



Presentazione dell'iniziativa ROSI

Return on Security Investment
Security Summit Roma
Alessandro Vallega – Oracle Italia

Sponsor dell'iniziativa

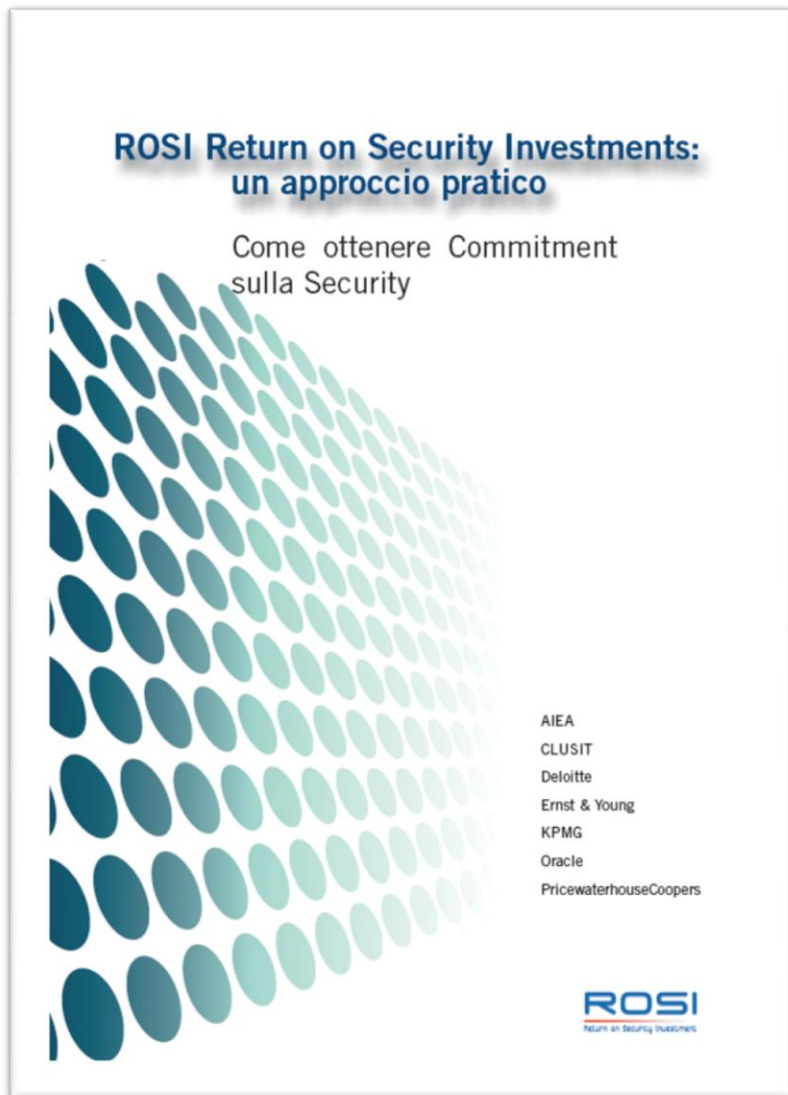
Ogni azienda / associazione ha investito il proprio tempo



Panel

- Alberto Piamonte (AIEA)
- Mauro Cicognini (CLUSIT)
- Andrea Longhi (Deloitte)
- Pierluigi Lonerio (KPMG)
- Alessandro Vallega (Oracle)

Prodotto



- Documento di 60 pagine
 - Avente lo scopo di facilitare e orientare il decision maker di investimenti di sicurezza
 - Licenza “Attribuzione-Condividi nello stesso modo”
- Mini sito di supporto

Motivazioni del gruppo di lavoro

- “Mettersi al servizio”
- Aiutare a fare “un passo avanti”
 - Serve sicurezza
 - Serve la capacità di scegliere gli investimenti “giusti” per la propria azienda
 - Serve la capacità di sostenere le proprie scelte
- Principali problemi identificati nel mondo reale

