



# **L'OUTSOURCING IT: BEST PRACTICE E AUDITING**

## **Classificazione dei rischi dell'outsourcing**

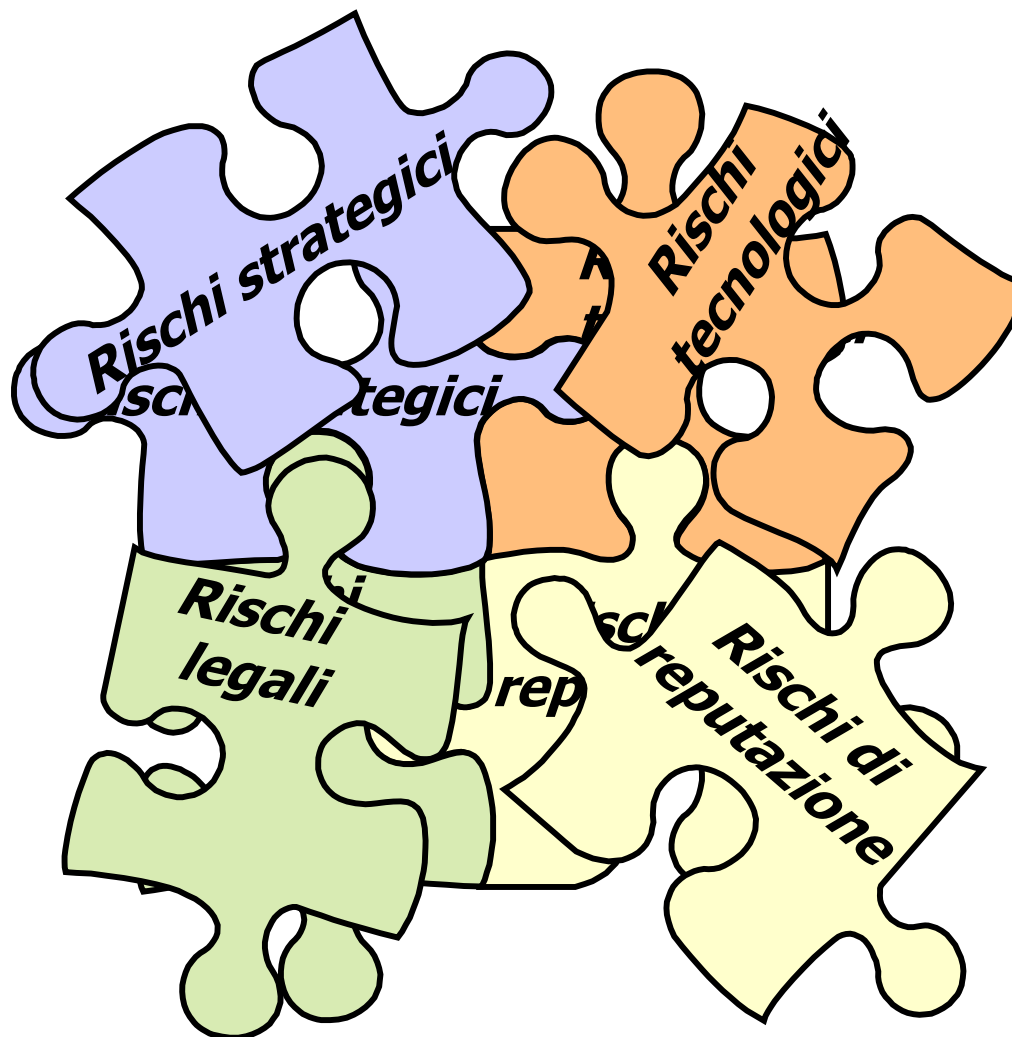
*Alessandro Ierardi, Consorzio  
Operativo Gruppo MPS*



# Agenda



- **Ambito di riferimento**
- **Il ruolo dell'Internal Auditing**
- **Classificazione e Ciclo di vita**
- **La Governance**



