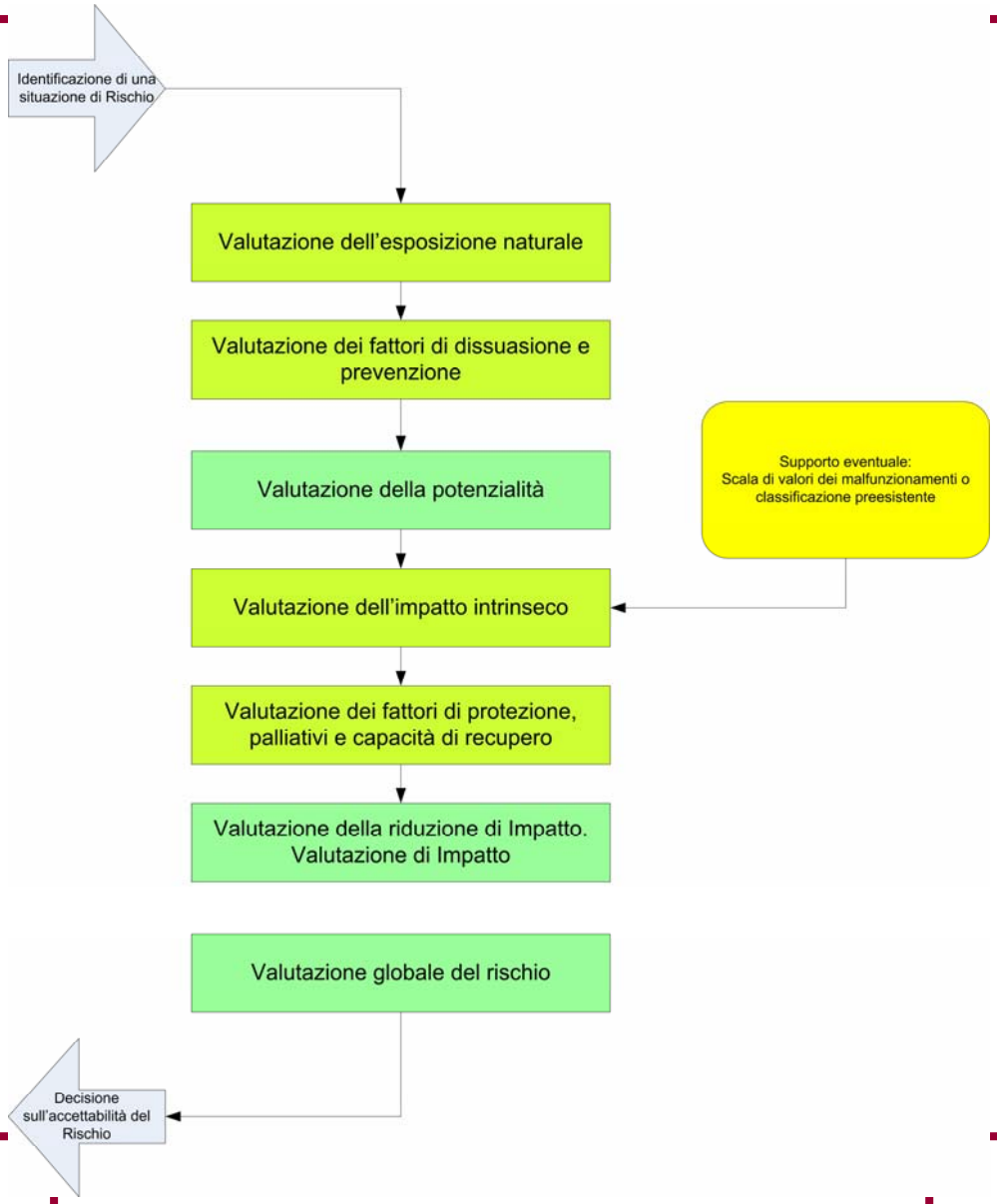


Nell'applicativo distribuito da CLUSIF vengono paragonate le Buone Pratiche (che potrebbero anche derivare da metodologie tipo ITIL) con le procedure correntemente adottate dall'azienda. In base al discostamento dalle buone pratiche si ha un punteggio e un calcolo corrispondente del Rischio.
Nel caso, mostrato in figura, ad esempio si stia valutando l'esposizione al Rischio di cancellazione di dati per effetto di un Trojan installato da un amministratore di sistema.

Le contromisure, che possono essere adottate a fronte di questo problema, sia preventivamente che in fase di Incident Response, riguardano più settori, ad esempio:

- Motivazione del personale
- Regole interne, Procedure e responsabilità, Sanzioni
- Analisi dei logs di sistema
- Gestione dei Privilegi del personale IT
- Protezione di files da modifiche illecite o indesiderate
- Piano di Backup e Ripristino
- Eventuali procedure di Sicurezza elevata
- Contratti di assistenza e Manutenzione
- Contratti di Assicurazione

Mehari


Identificazione di una situazione di Rischio
Valutazione dell'esposizione naturale
Valutazione dei fattori di dissuasione e prevenzione
Valutazione della potenzialità
Supporto eventuale:
Scala di valori dei malfunzionamenti o classificazione preesistente
Valutazione dell'impatto intrinseco
Valutazione dei fattori di protezione, palliativi e capacità di recupero
Valutazione della riduzione di Impatto.
Valutazione di Impatto
Valutazione globale del rischio
Decisione sull'accettabilità del Rischio

Mehari

Malfunzionamento	*Livello I (Non significativo)*	*Livello 2 (Importante)*	*Livello 3 (Molto Grave)*	*Livello 4 (Vitale)*
Frode dovuta alla falsificazione delle paghe	Perdita < 0.1 Mil. euro	Perdita compresa tra 0.1 e 1 Mil. euro	Perdita compresa tra 1 e 10 Mil. euro	Perdita > 10 Mil. euro
Divulgazione di dati personali	Divulgazione della paga di un impiegato	Divulgazione delle paghe dell'insieme del personale	Divulgazione ripetuta dei dati del personale	
Ritardo nel pagamento degli stipendi	Ritardo < 2 giorni	Ritardo compreso tra 2 e 15 giorni	Ritardo > 15 giorni	
Distruzione del database contenente le regole di calcolo degli stipendi	Cancellazione dei dati recenti (< 1 mese)	Cancellazione dei dati annuali	Distruzione dei dati e di tutto lo storico	

In Mehari, vengono individuati 4 livelli di gravità o di criticità.

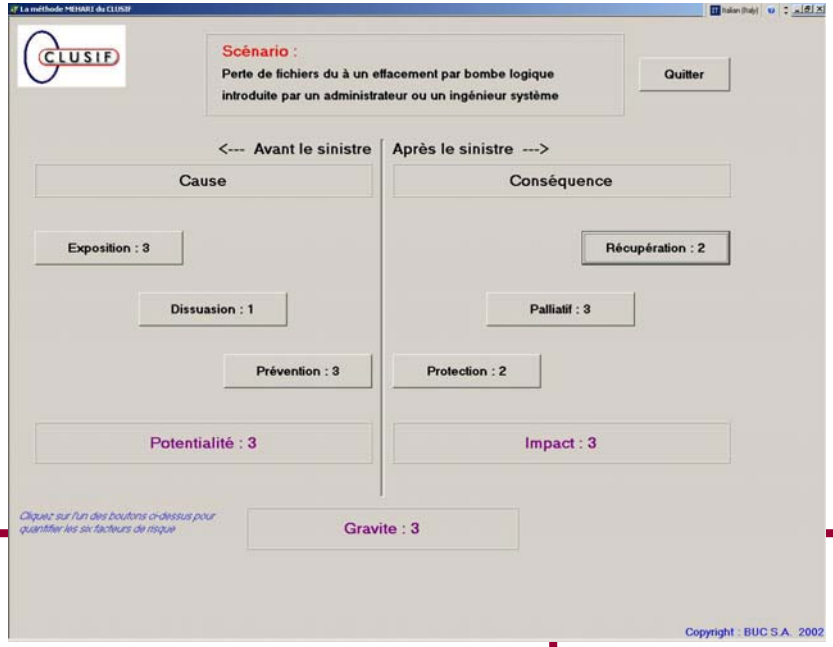
***Livello 4 (Vitale)*:** a questo livello di malfunzionamento, l'esistenza stessa dell'asset o delle sue attività principali è messa in pericolo. Nel caso dell'esempio del motore, fatto sopra, se questo è progettato per reggere velocità fino a 8000 giri al minuto e la sua velocità, per effetto di un malfunzionamento, si avvicina a questo valore, allora esso rischia di rompersi.

***Livello 3 (Molto Grave)*:** malfunzionamenti molto gravi ma che non pregiudicano un ripristino delle funzionalità

***Livello 2 (Importante)*:** malfunzionamenti che hanno un impatto sulle funzionalità ma che restano globalmente sopportabili

***Livello 1 (Non significativo)*:** a questo livello i problemi non hanno praticamente un impatto

Per ciascun malfunzionamento, occorre determinare quali sono i parametri significativi e quali sono i valori di soglia che fanno passare da un livello di gravità all'altro.



Mehari

Le **vulnerabilità** sono i punti attraverso cui un organismo può essere attaccato.