ROI → ROSI

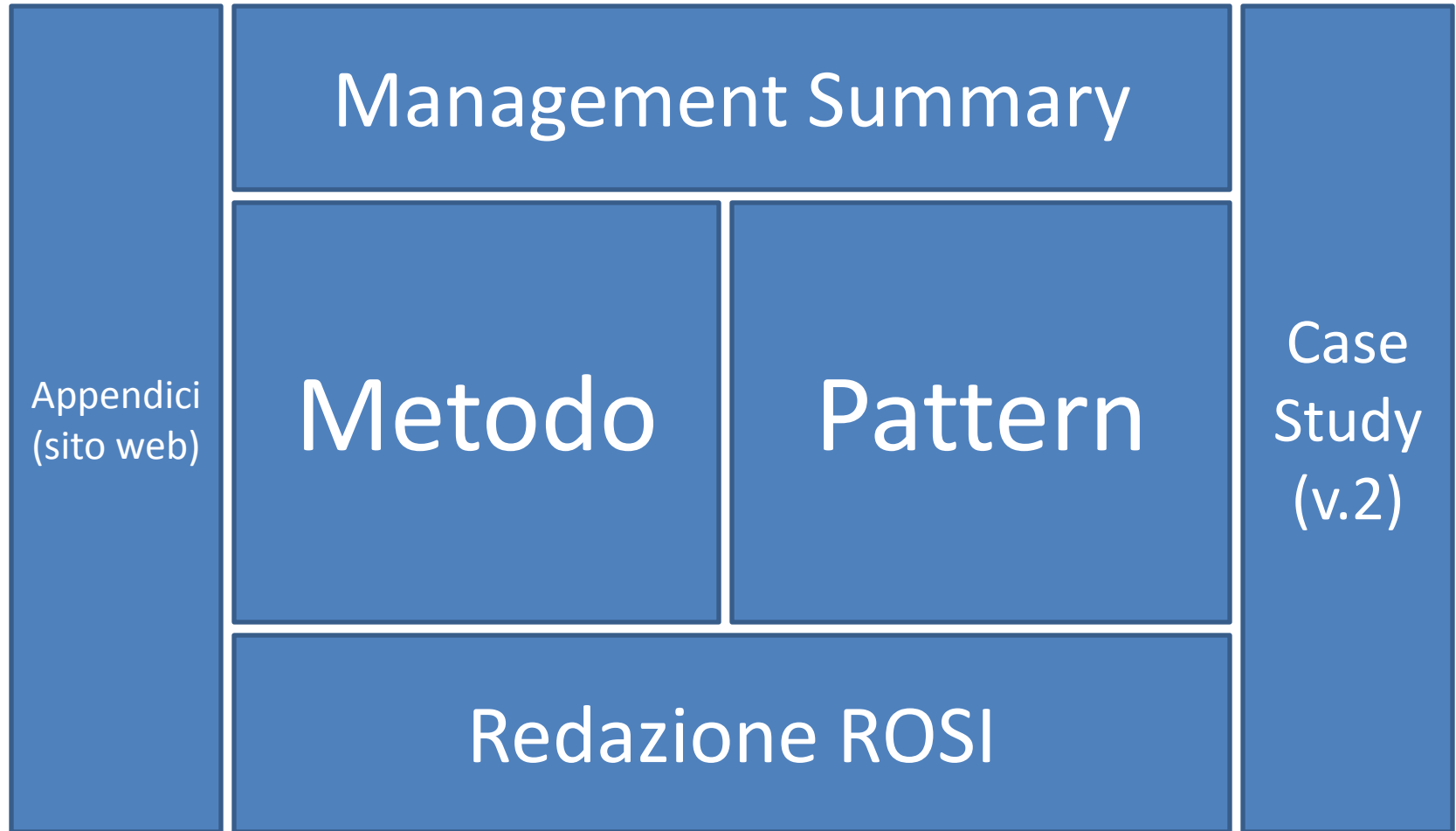
- Gli investimenti in sicurezza vengono effettuati per:
 - Contenere il **Rischio** operativo
 - Garantire la **Compliance**
 - Proteggere l' **Immagine** aziendale
 - Aumentare l' **Efficienza** dei processi di sicurezza
- L'approccio matematico del ROI fa fatica a rappresentare tali motivazioni

$$NPV = \sum_{t=0}^n \frac{C_t}{(1 + \bar{r})^t} = 0$$

ROSI

- Approccio strutturato per
 - Scegliere dove investire
 - Scegliere come investire
 - Spiegare le ragioni delle proprie scelte
- Flessibile
 - Top-Down
 - Verify (bottom-up)
- Potente
 - Frutto delle competenze del gruppo di lavoro
 - Forte riuso delle best practice internazionali

