IBM

NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

Francesco Scribano

GTS Business Continuity and Resiliency services Leader

Certificazione ISO 27001: l'esperienza IBM

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

Certificazione ISO 27001: l'esperienza IBM

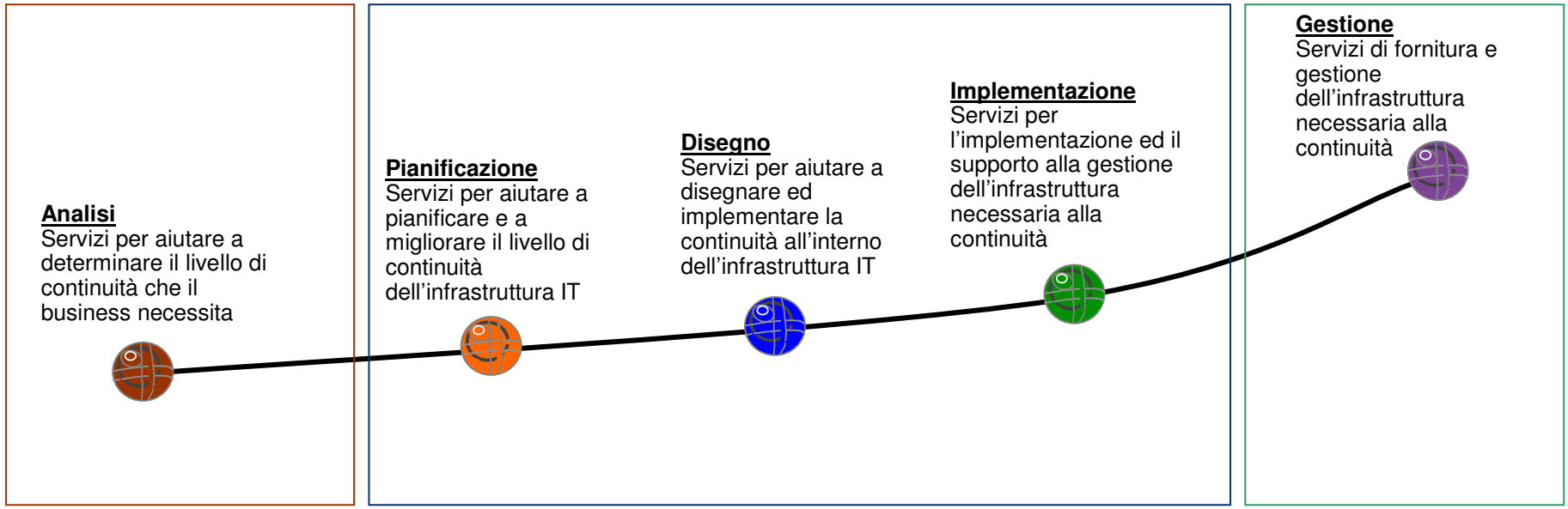
- **Il caso di IBM BCRS**

  - **Perchè certificarsi**

NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

Il team dei servizi di Business Continuity and Resiliency (BCRS) attraverso le proprie professionalità e gli asset tecnologici ha la missione strategica di supportare i clienti IBM a raggiungere e mantenere i loro livelli di continuità operativa

What should I do — *Help* me do it — *Do it for me*



ISO 27001 – Information Security Management System – Specification with guidance for use

- Modello di riferimento per la conformità del sistema di gestione della sicurezza informatica (ISMS) nel quale vengono individuate fasi di analisi e gestione del rischi informatici.
- I risultati delle analisi e le scelte di gestione vengono permanentemente messe in discussione in modo da garantire la capacità dell'azienda di mantenere nel tempo la sicurezza del proprio patrimonio informativo anche in presenza di cambiamenti dovuti a fattori esterni o interni all'azienda stessa.
- E' oggetto di certificazione e costituisce l'unica convalida effettiva della conformità allo standard da parte delle aziende.

