SECURITY SUMMIT

Verona, 10 ottobre 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

La gestione del rischio “terze parti”: l’importanza della corretta contrattualizzazione dei rapporti di fornitura, anche alla luce delle indicazioni normative

Anna Italiano, Partner, Partners4innovation

Anna Italiano

PARTNER – PARTNER4INNOVATION

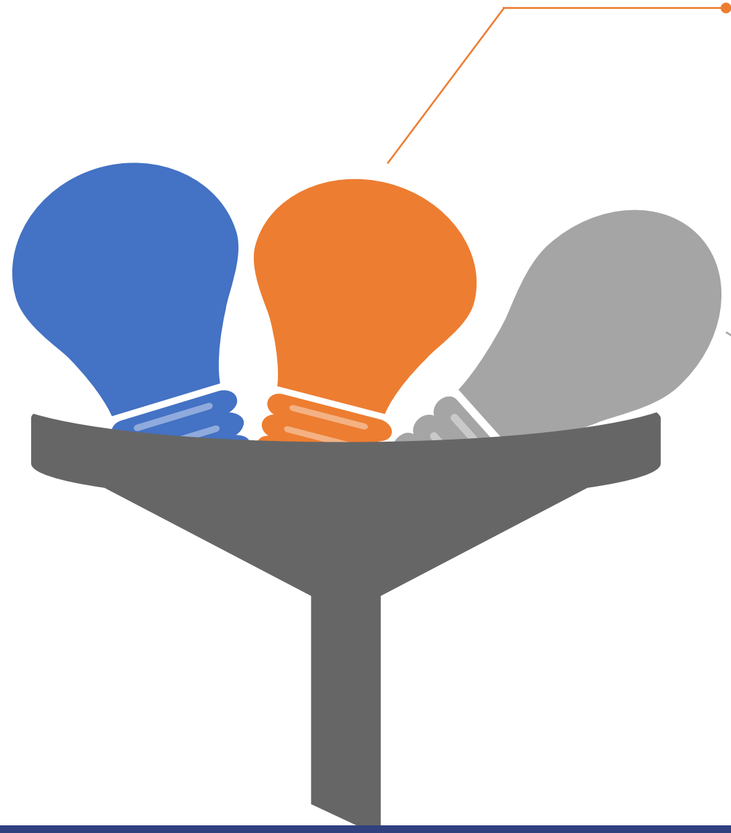
SENIOR ADVISOR – OSSERVATORI DIGITAL INNOVATION

BOARD MEMBER WOMEN 4 SECURITY

Introduzione: premesse generali

Contesto

Digitalizzazione: le organizzazioni hanno dovuto affrontare un processo di sviluppo tecnologico e digitale adattando le proprie procedure ed i propri modelli organizzativi



Outsourcing: la crescita dell'affidamento di servizi ICT a terzi fornitori ha portato alla definizione di meccanismi per la gestione del rischio in materia di esternalizzazione di servizi IT, specie in settori fortemente regolamentati (es. ambito Finance)

Resilienza: l'attuazione di piani di efficientamento dei propri asset IT è culminata in una filosofia di prevenzione e mitigazione dei rischi connessi all'uso di tecnologie

Introduzione: premesse generali

Il **processo di esternalizzazione ha reso più vulnerabile** l'infrastruttura organizzativa delle aziende che esternalizzano il trattamento delle loro informazioni.

Il crescente grado di **digitalizzazione e interconnessione ha amplificato i rischi** relativi alle tecnologie dell'informazione e della comunicazione rendendo così le catene di fornitura e l'intero ecosistema più vulnerabile alle minacce informatiche.

Per tali ragioni è necessario essere in grado di:

- **Conseguire un elevato livello di sicurezza operativa informativa**
- **Contrastare l'esfiltrazione dei dati e attacchi cyber**
- **Gestire i rischi, garantire la continuità e la cyber security**

L’evoluzione regolamentare dell’ICT Risk

2018

Direttiva PSD2

General Data Protection Regulation (GDPR)

Recepimento Direttiva NIS

2019

EBA Guidelines on outsourcing arrangements

Cybersecurity ACT

28esimo Aggiornamento Circolare 285

Istruzioni Banca d’Italia per gravi incidenti sicurezza

Perimetro di Sicurezza Nazionale Cibernetica

EBA Guidelines ICT & Security Risk Management

2020/2021

Segnalazione gravi incidenti ai sensi PSD2

Aggiornamento istruzioni Operative Banca d’Italia per gravi incidenti di sicurezza

