IBM Security and Privacy Services

Auditing, Compliance e Risk Management : IBM Approach

Roma 10 aprile 2007

Raffaella D'Alessandro

IBM Security and Privacy Services

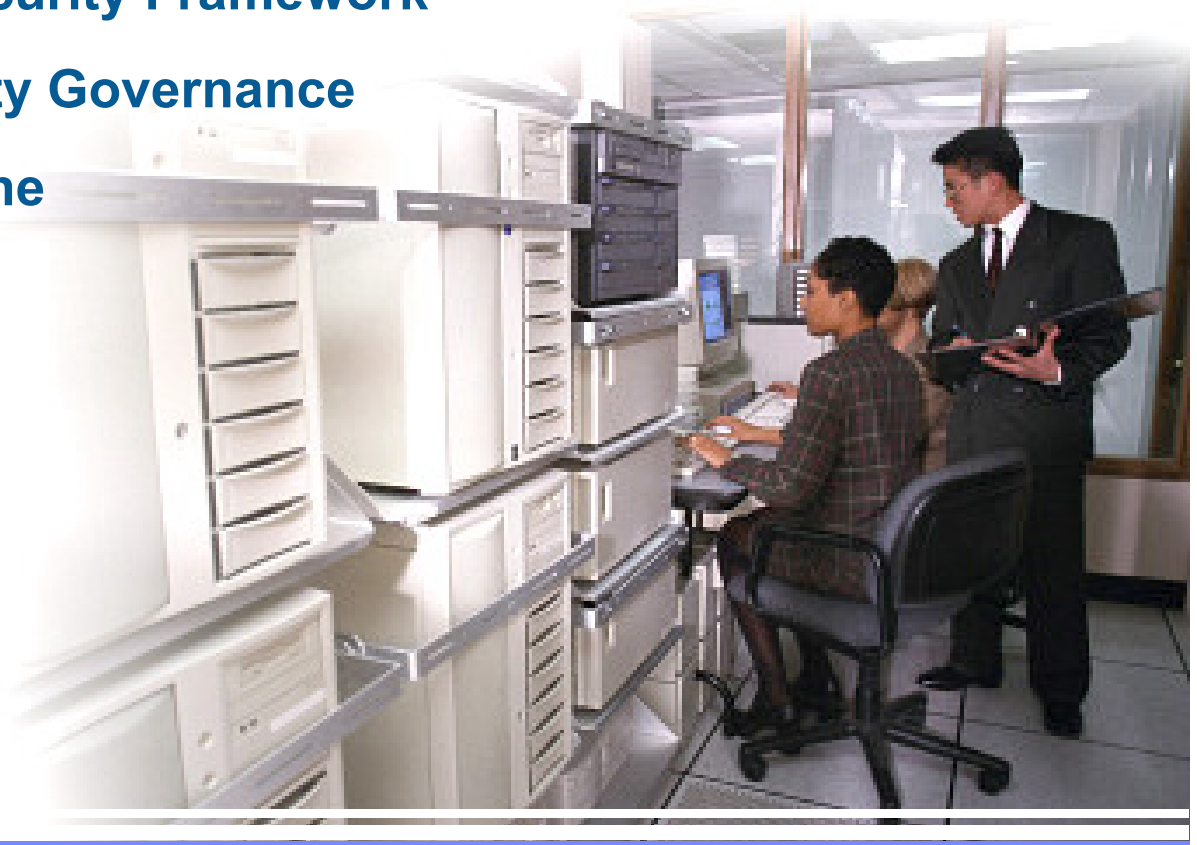
Information Security Consultant

CISA, Lead Auditor BS7799, ISMS Senior Manager

Raffaella.dalessandro@it.ibm.com

Agenda

- Information Security: approccio integrato
- IBM Information Security Framework
- Information Security Governance
- Step di progettazione



La sfida per la sicurezza è quella di trovare un punto di equilibrio fra la necessità di crescita e di innovazione e i rischi per il business …

- Crescente *complessità* delle problematiche di sicurezza nello scenario odierno
- Alti costi per la *gestione* e il supporto della sicurezza
- *Conformità* con i requisiti di legge e le esigenze *di audit*
- *Limitare* e *tracciare l'accesso* alle informazioni e agli asset sensibili
- Stabilire una *relazione di fiducia* con i clienti e i partner
- Proteggersi contro *le intrusioni e il furto di informazioni confidenziali*
- Difficile *realizzare* la sicurezza in ogni nuova applicazione e processo
- Le problematiche di Sicurezza stanno colpendo il *cuore dell'operatività!*

"To get more secure and spend less, enterprises should focus on process, not products."