Un **servizio di sicurezza** è una risposta ad un bisogno di sicurezza (ad esempio la necessità di autenticare gli utenti) e descrive una **funzione di sicurezza** (ad es. l'autenticazione).
Questa funzione è indipendente dai meccanismi e dalle soluzioni concrete che realizzazono effettivamente il servizio (ad es. una smart card).

Un **meccanismo** è un modo particolare di assicurare, totalmente o parzialmente, la funzione del servizio o del sottoservizio. Si può trattare di una procedura specifica, di un algoritmo, di tecnologie ecc.

Una **soluzione di sicurezza** è la realizzazione concreta di un meccanismo di sicurezza e comprende hardware e software necessari alla sua messa in opera.

L'**analisi delle vulnerabilità** viene fatta sulle soluzioni.

Per misurare le performance (**qualità**) di un servizio di sicurezza devono essere considerati i seguenti parametri:

- efficacia
- robustezza
- possibilità di monitorarne il buon funzionamento

***Qualità* – misura la capacità di un servizio di resistere agli attacchi**

I livelli previsti sono 4.

- ***Livello1***: il servizio ha una qualità minima e non impatta granchè l'attitudine di sicureza di un organismo
- ***Livello2***: il servizio resta efficace e resiste ad un'aggressione media.
- ***Livello3***: il servizio resta efficace e resiste ad un'aggressione di buon livello. Una misura di questo livello avrà effetto nella stragrande magguioranza dei casi ma potrebbe non essere adeguata a situazioni eccezionali
- ***Livello4***: è il livello di qualità più alta e richiede skills eccezionalmente elevati per essere superata.

Mehari

Uno **scenario di rischio** è la descrizione di un malfunzionamento e del modo in cui esso può sopraggiungere.
Ogni scenario di rischio è legato a due parametri importanti:

- **Probabilità di accadimento**
- **Impatto**

Per la probabilità, si utilizza uno schema a 5 livelli:

Livello 0: non analizzato
Livello 1: molto improbabile
Livello 2: improbabile
Livello 3: probabile
Livello 4: molto probabile

Mehari propone tre categorie risultanti di rischio:
Rischi non supportabili, che dovrebbero essere oggetto di contromosure di urgenza
Rischi inammissibili, che dovrebbero essere ridotti ed eliminati ad un valore da deterrminare
Rischi tollerati

	P = 1	P = 2	P = 3	P = 4
I 4 =	G = 2	G = 3	G = 4	G = 4
I 3 =	G = 2	G = 3	G = 3	G = 4
I 2 =	G = 1	G = 2	G = 2	G = 3
I 1 =	G = 1	G = 1	G = 1	G = 2

La scala d'impatto è identica alla scala dei malfunzionamenti.

Livello 4 (Vitale): a questo livello l'impatto è estremamente grave e mette in pericolo l'esistenza stessa dell'entità

Livello 3 (Molto Grave): impatto molto grave ma non viene pregiudicato il ripristino delle funzionalità

Livello 2 (Importante): impatto sulle funzionalità ma che restano globalmente sopportabili

Livello 1 (Non significativo): a questo livello i problemi non hanno praticamente un impatto

Mehari

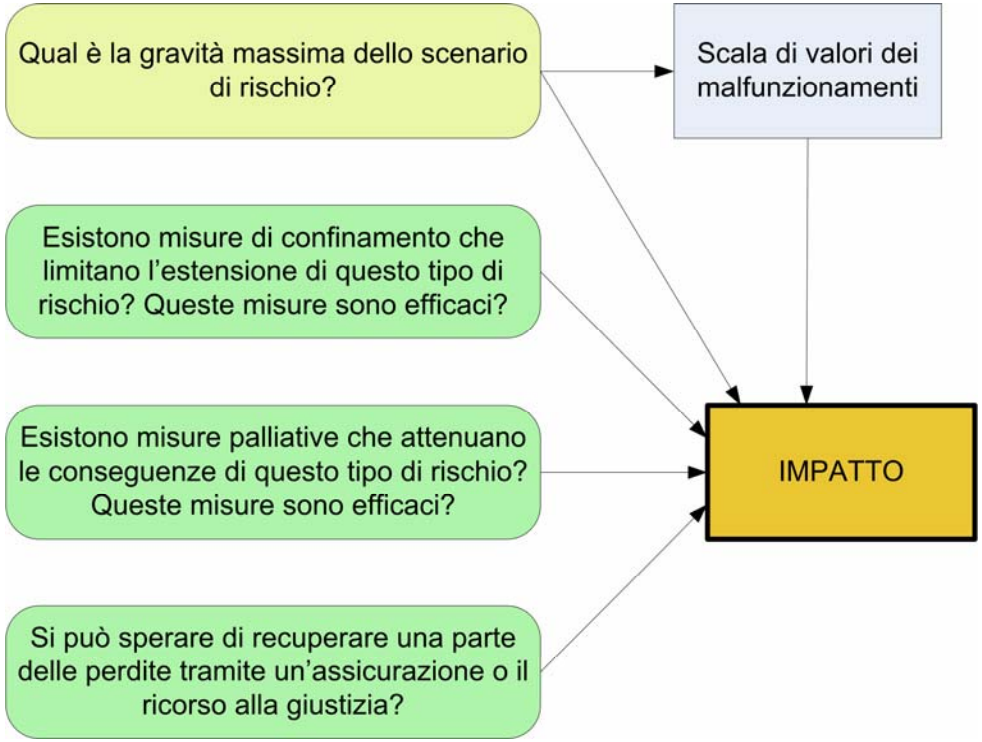
probabilità		
Esposizione tiene di conto della tipologia d'azienda, della sua collocazione geografica, socioeconomica e altro	Livello 1: esposizione molto debole Livello 2: esposizione debole Livello 3: esposizione media Livello 4: esposizione forte	**Misure strutturali** Costruzioni con criteri antisismici, in posizione sopraelevata se a rischio di inondazioni ecc.
Azione consapevole frodi, furti e altro	Livello 1: l'effetto dissuasivo è molto debole o nullo Livello 2: l'effetto dissuasivo è medio Livello 3: l'effetto dissuasivo è importante Livello 4: l'effetto dissuasivo è molto importante	**Misure dissuasive** rivelazione di tentativi di azioni nocive e registrazione delle azioni effettuate (ad es. una telecamera), imputabilità (non ripudiabilità) delle azioni tentate ed effettuate, autenticazione forte non contestabile, regolamentazioni e severità delle sanzioni, comunicazione sui sistemi di rivelazione e registrazione
Condizioni Password deboli, turni di ronda a orari regolari ecc.	Livello 1: l'effetto preventivo è molto debole o nullo Livello 2: l'effetto preventivo è medio Livello 3: l'effetto preventivo è importante Livello 4: l'effetto preventivo è molto importante	**Misure preventive** misure di sicurezza fisica, misure di controllo degli accessi, controlli preventivi incorporati neggli applicativi e nei processi

Mehari

Per valutare l'impatto finale, il metodo Mehari suggerisce prima di valutare il cosiddetto **impatto intrinseco** e poi l'azione delle contromisure o del trasferimento del rischio su terzi (come si fa stipulando un'assicurazione).
L'impatto intrinseco rappresenta la gravità massima delle conseguenze dello scenario di rischio.

Le contromisure da considerare, e da aggiungere all'impatto intrinseco, sono:

- **misure di protezione**, che portano al confinamento del rischio (es. una porta tagliafuoco)
- **misure palliative**, che attenuano le conseguenze indirette (es. training adeguato del personale)
- **misure di recupero** che consistono nel trasferimento di rischio verso terzi (assicurazioni o ricorso alla giustizia)



