



GRC: una questione di merito

La moltitudine delle fonti di informazioni, sistemi di sicurezza e di monitoraggio, e la complessità crescente delle organizzazioni che spesso ostacolano una visione d'insieme dei problemi e delle strategie da perseguire, pongono una duplice questione di merito: necessità di sintetizzare ed interpretare efficacemente i dati rappresentativi dello stato di sicurezza del target e necessità di centralizzare le azioni ed il monitoraggio della loro efficacia

a cura di: **Marco Fasciani – CTO Smetana Informatica**

Pasquale De Rinaldis – CISA, CISSP, LA ISO27001

Ombretta Palma – CISM, CISA, LA ISO27001



INDICE DELLA PRESENTAZIONE :

1. **GRC: Definizioni e Problematiche**
2. Una Proposta di Integrazione
3. InfoSec Governance
4. Risk Management
5. Compliance
6. Elementi che abilitano l'integrazione
7. Q&A



Informazioni, processi, regole e strumenti che consentono al Top Management di definire, indirizzare, concretizzare e monitorare la strategia aziendale



Strutturata e continua rilevazione e controllo dei rischi sul patrimonio informativo e produttivo



Verifica e Monitoraggio dell'applicazione e dell'aderenza all'assetto normativo, interno e cogente, applicabile



Storicamente, l'origine di ciascuna delle tre prassi aziendali che compongono il GRC, trova compimento a livello Corporate. Ciascuna delle tre componenti si è poi specializzata, sviluppandosi singolarmente, in ambiti e con livelli di maturità differenti, e supportata da strumenti diversi.



Troppo spesso gli strumenti a supporto sono stati caratterizzati nel tempo da specificità e disomogeneità.



Allo stato attuale, dunque, il rischio per le organizzazioni è quello di scegliere soluzioni adatte ad analizzare singole problematiche e gestire verticalmente determinati processi, complessi framework caratterizzati da ambizioni deterministiche o di contro da un eccessivo livello di astrazione.

Risultato?

- ✓ Duplicazione delle attività
- ✓ Ridondanza delle informazioni
- ✓ Dispersione di risorse / investimenti
- ✓ Perdita della visione trasversale e d'insieme
- ✓ Scarsa credibilità dei risultati e difficoltà nella comparazione degli stessi
- ✓ Minore percezione dei vantaggi.



Lavorare in modo collaborativo, condividendo **una visione unica** ed omogenea dei processi, dello scenario informativo dell'organizzazione, utilizzando un **linguaggio univoco** che impedisca le ambiguità e le incomprensioni e beneficiando di una gestione coerente delle strategie, delle iniziative e delle informazioni.

Delineare un sistema di gestione della sicurezza che disciplini, con metriche comuni, la definizione delle obiettivi da perseguire, le modalità di misurazione, controllo (auditing) e gestione e gli strumenti per attuarne la conformità nel tempo, costituendosi altresì come punto efficace per conciliare la visione di business con quella prettamente tecnologica.

GRC:Perchè



L'adozione di un sistema di GRC che supporti sia i processi decisionali a sostegno della definizione delle strategie aziendali, sia la gestione dei Rischi (siano questi di processo o prettamente tecnologici), che la Compliance rispetto alle normative (e.g. Privacy, BASEL II, PCI-DSS, HIPAA, D.Lgs 231-01), può rappresentare la chiave di volta per conciliare la visione di business con l'ambito tecnologico.

Un sistema integrato di GRC comporterebbe anche un non trascurabile rafforzamento di immagine delle funzioni coinvolte come portatrici di valore aggiunto in grado di contribuire, mediante l'integrazione di ambiti così strategici, a generare nuove opportunità.

GRC: Vantaggi



I principali vantaggi operativi nell'adozione di un sistema di GRC sono rappresentati da:

- ✓ Rapidità e completezza nella raccolta delle informazioni,
- ✓ Uniformità nell'approccio di analisi, decisione, trattamento e gestione,
- ✓ Centralizzazione degli strumenti di monitoraggio e controllo con conseguente maggiore proattività,
- ✓ Visione trasversale ed unitaria delle problematiche con possibilità di approfondimenti e verticalizzazioni per ambito,
- ✓ Abilitazione di una logica di partnership tra le funzioni IT, Information Security, Audit, Compliance, ed il Top Management che è richiesta per il perseguimento di obiettivi aziendali sempre più sfidanti.



La componente di **InfoSec Governance** rappresenta il contributo fornito dalle strategie di protezione delle informazioni aziendali e dai processi adottati per definirle, implementarle e monitorarle, al raggiungimento e miglioramento degli obiettivi aziendali.

Rappresenta quindi un punto di contatto diretto tra la gestione della sicurezza del patrimonio informativo aziendale e dei sistemi di Information & Communication Technology e gli obiettivi di business dell'azienda.



L'ambito **InfoSec Risk Management** riguarda la strutturata e continua rilevazione, valutazione, controllo dei rischi alla Riservatezza, Integrità e Disponibilità del patrimonio informativo sulla base del quale l'azienda indirizza e gestisce il proprio business.

Costituisce quindi l'elemento centrale per lo sviluppo di una strategia di Information Security a tutela e protezione del business dai cosiddetti rischi puri.



L'InfoSec Compliance Management invece si focalizza sulle modalità attraverso le quali l'azienda garantisce l'osservanza delle normative cogenti, generali e di settore, direttamente indirizzate alla sicurezza delle informazioni, dei sistemi ICT o nelle quali questi ultimi siano coinvolti nonché la conformità ai sistemi di autoregolamentazione stabiliti dall'azienda stessa.

Contribuisce dunque a tutelare gli interessi di stakeholders e shareholders dal rischio di coinvolgimento dell'azienda in illeciti amministrativi o reati.



INDICE DELLA PRESENTAZIONE :

1. GRC: Definizioni e Problematiche
2. **Una Proposta di Integrazione**
3. InfoSec Governance
4. Risk Management
5. Compliance
6. Elementi che abilitano l'integrazione
7. Q&A



- ✓ Sistema centralizzato di raccolta ed elaborazione delle informazioni capace di supportare il TOP Management nell'analisi e scelte di investimento, priorità ed intervento più opportune
- ✓ Identificazione e gestione dei cambiamenti dello scenario: Process Inventory e relazione con il mondo ICT – Asset modelling (correlazione tra CMDB, Asset e catalogo servizi)
- ✓ Computazione delle vulnerabilità tecnologiche in modo oggettivo, mentre quelle organizzative/fisiche in modalità soggettiva tramite questionari
- ✓ Coordinamento e correlazione delle operazioni di analisi, correlazione e calcolo



- ✓ Sintesi, in coefficienti di rischio, del grado di esposizione di un processo, servizio, asset tecnologico ad una o più minacce capaci di sfruttare possibili vulnerabilità
- ✓ Monitoraggio delle evoluzioni dei coefficienti e degli indicatori di rischio nel tempo
- ✓ Correlazione dei coefficienti di rischio con la criticità del processo (business impact analysis) e degli asset di riferimento
- ✓ Incident Management e Risk Management: tuning dei livelli di rischio in rapporto agli eventi ed incidenti di sicurezza occorsi, riducendo il grado di soggettività nella valutazione

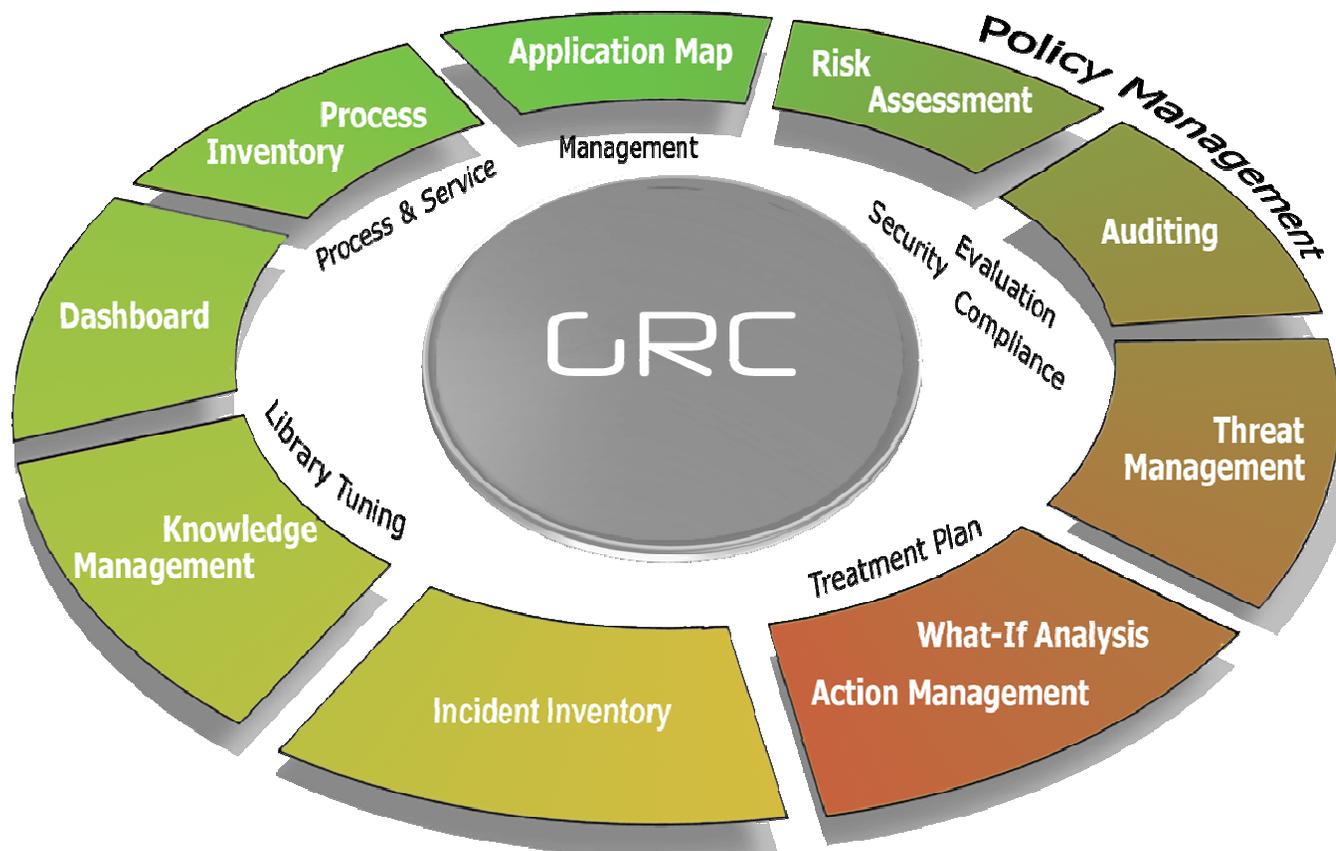


- ✓ Integrazione con la raccolta delle informazioni generate da apparati di sicurezza e sistemi di controllo e monitoraggio (SIEM, Vulnerability Scanner, IDS/IPS)
- ✓ Sviluppo di simulazioni per verificare l'efficacia degli scenari di intervento (what if analysis)
- ✓ Correlazione tra gli interventi necessari, in modo da ottimizzare le strategie di investimento (analisi costi – benefici), sia per le esigenze di riduzione dei rischi che di chiusura di non conformità o di mancata aderenza ai vincoli cogenti
- ✓ Gestione del Workflow relativo ai processi ed attività di miglioramento includendo la gestione dei processi di approvazione formale



- ✓ Reporting capace di sintetizzare e correlare informazioni rilevabili da molteplici sorgenti dati per rappresentare in maniera efficace ed intuitiva lo stato e l'andamento della sicurezza.
- ✓ Utilizzo di metriche per la valutazione del livello di Maturità del Processo di Information Security Governance
- ✓ Gestione delle metriche di verifica, delle misurazioni e delle evidenze, per identificare i gradi di aderenza agli obiettivi di controllo.