Struttura del documento



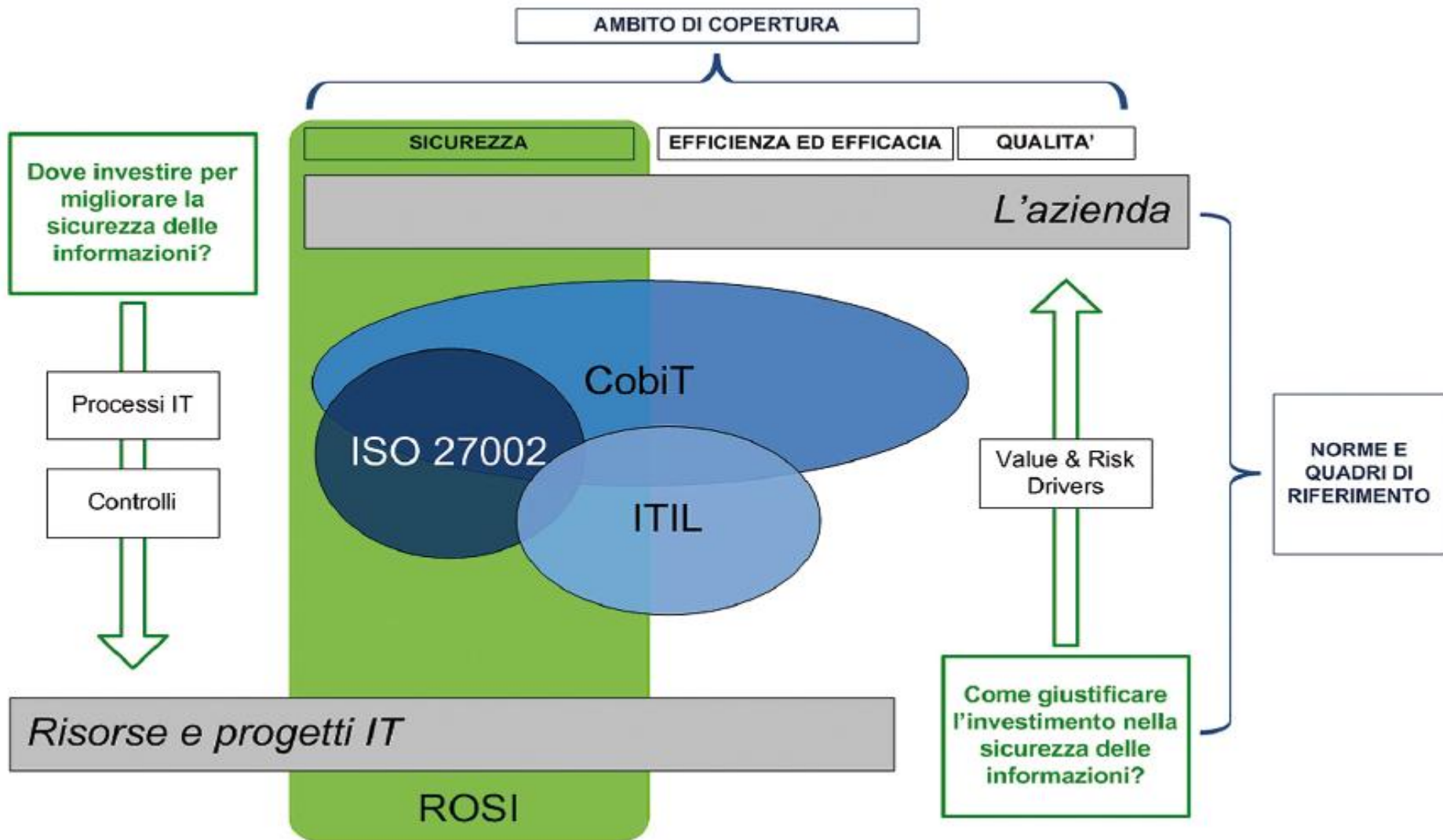
Definizione di sicurezza

*“Il termine **sicurezza dell’informazione** significa proteggere l’informazione e i sistemi informativi da accesso, uso, diffusione, interruzione, modifica e distruzione non autorizzati, al fine di fornire:*

- *Riservatezza*
- *Integrità*
- *Disponibilità”* *(title 44 of the US Code)*

... e perseguendo l’obiettivo ulteriore di Conformità a leggi e regolamenti!