Octave

Valutazione del rischio

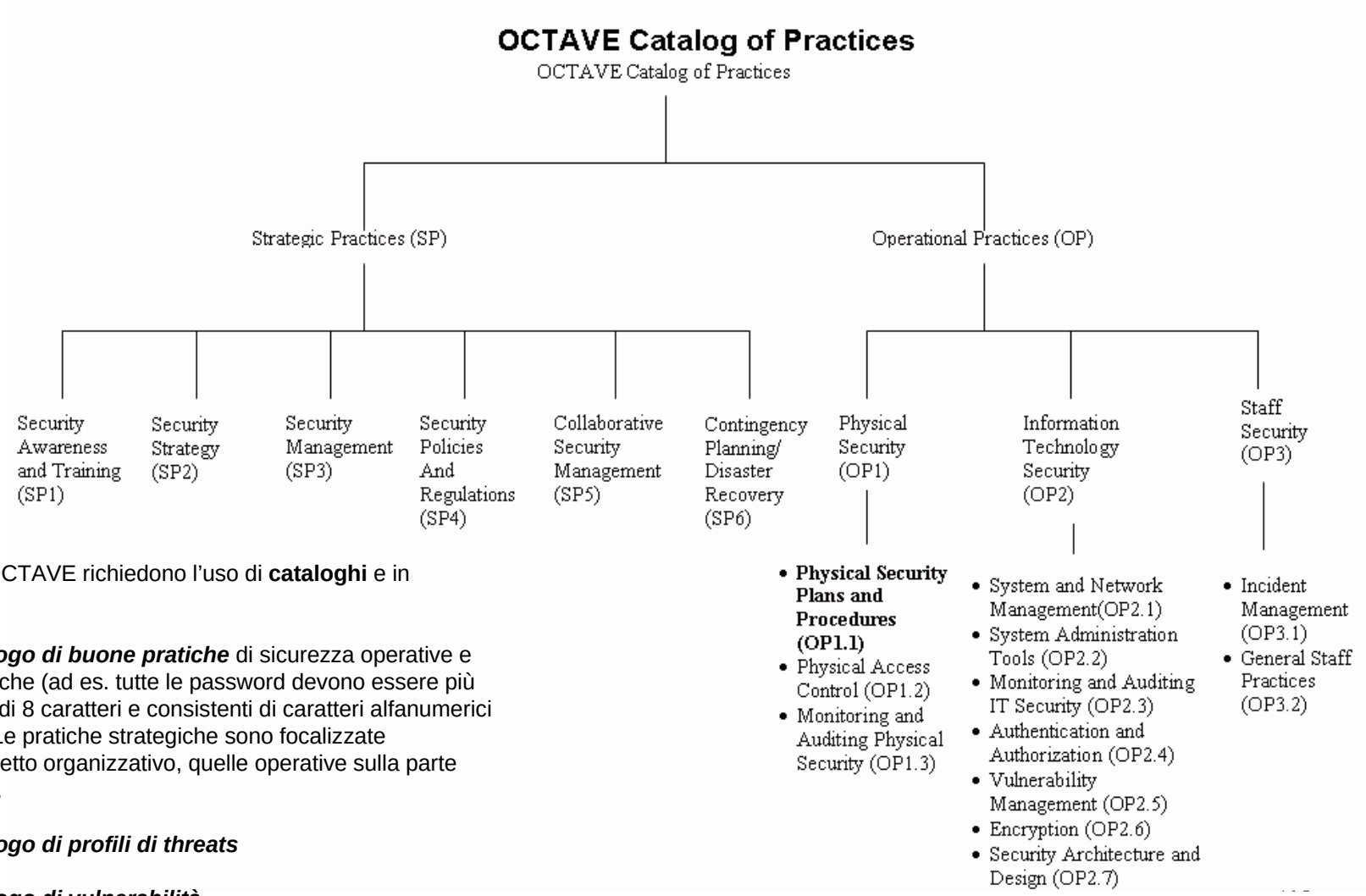
gestione del rischio

Organizzazione e cultura

OCTAVE Criteria								
Principles	Attributes		Outputs					
			Phase 1 Outputs		Phase 2 Outputs		Phase 3 Outputs	
Self-Direction	RA.1	Analysis Team	RO1.1	Critical Assets	RO2.1	Key Components	RO3.1	Risks to Critical Assets
Adaptable Measures	RA.2	Augment Analysis Team Skills	RO1.2	Security Requirements for Critical Assets	RO2.2	Technology Vulnerabilities	RO3.2	Risk Measures
Defined Process	RA.3	Catalog of Practices	RO1.3	Threats to Critical Assets			RO3.3	Protection Strategy
Foundation for a Continuous Process	RA.4	Generic Threat Profile	RO1.4	Current Security Practices			RO3.4	Risk Mitigation Plans
Forward-Looking View	RA.5	Catalog of Vulnerabilities	RO1.5	Current Organizational Vulnerabilities				
Focus on the Critical Few	RA.6	Defined Evaluation Activities						
Integrated Management	RA.7	Documented Evaluation Results						
Open Communication	RA.8	Evaluation Scope						
Global Perspective	RA.9	Next Steps						
Teamwork	RA.10	Focus on Risk						
	RA.11	Focused Activities						
	RA.12	Organizational and Technological Issues						
	RA.13	Business and Information Technology Participation						
	RA.14	Senior Management Participation						
	RA.15	Collaborative Approach						

I **principi** sono le motivazioni per la valutazione, gli **attributi** sono le caratteristiche distintive della valutazione o requisiti, e derivano dai principi. Gli **output** sono i risultati di ciascuna fase della valutazione. L'insieme di principi, attributi e output costituiscono i **criteri**

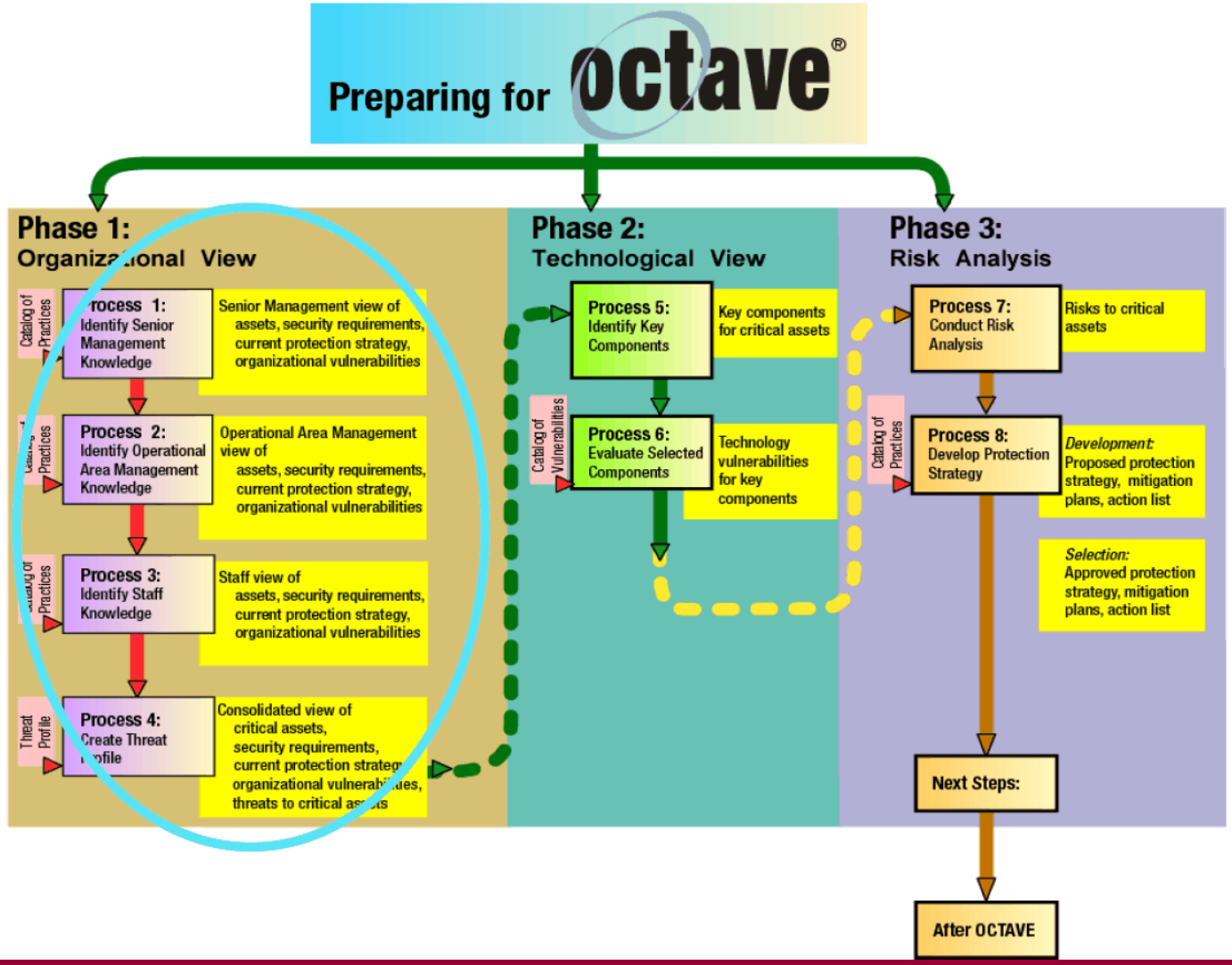
Octave



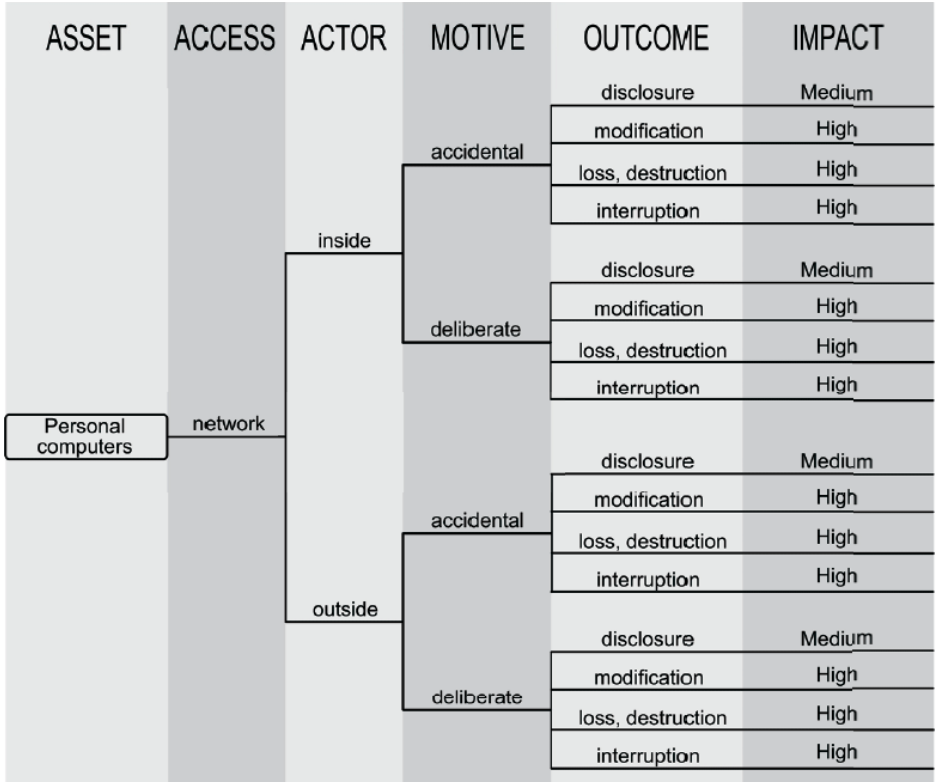
Infine, i criteri OCTAVE richiedono l'uso di **cataloghi** e in particolare:

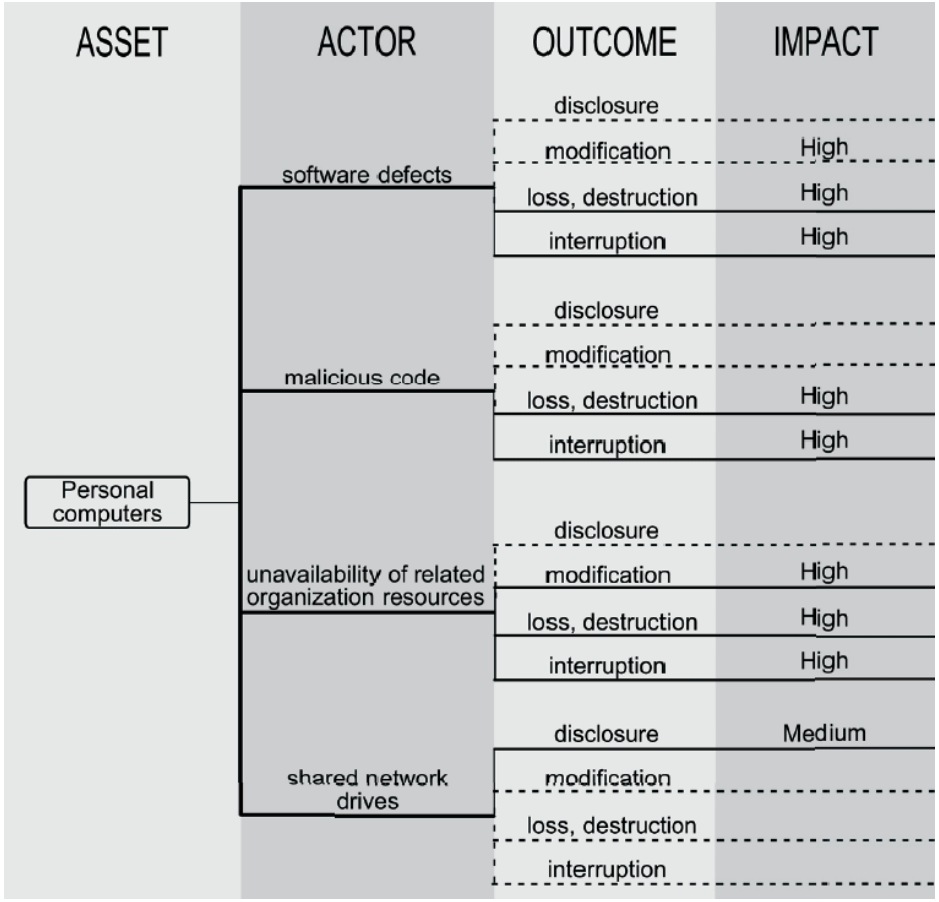
- ***catalogo di buone pratiche*** di sicurezza operative e strategiche (ad es. tutte le password devono essere più lunghe di 8 caratteri e consistenti di caratteri alfanumerici misti). Le pratiche strategiche sono focalizzate sull'aspetto organizzativo, quelle operative sulla parte tecnica.
- ***catalogo di profili di threats***
- ***catalogo di vulnerabilità***

Octave


Preparing for octave®
Phase 1:
Organizational View
Process 1:
Identify Senior Management Knowledge
Senior Management view of assets, security requirements, current protection strategy, organizational vulnerabilities
Process 2:
Identify Operational Area Management Knowledge
Operational Area Management view of assets, security requirements, current protection strategy, organizational vulnerabilities
Process 3:
Identify Staff Knowledge
Staff view of assets, security requirements, current protection strategy, organizational vulnerabilities
Process 4:
Create Threat Profile
Consolidated view of critical assets, security requirements, current protection strategy, organizational vulnerabilities, threats to critical assets
Catalog of Practices
Threat Profile
Phase 2:
Technological View
Process 5:
Identify Key Components
Key components for critical assets
Process 6:
Evaluate Selected Components
Technology vulnerabilities for key components
Catalog of Vulnerabilities
Phase 3:
Risk Analysis
Process 7:
Conduct Risk Analysis
Risks to critical assets
Process 8:
Develop Protection Strategy
Development: Proposed protection strategy, mitigation plans, action list
Selection: Approved protection strategy, mitigation plans, action list
Catalog of Practices
Next Steps:
After OCTAVE

Octave


ASSET
ACCESS
ACTOR
MOTIVE
OUTCOME
IMPACT
Personal computers
network
inside
outside
accidental
deliberate
accidental
deliberate
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption
Medium
High
High
High
Medium
High
High
High
Medium
High
High
High
Medium
High
High
High


ASSET
ACTOR
OUTCOME
IMPACT
Personal computers
software defects
malicious code
unavailability of related organization resources
shared network drives
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption
High
High
High
High
High
High
Medium

CRAMM

CRAMM (CCTA Risk Analysis and Management Method) è stato sviluppato nel 1985 da CCTA (Central Computer and Telecommunications Agency) ed è attualmente giunto alla versione 5.1, adeguata a BS7799-2. È un prodotto commerciale distribuito da Insight.

CRAMM è diviso in tre stadi:

- Identificazione e valutazione degli ***asset***
- ***Threat*** e assessment delle ***vulnerabilità***
- Selezione e raccomandazione delle ***contromisure***

CRAMM combina tre elementi e precisamente:

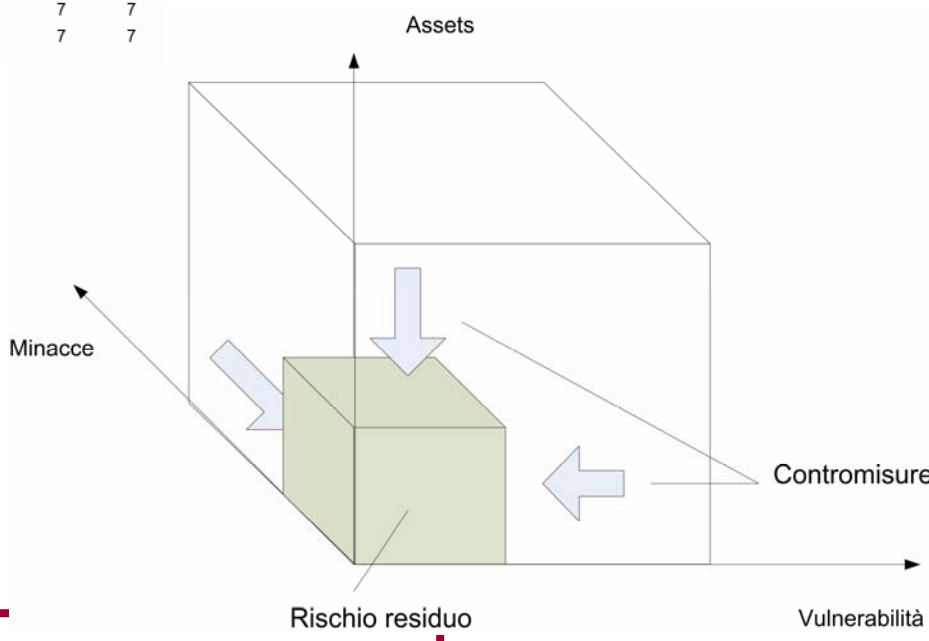
- la ***frequenza*** con cui le minacce potrebbero realizzarsi (livello di pericolo)
- la ***probabilità*** che la minaccia abbia successo e quindi produca un impatto (livello di vulnerabilità)
- la ***perdita economica potenziale*** se la minaccia avesse effetto (l'impatto)

CRAMM

Matrice di Rischio

Rischio=Asset x threat x vulnerabilità

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7



CRAMM

CRAMM suddivide gli assets in gruppi.
A ogni gruppo sono associate minacce e vulnerabilità. Il rischio associato ad un componente del gruppo viene valutato anche tenendo conto delle dipendenze di altri assets da quello considerato.

Il processo di valutazione delle contromisure è invece basato su tre aspetti:

- **Per ogni minaccia esiste un gruppo di contromisure associato**
- **Le classi di assets a cui una contromisura viene applicata sono paragonate al gruppo di appartenenza dell'asset in considerazione**
- **Le misure di rischio vengono confrontate con il livello di sicurezza delle contromisure adottate per determinare il rischio residuo**

CRAMM contiene una libreria di contromisure molto grossa che consiste di oltre 3000 contromisure dettagliate organizzate in 70 gruppi logici.
Ogni contromisura ha associati due valori, o *livelli di sicurezza*, che rappresentano i valori di soglia, minima e massima, dell'impatto della minaccia che la contromisura dovrebbe contrastare.
I livelli di sicurezza vengono confrontati dal valore del rischio dedotto dalla matrice di rischio.