—Neil MacDonald, vice president and distinguished analyst, Gartner

... in conformita' con normative e standard

CROSS INDUSTRY

- DL 196/2003: Codice in materia di protezione dei dati personali (Titolo V art. 31-36)
- Sarbanes-Oxley Act (SOX) section 402
- ICT Security BS 17799: 2005 ISO/IEC 27001.
- Enterprise security policies
- Homeland Security (PA, Utilities, Travel & Transportation, Telco)
- ISPS Code (emendamento 2002 Solas) per operatori portuali
- HIPAA Health Insurance Portability & Accountability Act of 1996
- D.L. 231/2001: Responsabilità amministrativa di enti su illeciti penali.

- Filiali di Aziende Multinazionali
- Aziende con modelli di business innovativi
- Aziende "sensitive": difesa, aerospaziale
- Terminalisti ed operatori portuali
- Altre aziende che eserciscono infrastrutture e servizi critici o dati sensibili

FINANCE

- BASILEA II: Prassi corrette per la gestione e il controllo del rischio operativo 2003
- Banca d'Italia: Linee Guida per la continuità di servizio delle Infrastrutture Qualificate dei sistemi di pagamento 2004
- ISVAP – Disposizioni in materia di sistema dei controlli interni e gestione dei rischi (Circolare n. 577/D del 30/12/2005)

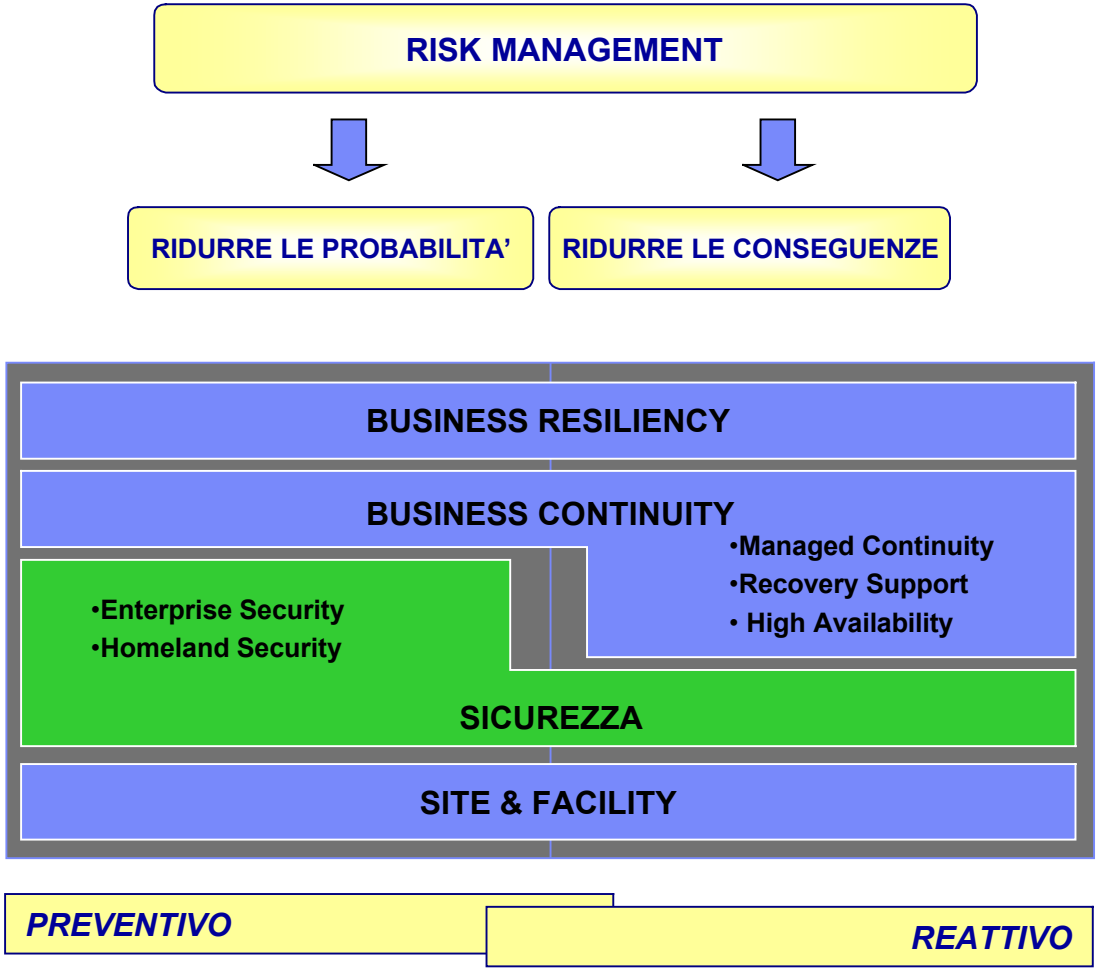
- Banche
- Società di Intermediazione Mobiliare (SIM)
- Società di Gestione del Risparmio (SGR)
- Infrastrutture Qualificate (sistema pagamenti)
- Compagnie di Assicurazione