ROSI e le best practices



Obiettivi del metodo

- Dove intervenire
- Perché intervenire
- Come intervenire
- I benefici
- Chi trae beneficio dall'intervento
- Come misurare l'efficacia dell'intervento
- Il ROSI
- Come illustrare il ROSI al management

Fase 1 Identificazione esigenze	Fase 2 Identificazione scenari di intervento	Fase 3 Valutazione ROSI per ogni scenario	Fase 4 Predisposizione documento ROSI
PDCA (Deming)	CMM (IT Gov. Institute)	ISF (Information Security Forum)	Common Sense
ISO/IEC 27001:2005	ISO/IEC 27005:2008	KCI / KRI	ValIT
Framework processi sicurezza ABI-LAB	Business Impact Analysis / Risk Management	GISS 2010 (Security Survey)	
RIDC	ISO/IEC 27002	ITIL	
CobiT 4.1	Stakeholder Identification		
Pattern (6)			
Case study (0)			

Pattern

- Disponibili

- Amministratori di sistema
- Identity and Access Management
- Single Sign On
- Intrusion Detection System
- Application Security
- Sicurezza Fisica

- In preparazione

- Information Rights Management
- Data Base security
- Data Loss Prevention
- SCADA e DCS Security Assessment

Struttura dei pattern

- Nome e Area di intervento (ISO 27000)
- Chiavi di classificazione
 - Criteri di sicurezza (RIDC)
 - Risorse impattate (Infrastruttura, Risorse, Applicazioni, Informazioni)
 - Driver di Business (Rischi, Compliance, Immagine, Efficienza)
- Contesto di riferimento
- Descrizione
- Driver / Motivazioni
- Punti di attenzione
- Elementi di valutazione
- Benefici / Vantaggi

Es. Identity & Access Management

NOME	Identity and Access Management
AREA DI INTERVENTO	11.1.1 Access Control Policy 11.2.1 User Registration 11.2.2 Privilege Management 11.2.3 User Password Management 11.2.4 Review of User Access Rights 11.5.2 User Identification and Authentication 11.6.1 Information Access Restriction
SINTESI	
Criteri di Sicurezza	<input checked="" type="checkbox"/> Conformita` <input checked="" type="checkbox"/> Riservatezza <input type="checkbox"/> Integrita` <input type="checkbox"/> Disponibilita`
Risorse Impattate	<input checked="" type="checkbox"/> Infrastruttura <input checked="" type="checkbox"/> Risorse Umane <input checked="" type="checkbox"/> Applicazioni <input type="checkbox"/> Informazioni
Driver di Business	<input checked="" type="checkbox"/> Rischi operativi <input checked="" type="checkbox"/> Compliance <input type="checkbox"/> Immagine aziendale <input checked="" type="checkbox"/> Efficienza processi
CONTESTO DI RIFERIMENTO	
La tematica dell'Identity and Access management si colloca nell'ambito delle attività di gestione degli accessi logici ai sistemi informativi aziendali.	
DESCRIZIONE	
Per soluzione di Identity and Access Management si intende la definizione di un modello organizzativo e procedurale che sia in grado, con il supporto di opportuni strumenti tecnologici, di gestire le identità degli utenti per l'intero loro ciclo di vita. L'adozione di una soluzione IAM consente pertanto la gestione in modalità automatica degli account utente e delle abilita-	

Business Case

“L'arte di dare alle cose la forma più adatta per raggiungere un obiettivo specifico”

Paul Rand (sul design)

- Executive Summary
- Stato dell'arte
- Obiettivo desiderato
- Proposta operativa

