

Certificazioni ISECOM *e* Certificazione PILAR advanced user

ISACA – Capitolo di Roma



Alberto Perrone

20 Novembre 2009

Chi siamo: @ Mediaservice.net

- Una società che opera dal 1997 nell'area della **Consulenza sulla Sicurezza**, da un punto di vista tecnologico e organizzativo
- @ Mediaservice.net è coinvolta nei comitati di normazione ISO per la famiglia 27000, nella contribuzione a standard per il penetration testing con ISECOM e ha forti rapporti con partner istituzionali quali CLUSIT, UNINFO, ISACA e ITSMF.
- I nostri consulenti hanno una formazione universitaria nell'area informatica, perfezionata attraverso l'ottenimento di svariati riconoscimenti professionali, tra cui ISO/IEC 27001 Lead Auditor, OPST, OPSA, OWSE, CISA, CISM, CISSP, ITIL, ISFS etc.
- Soci e consulenti sono costantemente coinvolti in interventi a conferenze nazionali e internazionali, nonché autori di pubblicazioni sulla stampa di settore.

Chi siamo: @ Mediaservice.net

Alberto Perrone

Lead Auditor qualificato ISO/IEC 27001:2005
OSSTMM Professional Security Tester

Referente formazione
Divisione Sicurezza Informazioni,
@ Mediaservice.net S.r.l.

I Valori



VENDOR NEUTRAL



RICERCA E SVILUPPO



METODO DI LAVORO



ETICITA'



PERSONALE INTERNO

ISECOM

Corsi e certificazioni

Chi è ISECOM ?

- Institute for **SEC**urity and **Open M**ethodologies
- Nasce nel 2001, fondata da Pete Herzog
- Non Profit Organization registrata in USA ed EU con sedi a New York e Barcellona
- Open Source Community registered OSI
- Sviluppa numerosi progetti di carattere open, tra cui:
 - OSSTMM
 - HPP
 - HHS
- Coordina e gestisce certificazioni del personale sulla sicurezza