Le 11 categorie di controlli di ISO/IEC 17799:2005

Politica di sicurezza

- Enunciare i principi generali di Sicurezza delle Informazioni che dovranno essere rispettati in tutte le attività operative dell'azienda e che guideranno la costituzione di tutte le fasi del ISMS.

Organizzazione di sicurezza

- Adottare un modello organizzativo di sicurezza delle informazioni sulla base del quale attribuire le responsabilità di sicurezza delle informazioni.

Gestione asset

- Classificare le risorse informative in funzione dell'uso, della criticità, della "sensitività" e associare adeguati livelli di protezione.

Sicurezza personale

- Ridurre i rischi di errore, frode e abuso; garantire il giusto livello di preparazione e controllo di attività del personale;

Sicurezza fisica e ambientale

- Prevenire l'accesso non autorizzato agli ambienti e alle infrastrutture; impedire la perdita o il danneggiamento o il furto degli apparati.

Gestione delle operazioni e delle comunicazioni

- Garantire il controllo e la registrazione di eventi, incidenti, minacce, abusi, ecc., la separazione di responsabilità e degli ambienti di elaborazione.

Controllo accessi

- Formalizzare il controllo degli accessi ai dati (userid, password, systemid, network access, ecc).

Acquisto, sviluppo e man.ne applicazioni

- Regolamentare lo sviluppo di applicazioni, la conduzione di progetti, l'applicazione di modifiche secondo norme di sicurezza condivise.

Gestione incidenti e vulnerabilità

- Gestire incidenti di sicurezza e vulnerabilità potenziali.

Gestione della continuità operativa

- Preparare a reagire a fronte di situazioni estreme di disastro al fine di garantire la continuità delle operazioni di business.

Compliance

- Rendere conformi a regole e norme interne ed esterne, leggi e statuti.

Usando la terminologia dello standard: “IBM BCRS definisce l’ambito di applicabilità dell’Information Security Management System a norma dello standard ISO/IEC 27001: 2005”.

Scope di certificazione di IBM BCRS

ATTIVITÀ DI BUSINESS

Progettazione, realizzazione e gestione dei servizi e delle soluzioni di Disaster Recovery, High Availability e Business Continuity