EIOPA Guidelines on information and communication technology s ecurity and governance

IVASS REG. 38/2018

2022/2023

40esimo aggiornamento Circolare 285

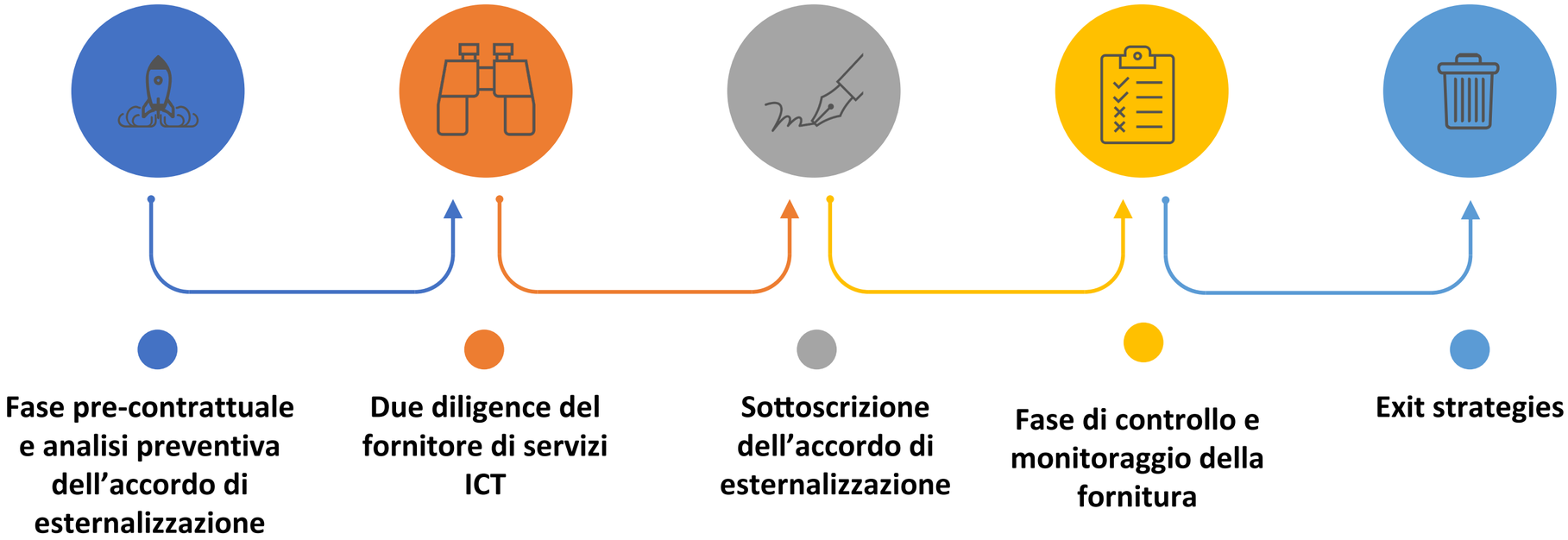
Aggiornamento novembre 2022 Disposizioni vigilanza IP e IMEL del 2016

Direttiva NIS 2.0

Il Regolamento DORA (è entrato in vigore il 16 gennaio 2023 e sarà vincolante dal 17 gennaio 2025)

La gestione del rischio in caso di servizi informatici esternalizzati o forniti da terze parti

CATENA DI FORNITURA DI SERVIZI ICT



I rischi da valutare in sede precontrattuale

1. Rischi intrinseci alla fornitura
2. Rischi informatici
3. Rischi connessi alla Business Continuity
4. Rischi relativi a integrità, autenticità e riservatezza delle informazioni
5. Rischi associati alla subesternalizzazione
6. Rischi derivanti dall'esternalizzazione di sevizi in paesi terzi
7. Rischi di concentrazione e lock in
8. Rischi reputazionali
9. Rischi ESG