Caratteristiche

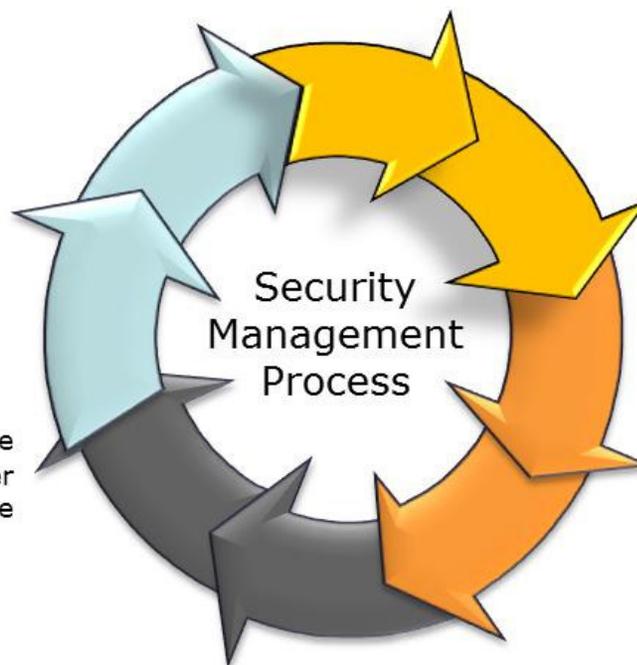


GRC vs ISO



PLAN: Individuazione degli obiettivi di sicurezza in base ai requisiti di business. Pianificazione e progettazione dell'ISMS da realizzare

ACT: realizzazione delle attività di miglioramento per eliminare anomalie e raggiungere gli obiettivi di sicurezza attesi



DO: Implementazione ISMS e relativa gestione

CHECK: Verifica e Monitoraggio dello stato di sicurezza esistente e confronto con quanto progettato



Fase 1: *Plan*

Obiettivi Contesto e Sessione
Risk Assessment
Business Impact Analysis
Risk Mitigation Plan
Security Auditing



Fase 2: *Do*

Action Management



Fase 3: *Check*

Risk Assessment
Security Auditing
Monitoraggio
Indicatori & Reporting
Incident Management



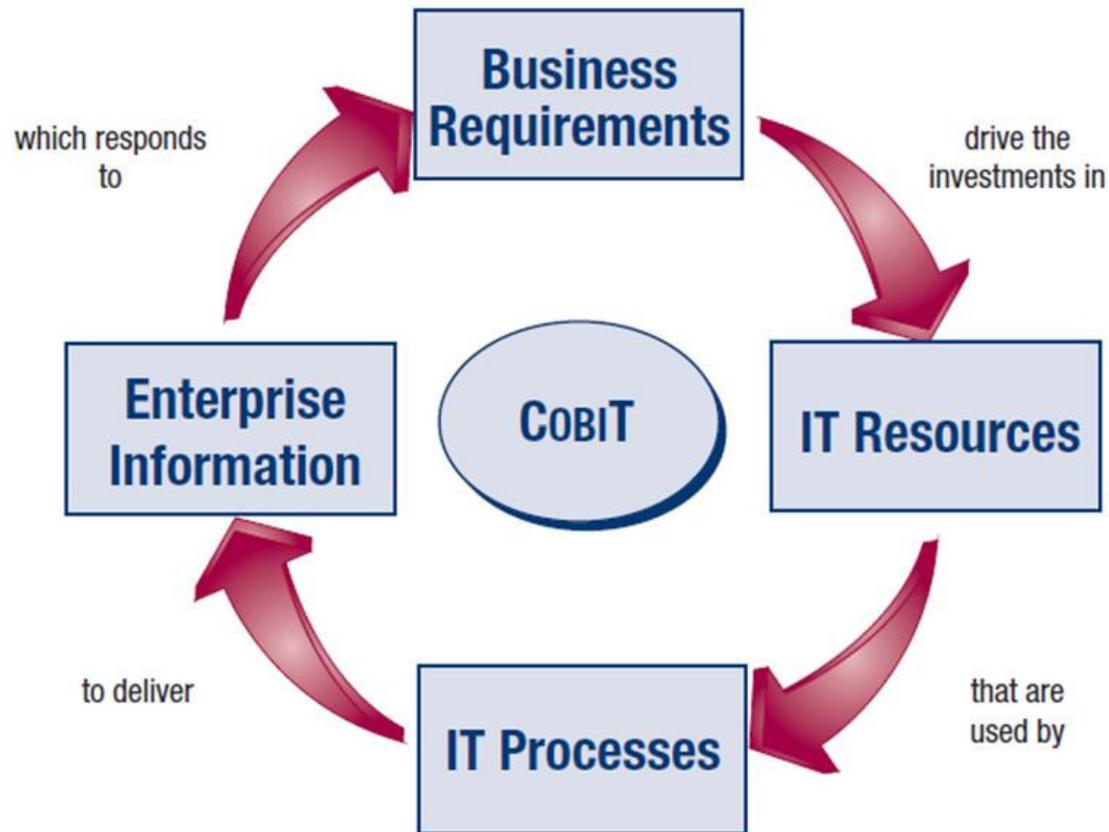
Fase 4: *Act*

Action Management



INDICE DELLA PRESENTAZIONE :

1. GRC: Definizioni e Problematiche
2. Una Proposta di Integrazione
- 3. InfoSec Governance**
4. Risk Management
5. Compliance
6. Elementi che abilitano l'integrazione
7. Q&A



Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



COBIT'S INFORMATION CRITERIA

Confidentiality concerns the protection of sensitive information from unauthorised disclosure

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities

Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



COBIT'S INFORMATION CRITERIA

Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner

Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources

Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor. Within the COBIT framework, these domains are called:

- **Plan and Organise (PO)**—Provides direction to solution delivery (AI) and service delivery (DS)
- **Acquire and Implement (AI)**—Provides the solutions and passes them to be turned into services
- **Deliver and Support (DS)**—Receives the solutions and makes them usable for end users
- **Monitor and Evaluate (ME)**—Monitors all processes to ensure that the direction provided is followed

Across these four domains, COBIT has identified 34 IT processes that are generally used

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



The COBIT framework is populated with the following core components:

- The 34 IT processes, giving a complete picture of how to control, manage and measure each process. Each process is covered in four sections, and each section constitutes roughly one page, as follows:
- Process description summarising the process objectives, with the process description represented in a waterfall.
- The mapping of the process to the information criteria, IT resources and IT governance focus areas by way of P to indicate primary relationship and S to indicate secondary.
- The control objectives for this process
- The process inputs and outputs
- The RACI chart
- The goals and metrics
- The maturity model for the process.

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



CobiT Process	Confidentiality	Integrity	Availability	Compliance
PO2 - Define the Information Architecture	S			
PO6 - Communicate Management Aims and Direction		P		S
PO8 - Manage Quality		S		
PO9 - Assess and Manage IT Risks	P	P	P	S
AI2 - Acquire and Maintain Application Software		S		
AI3 - Acquire and Maintain Technology Infrastructure		S	S	
AI4 - Enable Operation and Use		S	S	S
AI5 - Procure IT Resources				S
AI6 - Manage Changes		P	P	
AI7 Install and Accredite Solutions and Changes		S	S	

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



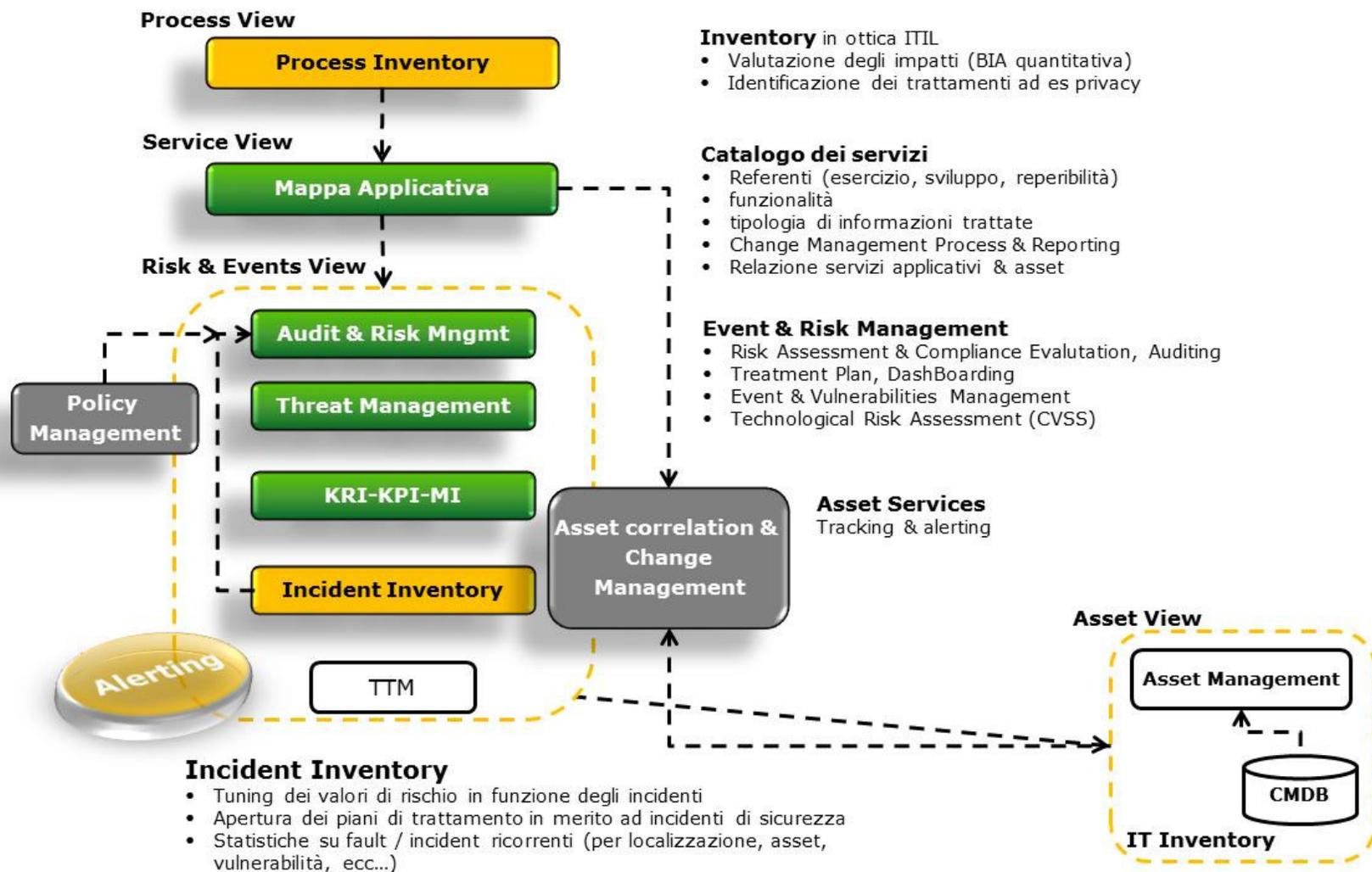
CobiT Process	Confidentiality	Integrity	Availability	Compliance
DS1 - Define and Manage Service Levels	S	S	S	S
DS2 - Manage Third-party Services	S	S	S	S
DS3 - Manage Performance and Capacity			S	
DS4 - Ensure Continuous Service			P	
DS5 Ensure Systems Security	P	P	S	S
DS9 - Manage the Configuration			S	
DS10 - Manage Problems			S	
DS11 - Manage Data		P		
DS12 - Manage the Physical Environment		P	P	
DS13 Manage Operations		S	S	