Evoluzioni in corso

- Revisione generale
- Nuovi Pattern
- Case Study aziendali
 - Framework e Strumenti per il gruppo di lavoro
- Prossima release del ROSI pianificata per settembre 2010



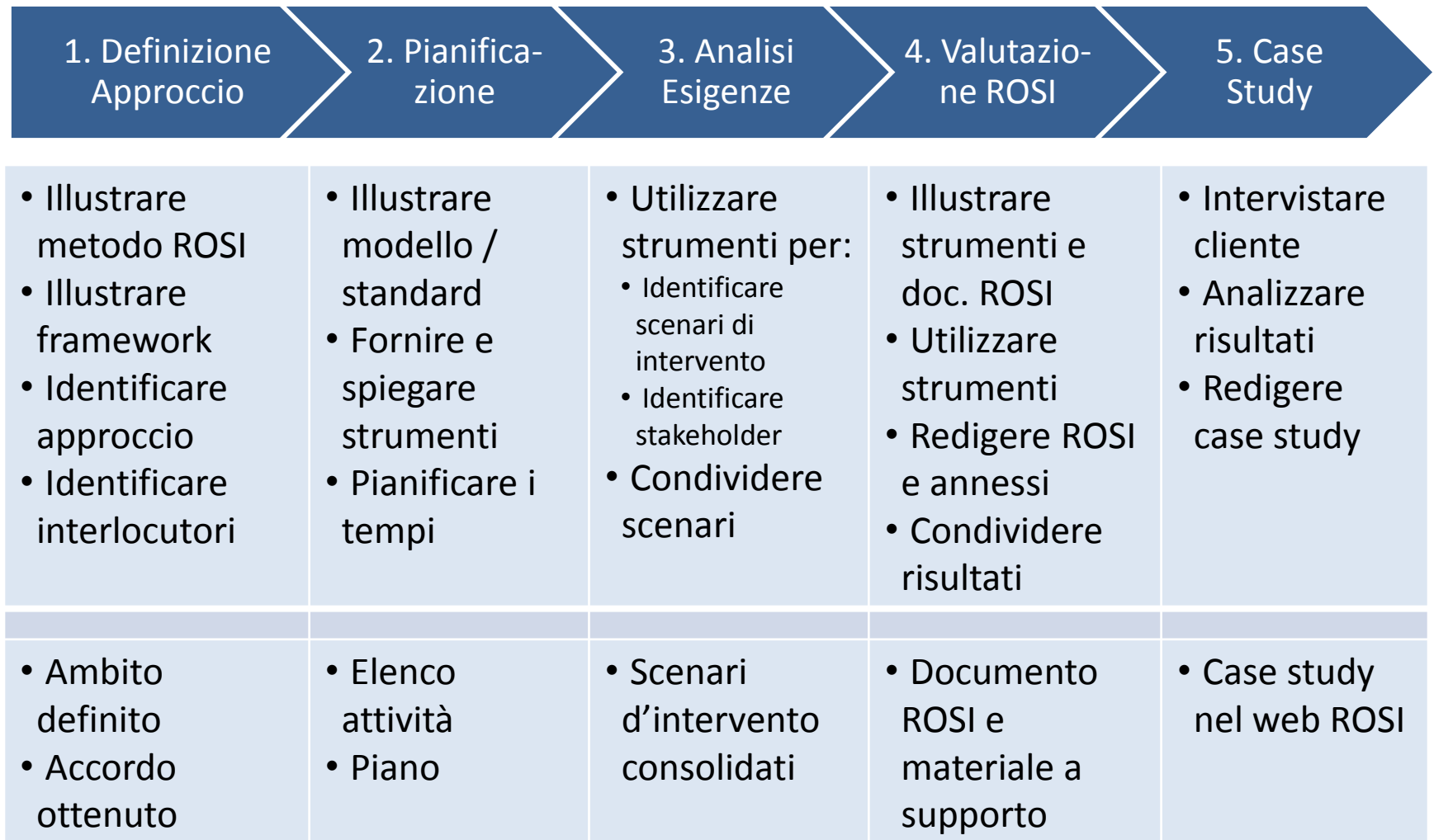
Framework di approccio ROSI

Gruppo di lavoro ROSI - maggio 2010

Criterio ispiratore: Spot light

- Semplificare, senza banalizzare, il processo decisionale relativo agli investimenti in sicurezza
- Procedere per passi, mettere a fuoco un “argomento” alla volta
 - Questo è a maggior ragione valido la prima volta e nel caso relativo alla redazione del case study
- Limitare gli strumenti all’approccio scelto

Il metodo...