Redazione del contratto e negoziazione

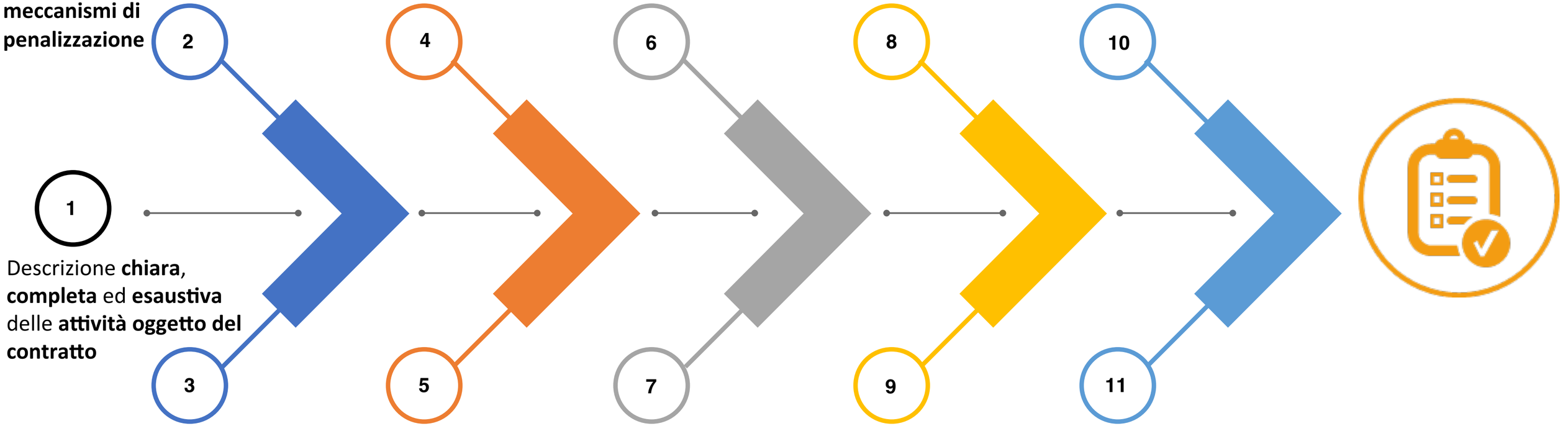
Fissazione di ***timeline*** (in caso di progetti) o di **SLA** (in caso di servizi) accompagnati da **meccanismi di penalizzazione**

Dettagliata disciplina del **subappalto**

Diritti di *audit*

Clausole di **responsabilità e manleva**

Previsioni relative alla ***exit strategy***



Descrizione **chiara**, **completa** ed **esaustiva** delle **attività oggetto del contratto**

Misure di sicurezza

Meccanismi di **reportistica e di comunicazione**

Disciplina delle **variazioni contrattuali**

Clausole di ***way out***

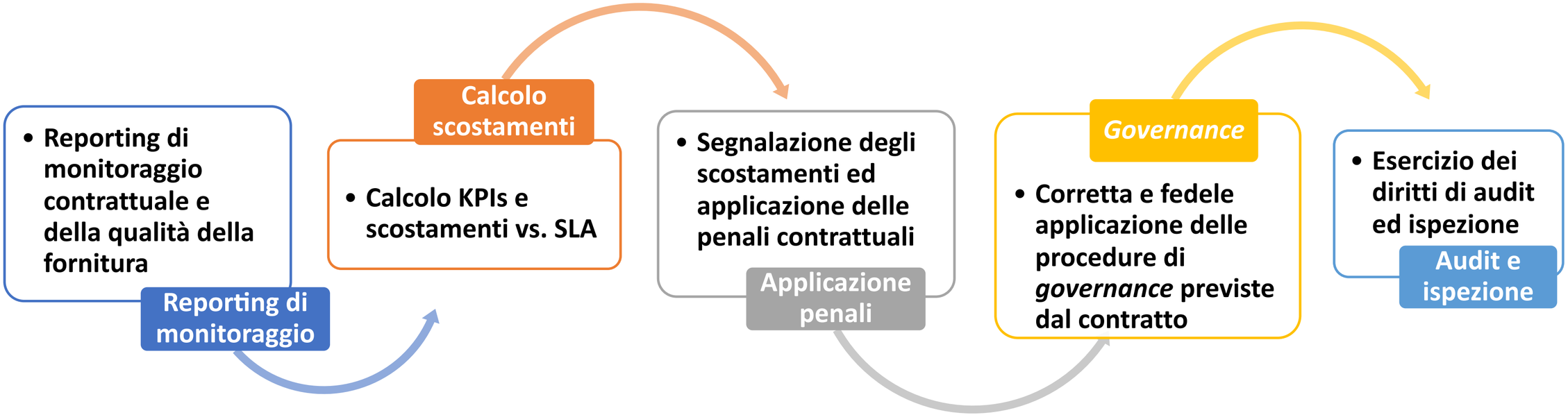
Clausole e documentazione *data protection* adeguata e coerente con quanto contenuto nel contratto (compresa la **disciplina dei luoghi del trattamento** e del **trasferimento del dato extra-UE**)