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



CobiT Process	Confidentiality	Integrity	Availability	Compliance
ME1 - Monitor and Evaluate IT Performance	S	S	S	S
ME2 - Monitor and Evaluate Internal Control	S	S	S	S
ME3 - Ensure Compliance With External Requirements				P
ME4 - Provide IT Governance	S	S	S	S

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



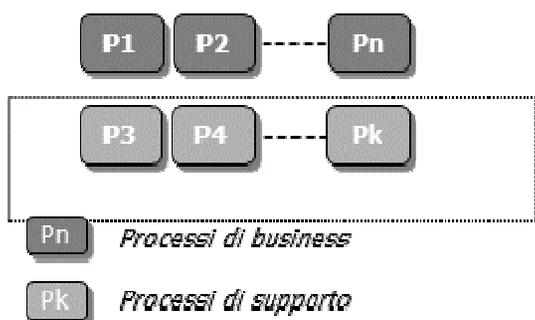


- ▶ Disporre di un **Inventory dei Processi** di Business e di Supporto
- ▶ **Classificare** i Processi di Business e di Supporto in base alla loro criticità
- ▶ **Valorizzare** in termini economico/finanziari gli impatti per l'azienda derivanti dalla perdita di disponibilità di un Processo
- ▶ Evidenziare il **Break Even Point** nell'indisponibilità di un Processo ovvero il tempo massimo di indisponibilità di un Processo oltre il quale la perdita economico/finanziaria per l'azienda risulterebbe insostenibile
- ▶ Disporre di elementi di **valutazione quantitativa** in base ai quali commisurare gli interventi di trattamento volti a ridurre ad un livello accettabile le occorrenze di indisponibilità dei Processi



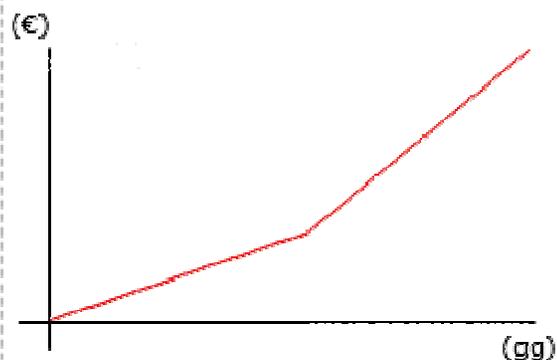


Caratterizzazione dei processi



Identificazione di tutti i processi aziendali mediante interviste ai responsabili HR/Qualità/ Audit ed eventualmente ai responsabili delle BU/ Aziende

Stima Impatto Economico

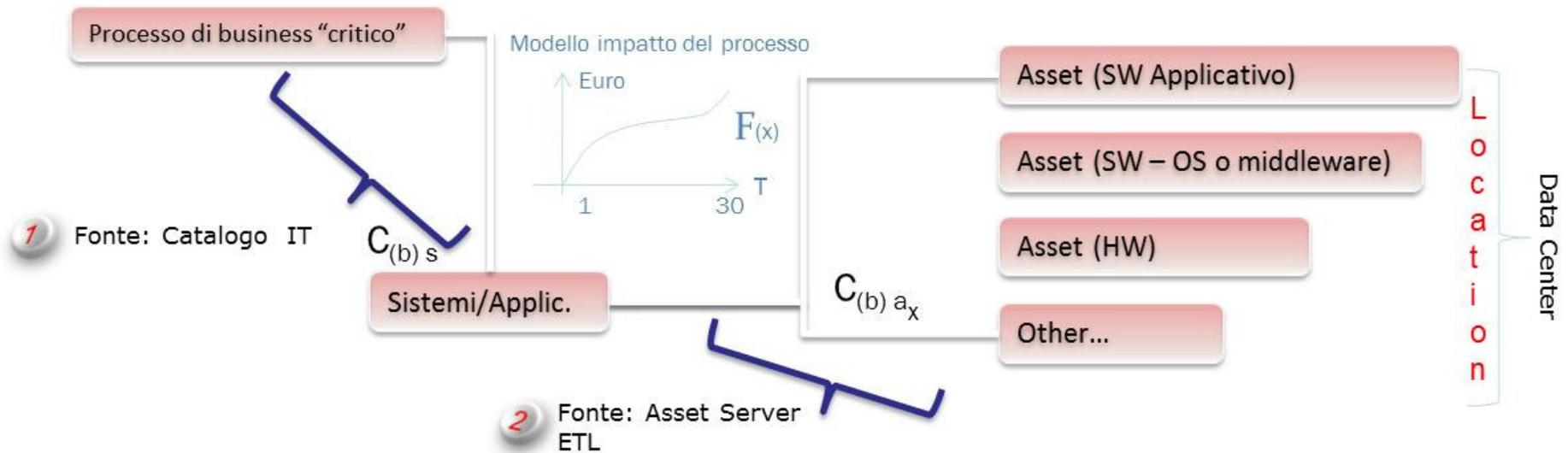


Valutazione degli impatti economici e finanziari di tutti i processi individuati (determinazione delle curve di impatto economico-finanziario in funzione del tempo)

Individuazione delle priorità

Processi	Impatto	Crit. Tot	RTO / RPO
Proc 1		●	
Proc 2	€ (Euro)	◐	gg
Proc 3		○	

Determinazione di una lista dei processi analizzati e prioritizzazione degli stessi in funzione dell'impatto eco-fin connesso alla loro interruzione



Dal modello di impatto sul processo e dalle relazioni costruiti con i relativi coefficienti di blocco posso desumere l'impatto su sistemi e sugli asset, nonché la distribuzione per site e costruire i relativi ranking





INDICE DELLA PRESENTAZIONE :

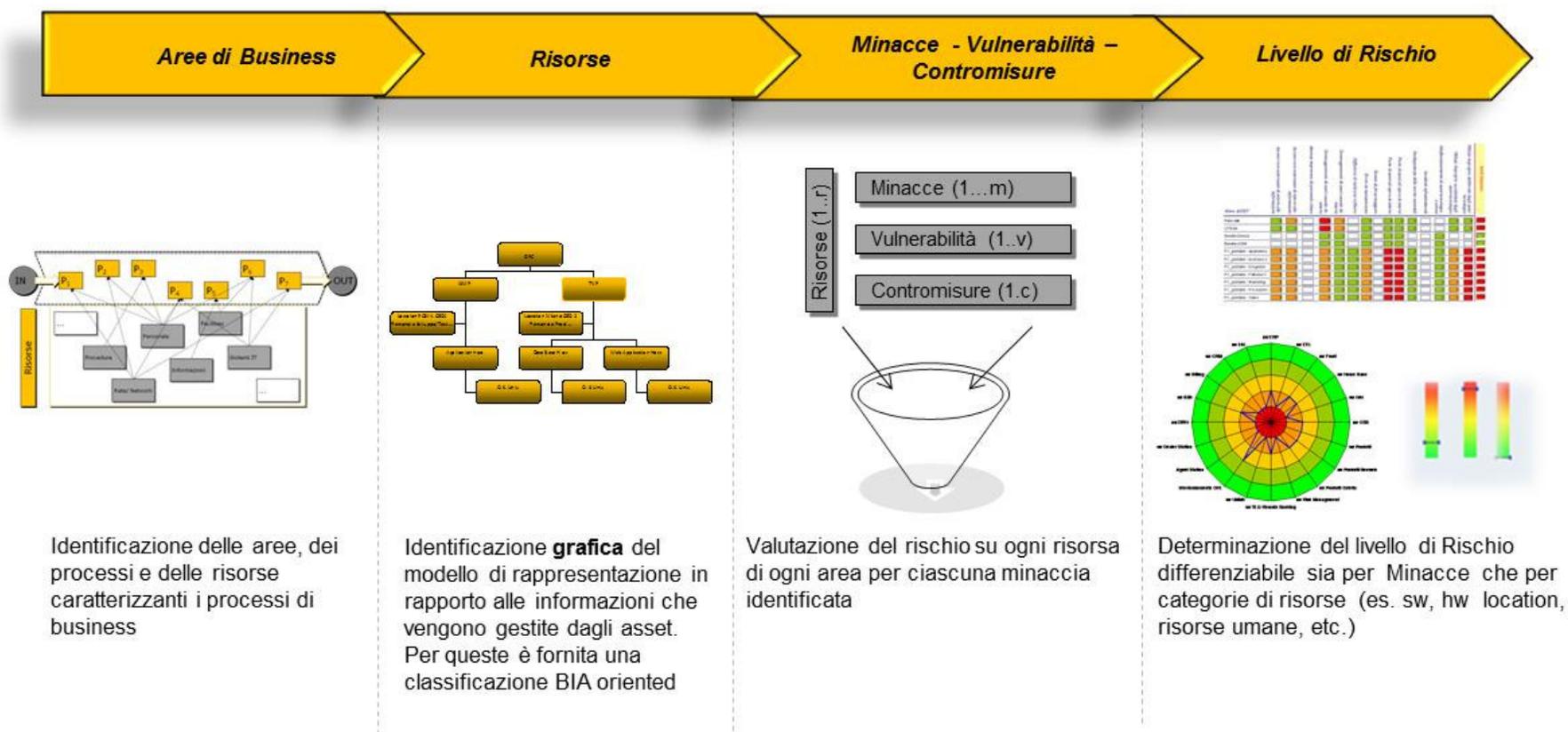
1. GRC: Definizioni e Problematiche
2. Una Proposta di Integrazione
3. InfoSec Governance
4. **Risk Management**
5. Compliance
6. Elementi che abilitano l'integrazione
7. Q&A