Approccio Top Down:Ambiti

Ambiti dell'approccio Top Down

- Security Governance
 - Come l'azienda gestisce la sicurezza da un punto di vista organizzativo
- Processi IT
 - Come l'IT incorpora e tratta la sicurezza nei suoi processi
- Security Risk Management
 - Come l'azienda valuta il rischio di sicurezza (riservatezza, integrità, disponibilità, compliance)

Approccio Verify: Esigenze

Esempi di potenziali esigenze per l'approccio Verify

- Amministratori di sistema
- Identity and Access Management
- Single Sign On
- Intrusion Detection System
- Data Security
- Sicurezza Fisica
- Information Rights Management
- Database Security
- Data Loss Prevention

Gli strumenti

		Approccio Top Down			Approccio Verify
Specifici	Ambito Security Governance	Ambito Processi IT	Ambito Security Risk Management	Esigenza d'interesse	
	<ul style="list-style-type: none"> • SG1 (Framework Processi Sicurezza) 	<ul style="list-style-type: none"> • IT1 (Processi IT security related) 	<ul style="list-style-type: none"> • ISO27005 	<ul style="list-style-type: none"> • Pattern 	
	<ul style="list-style-type: none"> • SG2 (CMM in ambito Sec Gov, con ISO27002) 	<ul style="list-style-type: none"> • IT2 (CMM in ambito Processi IT, con ISO27002) 	<ul style="list-style-type: none"> • SRM2 (CMM in ambito SRM, modello basato su RiskIT e CMM) 		
Comuni	Template Case study e schema d'intervista				
	Linee guida CMM				
	Template ROSI				
	Linee guida calcolo KRI / KCI				
	Linee guida identificazione stakeholder				

Conclusioni

Come accedere

<http://rosi.clusit.it>

ROSI

Return on Security Investment

A cura di



Cosa è il ROSI

Autori del ROSI e motivazioni

Perchè fare investimenti in sicurezza delle informazioni

Perchè valutare gli investimenti utilizzando il ROSI

A chi si rivolge

Guida alla lettura

Download

Appendici

Autori

Ulteriori sviluppi

FAQ

Contatti

ROSI sta per "Return On Security Investment", e, con questa sigla, s'intende il lavoro di valutazione dei vantaggi potenziali di un investimento in sicurezza, in particolare in sicurezza delle informazioni.

è un supporto decisionale rivolto in primis a quanti sono in posizioni di responsabilità sul settore di Information e Communication Technology delle organizzazioni, e devono allocare in modo prudente delle risorse scarse. Può essere anche, a posteriori, un supporto per la valutazione di efficacia di processi e/o impianti già in produzione.

Non è, come si può intuire, un'oggetto paragonabile al ROI che si calcola in ambito finanziario, in quanto non stiamo trattando un investimento nel senso tecnico del termine ovvero di una spesa per un bene che di per sé produrrà ricavi (a meno che il business principale dell'investitore sia proprio la sicurezza) ma uno strumento per analizzare, decidere e supportare le scelte di investimento in sicurezza delle informazioni basato su solide basi metodologiche e nel contempo adattabile alle esigenze dell'utilizzatore.

ROSI Return on Security Investments: un approccio pratico

Come ottenere Commitment sulla Security



AIEA
CLUSIT
Deloitte
Ernst & Young
KPMG
Oracle
PricewaterhouseCoopers



I contenuti di questo sito sono rilasciati sotto Licenza Creative Commons Attribuzione - Condividi allo stesso modo 2.5 Italia . Per informazioni o contatti scrivere a: rosi@clusit.it

Done

Come contribuire

- Nel minisito si trovano le istruzioni
- Sono graditi contributi rispetto:
 - Stesura di Pattern
 - Sperimentazione uso del ROSI presso la propria azienda (per sezione Case Studies)
 - Idee, correzioni, suggerimenti

ROSI

Return on Security Investment