



# **L'esperienza del Gruppo Ferrovie nella governance della sicurezza ICT**

Roma, 21 Giugno 2006

# Sommario

---

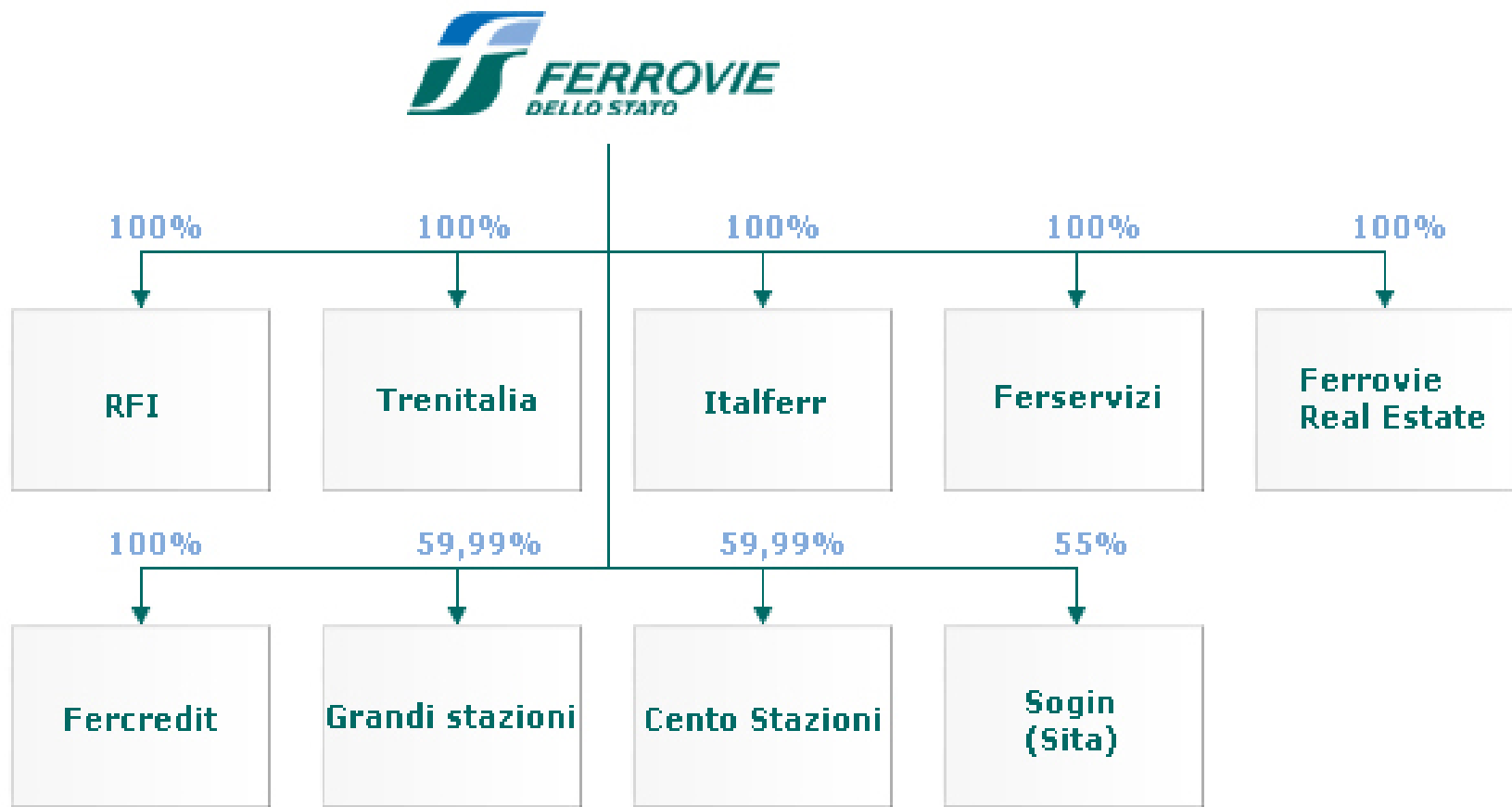
**La strategia**

**ICT Security vision**

**Le attività**

**Azioni fatte e pianificate**

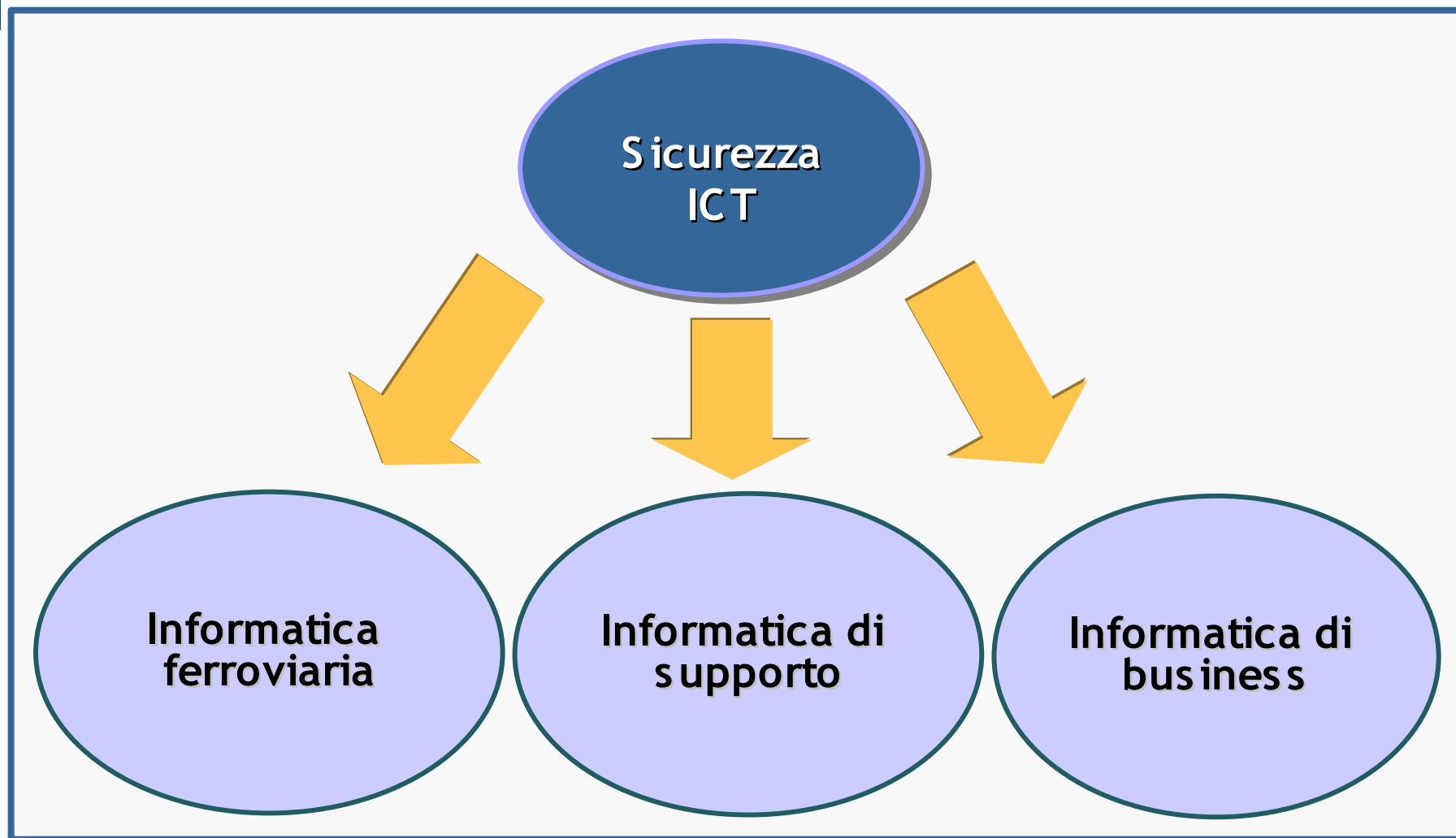