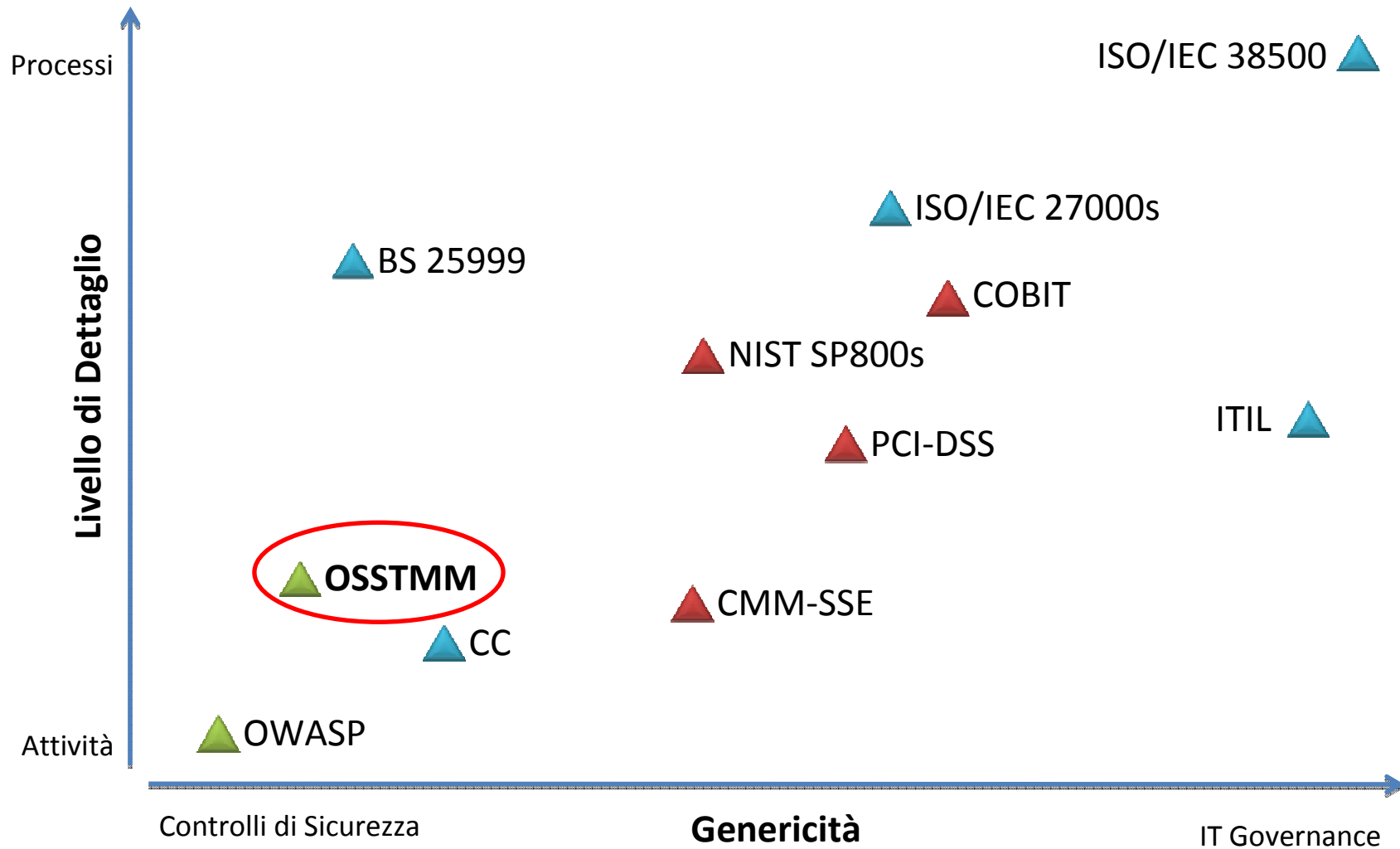


OSSTMM

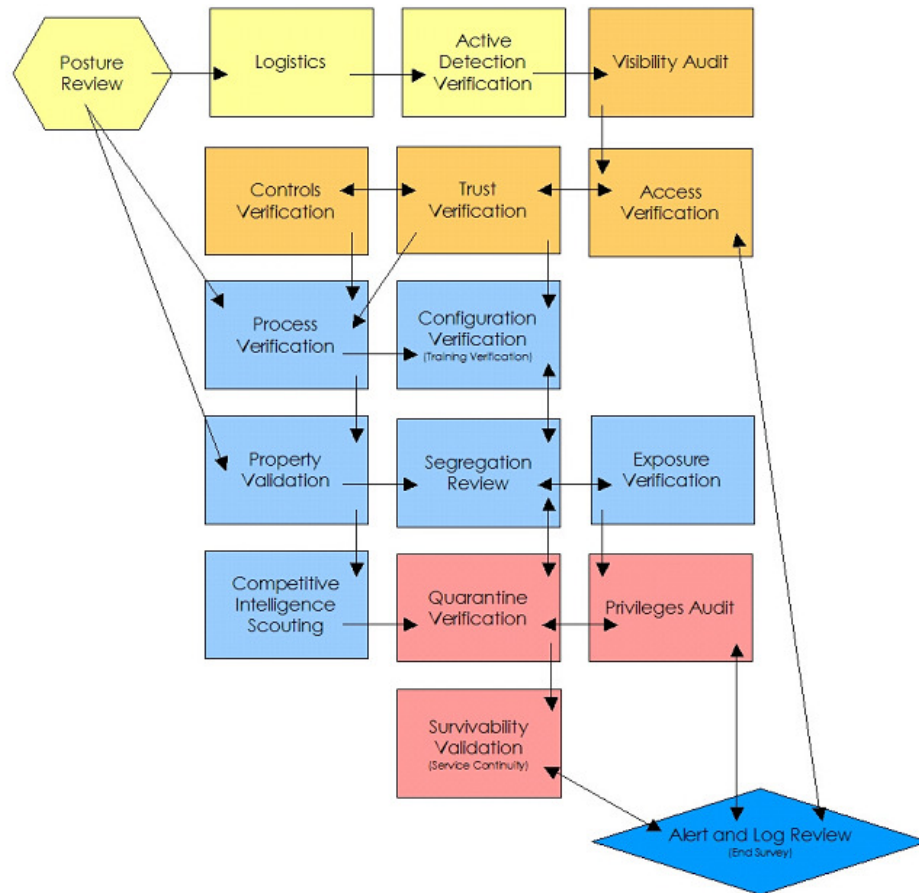
- Progetto principale di ISECOM
- **Open Source Security Testing Methodology Manual**
- + 3.000.000 di downloads
- Uno standard internazionale per i **test di sicurezza**
- Una metodologia basata su metodi scientifici
- Un mezzo per misurare precisamente la sicurezza operativa (RAVs)
- Un mezzo per ridurre **fortemente** i falsi positivi ed i falsi negativi
- Un processo concreto per essere **tecnicamente sicuri**
- Un **codice etico** con chiare **Rules of Engagement**
- **Rilasciato in Agosto 2008 nella sua terza versione (lite)**