PUBLIC SECTOR

- Direttiva Min. delle Innovazioni e delle Tecnologie – G.U. n.69 del 22/3/2002 Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali
- Centro Tecnico RUPA - 26/11/2002 Raccomandazione per la costituzione di un Centro Unico di Back-up per gli Enti Previdenziali e Assicurativi
- Protocollo d'intesa - 18/4/2003 Il Ministro del Lavoro e delle Politiche Sociali ed il Ministro per l'Innovazione e le Tecnologie esprimono l'intento di costituire il Centro Unico di Back-up
- ISPS Code (emendamento 2002 Solas) per autorita' portuali
- Codice della PA digitale
- CNIPA

- Amministrazioni dello Stato
- Aziende ed Amministrazioni autonome dello Stato
- Enti pubblici non economici nazionali
- Clienti / Fornitori di servizi a Enti pubblici

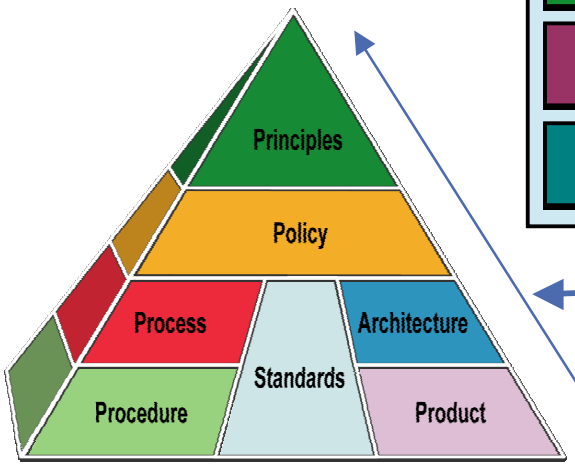
IBM's security philosophy: approccio basato sulla gestione del rischio

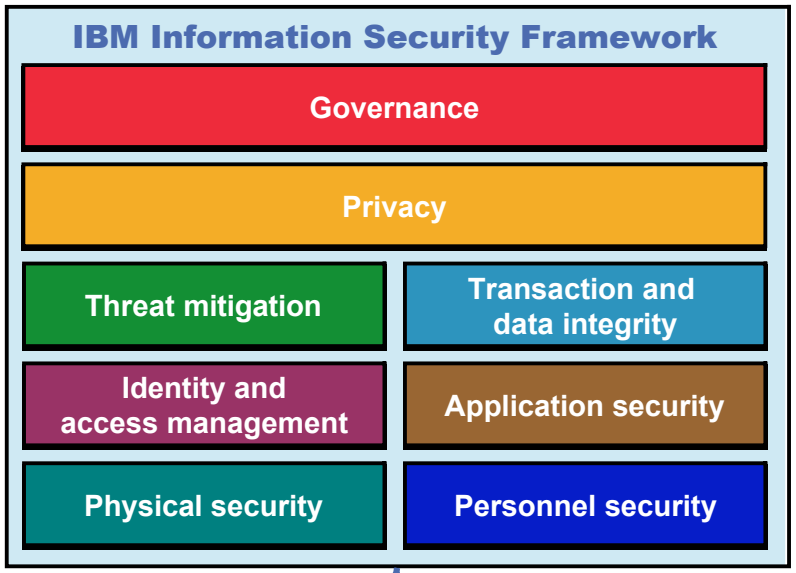


Information Security Framework (ISF): capability reference framework e maturity model

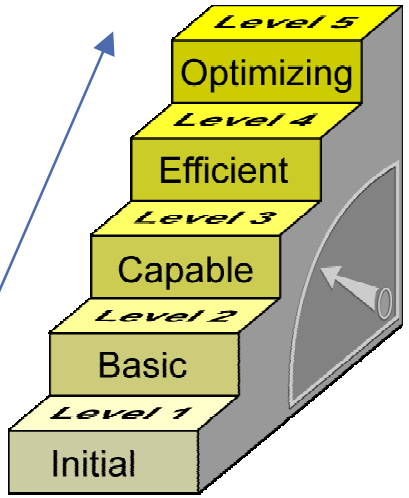
Per quanto riguarda le *capability* richieste per ogni requisito di sicurezza:

Per tutti gli *attributi* delle tematiche di sicurezza:





..e relativamente a tutti i livelli di *maturità* per i diversi obiettivi di sicurezza:

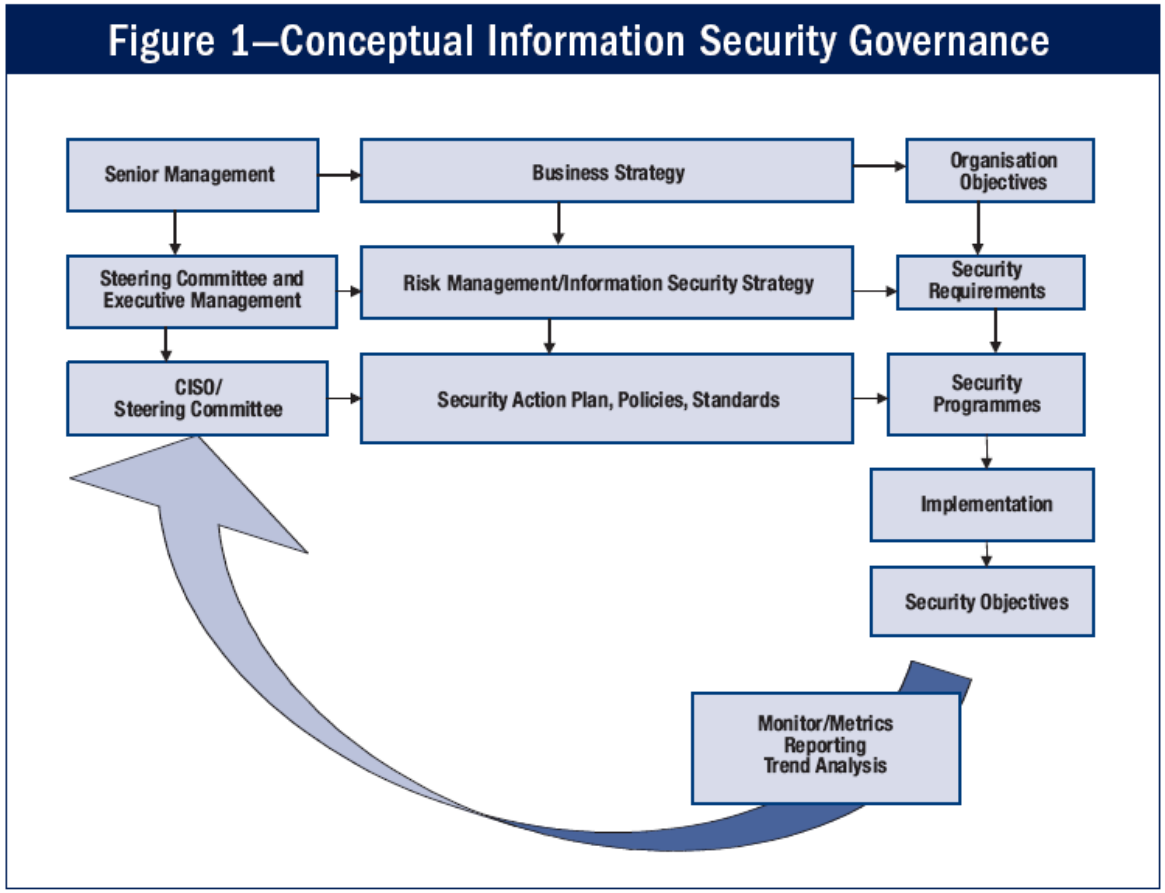


Risk Management + Compliance + Audit = Information Security Governance

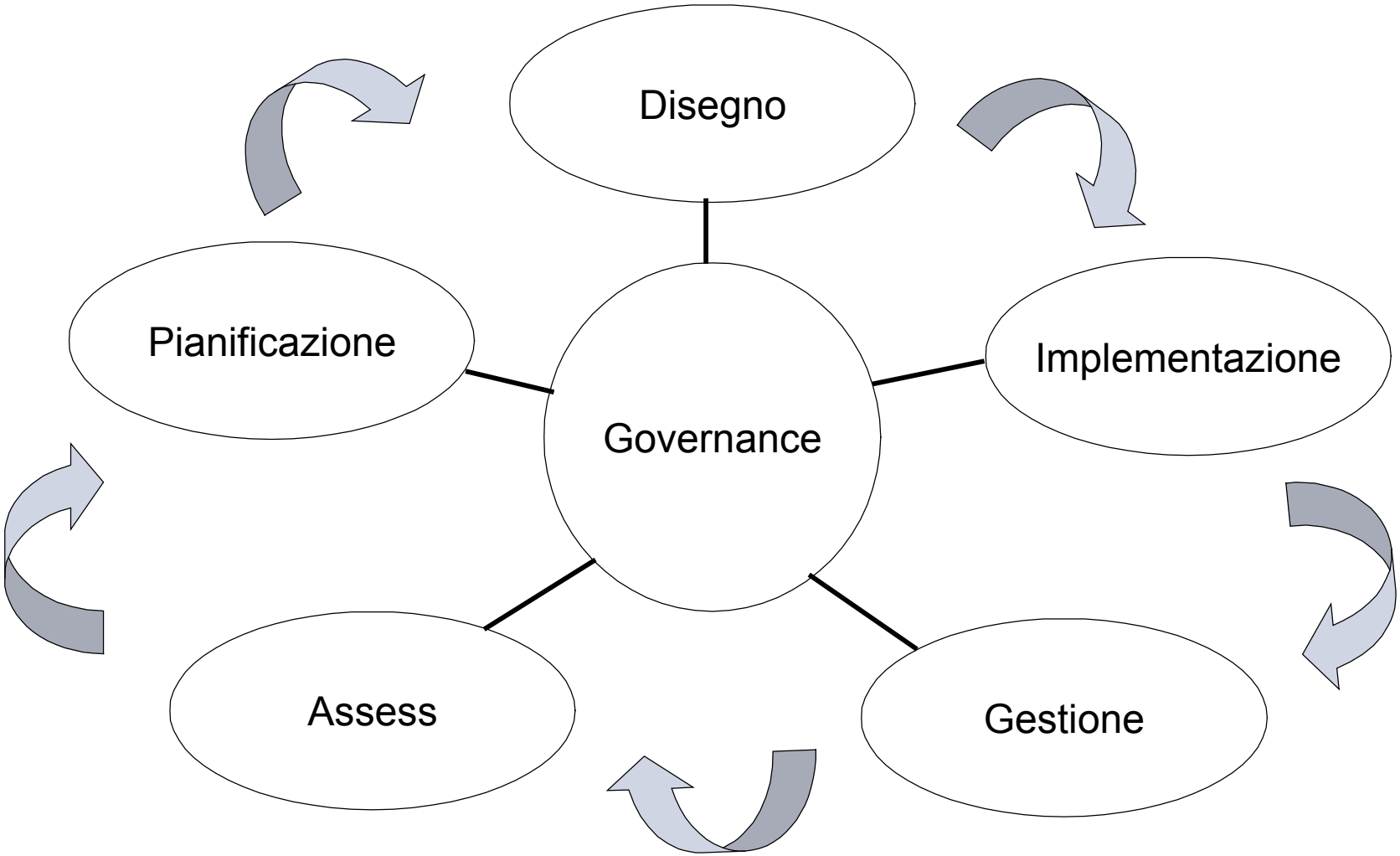
Information security governance is a subset of enterprise governance that

- provides strategic direction,
- ensures that objectives are achieved,
- manages risks appropriately,
- uses organisational resources responsibly,
- and monitors the success or failure of the enterprise security programme.

Il concetto di Information Security Governance



Information Security Governance è al centro del ciclo di vita dell'Information Security



La domanda fondamentale

Quali sono gli obiettivi da raggiungere?

efficacia	Raggiungimento degli obiettivi fissati inizialmente
efficienza	Utilizzo ottimale delle risorse
conformità	Rispetto delle leggi, regolamenti e clausole contrattuali
integrità	Esattezza, validità e completezza delle informazioni
confidenzialità	Protezione contro qualsiasi divulgazione non autorizzata
disponibilità	Disponibilità dei sistemi, delle risorse e dei dati
affidabilità	Messa a disposizione di informazioni affidabili

La risposta: IBM ISF e Information Security Governance

Governance

Strategy
- Information security policy
- Enterprise security architecture

Governance framework
- Governance structure

Information security advisory
- Consulting and advisory services

Security risk management framework
- Threat risk assessment
- Information asset profile
- Project risk assessment
- Security risk management

