NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

R. D'Alessandro

IBM Security & Privacy Services

Come affrontare la conformità per la Sicurezza delle Informazioni

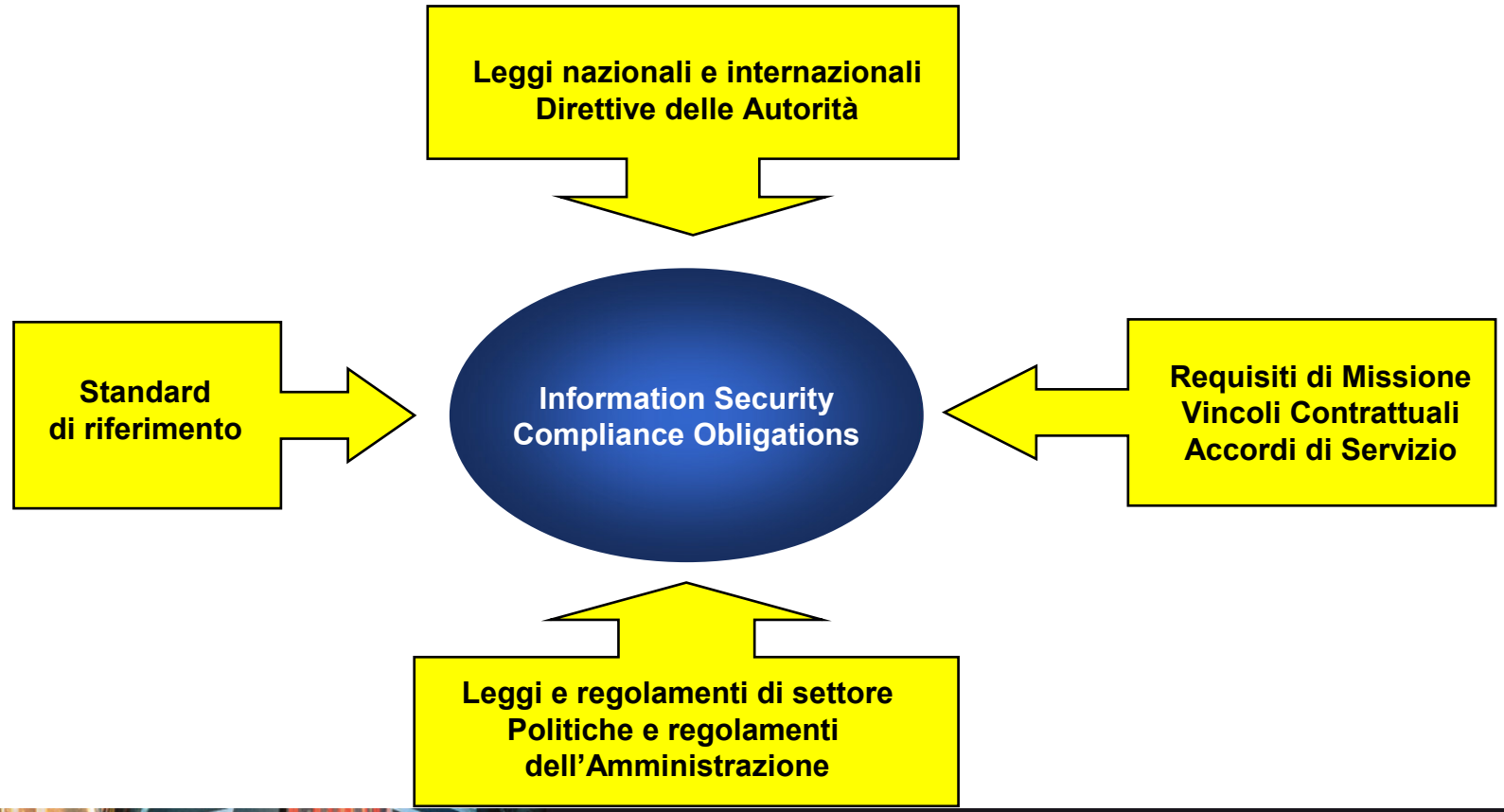
IBM ITALIA aderisce al progetto Impatto Zero® di LifeGate.
Riduce e compensa le emissioni di Co2 con la creazione di nuove foreste.