Risk Management

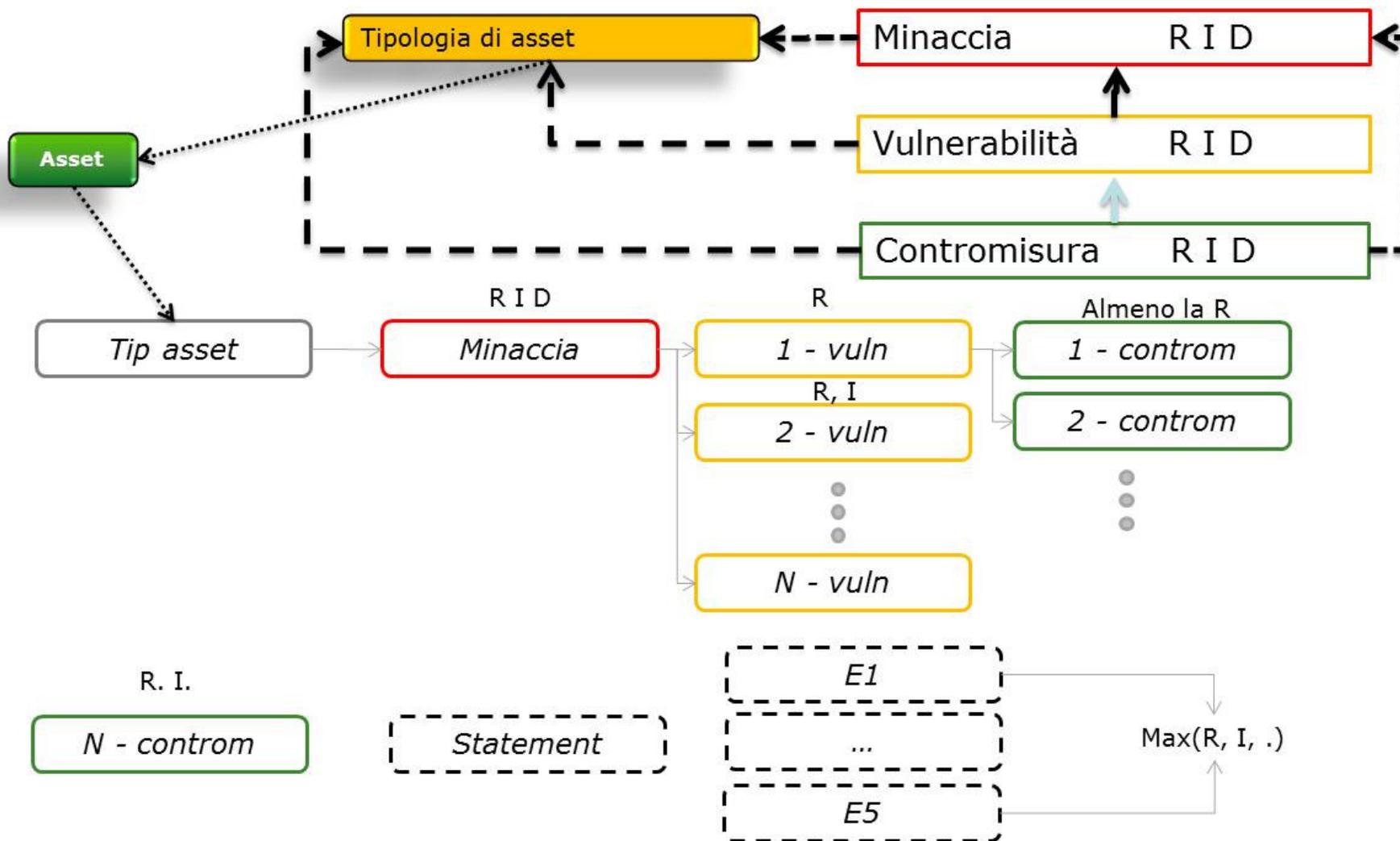




$$R = f(I, M, V, C)$$



Risk Management



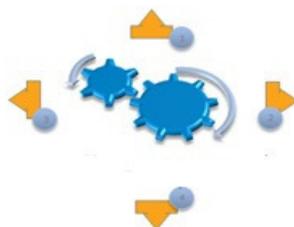


Un ICT Threat Management System consente di computare il profilo di rischio tecnologico:

- ▶ in maniera automatica (eliminando gli oneri e i tempi di interviste) e fornendo una valutazione real time del rischio
- ▶ oggettiva (basata cioè sui livelli di eventi di sicurezza occorsi, interni ed esterni al contesto, e sulle vulnerabilità presenti o intrinseche al sw).

Costruisce una knowledge base di informazioni, interne ed esterne, sulle vulnerabilità, Malware ed Attacchi (Security Intelligence Analysis)

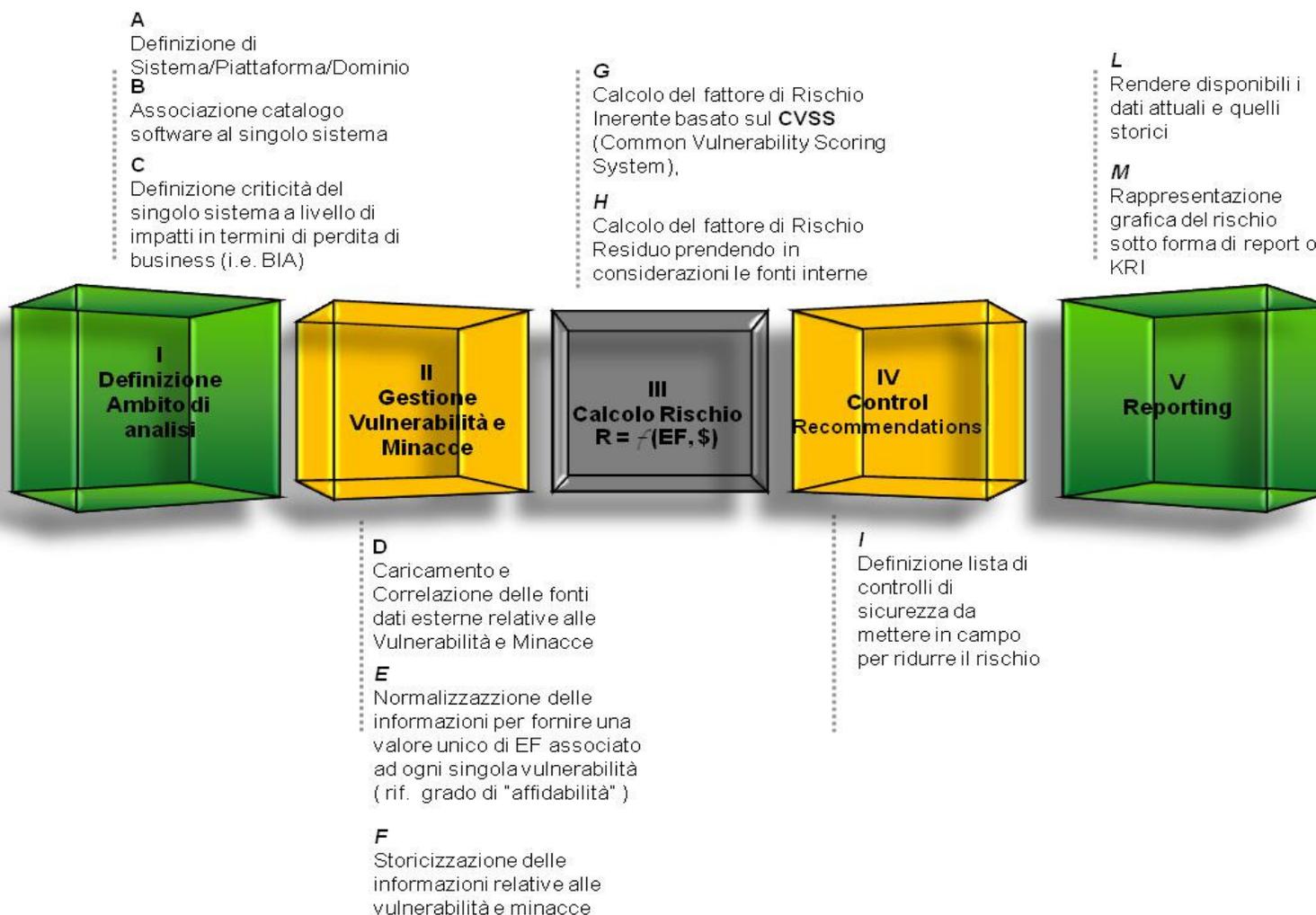
Fornire informazioni quantitative alle decisionali (DSS) legati alle strategie di intervento e trattamento



Valuta il rischio tecnologico correlando le vulnerabilità agli eventi e minacce (esterne ed interne)

Reporting sulle evoluzioni temporali del rischio con differenti livelli di dettaglio

Risk Management





► Computazione delle vulnerabilità logiche effettuata mediante una knowledge base delle vulnerabilità tecnologiche basata sullo standard CVE – Common Vulnerabilities & Exposure

CWE-20: Improper Input Validation
CWE-89: Failure to Preserve SQL Query Structure ('SQL Injection')
CWE-79: Failure to Preserve Web Page Structure ('Cross-site Scripting')
CWE-319: Cleartext Transmission of Sensitive Information
CWE-209: Error Message Information Leak
CWE-285: Improper Access Control (Authorization)
CWE-327: Use of a Broken or Risky Cryptographic Algorithm
CWE-259: Hard-Coded Password
CWE-732: Incorrect Permission Assignment for Critical Resource
CWE-330: Use of Insufficiently Random Values
CWE-250: Execution with Unnecessary Privileges
CWE-255: Credentials Management
CWE-399: Resource Management Errors
Ect...