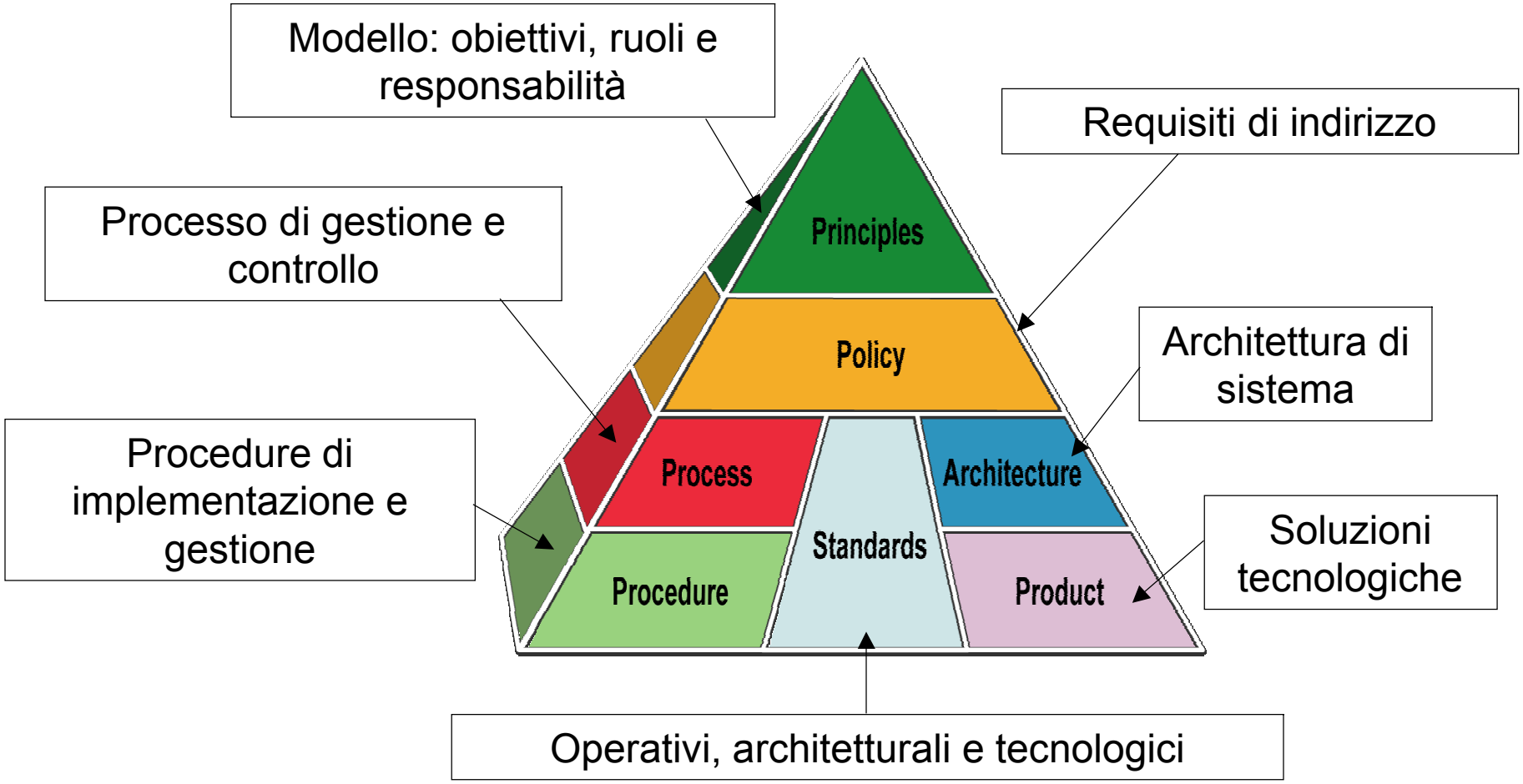
Compliance program
- Regulatory compliance
- Technical, policy and standards compliance
- Health checking
- Internal audit and response