## a.1. ANALISI (*Plan*)

### a.1.1. Individuazione esigenze e definizione strategie

### a.1.2. Identificazione team di analisi

Valutazione dei processi interni

Identificazione dei criteri di scelta

Scelta dei processi da esternalizzare e degli obiettivi

### a.1.4. Identificazione del fornitore

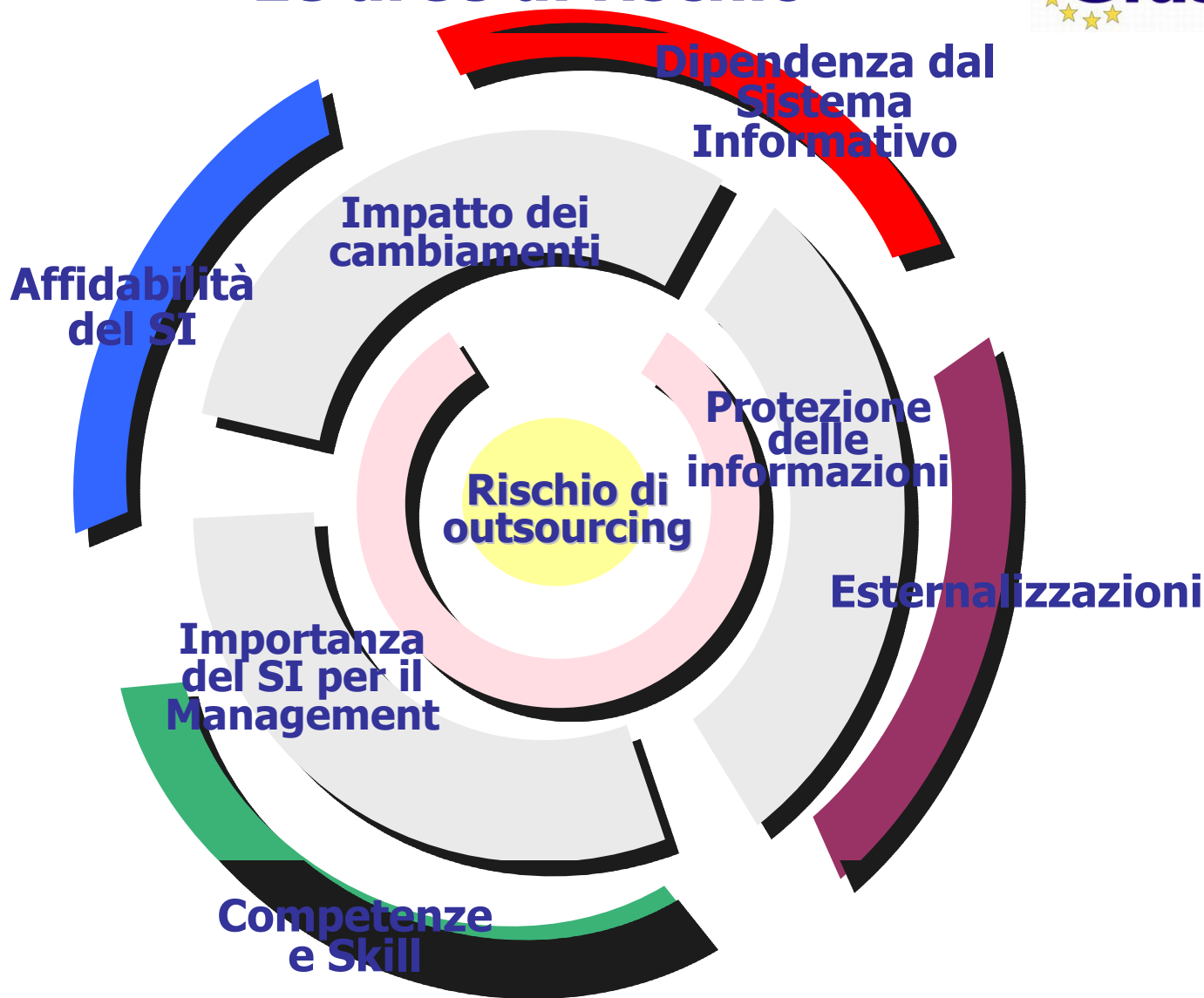
Ricerca di mercato

Identificazione forma di outsourcing

Identificazione outsourcer

### a.1.5. Definizione del progetto di attuazione e macro-plan

### a.1.6. Definizione del contratto

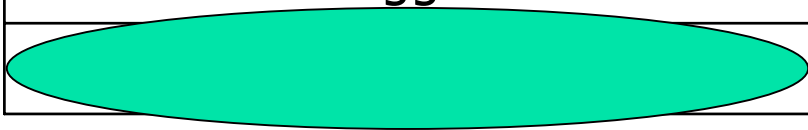




## **a.3. GESTIONE E VERIFICA DEL CONTRATTO (*Check*)**

### **a.3.1. Gestione del contratto e del fornitore**

### a.3.2. Monitoraggio dei livelli di servizio



## **a.4. EVOLUZIONE E REVISIONE DEL CONTRATTO (*Act*)**

### a.4.1. Miglioramento continuo

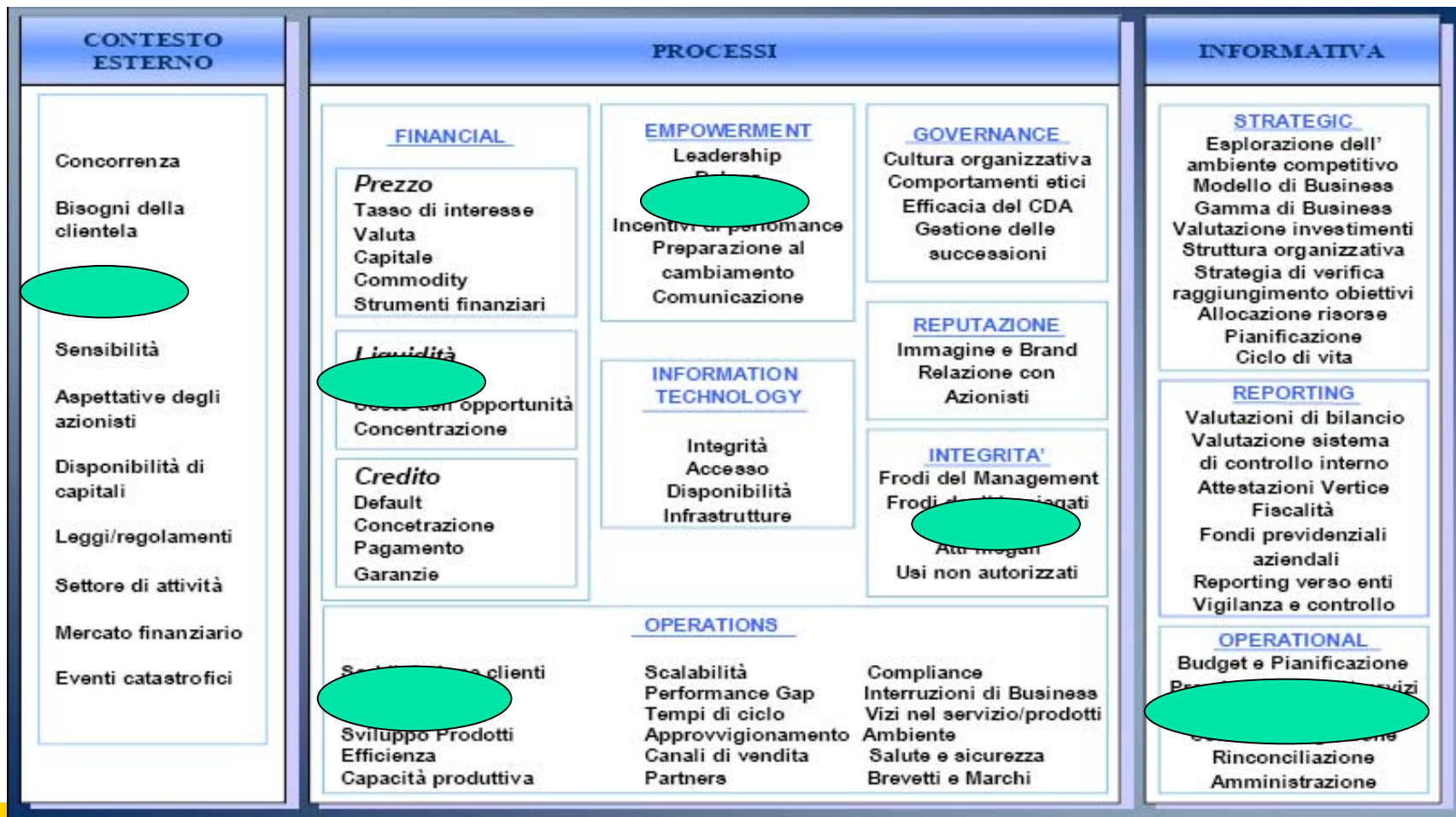
### **a.4.2. Valutazione economica e strategica del servizio di outsourcing**

### **a.4.3. Rinnovo del contratto/scelta diverso outsourcer**



# Un linguaggio comune

(in generale)



Fonte: Protiviti - Independent Risk Consulting



# Key Risk in Outsourcing

(Una classificazione internazionale)



<b>Strategic Risk</b> <b>Plan 1.4</b> <b>Do 2.3</b>	The third party may conduct activities on its own behalf which are inconsistent with the overall strategic goals of the regulated entity. Failure to implement appropriate oversight of the outsource provider. Inadequate expertise to oversee the service provider. <b>Do 2.5</b>
<b>Reputation Risk</b> <b>Check 3.2</b>	Poor service from third party. Customer interaction is not consistent with overall standards of the regulated entity. Third party practices not in line with stated practices (ethical or otherwise) of regulated entity. <b>Check 3.1</b>
<b>Compliance Risk</b> <b>Plan 1.4</b>	Privacy laws are not complied with. Consumer and prudential laws not adequately complied with. <b>Check 3.1</b> Outsource provider has inadequate compliance systems and controls.
<b>Operational Risk</b> <b>Plan 1.4</b>	Technology failure. <b>Check 3.1</b> Inadequate financial capacity to fulfil obligations and/or provide remedies. Fraud or error. Risk that firms find it difficult/costly to undertake inspections.