# Il Gruppo Ferrovie



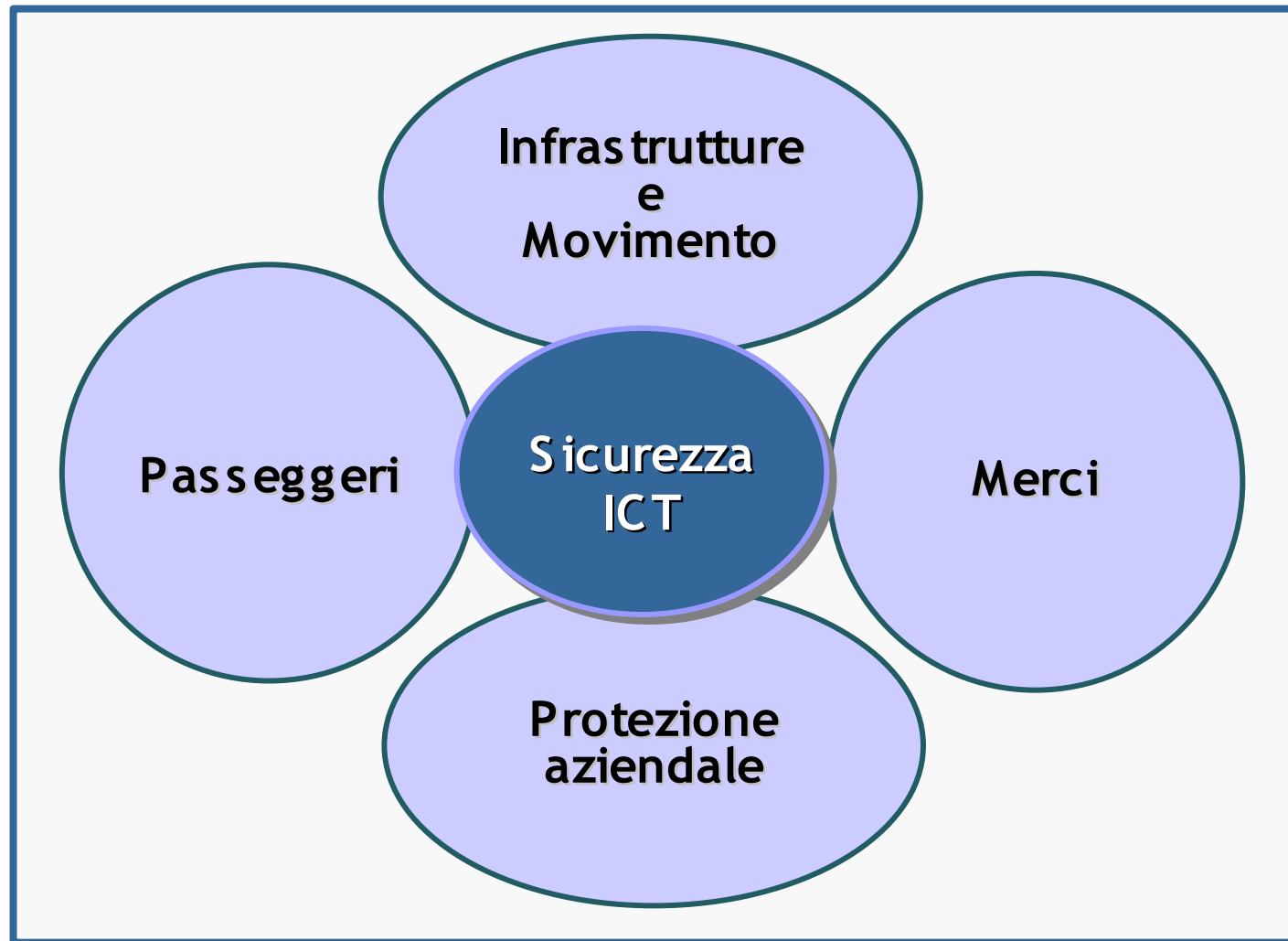
# I numeri dell'Informatica di Gruppo

- Utenti informatizzati: 35.000
- 1.400 Server
- 3 Data Center di grandi dimensioni
- 190 Servizi pubblicati su Internet
- Un autonomous system
- Percentuale di fatturato rilevante grazie all'IT