COBIT

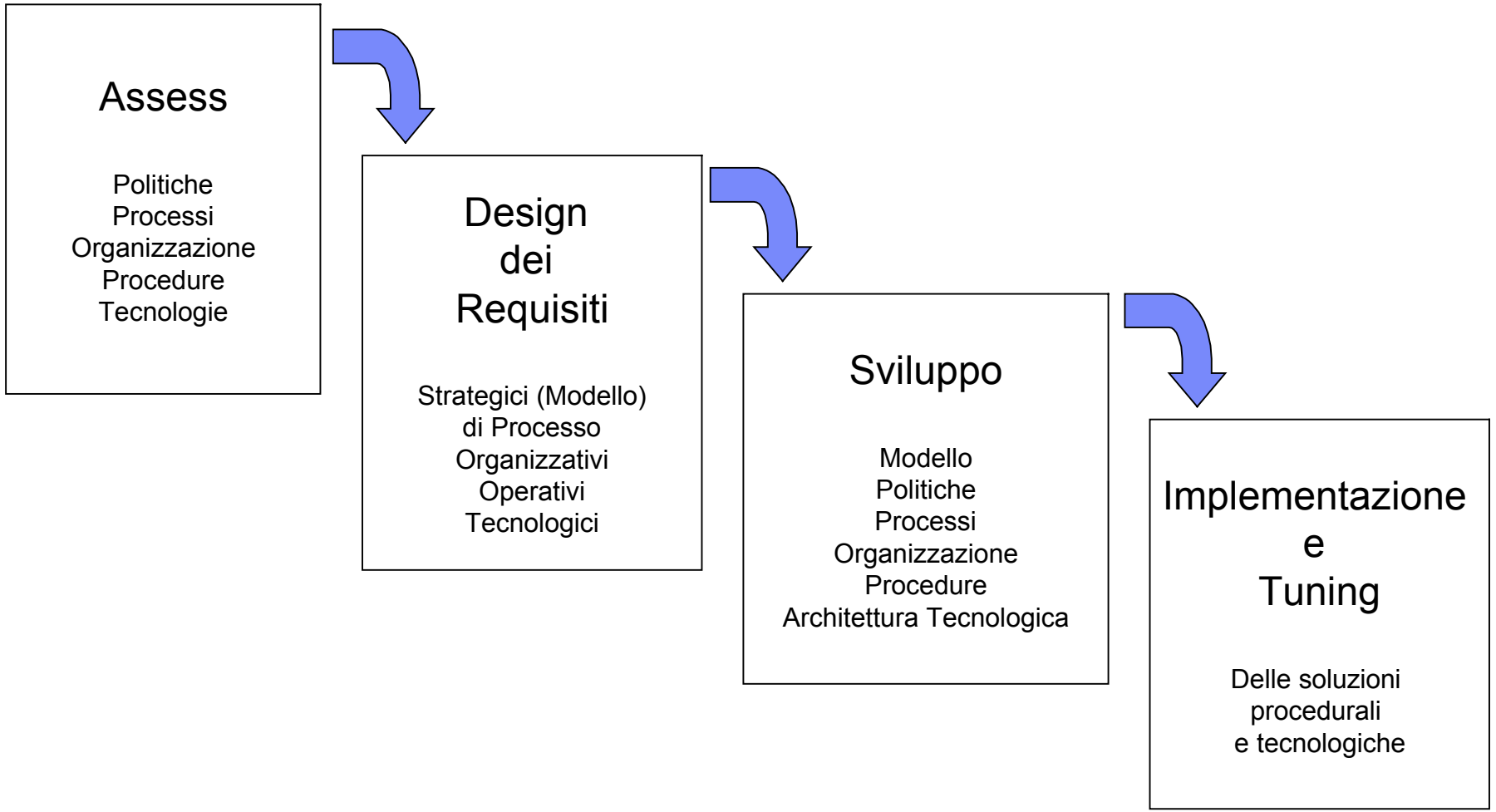
IT GOVERNANCE INSTITUTE®

ISO 17799

La risposta: il sistema integrato di Information Security Governance



Step di Progettazione



Analisi e disegno del Modello di Security Governance

- Obiettivi e contesto di Security Governance
- Definizioni di Information Security Event
- Verifica di conformità degli obiettivi di information security governance rispetto alle normative vigenti ed alle politiche di sicurezza
- Definizione eventi da monitorare e relativi log, su quali piattaforme (disegno delle correlazioni dei segnali con impatti sul business)
- Definizione delle regole di acquisizione (frequenza, tipo log,..)
- Individuazione ruoli e responsabilità
- Individuazione esigenze e livelli di reporting

Il Processo di Gestione e Controllo : alcune componenti a cui prestare attenzione