Vulnerabilità Logiche



Vulnerabilità varianti nel tempo

CVE – NVDB (NIST) – **Vulnerability Scanner**

Computati secondo la metrica CVSS 2.0

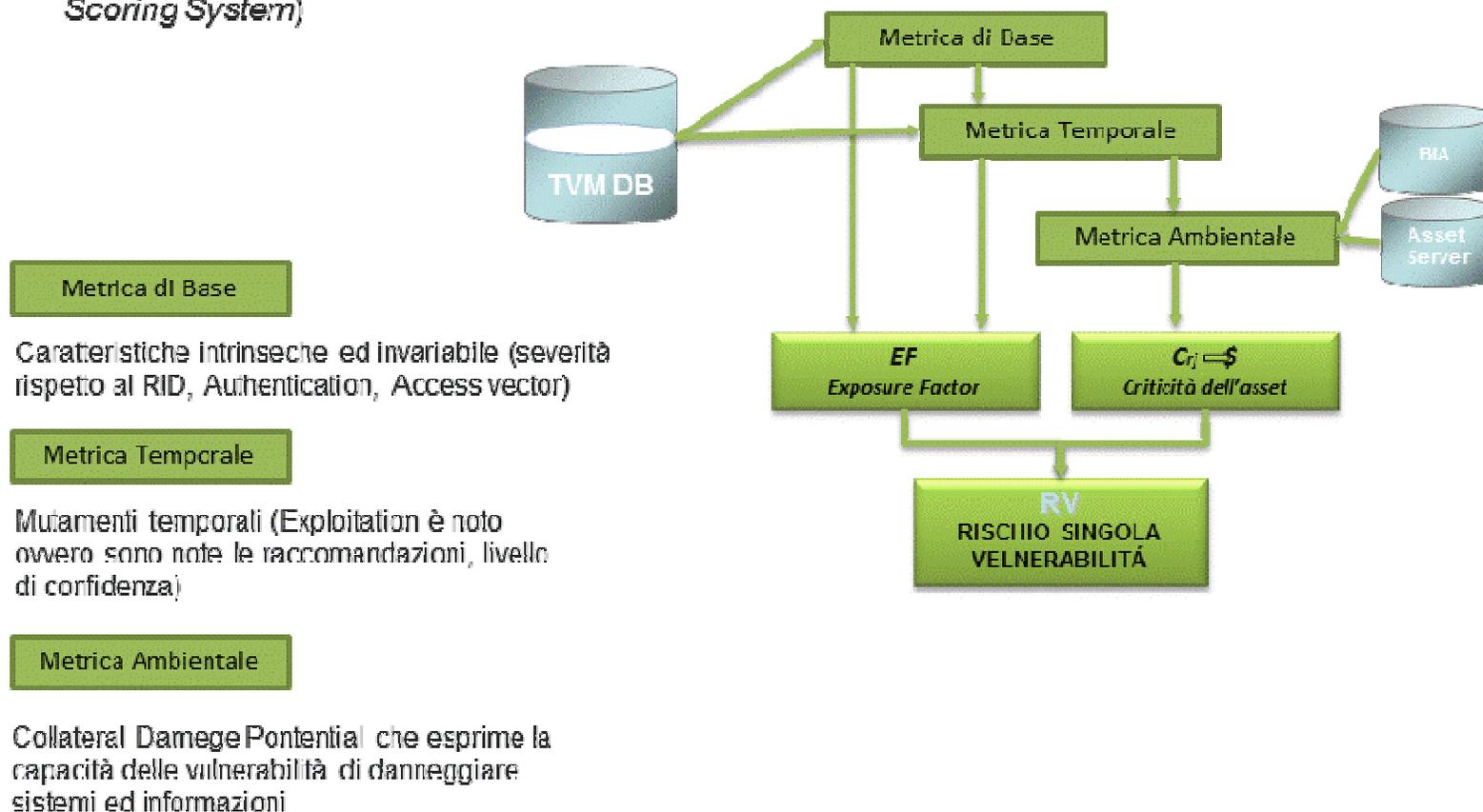
Metrica di base

Metrica temporale

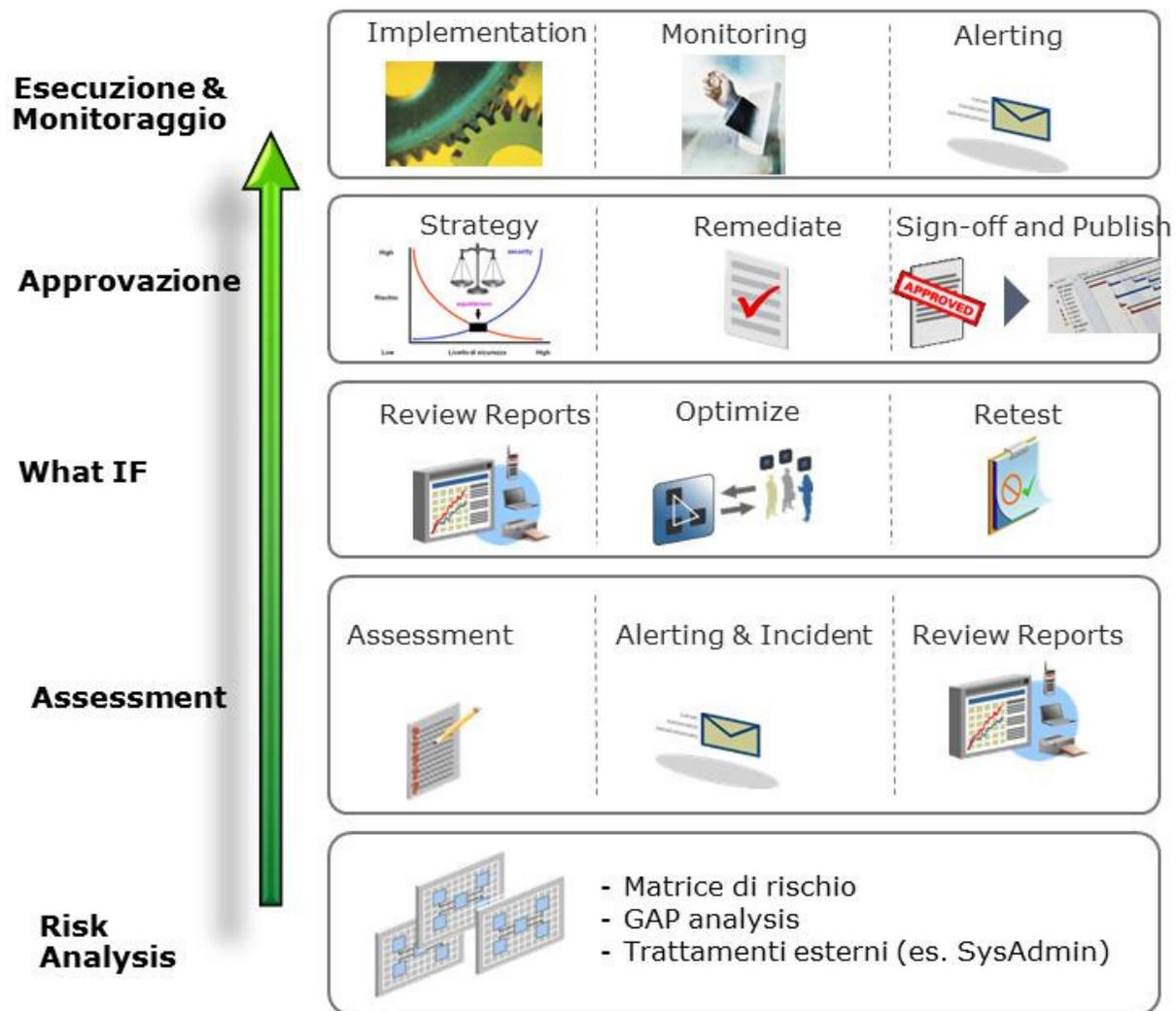
Metrica di ambiente



► Gli indici di rischio possono essere calcolati sulla base dell'algoritmo **CVSS** (*Common Vulnerability Scoring System*)



Action Plan

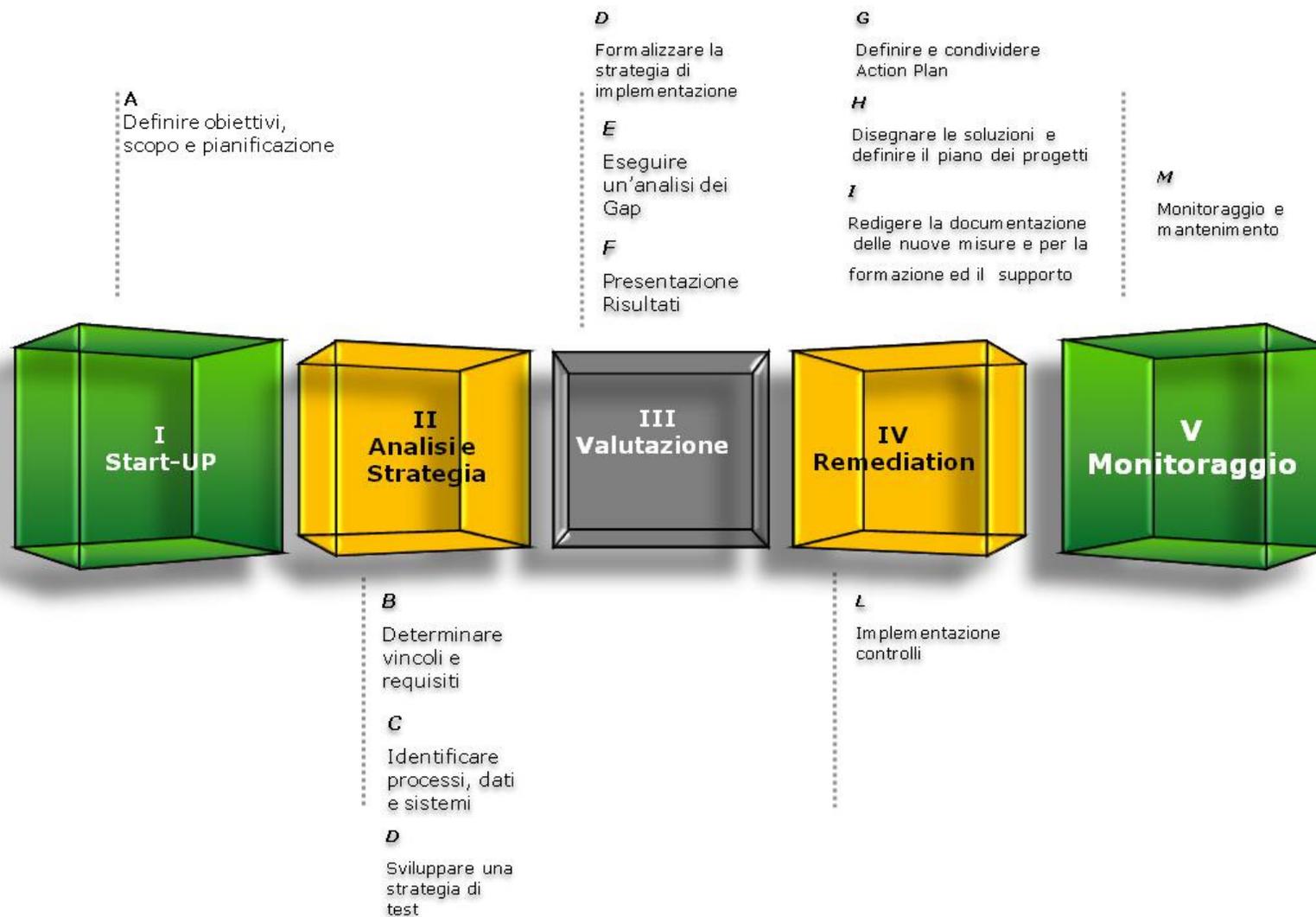




INDICE DELLA PRESENTAZIONE :

1. GRC: Definizioni e Problematiche
2. Una Proposta di Integrazione
3. InfoSec Governance
4. Risk Management
5. **Compliance**
6. Elementi che abilitano l'integrazione
7. Q&A