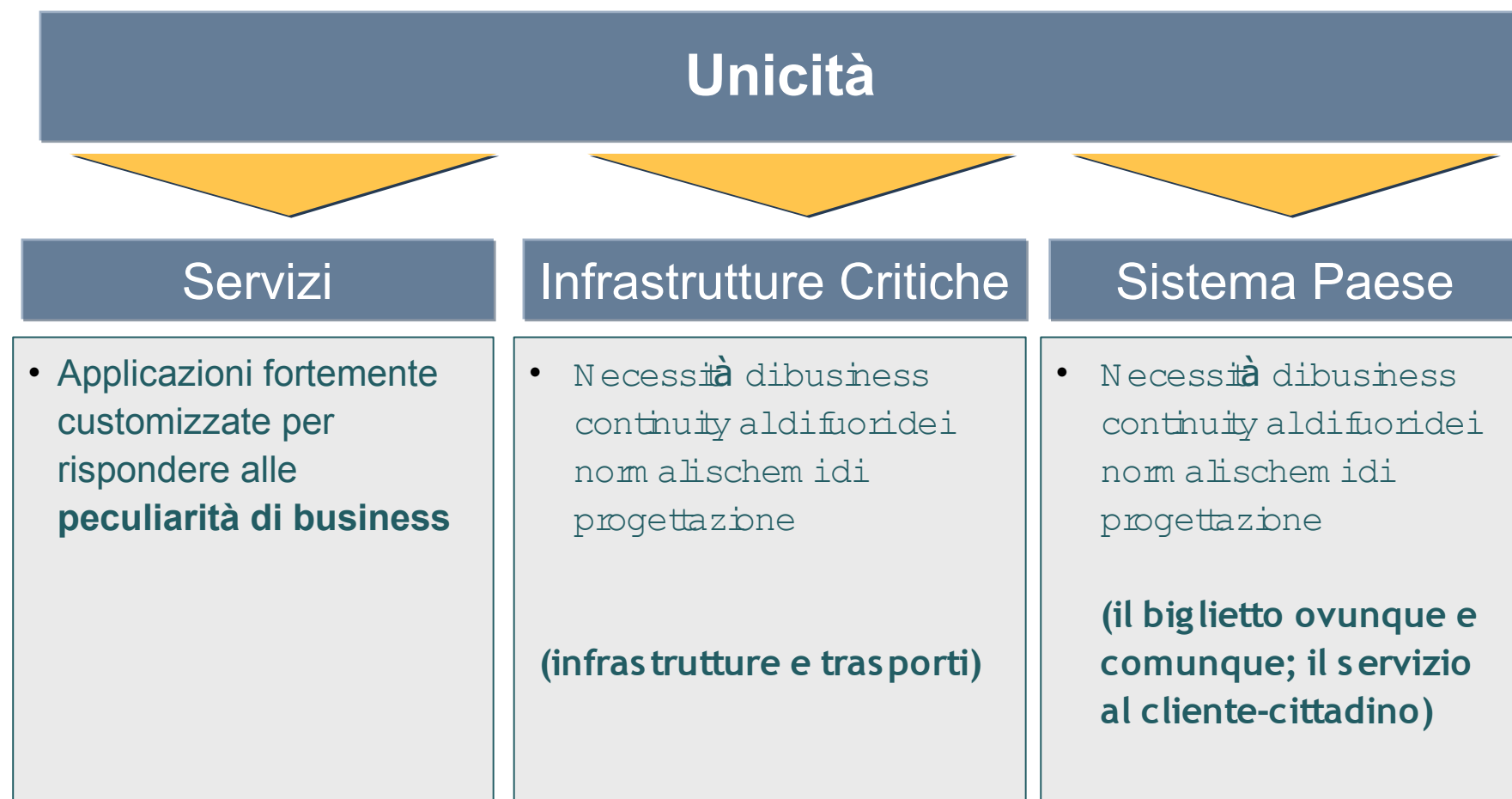
# La Sicurezza ICT in Ferrovie



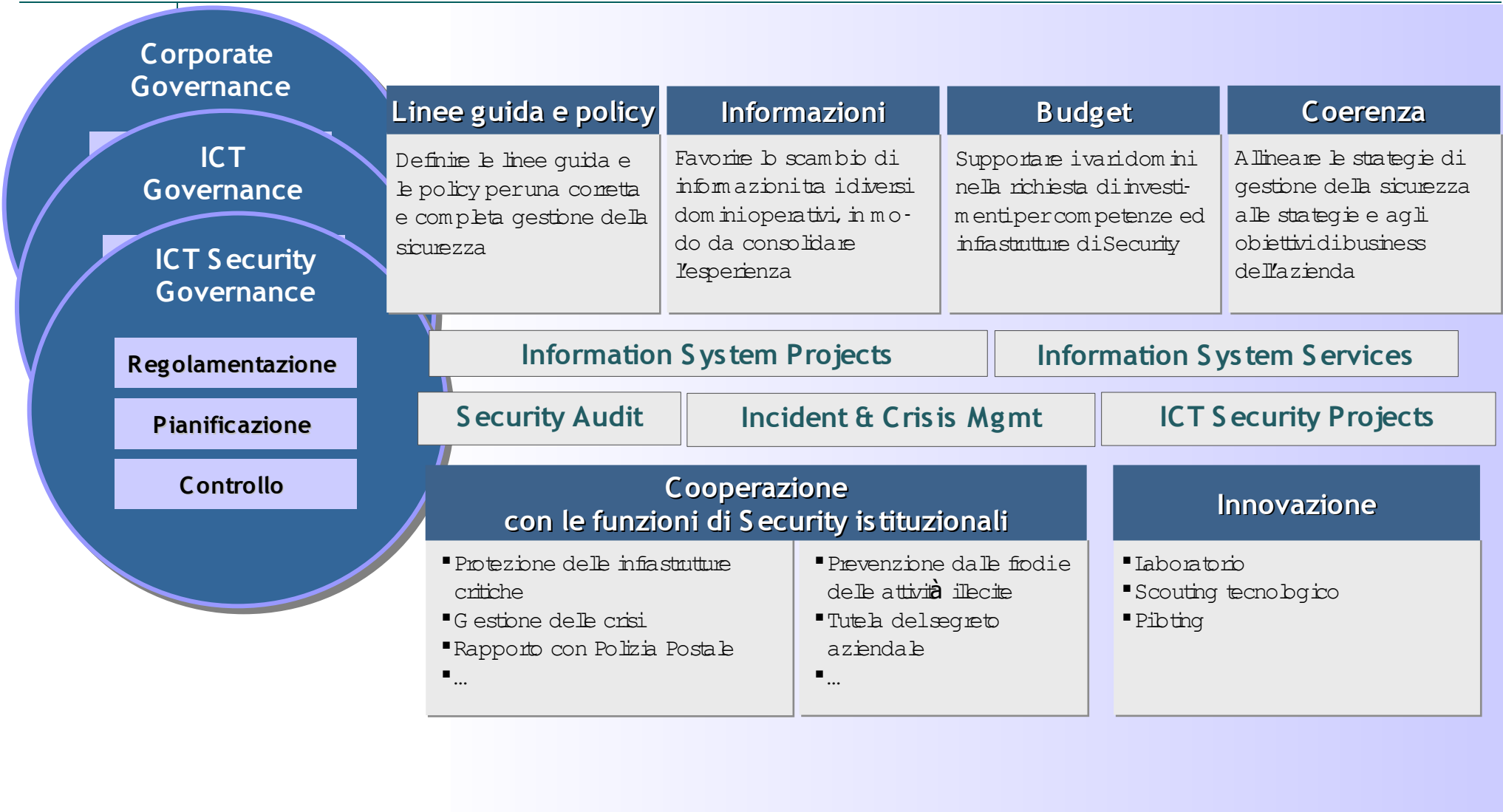
# La Sicurezza in Ferrovie



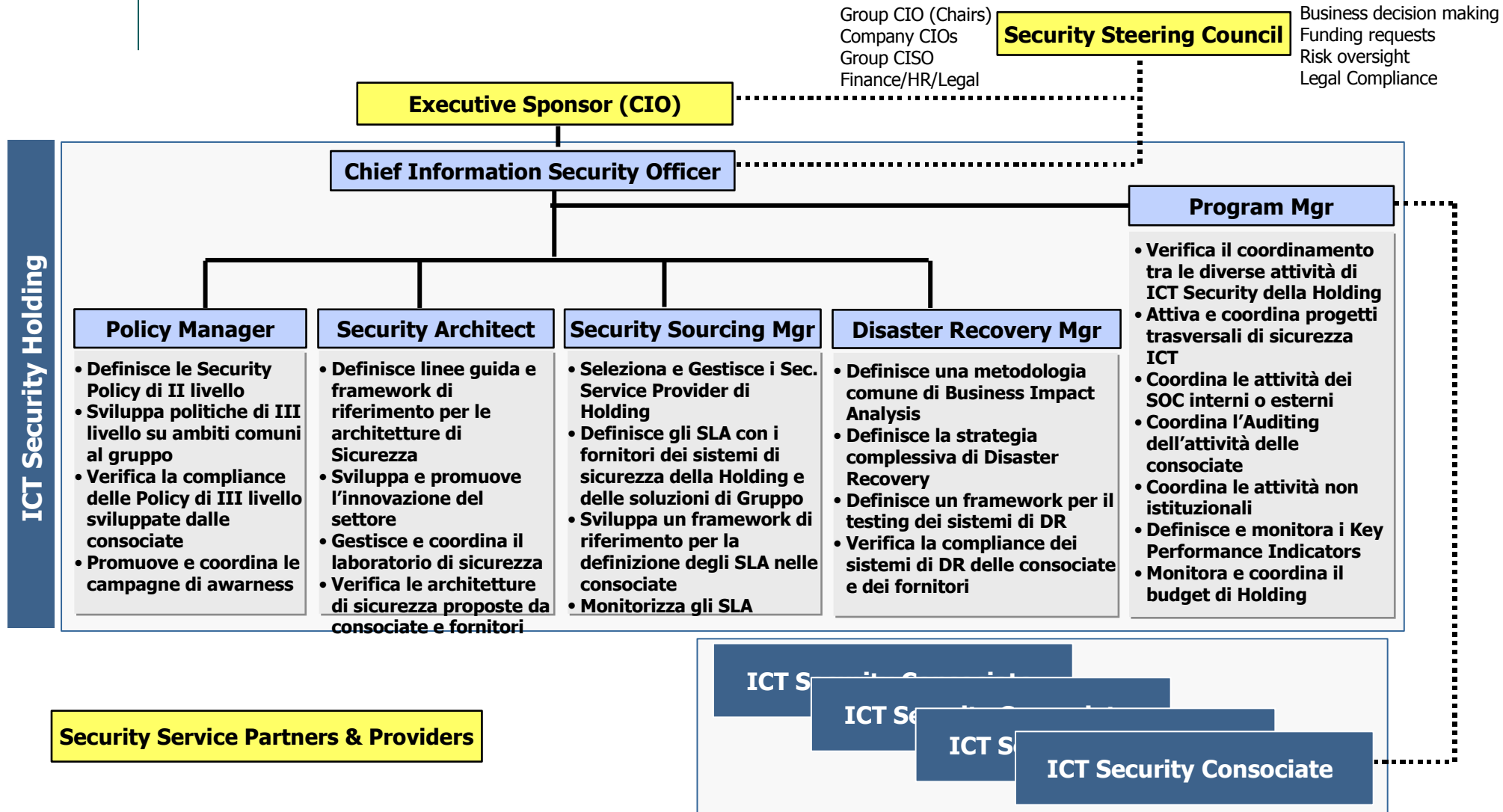
# ICT Security Vision



# Il ruolo della ICT Security di FS



# Modello Organizzativo della ICT Security



# Sommario

---

La strategia

ICT Security vision

**Le attività**

**Azioni fatte e pianificate**

# Il SOC su Internet - L'approccio

## Strategia

### Efficienza Economica

- **Diminuzione del rischio intrinseco** grazie al miglior controllo
- **Trasferimento del rischio operativo** a mezzo dell'investimento