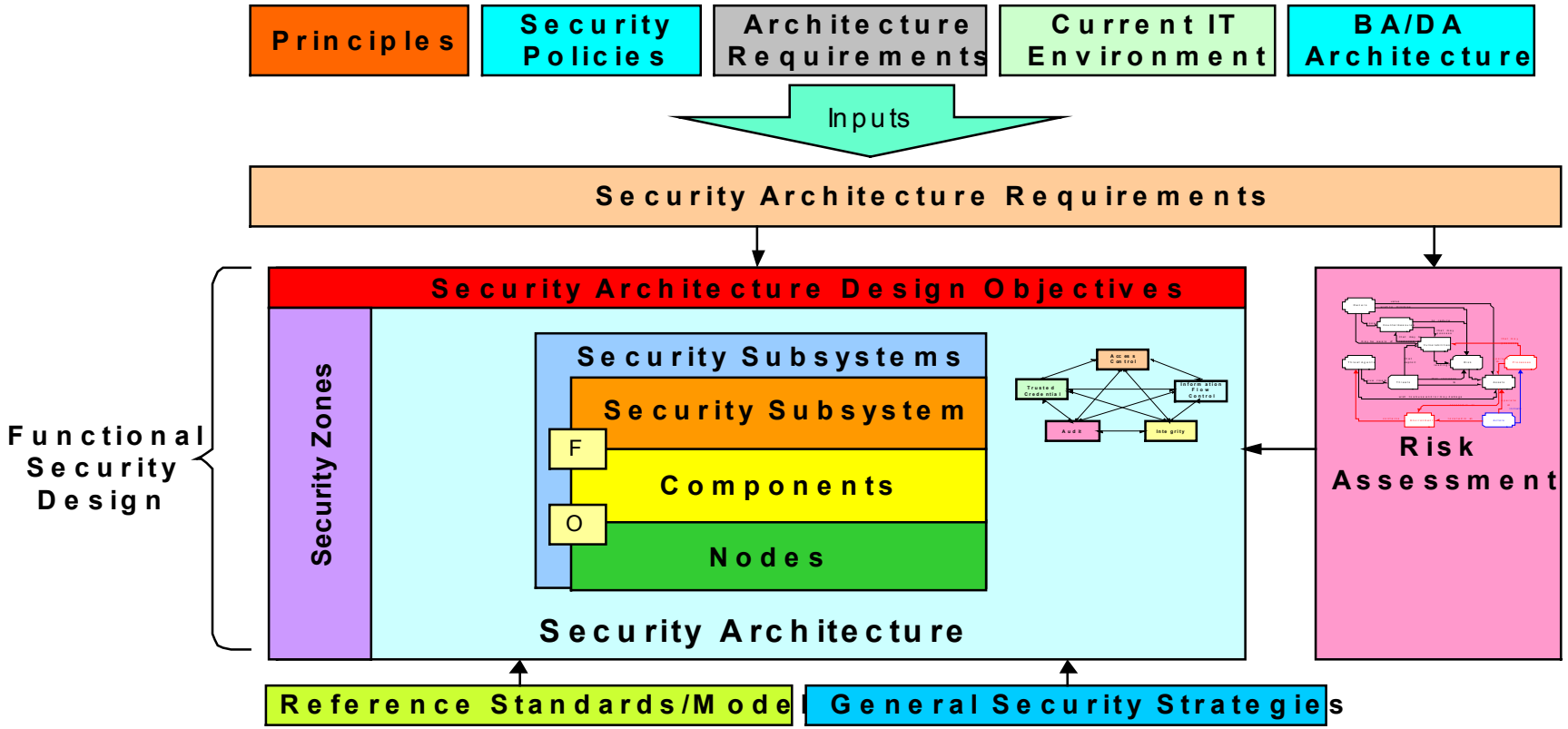
- Allineamento agli obiettivi e al contesto di Information Security Governance
- Major Process e sottoprocessi, flow requirement e specific I/O requirement
- Altri processi aziendali impattati / impattanti (Asset Mgmt, Change Mgmt,...)
- Ruoli e responsabilità
- Performance Measurement (Indicatori e metriche)
- Auditabilità

Politiche e Procedure: alcune componenti a cui prestare attenzione

- registrazione eventi (Modello dei criteri di sensitivity, threat & Risk) in base ai quali settare i sensori di rilevamento e le relative registrazioni di log
- acquisizione log (definizione dei criteri per stabilire i livelli di soglia o i trigger events in base ai quali far scattare l'acquisizione dei log, e relative priorità)
- correlazione (definizione dei criteri per effettuare la correlazione dei log segnalati in funzione dei possibili impatti)
- accesso (definizione dei criteri (need to know) in base ai quali individuare chi puo' accedere ed in che modalità ai log)
- conservazione e distruzione (identificare i criteri in base ai quali effettuare la conservazione e la distruzione dei log)
- ciclo di vita gestione eventi (classificazione, segnalazione, risposta, contenimento, eliminazione, ripristino,...)
- reporting degli eventi (cosa, a chi, con quale frequenza, in base a quale evento)
- valutazione efficacia ed efficienza del sistema di information security governance (modello di indicatori e metriche)

Aspetti architetturali delle soluzioni di IT Security :IBM Methodology for Architecting Secure Solutions (MASS)

IBM Methodology for Architecting Secure Solutions (MASS) è una metodologia a supporto della progettazione di una architettura di sicurezza adeguata ad implementare le strategie e l'Information Security Program .



Disegno e sviluppo delle soluzioni tecnologiche di IT security

IT security design consiste di sei attività:

1. Disegno delle security zones
2. Disegno del sottosistema di trust delle credenziali di identificazione e di autenticazione
3. Disegno del sottosistema di controllo degli accessi
4. Disegno del sottosistema di information flow control
5. Disegno del sottosistema di audit
6. Disegno del sottosistema di integrity

Thank You