Compliance





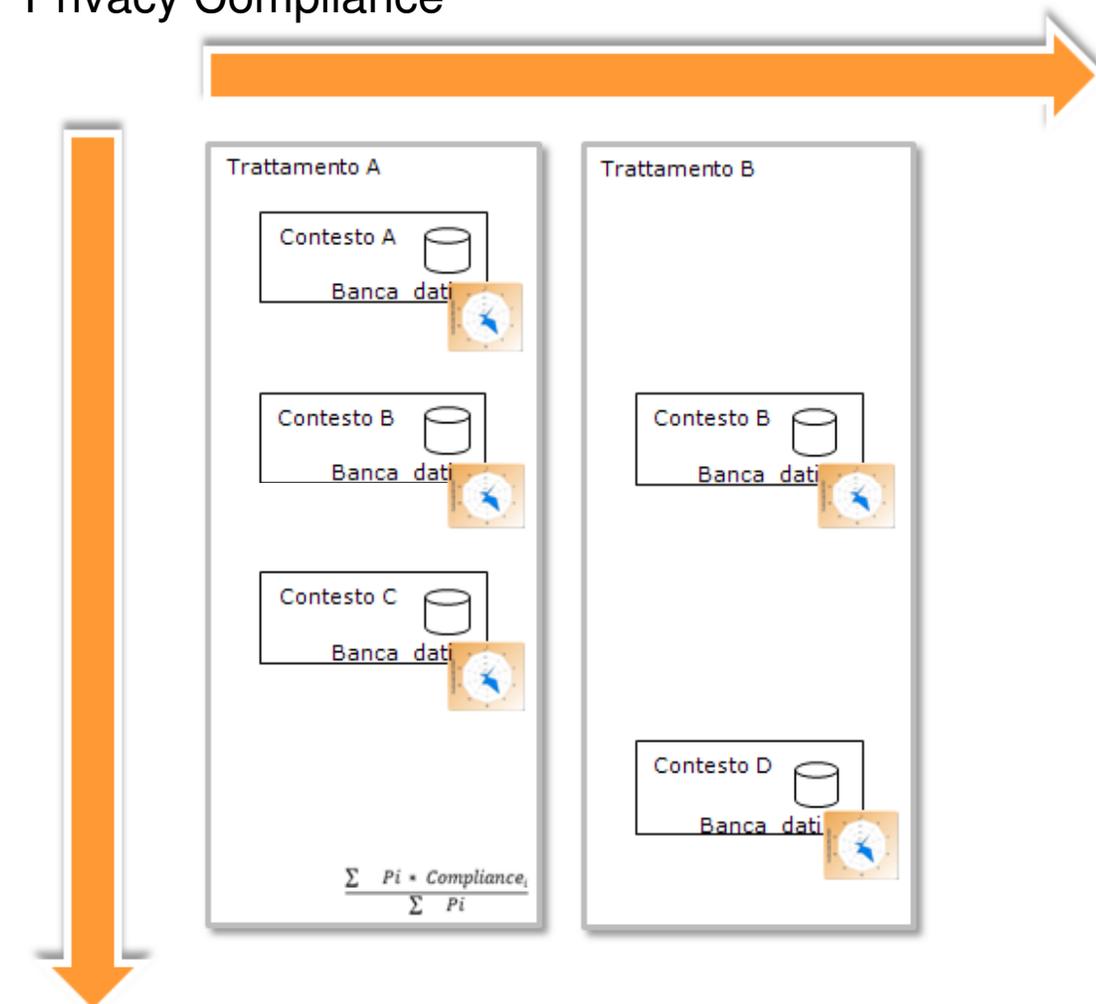
Privacy Compliance





Privacy Compliance

Stima del livello di rischio e Compliance Complessivo



Stima del livello di rischio e Compliance per Tattamento

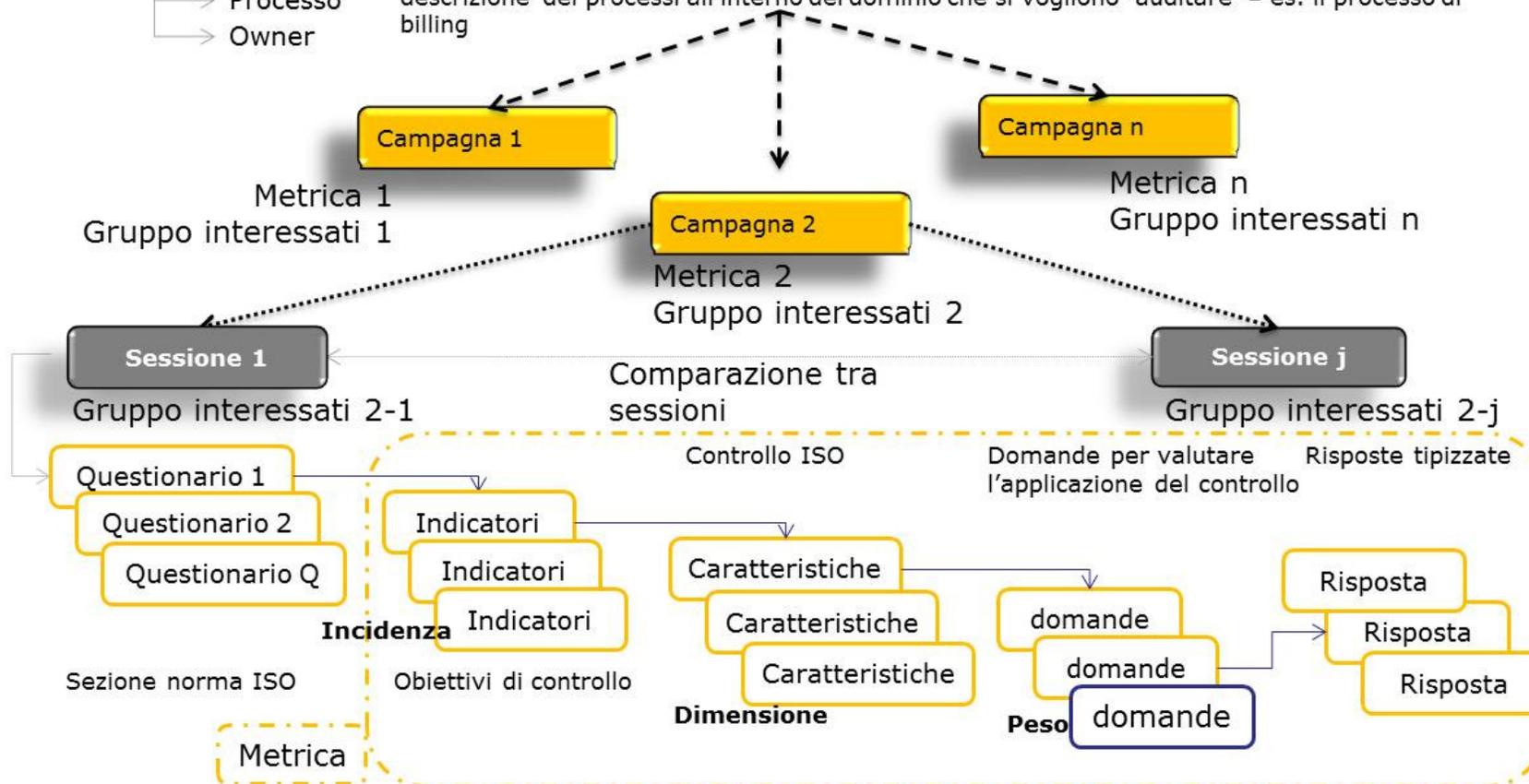




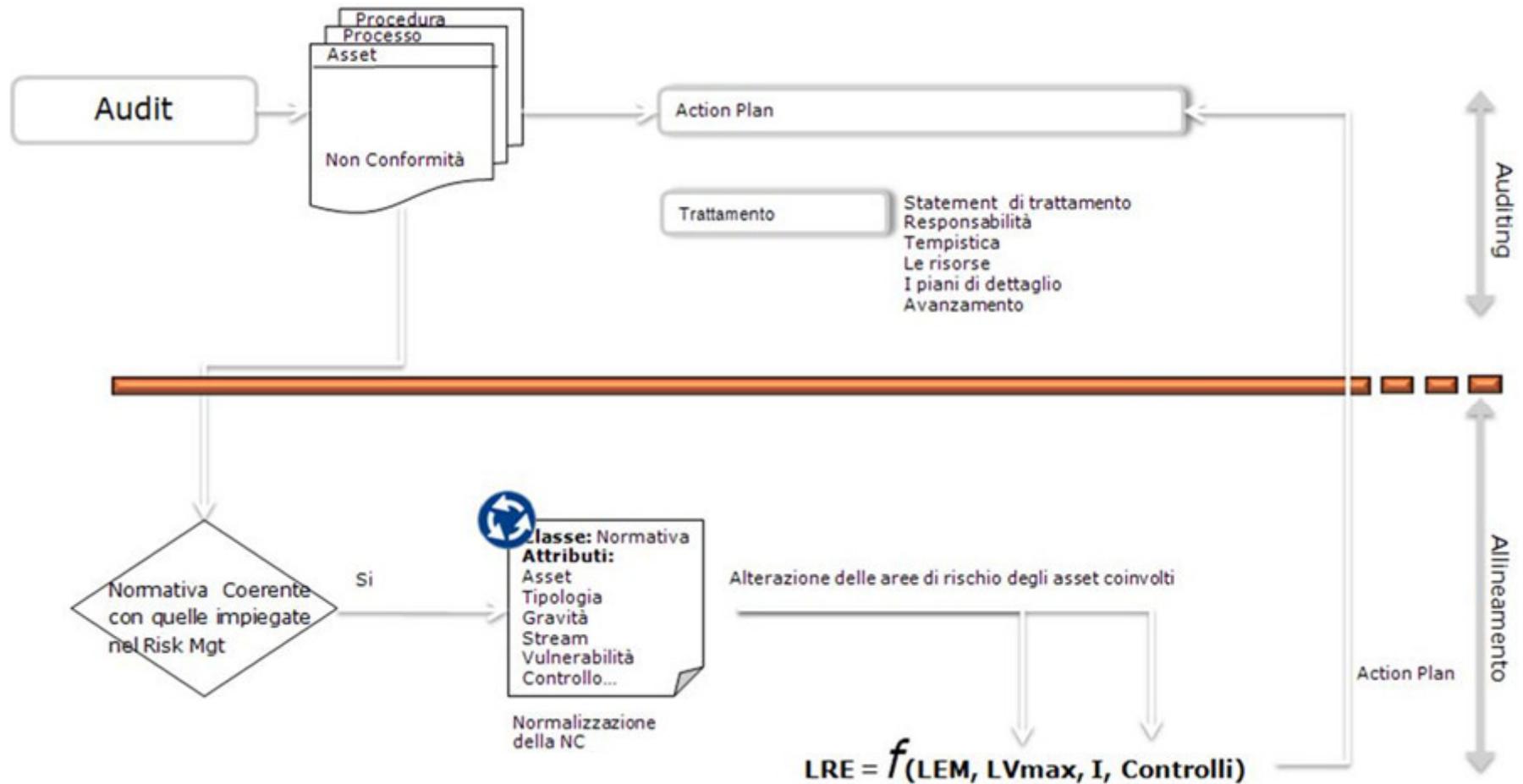
Amministratore del dominio

Dominio può essere un area (area IT, area NW), una piattaforma (billing), un attività trasversale (assurance, provisioning)

Processo descrizione dei processi all'interno del dominio che si vogliono "auditare" - es. il processo di billing
Owner



Audit





INDICE DELLA PRESENTAZIONE :

1. GRC: Definizioni e Problematiche
2. Una Proposta di Integrazione
3. InfoSec Governance
4. Risk Management
5. Compliance
6. **Elementi che abilitano l'integrazione**
7. Q&A



Il **Processo di Configuration Management (CM)** risponde all'obiettivo di rendere disponibile a diversi processi e strutture aziendali una **mappatura dell'infrastruttura IT** (IT Baseline) che consenta di fruire in maniera centralizzata delle informazioni relative ai singoli elementi, i cosiddetti **Configuration Item** (*elemento della Classe di un CMDB*).