Agenda

- **Definizioni**
- **Alcune criticità**
- **Obblighi, Requisiti e Misure di Sicurezza**
- **Conclusioni**

Information Security Compliance

E' definita in termini di **conformità con gli obblighi** connessi alle esigenze di assicurare **confidenzialità, integrità, disponibilità e non-ripudio** agli asset informativi dell'azienda



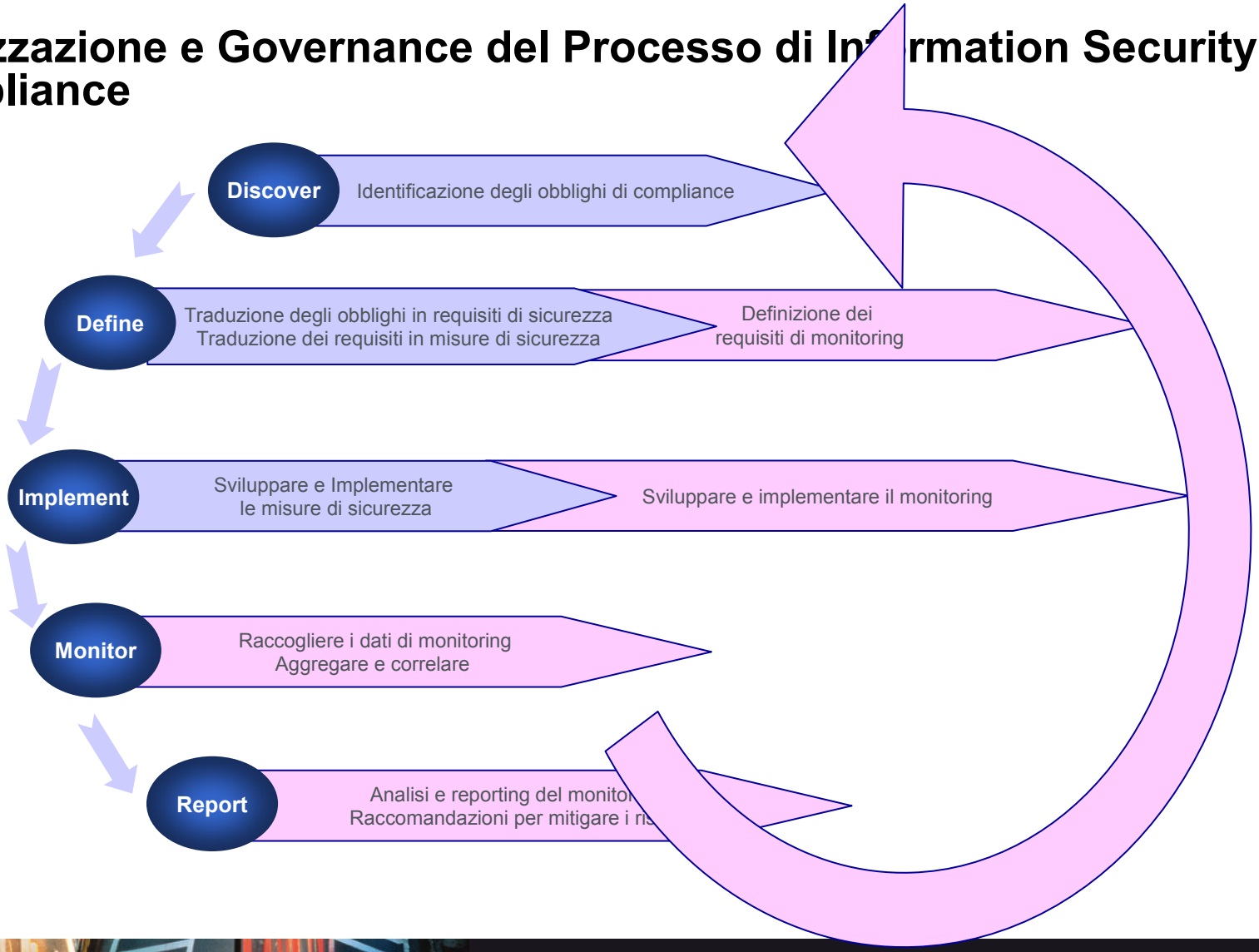
Alcune criticità

- Le leggi ed i regolamenti in genere non forniscono precise indicazioni sulle misure di Information Security atte a conferire la conformità e devono pertanto essere **interpretate** nello specifico contesto dell'Amministrazione **da parte degli esperti**
- La molteplicità di leggi e regolamenti che impattano sulla specifica Amministrazione possono condurre ad individuare requisiti e misure di sicurezza che presentano **conflitti** (es: Sicurezza vs Privacy)
- I costi correlati alla realizzazione e gestione delle misure di sicurezza dovrebbero essere giustificati in funzione del rischio correlato alla non conformità legislativa, e questo comporta l'indirizzamento dell'esigenza da parte **dell'alta direzione** dell'organizzazione (esempio Comitato di Risk Mgmt)