OSSTMM: Mappa



OSSTMM: Moduli



Ogni modulo è composto da una serie di attività (task), che variano a seconda del canale sotto esame, ad esempio

Configuration Verification

1) Configuration Controls

(a) Examine controls to verify baseline configurations for OS's, applications and equipment within the scope to validate secure configurations, ensure proper security and best practices.

(b) Examine controls to verify the configurations and baselines of systems, equipment and applications meet the intent of the organization and reflect a business justification.

(c) Examine Access Control Lists (ACLs) and business roles configured on networks, systems, services and applications within the scope to ensure they meet the intent of the organization and reflect a business justification.

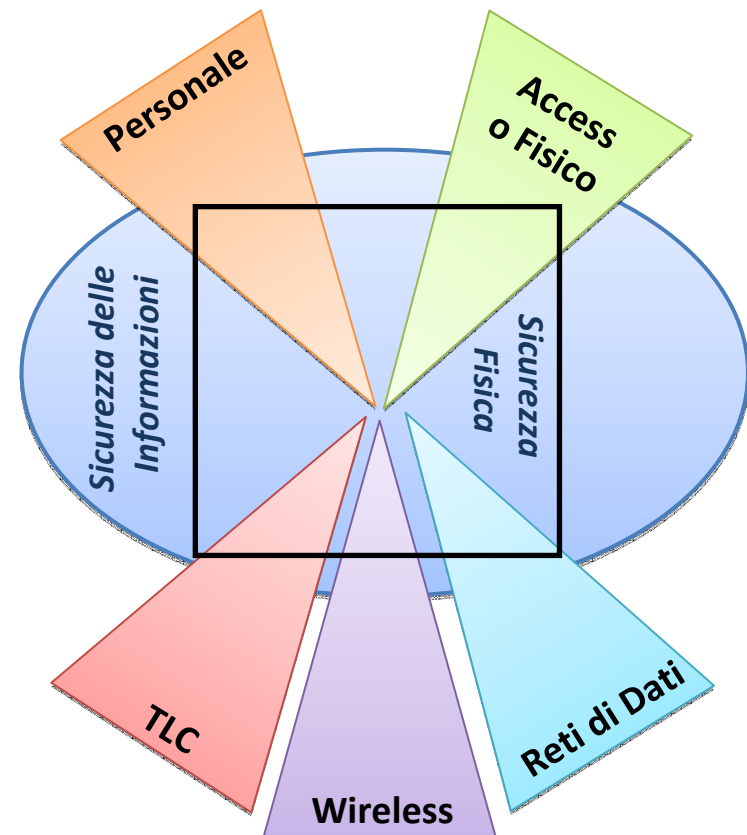
2) Common Configuration Errors ...

Struttura di OSSTMM

Ogni **canale** prevede una serie di verifiche che ne permettono di vagliare tutti gli aspetti rilevanti per la sicurezza.