- Housing & Hosting Management
- Test Operations
- Real Disaster operations

UNITÀ ORGANIZZATIVE

IBM BCRS e altre unità organizzative di IBM che operano presso il sito fisico

SITO

Centro di Disaster Recovery e sistemi ivi attestati

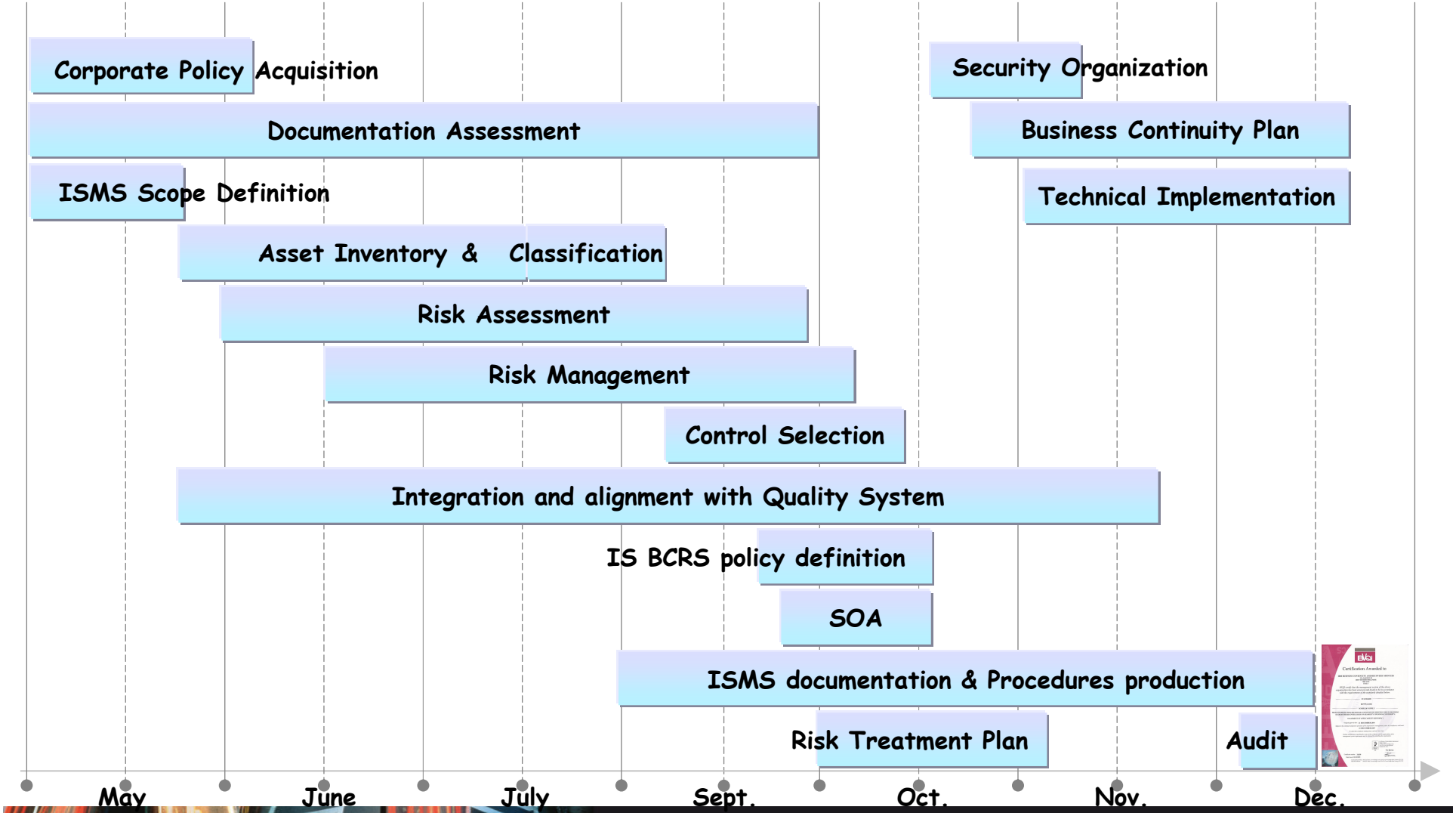
IBM BCRS Center – Settimo Milanese (Milan)

Politica di sicurezza di IBM BCRS

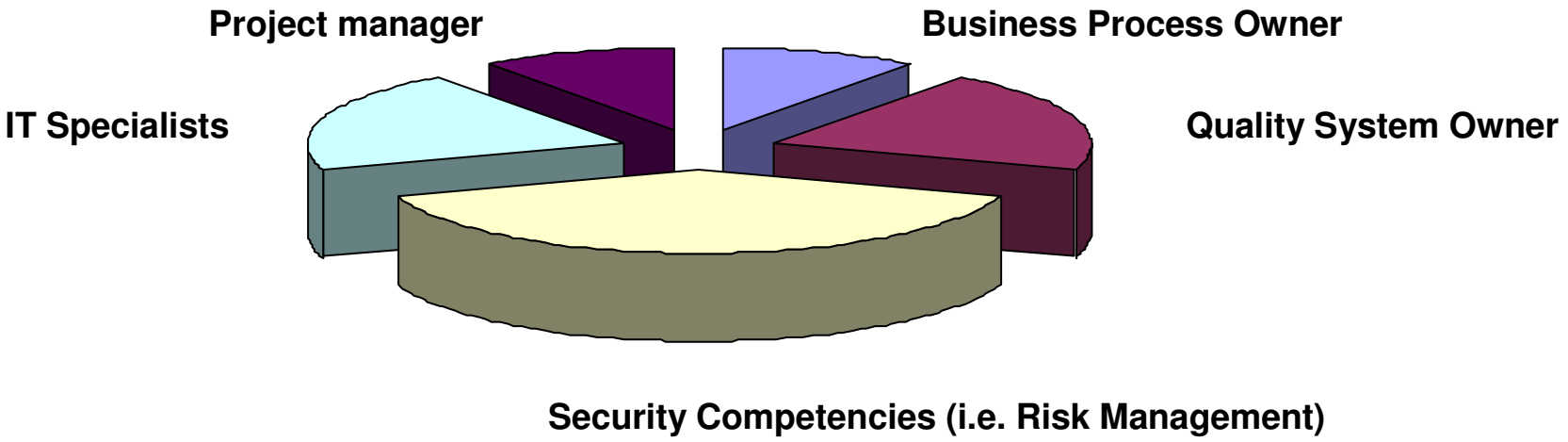
IBM BCRS intende adottare tutte le necessarie misure al fine di garantire:

- l' attribuzione di aggiornate responsabilità di sicurezza;
- la protezione degli asset informativi in modo commisurato al loro valore e in funzione dei risultati dell' analisi dei rischi;
- una continua promozione di comprensione e armonizzazione con leggi e regolamenti generali e specifici per le proprie attività;
- la progettazione, lo sviluppo e l'erogazione di servizi in rispetto dei requisiti di sicurezza e dei requisiti contrattuali sottoscritti;
- la formazione adeguata del personale sul tema della sicurezza in funzione dei ruoli e delle responsabilità di sicurezza ad esso assegnate.
- la tutela della riservatezza, integrità e disponibilità del patrimonio informativo mediante un sistema di gestione della sicurezza, integrato con il sistema qualità.

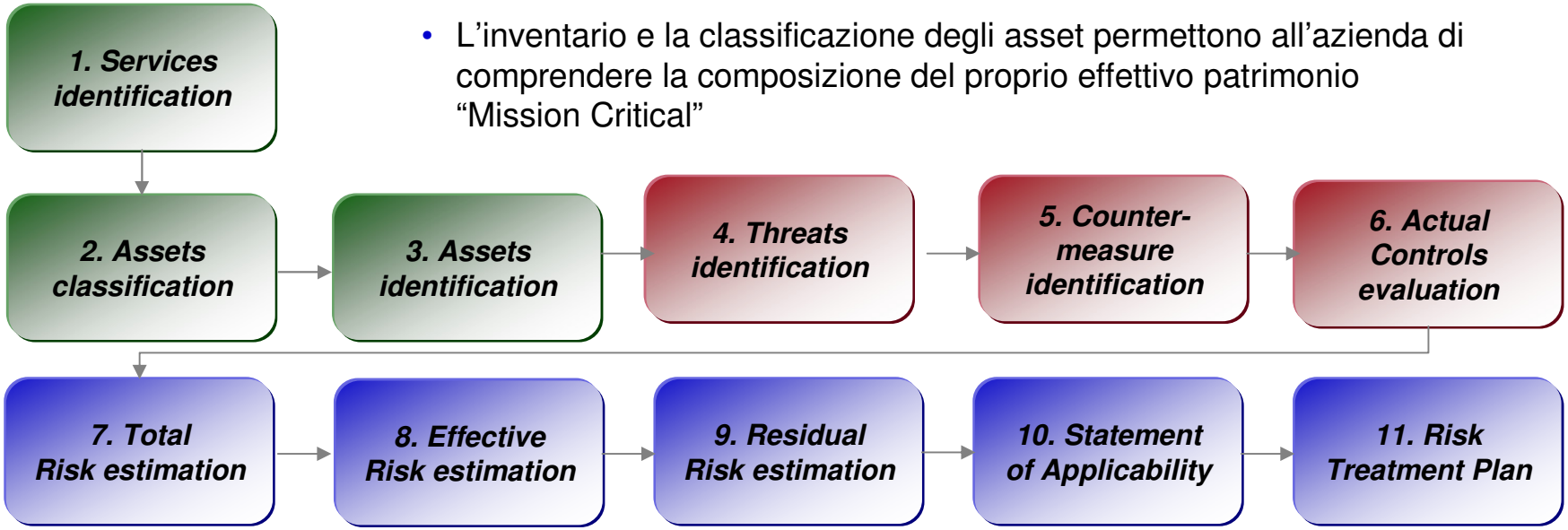
Il percorso di certificazione di IBM BCRS (nel 2004)