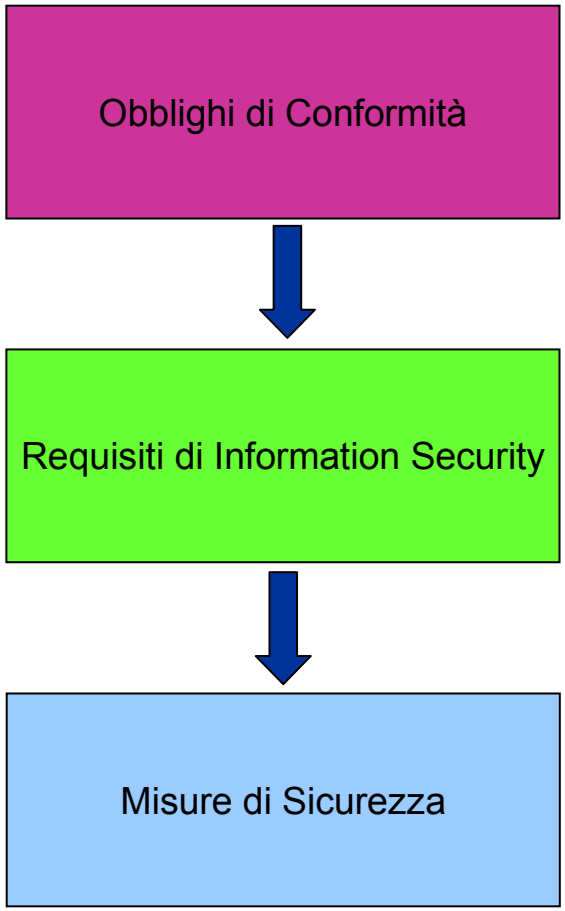
Il Processo di Information Security Compliance Management

- Ha l'obiettivo di consentire all Amministrazione di gestire le esigenze di Information Security Compliance, **individuando ed armonizzando** gli obblighi di conformità, i requisiti, le misure di sicurezza e **controllando che nel tempo** sia mantenuta la conformità
- Dovrebbe essere parte del **processo piu' ampio di compliance management** dell'Amministrazione
- Dovrebbe vedere la funzione **Information Security** come **owner** del processo
- Dovrebbe vedere la partecipazione di diverse funzioni dell'Amministrazione alle diverse attività di processo per garantire la **corretta rispondenza** tra obblighi di compliance, requisiti di sicurezza e Misure di Sicurezza
- Deve essere realizzato come **processo di miglioramento a ciclo continuo**

Realizzazione e Governance del Processo di In rmation Security Compliance



Relazione tra obblighi di conformità, requisiti di sicurezza e misure di sicurezza



Obblighi di Information Security Compliance:

Obblighi imposti da leggi,clausole contrattuali, specific agreement, responsabilità e doveri derivanti da Politiche e Regolamenti

Requisiti di Information Security:

Azioni necessarie per soddisfare gli obblighi, possono essere di natura organizzativa,procedurale , tecnologica

Misure di Sicurezza:

Strumenti organizzativi e procedurali e meccanismi tecnologici per realizzare le azioni individuate come requisiti

Conclusioni

- La conformità alle normative deve essere indirizzata tramite il **Processo di Information Security Compliance:**
  - con il forte **committment** dell Alta Direzione
  - attribuendo i ruoli e le responsabilità presso **ciascuna funzione coinvolta**
  - individuando step di **realizzazione** e step di **monitoraggio**
  - realizzando il **ciclo continuo** per il **mantenimento nel tempo**
- La conformità richiede la collaborazione tra le funzioni legali, organizzative, dei servizi ai clienti e di Information Security: **dobbiamo imparare a comunicare tra di noi**
- La mappatura delle Misure di Sicurezza secondo gli standard di riferimento rappresenta un valido strumento per indirizzare i requisiti di Information Security Compliance gestendo la Governance

Domande e risposte

Raffaella.dalessandro@it.ibm.com