- **Consolidamento delle connessioni** esistenti e delle **web farm**
- **Riduzione della spesa** grazie alla concentrazione ed armonizzazione

### Governo

- Creazione di **strumenti** a garanzia della **disponibilità** dei servizi e a **contrasto di attacchi**
- Definizione di **policy e procedure** mirate a regolamentare e standardizzare la pubblicazione dei servizi su web
- **Ottimizzazione** dei server che ospitano i servizi pubblicati

# Il SOC su Internet

## I servizi

Sicurezza Perimetrale

- **Governo della protezione locale e geografica** per tutte le società del Gruppo
- Infrastruttura proattiva di **prevenzione e gestione** degli attacchi informatici

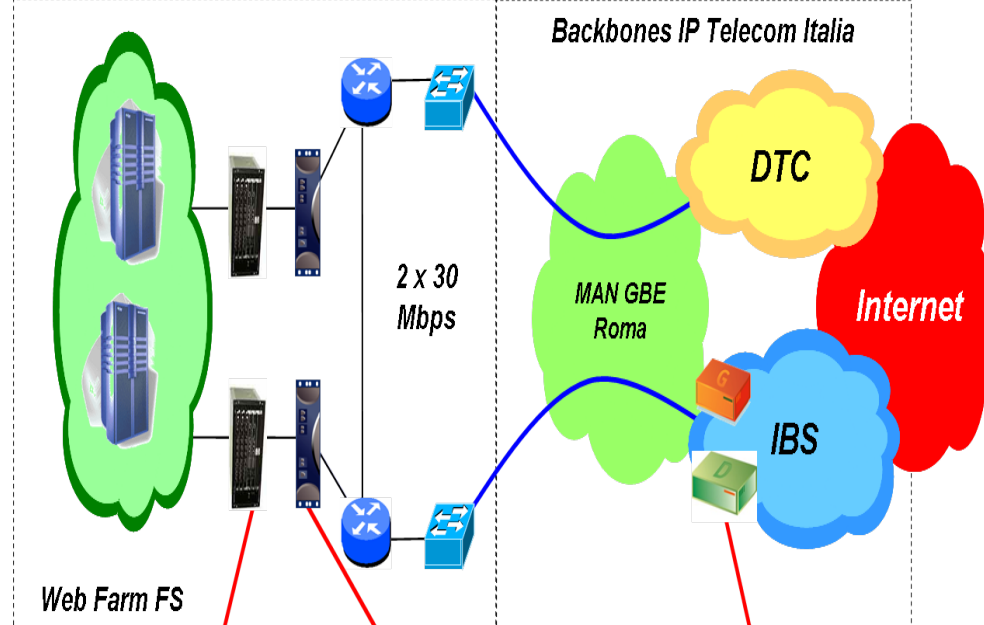
Gestione Incidenti e Crisi

- **Organizzazione di Gruppo dedicata al governo** delle situazioni anomale e di pericolo
- **Gestione e coordinamento** delle attività di segnalazione, contenimento, risoluzione e analisi ex-post degli incidenti rilevati

Early Warning

- Correlazione e verifica delle **vulnerabilità** associate ai servizi di Gruppo
- Segnalazione proattiva delle problematiche di sicurezza in tempo utile per la loro **mitigazione**