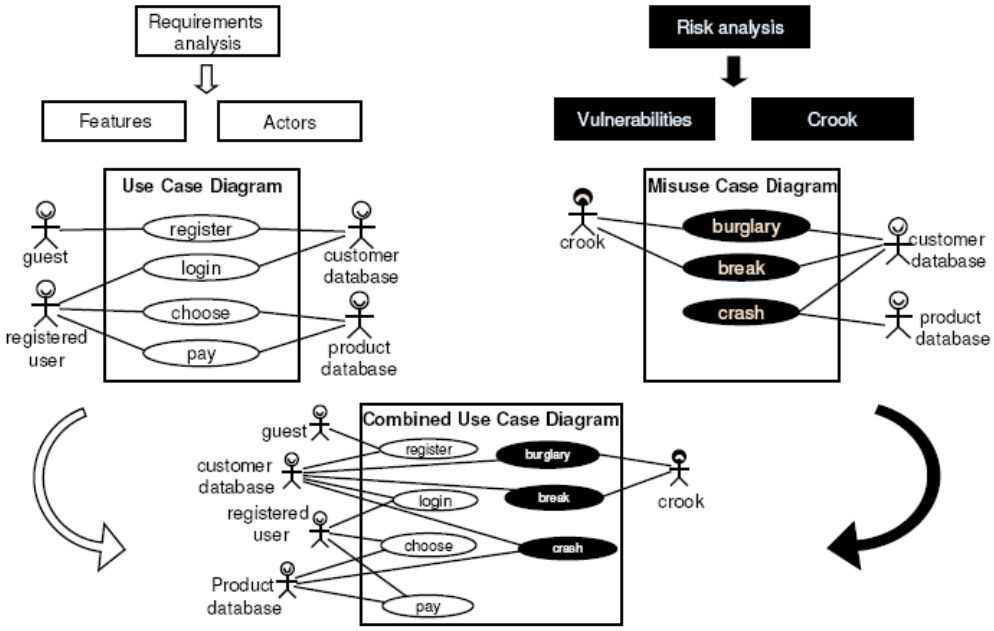
CORAS

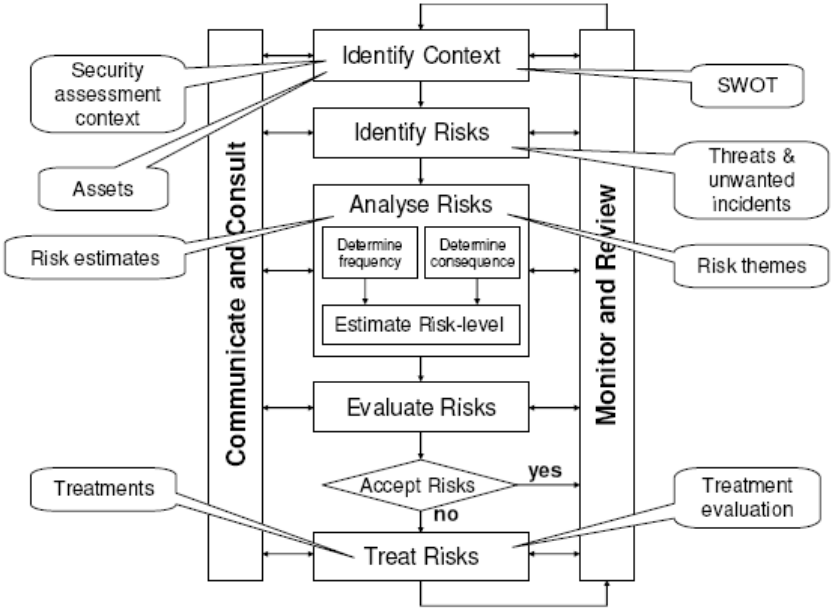
Coras è un progetto di ricerca e sviluppo tecnologico della Comunità europea.

CORAS è una metodologia supportata da un tool software e fornisce:

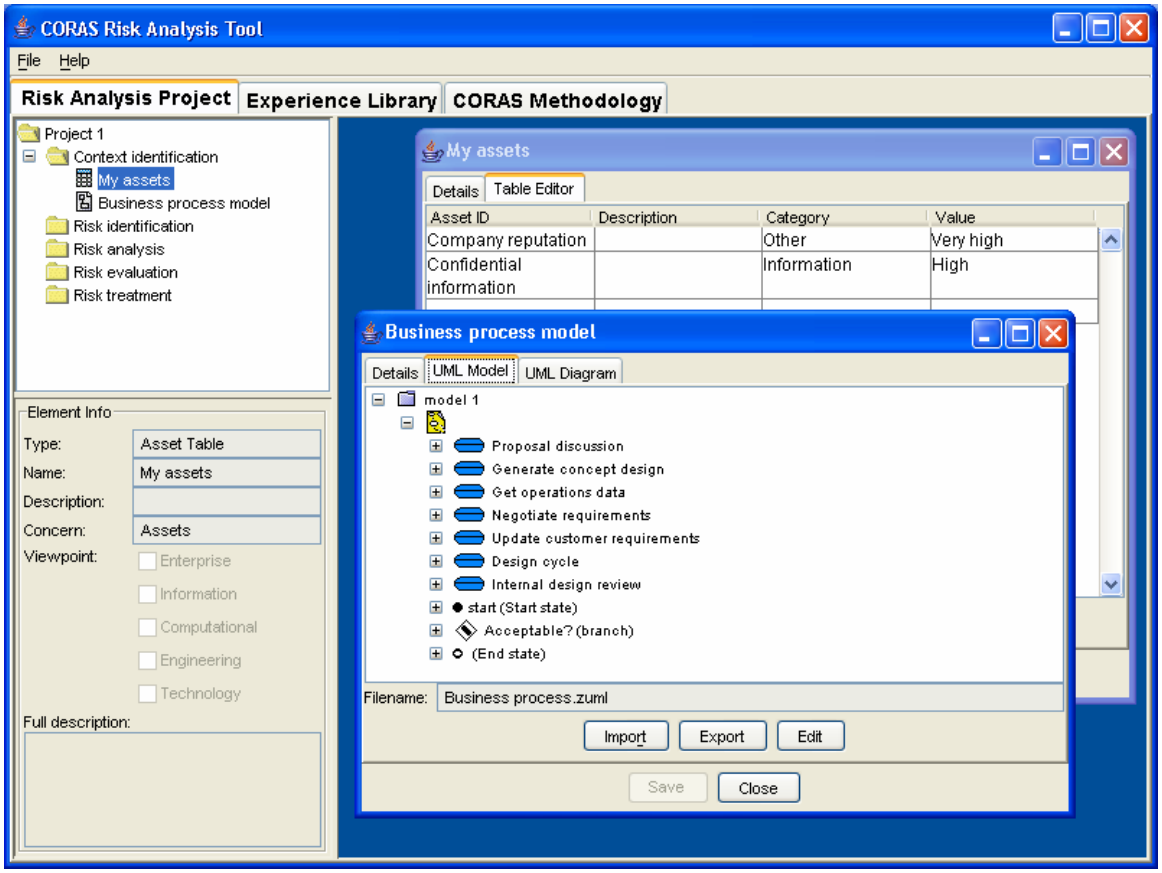
- una metodologia per l'assessment di rischi di sicurezza basata su modelli
- un linguaggio di specifiche basato su UML, specificatamente orientato all'assessment del rischio
- una libreria di pacchetti di esperienze riusabili
- uno strumento che supporta la metodologia e basato su due repositories: un repository di assessment e uno di pacchetti di esperienze riusabili
- XML per lo scambio di dati di assessment sul rischio
- Un formato di report per l'assessment di vulnerabilità

CORAS


Requirements analysis
Features
Actors
Use Case Diagram
register
login
choose
pay
guest
registered user
customer database
product database
Risk analysis
Vulnerabilities
Crook
Misuse Case Diagram
burglary
break
crash
crook
customer database
product database
Combined Use Case Diagram
guest
customer database
registered user
Product database
register
login
choose
pay
burglary
break
crash
crook


Identify Context
Identify Risks
Analyse Risks
Determine frequency
Determine consequence
Estimate Risk-level
Evaluate Risks
Accept Risks
yes
no
Treat Risks
Communicate and Consult
Monitor and Review
Security assessment context
Assets
Risk estimates
Treatments
SWOT
Threats & unwanted incidents
Risk themes
Treatment evaluation

CORAS



Il tool associato alla metodologia è distribuito come un eseguibile windows ed è composto di due parti: un server e un client. Esso è scaricabile dalla URL coras.sourceforge.net

Un progetto è strutturato in cartelle che corrispondono ai 5 sottoprocessi visti sopra e può utilizzare varie tipologie di oggetti:

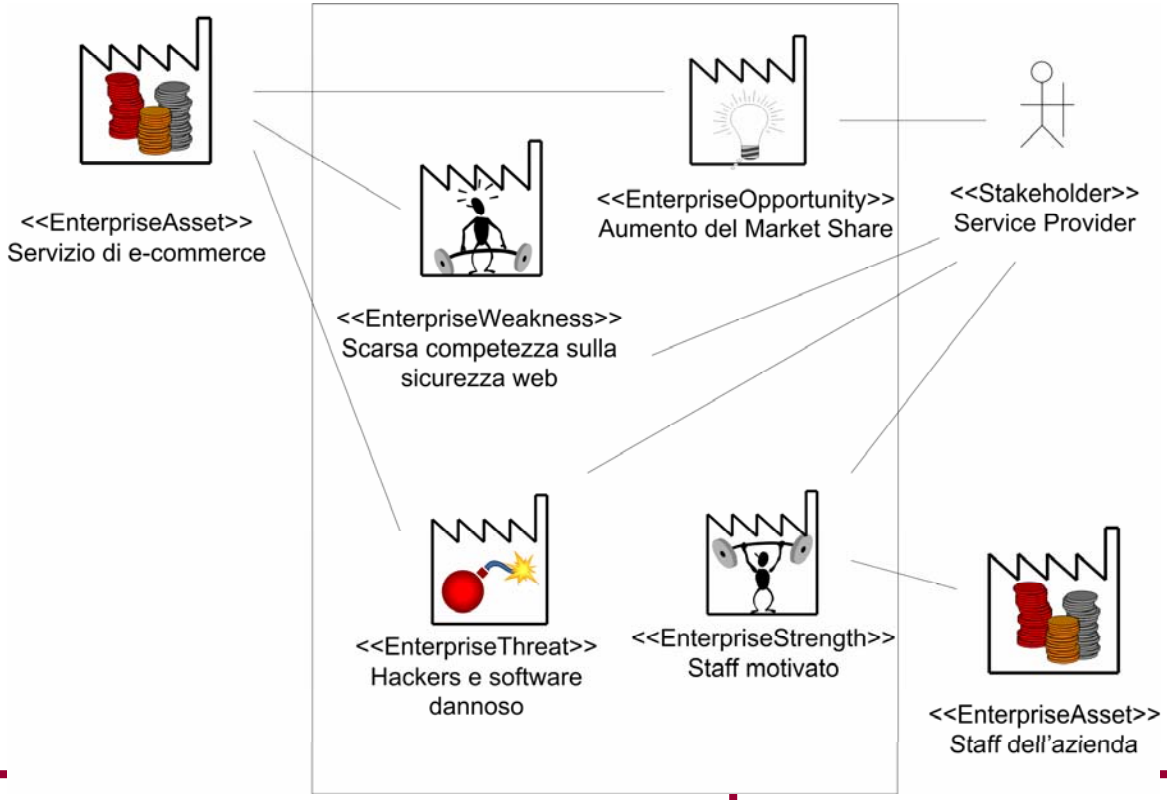
- tabelle
- modelli UML Coras
- Fault tree (come definito da OpenFTA, www.openfta.com)
- Documenti (file HTML, immagini ecc.)

CORAS

I profili definiscono un linguaggio astratto per supportare l'assessment del rischio basato su modelli. Il profilo usa il meccanismo di estensione UML chiamato "stereotipo" per adattarsi ad un dominio particolare, nel nostro caso assessment del rischio.

I profili CORAS UML sono utilizzati per forinire un supporto di modellazione a:

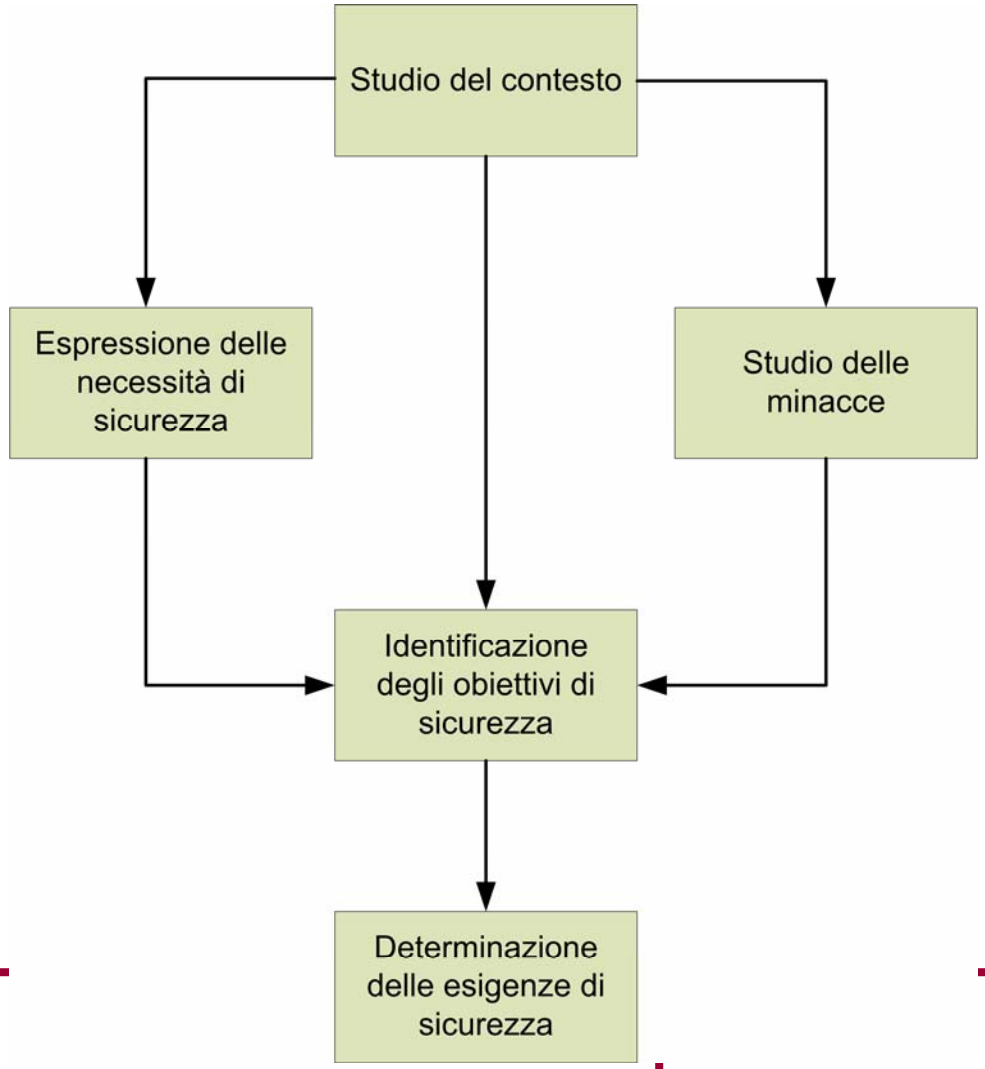
- Security assessment
- Analisi SWOT (Strengths, Weakness, Opportunities and Threats)
- Assets
- Threats e incidenti non volute
- Stime di rischio
- Temi di Rischio
- Contromusire
- Valutazione delle contromisure



EBIOS

Ebios (Expression des Besoins et Identification des Objectifs de Sécurité), segue da vicino, nell'approccio e nella nomenclatura, i Common Criteria (ISO 15408).

Il metodo è composto da 5 tappe e ogni tappa è composta da attività



EBIOS

Attività 1.1: studio dell'organizzazione

La **presentazione dell'organizzazione** permette di richiamare gli elementi caratteristici che identificano l'organizzazione, come ad esempio:

La Vocazione – cosa l'organizzazione vuole fare
Il Mestiere – cosa l'organizzazione sa fare
La Mission – cosa l'organizzazione deve fare
I Valori – ciò che l'organizzazione fa bene
La struttura (divisionale o funzionale)
L'Organigramma

l'elencazione dei vincoli, interni o esterni, a cui l'organizzazione è sottoposta. I vincoli possono essere di tipo diverso: politico, strategico, territoriale, congiunturale, strutturale, funzionale, personale, temporale, metodologica, culturale, economico

l'elencazione delle leggi e normative a cui l'organizzazione è sottoposta, ad esempio la legge della privacy.
Si procede, quindi, alla descrizione del Sistema informativo nella sua globalità. In particolare si identificano:

le *funzioni operative*, che hanno direttamente a che fare con gli obiettivi dell'organizzazione
le *funzioni di supporto*, che sono di appoggio alle funzioni operative
le *funzioni di controllo*, che sono di gestione

EBIOS

Attività 1.1: studio del Target of Evaluation

Questa attività ha lo scopo di mettere in evidenza il **compito e l'importanza** del ToE all'interno del Sistema Informativo, anche in relazione ad altre entità.
In questa fase si identificano gli elementi costitutivi del ToE ed è importante sottolineare:

- le funzioni la cui perdita o degradazione porta all'impossibilità di raggiungere la mission
- le funzioni che gestiscono dati di segretezza o di alto livello
- le funzioni la cui modifica può penalizzare fortemente il raggiungimento della mission del sistema

Occorre anche caratterizzare la natura delle informazioni trattate dal ToE e in particolare:

- informazioni di natura sensibile
- dati personali
- informazioni classificate
- informazioni vitali al raggiungimento dell'obiettivo del ToE
- informazioni strategiche per come raggiungere l'obiettivo
- informazioni di costo elevato, per quanto riguarda la loro raccolta e/o trattamento

L'obiettivo di questa attività è una descrizione funzionale del ToE e in particolare quello di mettere in evidenza delle informazioni in entrata e in uscita e il loro trattamento.