Competenze e team di lavoro



La creazione di un ISMS è parte del processo di analisi e gestione dei rischi

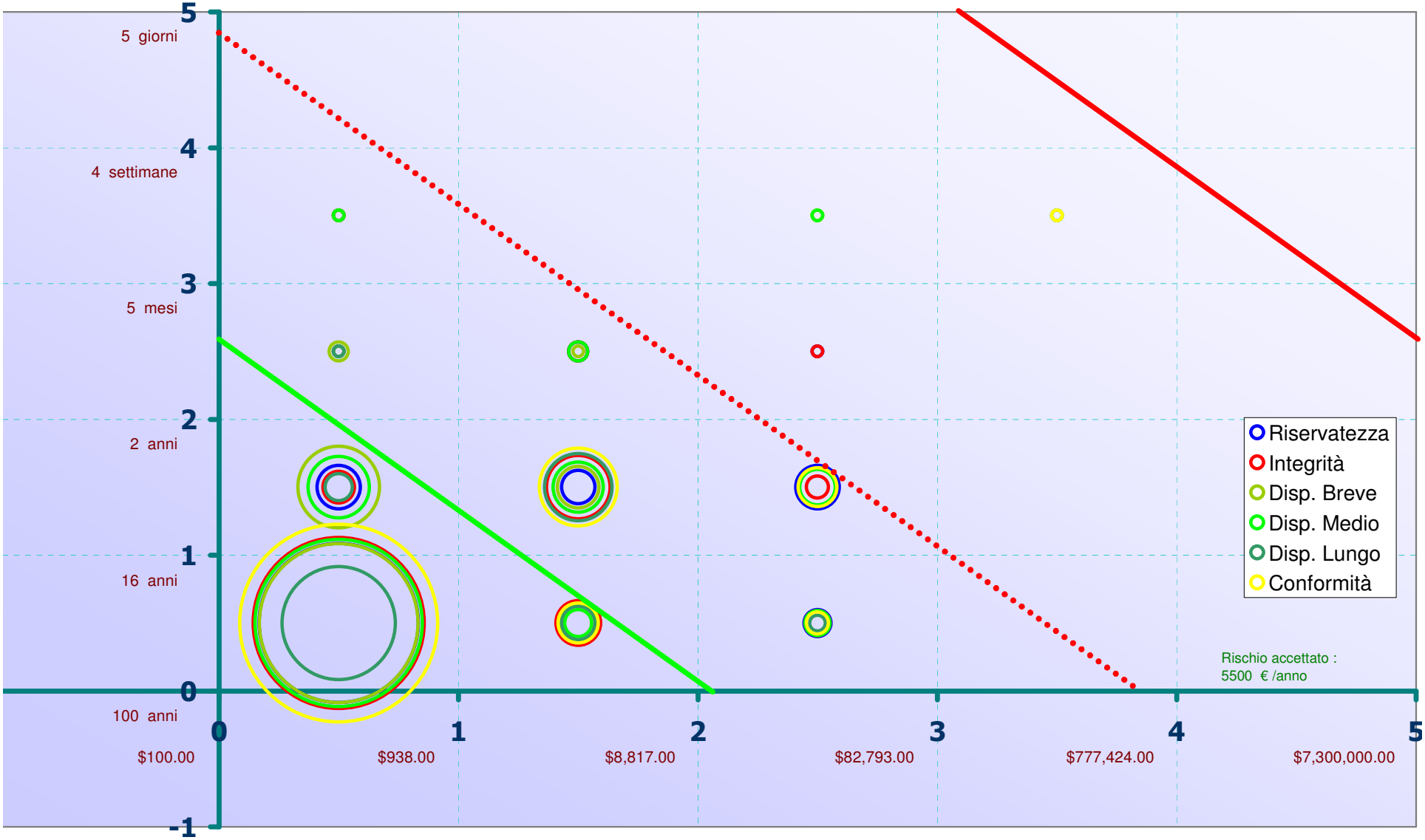


- L'inventario e la classificazione degli asset permettono all'azienda di comprendere la composizione del proprio effettivo patrimonio "Mission Critical"

- L'analisi del rischio permette all'azienda di individuare i requisiti operativi, in funzione del valore degli asset, necessari a tutelare e gestire correttamente il proprio patrimonio
- La gestione del rischio permette all'azienda di ottimizzare i propri investimenti in funzione del rapporto costi / benefici.