Contrattualizzazione & Monitoraggio

Tenendo conto di tutte le tematiche discusse precedentemente è importante che il **contratto** e la **nomina** siano **completi ed esaustivi**

Anche se vengono definiti correttamente tutti gli aspetti, è indispensabile **verificare che il contrattualizzato sia rispettato** e che ne **esista evidenza formale**

Fase di controllo e monitoraggio



EXIT PLAN

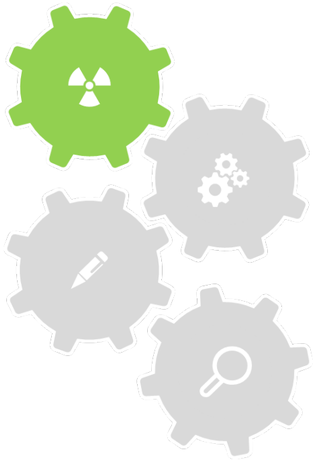
Risk Assessment

Exit Plan - Strategy

Exit Plan – Phase Out Contrattuale

Exit Plan - Execution

EXIT PLAN – STRATEGY



Il **Risk Assessment** è volto a valutare preventivamente il rischio di Fornitura e comprendere quanto ciò che si sta andando ad acquistare sarebbe facilmente sostituibile e quanto sarebbe lungo il periodo di transizione.

A titolo esemplificativo, alcune domande che vale la pena porsi sono:

- Il Fornitore in questione è economicamente stabile?
- Ha mai avuto problemi giuridici di qualche tipo?
- Che tipo di dati vengono trattati in connessione con la gestione (anagrafici, sensibili o relativi a condanne e reati)?
- Il servizio che si sta acquistando è continuativo o ha un orizzonte temporale definito?
- Ci si sta affidando a un big player di mercato o ad un fornitore specialistico, con una soluzione proprietaria che in futuro può manutenere solo lui?
- Un eventuale passaggio di consegne obbliga l'organizzazione a sostituire solo il Fornitore o anche il servizio stesso?

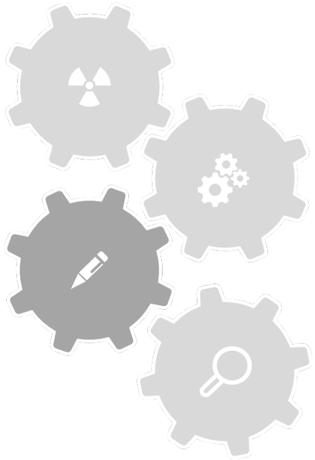
EXIT PLAN – STRATEGY

L’**exit strategy** è uno degli output del Risk Assessment ed è definita ex ante rispetto alla selezione del Fornitore. Disciplina le modalità con cui il cliente si aspetta di sostituire il fornitore, qualora nell’arco dell’erogazione della Fornitura, il monitoraggio dovesse evidenziare condizioni tali per una risoluzione anticipata del contratto.

È composta da due elementi:

- Tempi: stabilisce i tempi per le varie attività
- Contenuti: stabilisce cosa il fornitore è tenuto a fare, in termini di attività e deliverables, ad alto livello.

EXIT PLAN – PHASE OUT CONTRATTUALE



L’eventuale messa in operatività dell’exit strategy deve essere disciplinata, tanto all’interno degli allegati tecnici al capitolato quanto nei contratti, all’interno di un paragrafo chiamato **«Phase out»** .

Nella sezione di «Phase out» vengono dettagliate le aspettative nei confronti del Fornitore uscente, in caso il Committente decida di terminare anticipatamente il contratto, quindi gli obblighi che il potenziale Fornitore si impegna a rispettare, in termini di attività da svolgere, tempistiche e garanzie, rispondendo alla gara con un’offerta.