Esempio: Reti di Dati

- *Network Surveying*
- *Port Scanning*
- *Services Identification*
- *System Identification*
- *Vulnerability Research & Verification*
- *Internet Application Testing*
- *Router Testing*
- *Trusted Systems Testing*
- *Firewall Testing*
- *Intrusion Detection System Testing*
- *[...]*



OSSTMM: requisiti etici

Esistono precise regole (“**rules of engagement**”) tra cui:

- non usare la paura o il dubbio (FUD) come strumento per stimolare soluzioni di sicurezza
- effettuare test di sicurezza solo dopo autorizzazione scritta
- mantenere la riservatezza delle informazioni inerenti i test anche dove non esplicitamente concordato
- effettuare prima i test non privilegiati e poi quelli privilegiati
- le criticità inerenti a rischi gravi e immediati devono essere comunicate subito al committente
- la reportistica deve includere soluzioni pratiche alle criticità
- processo di security testing trasparente verso il Cliente

OSSTMM: Dati

- Oltre 400 persone certificate solo in Italia
- Requisiti di certificazione OSSTMM già presenti in numerose RFQ e gare
- Differenze significative rispetto ad altre certificazioni in materia, tra cui:
 - *Carattere comprensivo e pratico*
 - *Basate su una metodologia internazionale affermata e riconosciuta e non su meri strumenti software*
 - *Presenza sul mercato da oltre 8 anni*
 - *Carattere open-source*

OSSTMM: perché utilizzarla?

- E' una metodologia **completa**, collaudata e condivisa tra i migliori esperti del settore;
- Fissa una **terminologia** e un'impostazione condivisa in un campo sempre in evoluzione;
- Permette di effettuare verifiche di sicurezza **esaustive** che considerano anche canali non convenzionali;
- Fornisce gli strumenti per **paragonare** diverse analisi effettuate da fornitori differenti.

Presupposto: è necessario effettuare verifiche costantemente.