## La tecnologia



Fortigate 5050

- Firewall
- IDS/IPS
- 500 VLAN supportate
- Alta affidabilità

Service Engine 2020

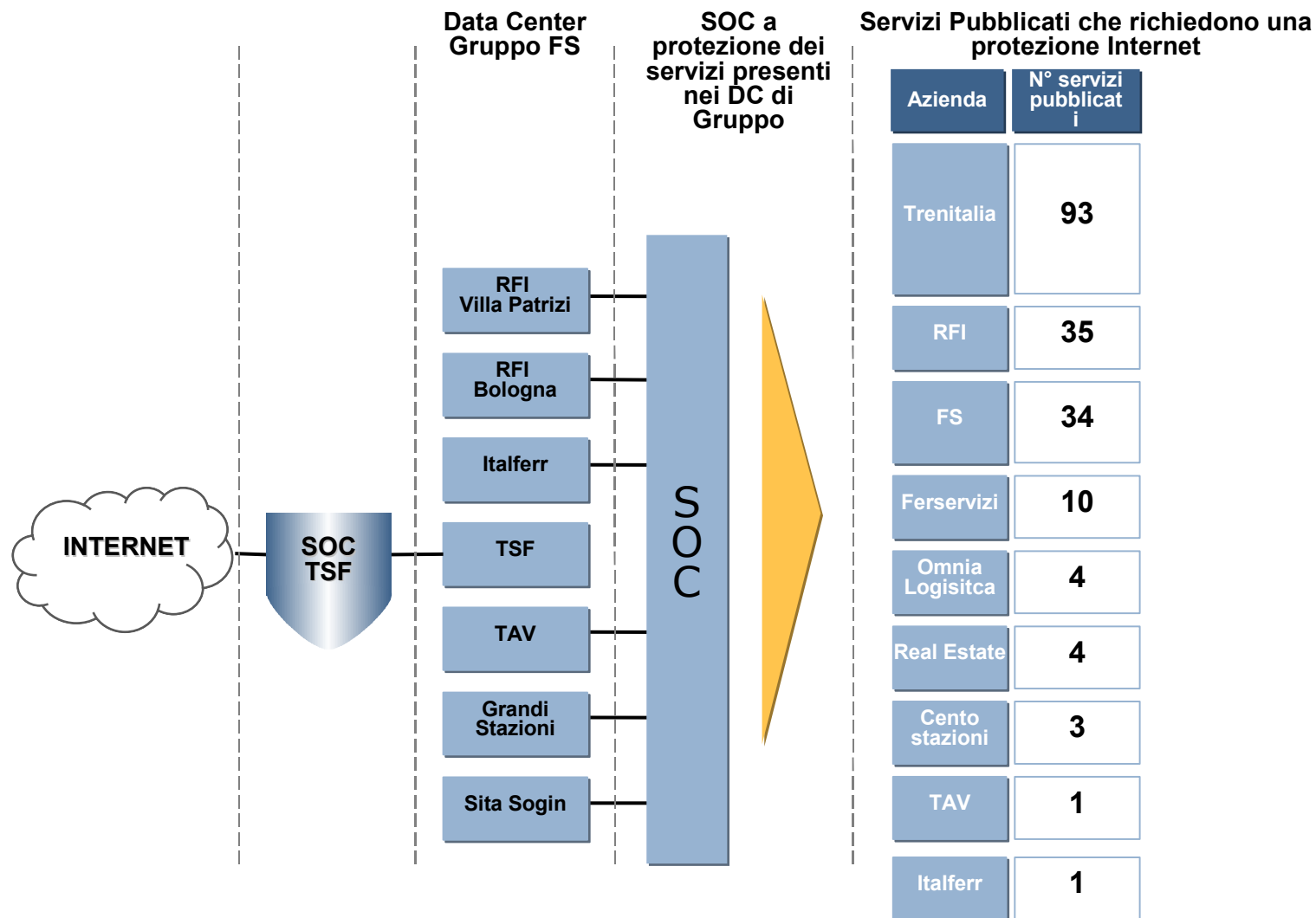
- Bandwidth management
- Reportistica
- Alta affidabilità

Detector e Guard

- DDoS mitigation

**Managed Security Services**

# L'ombrello unico di protezione



# Il “Disaster Recovery di Gruppo”

## Obiettivo

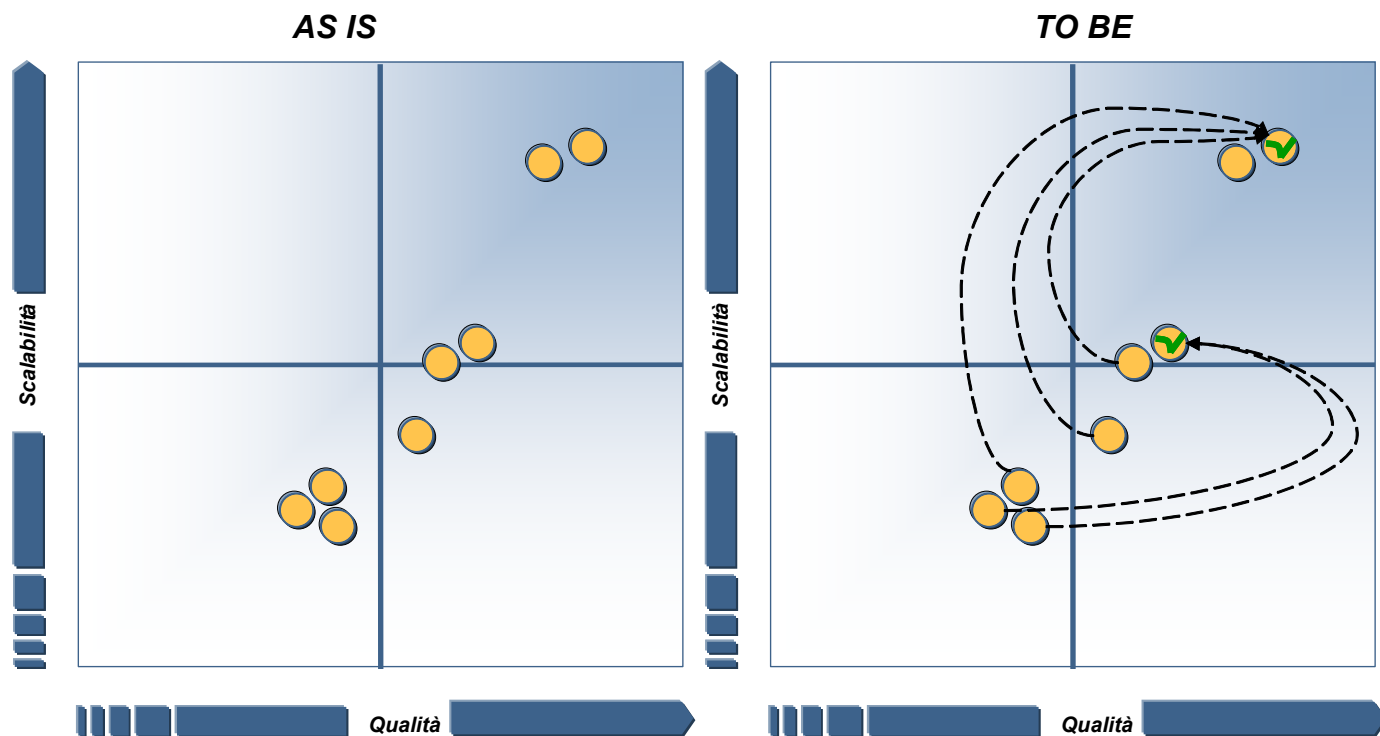
**Teamwork** tra le Società per le **azioni** attuative per