Elencazione delle ipotesi

Elencazione delle regole di sicurezza

Elencazione dei vincoli

EBIOS

Attività 1.3: determinazione dell'obiettivo della sicurezza

La prima fase consiste nell'elencare e descrivere le **entità** del sistema (hardware, software, reti, persone, siti ecc.).
Il passo successivo è quello di fare una **matrice** che metta in relazione le funzioni e le informazioni essenziali con le entità.

Entités / Éléments essentiels	MATERIELS				LOGICIELS				RESEAUX				PERSONNELS					SITES			ORGA.		
	M1	M2	M3	M4	L1	L2	L3	L4	R1	R2	R3	R4	P1	P2	P3	P4	P5	S1	S2	S4	O1	O2	O3
Fonction 1	+					+	+	+					+	+	+	+			+			+	+
…	+					+	+	+					+	+	+	+	+	+	+		+		+
Fonction N	+	+			+	+		+	+			+		+	+	+	+	+	+			+	+
Information 1	+		+		+	+		+		+		+		+	+	+	+	+	+			+	+
…	+			+	+	+		+			+	+		+	+	+	+	+	+			+	+
…	+					+	+	+					+	+	+	+			+	+	+	+	+
Information N	+					+	+	+					+	+	+	+	+	+	+	+			+

Matrice funzioni-entità

EBIOS

Attività 2.1: realizzazione delle matrici dei requisiti

Il primo passo è scegliere i criteri di sicurezza a cui attenersi. I tre irrinunciabili sono Riservatezza, Integrità e Disponibilità. A essi possono aggiungersi non Ripudiabilità, Anonimato, Affidabilità ecc.
Occorre poi stabilire delle priorità tra questi criteri, ad esempio da 0 (non necessario) a 4 (molto importante).
I Threats hanno la caratteristica, se si verificano, di produrre degli impatti sui criteri di sicurezza. Ad esempio, lo Spoofing Identity ha un impatto sulla Riservatezza, nel senso che ne produce una perdita.

Nom de l'élément essentiel	***Impact 1***	***…***	***Impact n***	***Besoins de sécurité***	***Commentaires***
Critère de sécurité 1	*B11*	*…*	*B1n*	*f(B11…B1n)*	
…	*…*	*…*	*…*	*…*	
Critère de sécurité n	*Bn1*	*…*	*Bnn*	*f(Bn1…Bnn)*	

Matrice criteri-impatto

EBIOS

Attività 2.2: sintesi dei requisiti di sicurezza

Liste des éléments essentiels	Synthèse des besoins de sécurité		
	Confidentialité	Intégrité	Disponibilité
Fonction 1	0	3	3
Fonction 2	1	3	2
…	…	…	…
Fonction n	0	4	2
Information 1	2	1	1

Attività 3.1: studio delle origini delle minacce

		Éléments menaçants						Critères de sécurité touchés		
		Type			Cause					
	Méthodes d'attaque	Naturel	Humain	Environnemental	Accidentelle	Délibérée	Potentiel d'attaque	Disponibilité	Intégrité	Confidentialité
1	Incendie	+	+	+	+	+	2	+	+	
13	Perte des moyens de télécommunications			+	+	+	1	+		
19	Écoute passive		+	+		+	2			+
20	Vol de supports ou de documents			+		+	2			+
21	Vol de matériels			+		+	1	+		+
23	Divulgation		+	+	+	+	1			+
26	Piégeage du logiciel			+		+	1	+	+	+
42	Atteinte à la disponibilité du personnel	+	+	+	+	+	1	+		

Matrice threats-threat agents-criteri di sicurezza impattati

EBIOS

Attività 3.2: studio delle vulnerabilità

Per ogni modo d'attacco individuato, occorre mettere in evidenza eventuali vulnerabilità da parte del ToE.
Una vulnerabilità è una caratteristica del sistema che potrebbe essere impiegata da un elemento di minaccia e permettere quindi la realizzazione di un metodo d'attacco.
L'associazione vulnerabilità-metodo d'attacco-entità è fornita dalle **Basi di Conoscenza**.

Méthodes d'attaque		*Vulnérabilités*	*Matériel et logiciel*	*Réseaux internes*	*Réseaux externes*	*Site*	*Personnel*	*Organisation*
1	*Incendie*	*Manque de cohérence des mesures incendie avec le système informatique*				*2*		
		Absence de consignes (alerte, prévention, formation…)						*2*
		Absence d'organisation sécurité incendie						*3*
13	*Perte des moyens de télécommunications*	*Défauts d'exploitation du réseau téléphonique interne*				*1*		
		Dysfonctionnement des réseaux externes (RTC)			*1*			
		Dysfonctionnement des réseaux externes (services réseaux)			*1*			
…	…	…	…	…	…	…	…	…

Matrice threat-vulnerabilità-entità

EBIOS

Attività 3.3: formalizzazione delle minacce

L'output di questa attività è una matrice che correla le minacce con il metodo e il potenziale d'attacco, i criteri di sicurezza e l'opportunità

	Menaces	*Méthode d'attaque*	*Potentiel d'attaque*	*D*	*I*	*C*	*Opportunité*
M.INCENDIE	*Aggravation des conséquences d'un incendie à cause du manque de cohérence des mesures incendie avec le système informatique (site du cabinet d'études), de l'absence de consignes ou d'organisation sécurité incendie (organisation du cabinet d'études)*	*1*	*2*	*+*			*2*
M.TELECOM	*Perte des moyens de télécommunications à cause d'un dysfonctionnement des réseaux externes (Internet)*	*12*	*1*	*+*			*1*
M.VOL-DOC	*Vol de supports ou de documents par une personne en visite ou un personnel de nettoyage du fait de la facilité de pénétrer dans les locaux pendant les heures ouvrables (site du cabinet d'études)*	*19*	*2*			*+*	*3*
…	…	…	…	…	…	…	…

Matrice threat-potenziale-criterio

EBIOS

Attività 4.1: confronto delle minacce con i requisiti

La determinazione del rischio consiste nel capire come gli elementi essenziali e prioritari per l'organizzazione possono essere impattati dalle minacce.
Da un lato, i requisiti di sicurezza sono stati espressi tramite i criteri di sicurezza, dall'altro, le minacce sono state categorizzate tramite i criteri di sicurezza che vanno ad impattare.
Per ciascun elemento essenziale, si può quindi fare una matrice che riporti il metodo d'attacco e i criteri di sicurezza impattati.

I.VISU (Visualisation)		*Besoins de sécurité:*			*D*	*I*	*C*
					2	*2*	*0*
Méthodes d'attaque		*Atteinte*			***Besoins de sécurité concernés***		
		D	*I*	*C*	***D***	***I***	***C***
1	*Incendie*	+	+		*2*	*2*	
13	*Perte des moyens de télécommunications*	+			*2*		
19	*Écoute passive*			+			
20	*Vol de supports ou de documents*			+			
21	*Vol de matériels*	+		+	*2*		
23	*Divulgation externe*			+			
26	*Piégeage du logiciel*	+	+	+	*2*	*2*	
42	*Atteinte à la disponibilité du personnel*	+			*2*		
…	…	…	…	…	…	…	…

Matrice threat-criteri di sicurezza impattati

EBIOS

Attività 4.2: formalizzazione degli obiettivi di sicurezza

Questa è la fase di gestione del rischio vera e propria.
Gli obiettivi di sicurezza vanno a trattare i seguenti aspetti del rischio:

- l'origine delle minacce
- le vulnerabilità impiegate
- le conseguenze

La nomenclatura prevede che gli obiettivi vengano indicati come O.xxxx, ad esempio O.INC-ORIGINE è l'obiettivo che prevede la messa in atto di contromisure per contrastare la nascita di incendi.
Ogni obiettivo va a coprire in una certa misura i rischi. Tale copertura è espressa tramite i valori

0 – nessuna copertura
1 – copertura parziale
2 – copertura completa

Matrice rischi-obiettivi

Risques	*Objectifs de sécurité*	*Justification de la couverture*	*Couverture*	*Potentiel d'attaque*
R.PIEGEAGE	*O.SYS-COMMANDES* *O.SYS-ACTIONS*	*Les deux objectifs de sécurité couvrent l'ensemble des vulnérabilités exploitées dans le risque :* *- possibilité de modifier les commandes systèmes via Internet,* *- possibilité d'implanter des programmes pirates via Internet,* *- possibilité de modifier un applicatif via Internet,* *- possibilité d'agir sur les logiciels des ressources du système via Internet.*	*2*	*1*
R.VOL-VISITEUR	*O.LOCAUX* *O.VOL-PROTECTION* *O.PRISE-EN-CHARGE* *O.AUTH-DOC*	*Les deux premiers objectifs de sécurité couvrent les vulnérabilités exploitées dans le risque :* *- facilité de pénétrer dans le cabinet d'études,* *- matériel reconnu comme particulièrement attractifs (valeurs marchande et technologique).* *Le troisième objectif de sécurité améliore la réduction du risque en responsabilisant les utilisateurs.* *Le dernier objectif de sécurité offre une garantie d'authentification du rédacteur des documents.*	*2*	*1*
...	...	...	...	...