La principale componente IT a supporto del processo di CM è costituita dal **CMDB** ovvero dal repository che ospita il framework di riferimento e tutte le informazioni relative ai Configuration Items.

La corretta impostazione e gestione del CMDB consente di:

- ▶ Avere una mappatura puntuale ed aggiornata nel tempo degli asset afferenti l'infrastruttura IT e delle loro relazioni con i processi di business o di supporto dell'organizzazione
- ▶ Fornire output concreti per i processi di Incident Management, Problem Management, Change Management e Release Management
- ▶ Fornire supporto per la gestione delle licenze e per la gestione delle manutenzioni degli asset



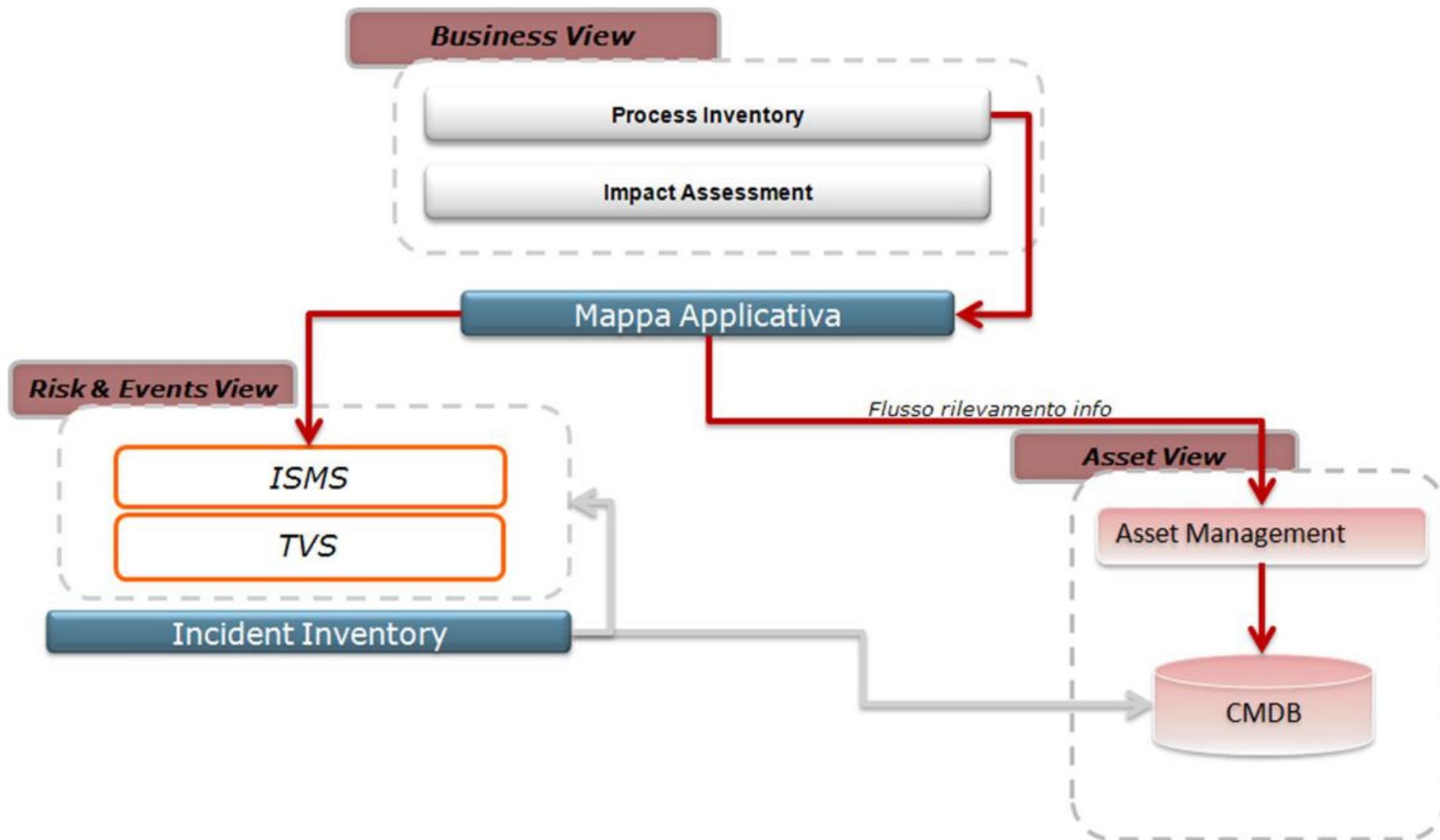
Realizzare un Incident Inventory che consideri gli eventi di Fault, Error e Incident relativi ad ogni asset e che collezioni:

1. Gli eventi rilevanti e codificati dai sistemi aziendali
2. Gli incidenti segnalati dal personale dell'organizzazione.

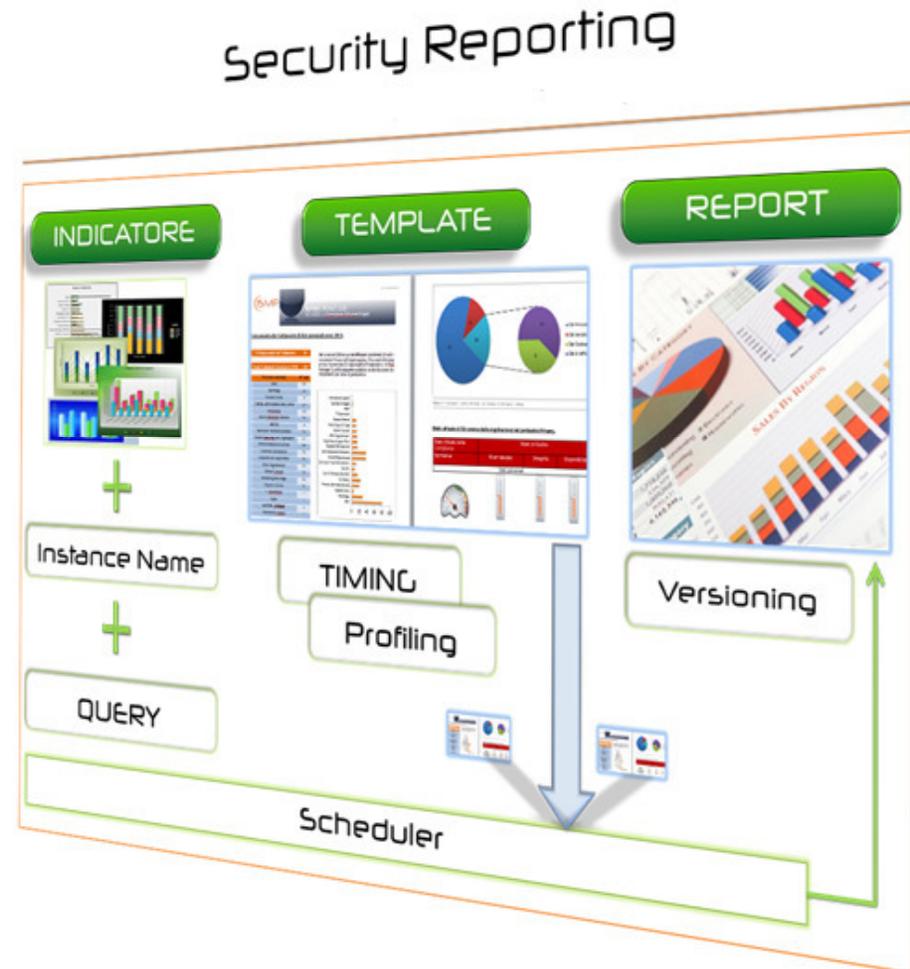
Oltre a razionalizzare e collezionare tutte le informazioni (attributi) relative a quegli eventi che possono avere un impatto ai fini della sicurezza, occorre renderle disponibili per una loro integrazione con il Risk Management e di utilizzarle per la costruzione di Indicatori e Cruscotti di Monitoraggio delle performance dei processi di sicurezza.

Gli eventi devono essere classificati e codificati (ad es. per Tipologia di Incidente, Stream di riferimento,...) al fine di indirizzare le modifiche, per l'asset in oggetto dell'incidente, sui livelli di vulnerabilità e contromisure applicate, con l'obiettivo di rendere coerenti le misure di rischio.