Entità dei Rischi Attuali di Sicurezza : Housing & Hosting Management

“Dati indicativi a titolo di esempio usati a scopo accademico”



conseguenze

BASTA PARLARE **INIZIAMO A FARE**

Organizzazione Sicurezza Informatica

BCRS Leader

Information Security Steering Forum
- BCRS Leader
- Security Manager
- Security Delivery Referent

2 x anno

Security Org. Ref.

BCRS Offering Management
- .....

Security Delivery Ref

Security Site Manager

BCRS Consulting
- .....
- .....
- .....

Security Manager

BCRS Local / Central Delivery

BCRS Local Delivery
- .....
- .....
- .....
- .....
- .....
- .....

BCRS Solution Design
- I.....
- .....
- .....
- .....

Security Tech. Ref.

BCRS Central Delivery
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....

Security Wintel FP

Security zSeries FP

Security Org. Focal Point

System Security Focal Points

Network Security FP

Information Security Cross-function Committee
- Security Manager
- Security Delivery Referent
- Technical Security Referent
- Organizational Security Referent
- Organizational Security Focal Point

4 x anno

Controllo e mantenimento del sistema di sicurezza (cenni)

Sempre

- **Conduzione dei progetti/azioni previsti dal Risk Treatement Plan approvato anno precedente**
- **Tracciatura degli incidenti di sicurezza per identificare nuove minacce e vulnerabilità**
- **Controllo della security checklist per ogni nuova proposta di contratto**
- **Mantenimento / aggiornamento documentazione**
- **Ronda mensile.**

Trimestrale

- **Information Security Cross Function Committee - ISCC: Status RTP, analisi Incident Report, analisi Security checklist, analisi KPI**
- **Ronda trimestrale**

Semestrale

- **Information Security Steering Forum - ISSF: definizione / approvazione delle politiche, criteri di analisi e gestione rischi, organizzazione, analisi KPI**

Annuale

- **Avvio Risk Analysis**
- **Audit Interno ISO27001**
- **Avvio Risk Management**
- **Preparazione nuovo RTP**
- **Preparazione Statement of Applicability (SOA)**
- **ISCC: verifica risultati Risk Management, verifica contenuti RTP e SOA**
- **ISSF: Approvazione Risk Acceptance, RTP, SOA**
- **Audit interno ISO27001**
- **Audit Esterno ISO27001 (Bureau Veritas – BVQI)**

Apparato documentale integrato con il sistema di qualità

Certificazione ISO 27001: l'esperienza IBM

- **Il caso di IBM BCRS**

- **Perchè certificarsi**

Alcune considerazioni sulla certificazione ISO 27001.

- **Scopo della certificazione non è "fotografare" l'azienda in un dato momento, bensì porre le basi per un'efficace gestione "nel tempo" del suo assetto nei confronti delle tematiche di sicurezza delle informazioni;**
- **La certificazione contribuisce ad incrementare il valore dell'azienda per gli stakeholders e rappresenta - di frequente - un requisito essenziale per progetti di partnership / outsourcing;**
- **La certificazione comporta per l'azienda uno sforzo continuo di miglioramento delle metodologie di governo della sicurezza;**
- **L'azienda può scegliere un approccio alla certificazione meno invasivo decidendo ad esempio di certificare esclusivamente specifici processi / servizi (mission critical);**
- **Il commitment della direzione e del personale, come in qualsiasi altra attività di certificazione, è essenziale per il buon esito del processo.**