EBIOS

Attività 4.3: determinazione dei livelli di sicurezza

Per ogni obiettivo di sicurezza, si può valutare il livello di resistenza (1-elementare, 2-medio, 3-elevato) , che esprime lo sforzo minimo necessario per mettere in difetto il comportamento di sicurezza raggiunto dal sistema dopo l'applicazione delle contromisure ai rischi individuati. Un altro parametro che si può prendere in considerazione è l'Evaluation Level Assurance, da EAL1 a EAL7, come proposto dai Common Criteria.

Attività 5.1: determinazione delle esigenze di sicurezza funzionali

Le esigenze di sicurezza funzionali rappresentano i modi di raggiungere gli obiettivi di sicurezza e quindi è la fase in cui si selezionano le contromisure.

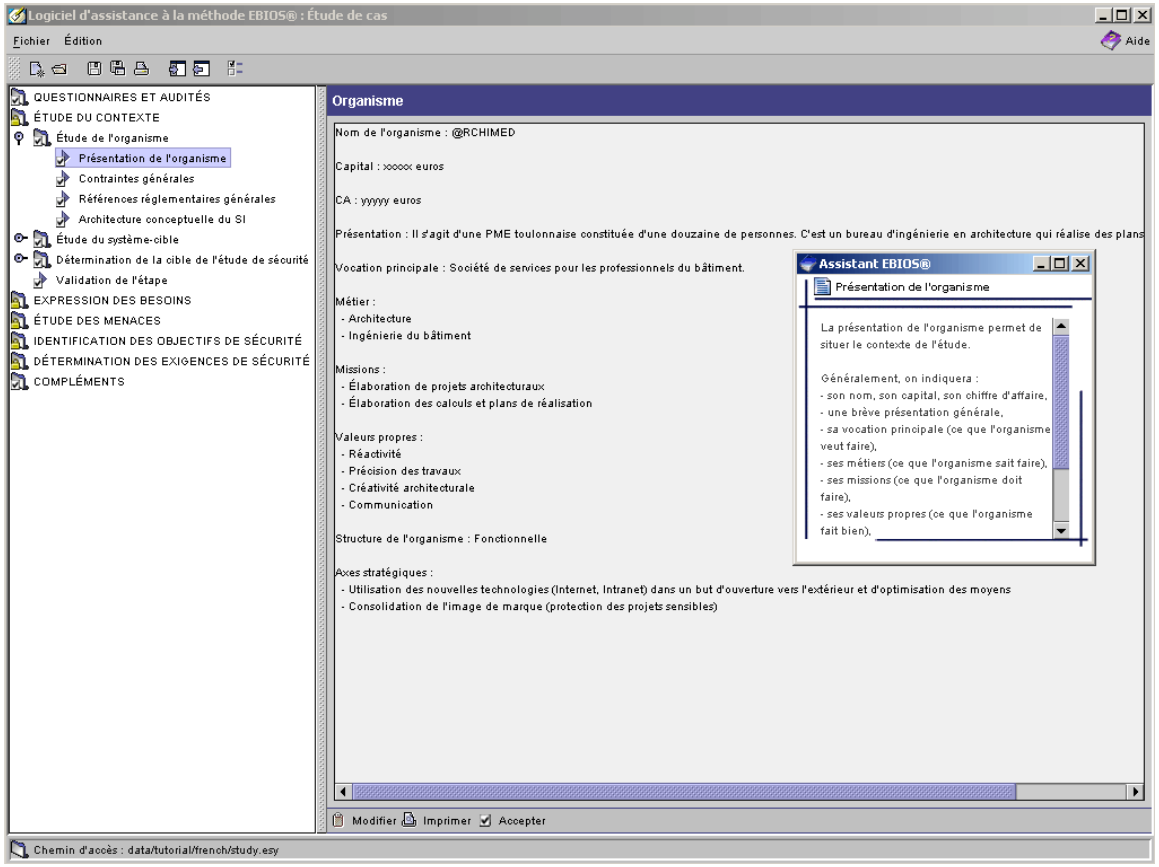
La formulazione di un'esigenza di sicurezza funzionale dovrebbe essere (SMART):

- **S**pecifica
- **M**isurabile
- **A**ttuabile
- **R**ealista
- legata ai **T**empi

EBIOS

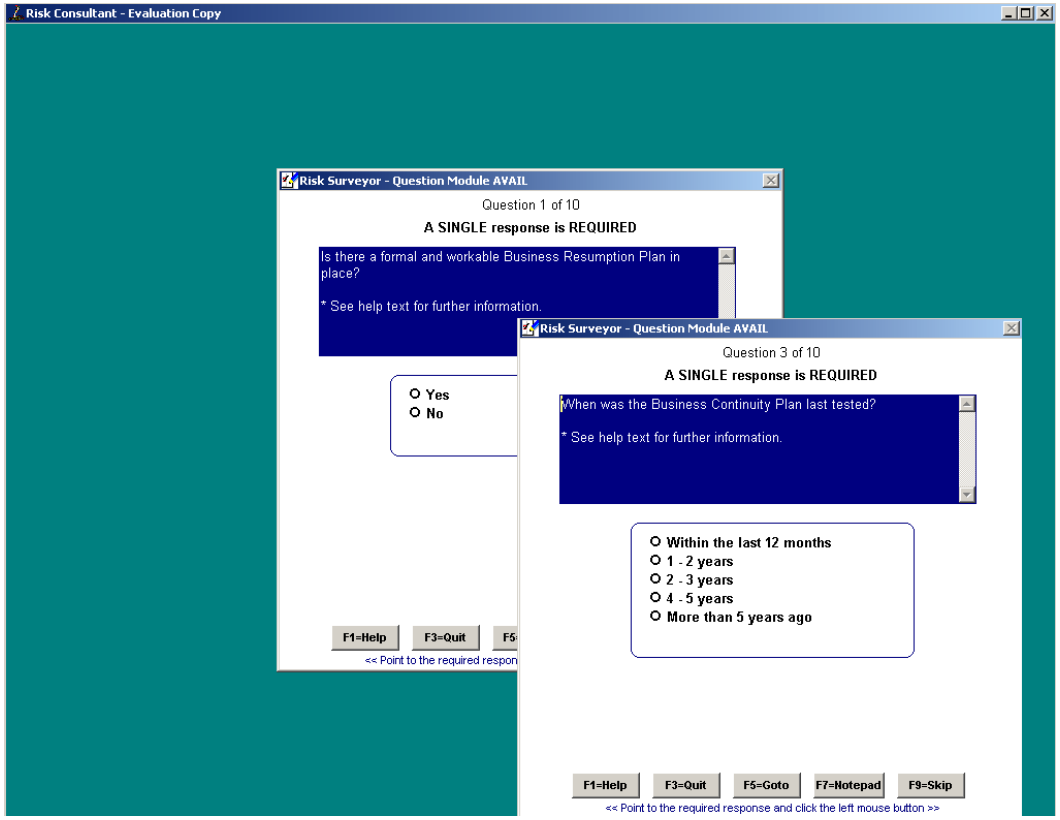
Attività 5.2: determinazione delle richieste di security assurance

La fiducia (assurance) che gli obiettivi di sicurezza sono raggiunti per mezzo delle funzioni di sicurezza selezionate proviene dai due fattori seguenti:
la fiducia nella conformità dell'implementazione delle misure di sicurezza
la fiducia nell'efficacia delle funzioni di sicurezza



COBRA

Cobra Risk Consultant è un software per Windows basato su questionari. Esso si appoggia a basi di conoscenza, tra cui ad esempio quella di ISO 17799. Le basi di conoscenza possono essere personalizzate tramite Module Manager, fornito separatamente. Il questionario è diviso in moduli: Availability, Confidence, Integrity e Business Impact Analysis. Quando si crea il questionario, è possibile scegliere quali moduli includere.



NETWORK SOLUTIONS S.R.L. (EVALUATION COPY)

Question & Response Listing (continued)

Question Module: AVAIL - Availability

Question 3 **Risk Category: Availability**

Status: Answered

When was the Business Continuity Plan last tested?

* See help text for further information.

Within the last 12 months
1 - 2 years ✓ Score: 0.50
2 - 3 years
4 - 5 years
More than 5 years ago

Question 4 **Risk Category: Availability**

Status: Answered

Are the contingency arrangements for all key components reasonable and appropriate?

Consider all components for mission critical services. These might include PCs, software, modems, hardware, stationary, etc. Consider also whether arrangements exist for replacement or recovery for backups within an acceptable time frame.

* See help text for further information.

Yes
No ✓ Score: 50.00

Conclusioni

"L'hacking è creatività, la sicurezza è una scienza"

"non possiamo gestire quello che non possiamo misurare"

Pete Herzog, autore di OSSTMM

Bibliografia e sitografia :

1. http://www.iso27001security.com/html/others.html
2. http://www.enisa.eu/doc/pdf/deliverables/WGRARM/ENISA_RM-Deliverable2-Final-Version-v1.0-2006-03-30.pdf
3. http://www.bpmn.org
4. http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2
5. http://www.sans.org/whatworks
6. http://www.isecom.org/
7. "Risk Management", A. Sinibaldi, Hoepli 2007

Grazie a tutti per la cortese attenzione!

Domande?

alessandro_sinibaldi@virgilio.it