# Key Risk in Outsourcing

(Una classificazione internazionale)



<b>Exit Strategy Risk</b> <b>Act 4.3</b>	The risk that appropriate exit strategies are not in place. This could arise from over-reliance on one firm, the loss of relevant skills in the institutions itself preventing it bringing the activity back in-house and contracts which make a speedy exit prohibitively expensive. Limited ability to return services to home country due to lack of staff or loss of intellectual history.
<b>Counterparty Risk</b>	Inappropriate underwriting or credit assessments. <b>Plan 1.4</b> Quality of receivables may diminish.
<b>Country Risk</b>	Political, social and legal climate may create added risk. <b>Plan 1.4</b> Business continuity planning is more complex.
<b>Contractual Risk</b>	Ability to enforce contract. For off-shoring, choice of law is important. <b>Plan 1.6</b>
<b>Access Risk</b>	Outsourcing arrangement hinders ability of regulated entity to provide timely data and other information to regulators. <b>Plan 1.6</b> Additional layer of difficulty in regulator understanding activities of the outsource provider.
<b>Concentration and Systemic Risk</b>	Overall industry has significant exposure to outsource provider. This concentration risk has a number of facets including: <ul style="list-style-type: none"><li>▪ Lack of control of individual firms over provider; and</li><li>▪ Systemic risk to industry as a whole</li></ul>



“Il ricorso all’outsourcing, più che considerarsi come una fonte specifica di rischio, assume rilevanza per il fatto di aumentare l’esposizione alle varie tipologie di rischio”.

In particolare, l’affidamento a terzi, in tutto o in parte, del proprio sistema informativo può essere causa di:

- rischi tecnologici
- rischi strategici
- rischi legali
- rischi di reputazione

Convenzione Interbancaria per i Problemi dell'Automazione - **CIPA**

RISCHI STRATEGICI	RISCHI TATTICI	RISCHI OPERATIVI
<p>Chiara comprensione delle necessità del business <b>Plan 1.1</b></p> <p>Comprensione dei tempi necessari per raggiungere gli obiettivi dell'operazione <b>Plan 1.3</b></p> <p>Ruoli e responsabilità compresi e condivisi <b>Plan 1.6</b></p> <p>Esistenza di un sistema di valutazione (scorecard) del successo <b>Do 2.3</b></p>	<p>Dipendenza dal sistema informativo <b>Act 4.3</b></p> <p>Competenze e skill <b>Do 2.5</b></p> <p>Affidabilità del sistema informativo <b>Check 3.1</b></p> <p>Cambiamenti <b>Do 2.2</b></p> <p>Esternalizzazioni <b>Check 3.1</b></p> <p>Importanza del Sistema Informativo per il management della società <b>Act 4.2</b></p> <p>Protezione delle informazioni <b>Do 2.4</b></p>	<p>Il contratto e la parte legale <b>Plan 1.6</b></p> <p>La sicurezza <b>Check 3.1</b></p> <p>Gli SLA ed il loro monitoraggio <b>Plan 1.6</b></p> <p>La Governance <b>Check 3.2</b></p> <p><b>Do 2.1</b></p>



*“L’outsourcing coinvolge due entità che interagiscono fra loro in una relazione commerciale molto stretta e che si traduce in una ricetta per complicazioni legali.”*

- IT Governance:

modalità con cui un'organizzazione governa e controlla in modo efficace le attività che richiedono l'impiego di sistemi informativi

- Gestione dei rischi informatici ed all'allineamento dei sistemi alle finalità di business

## Interventi normativi

## Obiettivi:

- valore per l'azienda
- gestire e mitigare i rischi IT

Struttura organizzativa - ruoli e responsabilità ben chiari: sicurezza, processi aziendali, infrastruttura, analisi dei rischi, applicazioni.



## AMBITO DI CRITICITA'

- SELEZIONE DELL'OUTSOURCER
- ACCORDI CONTRATTUALI
- ASPETTI STRATEGICI
- STRUTTURE ORGANIZZATIVE
- CONTROLLO SUL SERVIZIO RICEVUTO
- COMPETENZE INTERNE SULL'ICT
- DIPENDENZA DAL FORNITORE

## FASE CICLO DI VITA

- PLAN (1.4)
- PLAN (1.6)
- PLAN (1.1) - ACT (4.3)
- DO (2.4) - CHECK (3.1)
- CHECK (3.2) - PLAN (1.6)
- PLAN (1.2) - DO (2.1/2.5)
- PLAN (1.4) - DO (2.4) - CHECK (3.2) - ACT (4.3)



- Aree di carattere economico, strategico, di mercato, operativo.
- **Rischio di non conformità alle norme** - inteso come il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme di legge, di regolamenti, ovvero di norme di autoregolamentazione o di codici di condotta
- La **responsabilizzazione** di tutti i dipendenti o collaboratori di terze parti





***Grazie per l'attenzione***