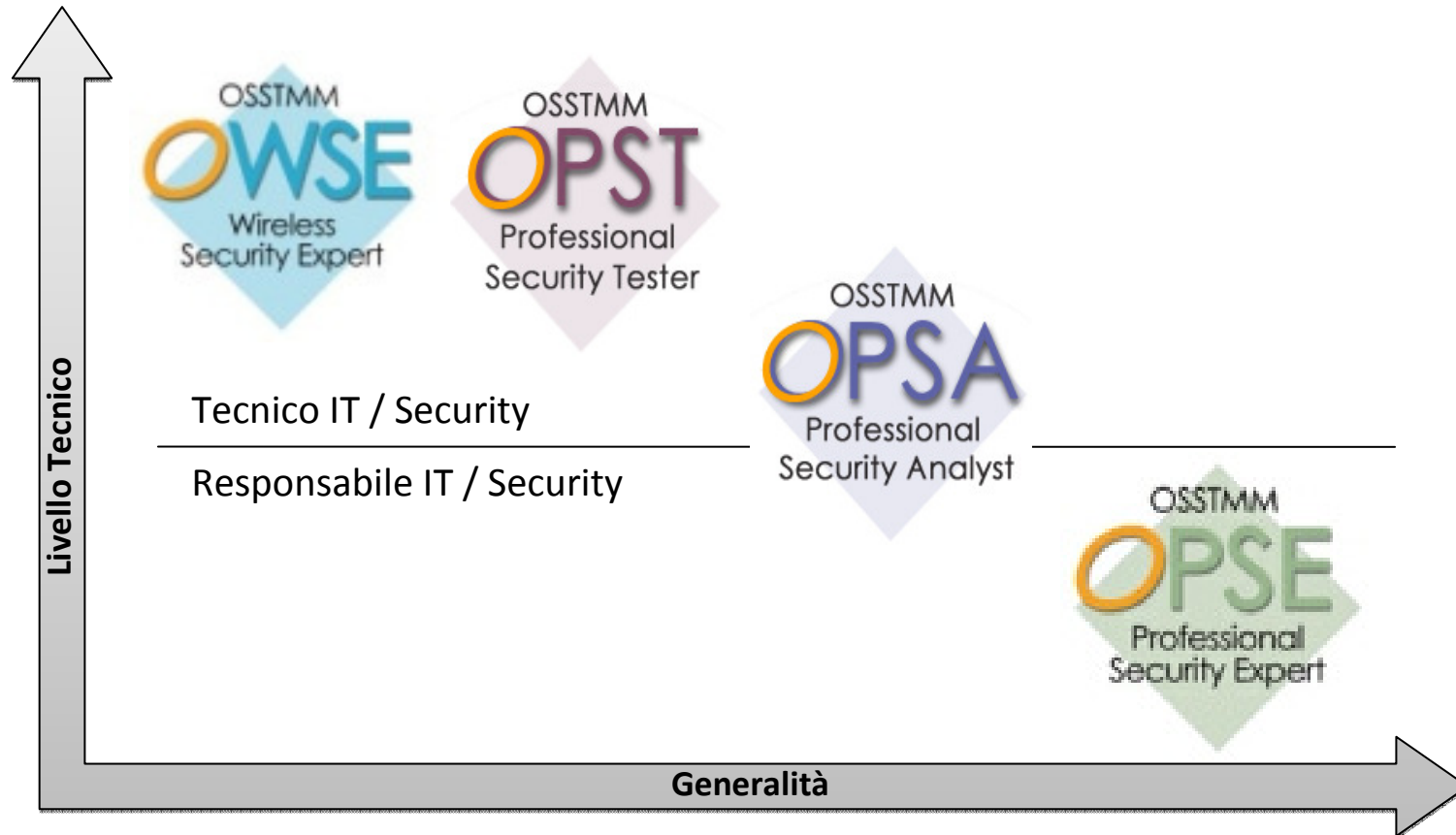
OSSTMM: Perché certificarsi

- Personale non preparato che esegue test sui sistemi e sulle reti può provocare danni consistenti
- Non è sufficiente lanciare uno (o più) software per effettuare un test di sicurezza, neanche a livello di vulnerability assessment
- Permettere a persone che non si impegnano a rispettare un forte codice etico di effettuare test di sicurezza equivale a dare le chiavi del proprio reame al primo che passa
- Non è solo importante trovare le vulnerabilità ma anche reportizzarle correttamente e individuare le soluzioni

... un ottimo hacker non è detto che sia un ottimo tester!

ISECOM: Formazione

Le certificazioni di ISECOM sono quattro, orientate a diversi profili professionali



OPST

OSSTMM Professional Security Tester

Prepara chi conduce in prima persona i test di sicurezza

Capacità acquisite:

- Effettuare test di sicurezza conformi all'OSSTMM
- Configurare e utilizzare correttamente gli strumenti necessari ai test di sicurezza
- Distinguere i falsi positivi e i falsi negativi
- Comprendere i fattori critici per la sicurezza

Audience:

- Amministratori di sistema e di rete
- Security tester / auditor
- Consulenti

Durata: 5 giorni

OWSE

OSSTMM Wireless Security Expert

Prepara chi effettua test su infrastrutture wireless

Capacità acquisite:

- Effettuare test di sicurezza conformi all'OSSTMM sui vettori d'attacco wireless
- Configurare e utilizzare gli strumenti per effettuare i test
- Comprendere il funzionamento e le possibili criticità dei protocolli e delle infrastrutture senza fili

Audience:

- Security tester / auditor
- Consulenti

Durata: 3 giorni



OPSA

OSSTMM Professional Security Analyst

Prepara chi coordina i test di sicurezza sul campo

Capacità acquisite:

- Pianificare e coordinare i test di sicurezza
- Comprendere e analizzare i risultati e i report dei test
- Derivare le debolezze della sicurezza e i rischi connessi a partire dai risultati dei test

Audience:

- CSO / CISO
- Senior security tester / auditor
- Consulenti

Durata: 5 giorni



OPSE

OSSTMM Professional Security Expert

Prepara le figure di più alto livello per la gestione della sicurezza

Capacità acquisite:

- Programmare i test di sicurezza
- Comprendere le problematiche legate ai test
- Analizzare e gestire i rischi individuati durante i test

Audience:

- CSO / CISO
- Risk manager
- Responsabili per la sicurezza

Durata: in via di definizione



MAGERIT e PILAR

Tool di supporto all'analisi del rischio

MAGERIT

Metodologia creata nel 1997 (Magerit1) ed aggiornata nel 2005 (Magerit2) dal **Ministero delle Pubbliche Amministrazioni spagnolo** con la collaborazione del CNI (Centro Nazionale di Intelligence)

> **Metodologia per l'Analisi e la Gestione del Rischio IT** <

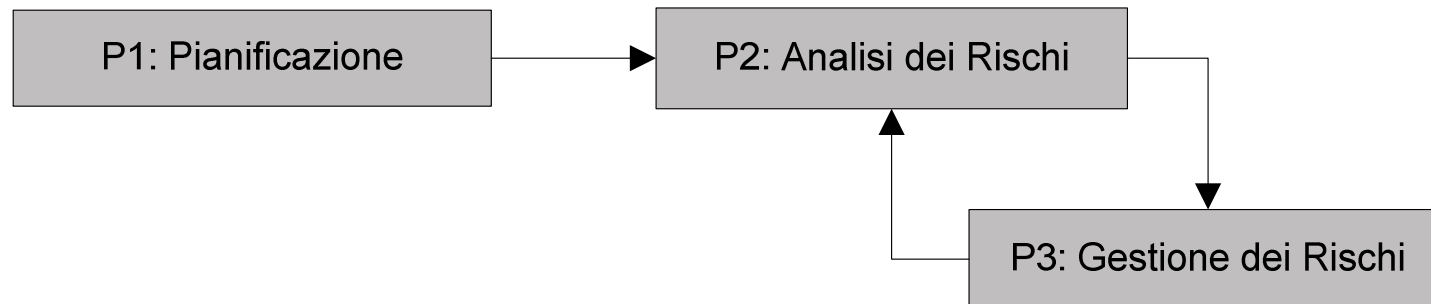
Attualmente impiegata principalmente in:

- Ministeri spagnoli di Ambiente, Economia, Interni, Agricoltura, Difesa
- Zecca Spagnola (FNMT) e NATO
- Imprese di consulenza e aziende private



MAGERIT

- Conforme agli standard ISO/IEC 27001 (con certificazioni attive anche in Italia), 27002, 27005 e 13335
- Censito dall'ente europeo ENISA (http://www.enisa.europa.eu/rmra/rm_home.html)
- Ampliamente impiegata in Europa, Sud America, ME, USA
- Disponibile in Inglese e Spagnolo e in Italiano (il libro 1)
- Metodologia liberamente accessibile e in continua evoluzione



MAGERIT

Libro 1: La Metodologia

Approccio descritto da tre diversi punti di vista:

- Aspetto teorico: analisi dei rischi e mitigazione (capitolo 2);
- Passi base: step principali da intraprendere in un progetto di analisi del rischio (cap.3);
- Applicazione della metodologia nell'intero sviluppo di sistemi informativi.