- i **processi** con necessità di **Business Continuity**
- il percorso “**as is**” -> “**to be**”
- il **perfezionamento** dei siti e la **realizzazione** delle soluzioni di Disaster Recovery

# Data Centers Scorecard

Are di valutazione	Peso
Caratteristiche generali	10%
Disaster Recovery best practices	20%
Disaster Avoidance	20%
Caratteristiche infrastrutturali	6%
Impianto meccanico/ termico	6%
Impianto idraulico	6%
Impianto elettrico	6%
Sicurezza fisica	10%
Reti di telecomunicazioni	6%
Protezione da incendi	10%
<b>Qualità</b>	
<b>Scalabilità</b>	
▼	
<b>Valutazione complessiva</b>	

## ESEMPIO



# Il Disaster Recovery di gruppo

## Strategia

### DC Planning

- Censimento e **pianificazione** degli datacenter aziendali
- Razionalizzazione delle **connettività**
- Definizione della **strategia di sourcing**

### Disaster Recovery / BCP

- **Messa in sicurezza** delle **applicazioni** con necessità di **D.R. o B.C.**
- Criteri per la definizione di **RTO e RPO comuni e per aree di business omogenee**
- **Coerenza** con la strategia di Gruppo per il **sourcing**

# Il Governo delle Identità e degli Accessi

Soluzione organizzativa che usa la tecnologia per abilitare  
il governo dei processi aziendali  
attraverso la coerenza tra gli individui e le autorizzazioni

## Processi

- **Profilazione** basata sul ruolo
- **Accountability & Auditability**
- **Automazione** dei processi aziendali