CM & IM



Monitor & Control





Patch management

Accounting

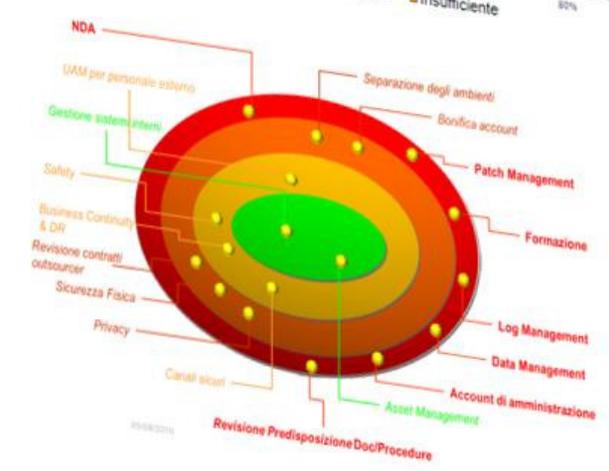
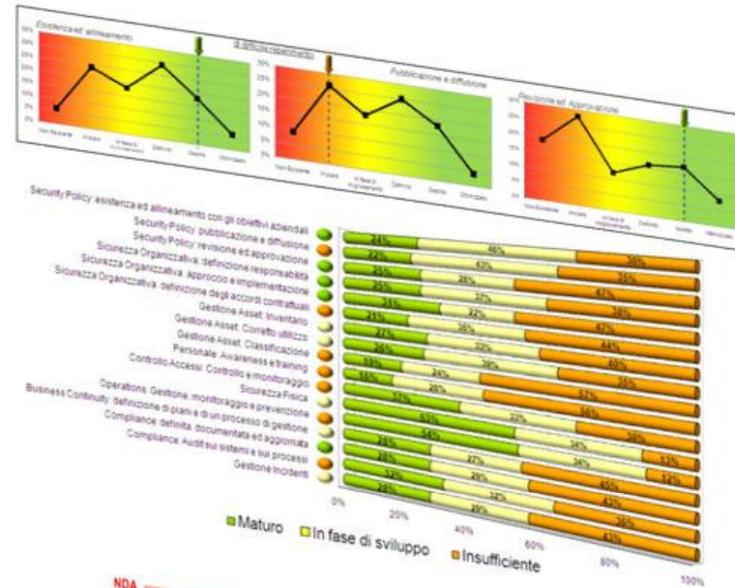
Hardening

Incident / Fault Management

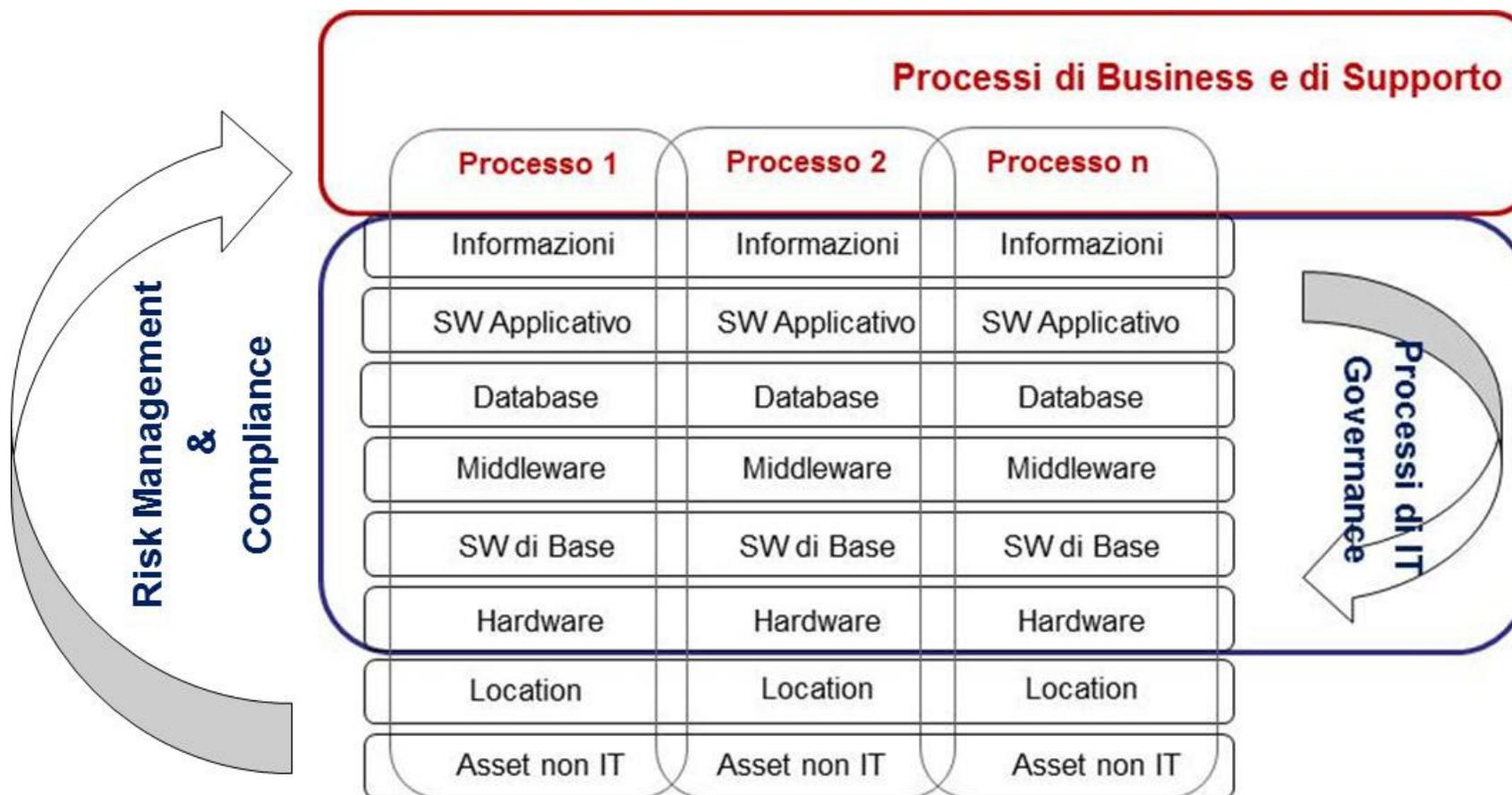
Release management

Change Management

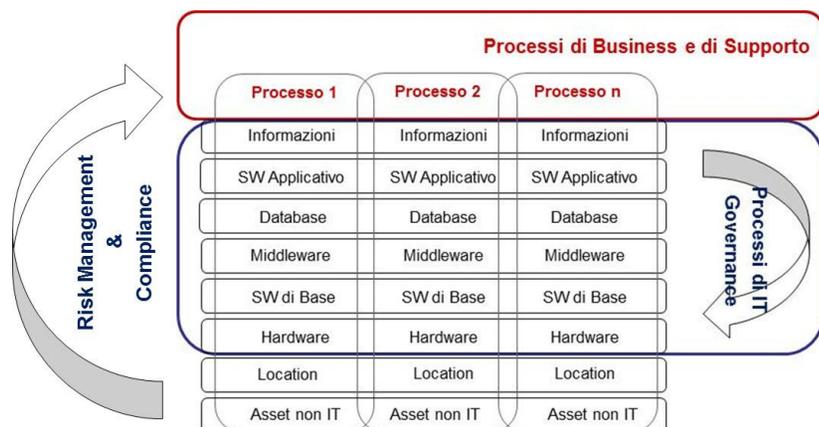
Risk Treatment



Per Concludere



Per Concludere

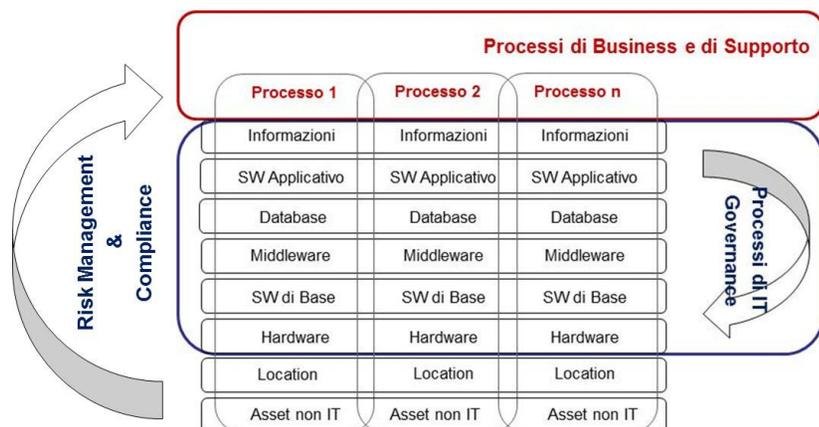


Nell'ambito del modello proposto, il CobiT può essere utilizzato come una metrica per valutare l'applicazione degli Obiettivi di Controllo e dei Controlli previsti per i Processi IT.

Tali processi così come caratterizzati dal CobiT possono essere censiti nell'Asset Inventory e nel ciclo di esecuzione delle attività di Risk Management e Compliance.

Per questi stessi processi vengono eseguite le attività di Audit, Incident Management, Monitoraggio e Controllo.

Per ognuno viene quindi individuato un Piano di Trattamento che contiene le misure per il suo adeguamento e/o miglioramento.



Anche i processi di gestione dell'infrastruttura IT, nel modello proposto così come nell'ottica del CobiT, sono considerati come processi mediante i quali vengono trattate le informazioni rilevanti per il business aziendale.

I risultati delle attività di InfoSec Assessment & Analysis fin qui descritte rappresentano un input importante per calcolare e analizzare:

- ✓ gli Indicatori di Monitoraggio e Controllo
- ✓ gli Indicatori di Maturità

**DEI PROCESSI DI InfoSec GOVERNANCE
UTILIZZANDO LE METRICHE DEFINITE DAL COBIT**



Un esempio

AI6: Manage Changes

Process Description:

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



AI6: Manage Changes - Control Objectives:

AI6.1 Change Standards and Procedures

Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.2 Impact Assessment, Prioritisation and Authorisation

Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised.

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



AI6: Manage Changes - Control Objectives:

AI6.3 Emergency Changes

Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process.

AI6.4 Change Status Tracking and Reporting

Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.

AI6.5 Change Closure and Documentation

Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.

Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



Metrics for IT Goals*	Value	Impact
▶ Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment	> k	✓ Increased Risk
Metrics for Process Goals*		
▶ Amount of application rework caused by inadequate change specifications	> k	✓ Increased Risk
▶ Reduced time and effort required to make changes	% >k	✓ Impact Reduction in BIA
▶ Percent of total changes that are emergency fixes	>k	✓ Increased Risk
▶ Percent of unsuccessful changes to the infrastructure due to inadequate change specifications	>k	✓ Increased Risk
▶ Number of changes not formally tracked, reported or authorised	>k	✓ Increased Risk
▶ Number of backlogged change requests	>k	✓ Impact Increasing in BIA

*Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)



Metrics for Activities Goals*	Value	Impact
▶ Percent of changes recorded and tracked with automated tools	> k	✓ Reduced Risk
▶ Percent of changes that follow formal change control processes	> k	✓ Reduced Risk ✓ Impact Reduction in BIA
▶ Number of different versions of each business application or infrastructure being maintained	>k	✓ Increased Risk ✓ Impact Increasing in BIA
▶ Number and type of emergency changes to the infrastructure components	>k	✓ Increased Risk ✓ Impact Increasing in BIA
▶ Number and type of patches to the infrastructure components	%>k	✓ Increased Risk ✓ Reduced Risk

*Fonte: IT Governance Institute® (ITGI™) (www.itgi.org)

Per Concludere



InfoSec GRC Metric	Value	Impact
✓ N° di change effettuati vs numero di analisi di impatto	> k	▶ Maturity Decreased
✓ N° di vulnerabilità riscontrate dovute a inadeguate procedure di change	> k	▶ Maturity Decreased
✓ N° di incidenti legati a vulnerabilità riscontrate dovute a inadeguate procedure di change	>k	▶ Effectiveness Decreased ▶ Impact Increasing in BIA
✓ Tempo di indisponibilità di processi/servizi legati a inadeguate procedure di change	>k	▶ Impact Increasing in BIA ▶ Effectiveness Decreased
✓ Impatto economico di indisponibilità di processi/servizi legati a vulnerabilità riscontrate dovute a inadeguate procedure di change	>k	▶ Effectiveness Decreased



Question & Answers