Libro 2: Catalogo degli Elementi

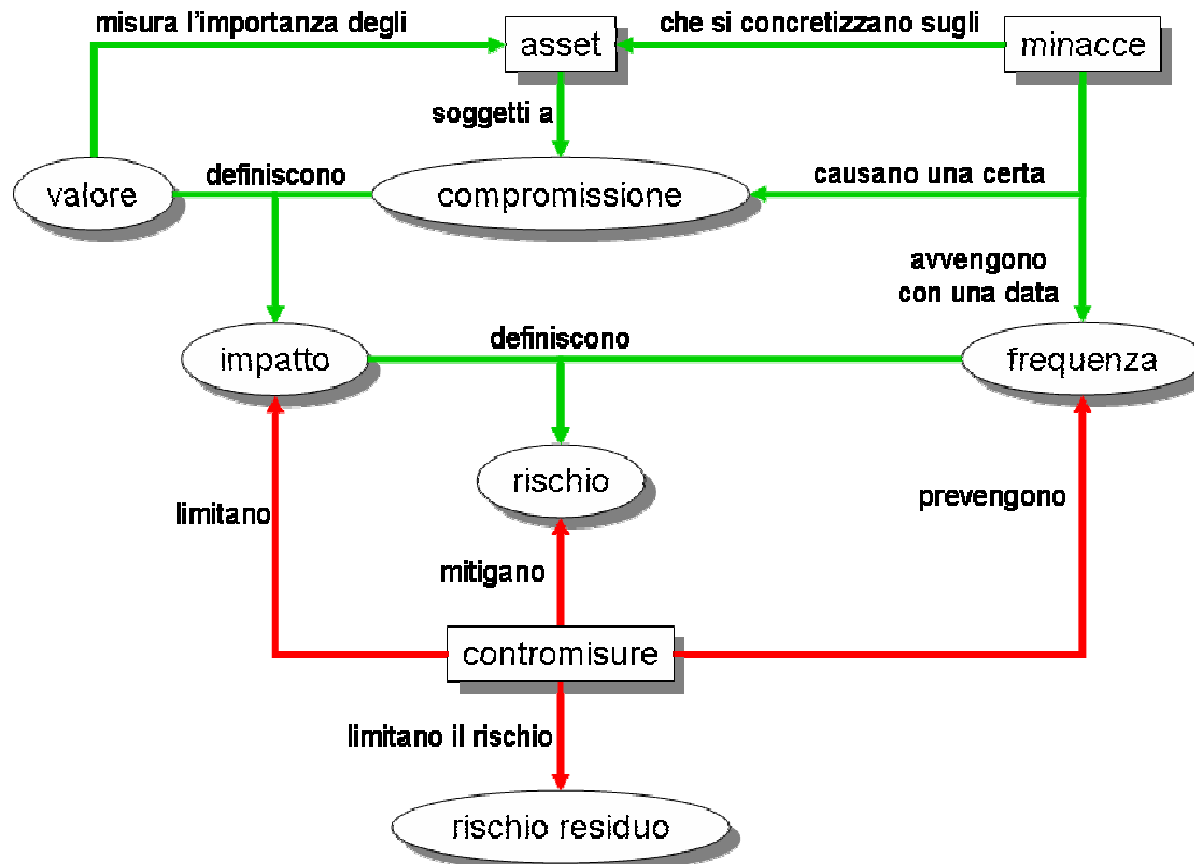
Contiene un elenco specifico di tipi di asset, dimensioni di valutazione, criteri, minacce e contromisure.

Libro 3: Tecniche

Contiene descrizione di tecniche utilizzabili in ambito di analisi del rischio e gestione di progetti.

MAGERIT

Schema di calcolo del rischio / nomenclatura utilizzati da MAGERIT



MAGERIT: Strumenti di supporto

Per l'impiego della metodologia sono stati sviluppati, con il coordinamento di J.M Mañas, una serie di strumenti di supporto software, tutti di carattere cross platform (Java) e stand-alone:

PILAR (già EAR) – strumento principale per l'effettuazione di Risk Assessment con la metodologia MAGERIT

PILAR Basic – versione “light” dello strumento PILAR

RMAT – strumento per la modifica dei principali parametri di PILAR

Questi strumenti sono mantenuti e distribuiti in lingua italiana (in esclusiva) attraverso il sito internet www.sgsi.net

IT Risk Management con PILAR

Prepara in modo pratico le figure che devono eseguire delle attività di analisi e gestione del rischio.

Programma del corso:

- Introduzione al Risk Management
- ISO 27001 e 27005: lo standard
- Metodologie e Strumenti
- Elementi dell'analisi del rischio
- Livelli di rischio
- Opzioni di trattamento del rischio
- Introduzione alla Gestione della Continuità Operativa (BCM)
- Analisi degli impatti (BIA) e gestione degli incidenti
- Campi d'impiego (DPS, PCI, Rischi Operativi, ERM, 231)



Durata: 3 giorni

Contatti



<http://www.mediaservice.net>

info@mediaservice.net

Via San Bernardino 17, 10141
Torino, ITALY

Tel. +39 0113272100

Fax. +39 0113246497