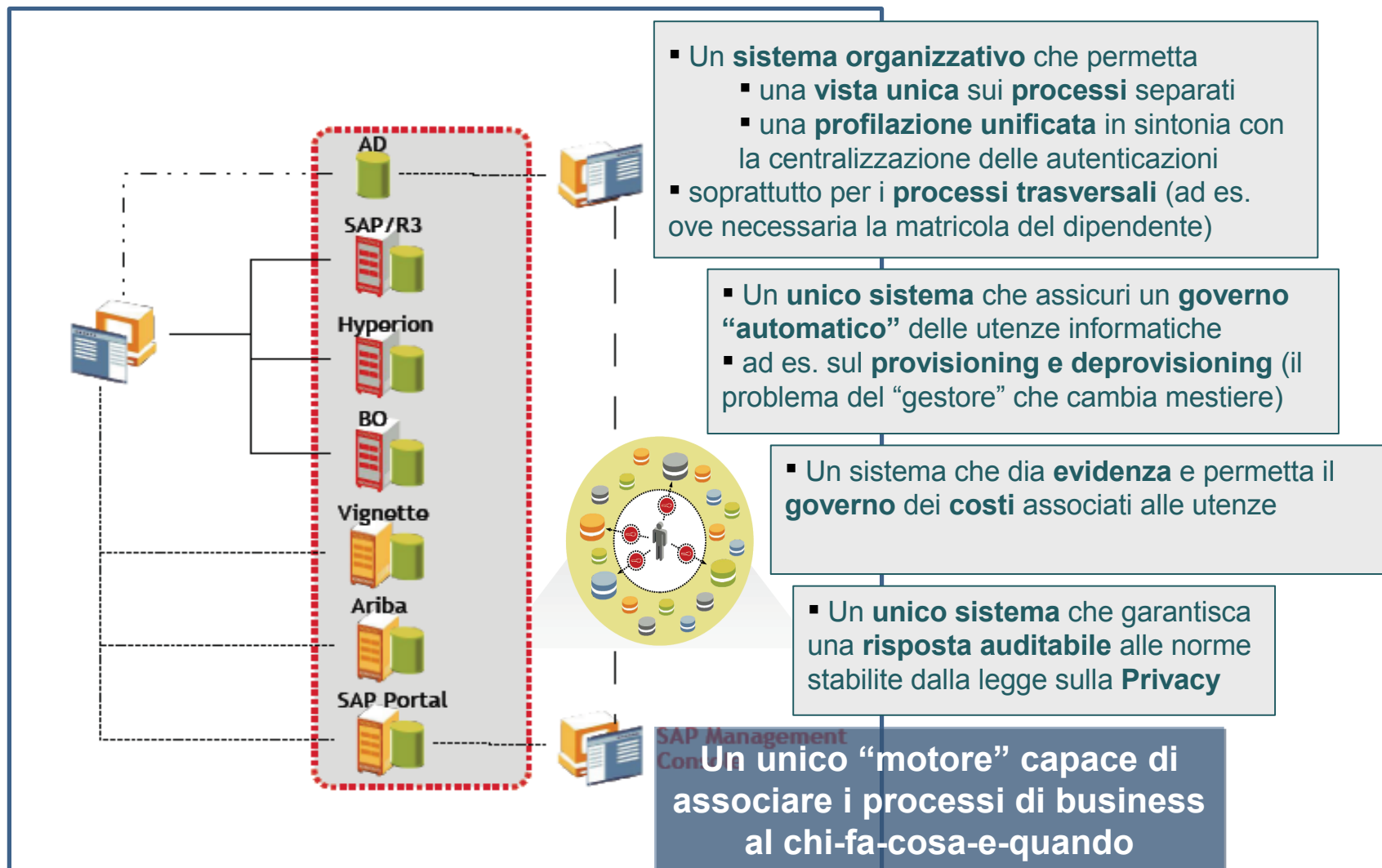
## Organizzazione

- Corrispondenza tra **profilo informatico e posizione organizzativa**
- **Provisioning e deprovisioning** sincrono ed automatico

## Operazioni

- **Cross-Application & Cross-Platform**
- **Centralità** di autenticazioni e autorizzazioni
- **Policies & standards** distribuiti

# Lo IAM nel disegno di unità in FS



# La creazione di Valore dello IAM

Valore Economico
<ul style="list-style-type: none"><li>• <b>Consolidamento</b> delle infrastrutture tecnologiche</li><li>• <b>Automazione</b> dei processi aziendali</li><li>• <b>Provisioning e deprovisioning</b> automatico</li></ul>
Valore al Management
<ul style="list-style-type: none"><li>• Corrispondenza tra <b>profilo informatico e posizione organizzativa</b></li><li>• Semplicità di <b>Auditing</b></li><li>• <b>Single Sign On</b></li></ul>
Valore Normativo
<ul style="list-style-type: none"><li>• <b>Governo</b> del ciclo di vita di <b>utenze e password</b></li><li>• Gestione del conflitto organizzativo di <b>ruolo e posizione</b></li><li>• <b>Profilazione</b> basata sul <b>ruolo</b></li><li>• Trasparenza sui <b>processi organizzativi e di gestione</b></li></ul>
Valore Tecnologico
<ul style="list-style-type: none"><li>• <b>Role Based Access Control</b></li><li>• <b>Sincronizzazione</b> Password fra sistemi</li><li>• <b>Cross-Application &amp; Cross-Platform</b></li></ul>

Riduzione dei Costi
<ul style="list-style-type: none"><li>• <b>Esatta</b> quantificazione degli investimenti</li><li>• <b>Coerenza</b> del TCO</li><li>• <b>Minimo onere</b> nella gestione delle utenze</li></ul>
Aumento Produttività
<ul style="list-style-type: none"><li>• <b>Workflow</b> informatico congruente con il processo organizzativo</li><li>• Semplicità nell'identificare il <b>"chi-fa-cosa"</b></li><li>• <b>Reporting</b> affidabile</li></ul>
Rispetto delle Leggi e Norme Internazionali
<ul style="list-style-type: none"><li>• Testo unico sulla <b>Privacy</b> sulla gestione delle credenziali di accesso e delle utenze, con eliminazione del rischio di sanzioni <b>penali</b></li><li>• Aderenza a <b>normative internazionali</b> quali <b>SOX - ISO17799 - BASILEA 2</b></li></ul>
Sicurezza
<ul style="list-style-type: none"><li>• <b>Centralità</b> di autenticazioni e autorizzazioni</li><li>• Policies &amp; standard distribuiti</li><li>• <b>Strong Authentication</b></li></ul>

# Altre azioni in corso

Documento  
Programmatico sulla  
Sicurezza

Il **DPsS: strumento operativo**, non solo documento a valore legale; framework comune; **risk analysis** di Gruppo; **strumenti di Governo**; **autonomia delle Società** nella redazione dei futuri DPsS.

Governance Sicurezza  
delle Applicazioni

Adozione di un prodotto specializzato per un **sistema di governance** della sicurezza delle applicazioni, con creazione di **piani di rientro** suggeriti e controllati su base BS7799 e Common Criteria.

Disaster Recovery &  
Business Continuity  
Management

Adozione di un prodotto specializzato per **sistema di governance** per la **gestione automatica delle procedure** di Disaster Recovery e Business Continuity.

Secure Development

Attuazione di **procedure** che garantiscano la **sicurezza** delle **applicazioni sviluppate** all'interno del Gruppo. Integrazione di ogni appalto/commissa con specifiche e **controllo qualità sul codice**.

# Altre azioni in corso

## Security HW Consolidation

Consolidamento delle attuali infrastrutture di sicurezza (proxy e firewall): **governo e savings**.

## UTM + Hardening + NAC + Content Protection

**Inibizione** di navigazione su categorie di siti pericolosi o illegali o impropri - Propagazione **best practice** da Società - Servizi di **prevenzione** da “log correlation” - ...

## Campagna di Awareness

Programma di **Formazione & Education**, strutturato per i diversi livelli aziendali e per tipologia di utenti; in fase di costruzione con **HR**. Primo evento “**Security Day**” il **25 Maggio**.

# Azioni principali entro 12 mesi

## Crescita dell'ICT Security in FS

- **Security Competence Center**
  - supporto - controllo - misura
  - strumenti di governo

## Realizzazione di Progetti Rilevanti di Gruppo

- **Disaster Recovery & Business Continuity**
- **SOC su Internet, Extranet ed Intranet**
- **Governo delle Identità e degli Accessi**

# GRAZIE

---