EXIT PLAN – EXECUTION

Qualora il Committente decida di terminare il rapporto di Fornitura e l'exit plan venga quindi effettivamente messo in atto, il cliente dovrà avere a disposizione degli strumenti definiti di monitoraggio, per essere certo che tutte le attività e garanzie inserite all'interno dell'allegato tecnico e del contratto vengano rispettate dal Fornitore uscente.

EXIT PLAN

Le aziende che adottano questo meccanismo di valutazione del rischio e di definizione di un piano di uscita sono totalmente tutelate?

EXIT PLAN

Le aziende che adottano questo meccanismo di valutazione del rischio e di definizione di un piano di uscita sono totalmente tutelate?

NO

EXIT PLAN

Risk Assessment

Exit Plan – Phase Out

Exit Plan – Phase In

Exit Plan - Strategy

Exit Plan - Testare

EXIT PLAN – PHASE IN

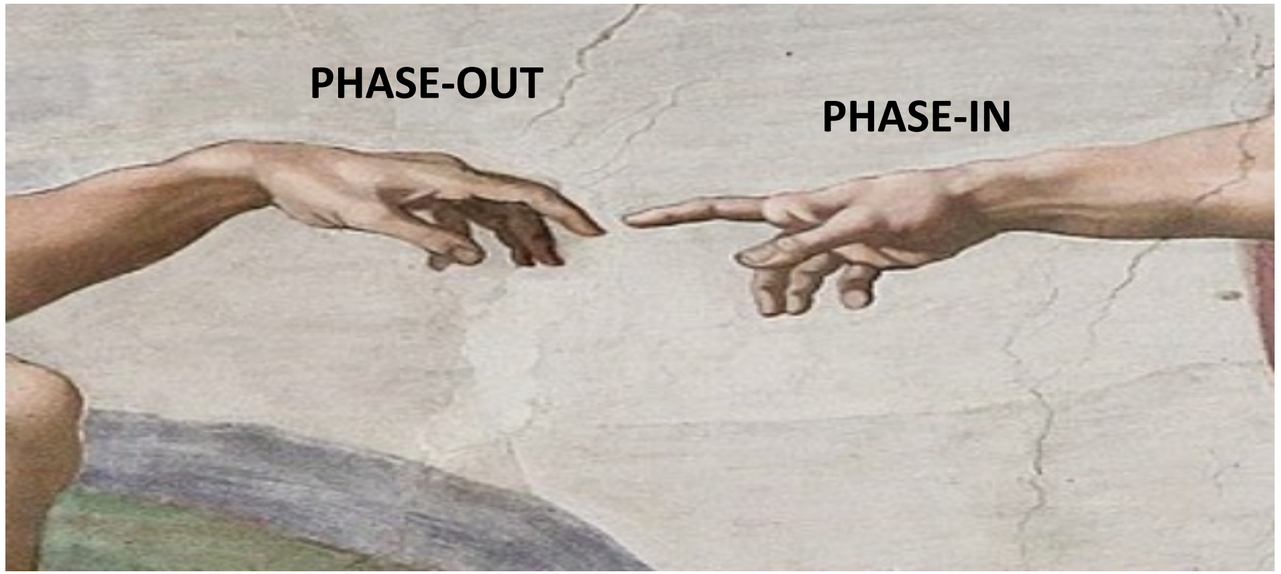
Per una tutela completa dai rischi, l'azienda deve prevedere un piano di «**Phase In»** speculare a quello di Phase Out, che disciplini il «passaggio di testimone» dal Fornitore uscente a quello subentrante.

Il Phase In, regolamenta le garanzie che il Fornitore subentrante deve offrire al Committente. In un processo in cui si attiva un percorso di exit strategy deve esserci sempre un meccanismo di attuazione di un processo di Phase In.

Un utilizzo coniugato di Phase-In e Phase-Out permette di esplicitare all'interno degli accordi a chi è in carico la garanzia della continuità dei servizi in gestione ed evitare profili di indeterminatezza delle responsabilità, in cui Fornitore uscente e subentrante finiscono per «palleggiarsi» le attività.

EXIT PLAN – PHASE IN

- Non esiste un meccanismo di exit strategy che funzioni bene se il fornitore subentrante non ha regolamentato un processo di phase in.

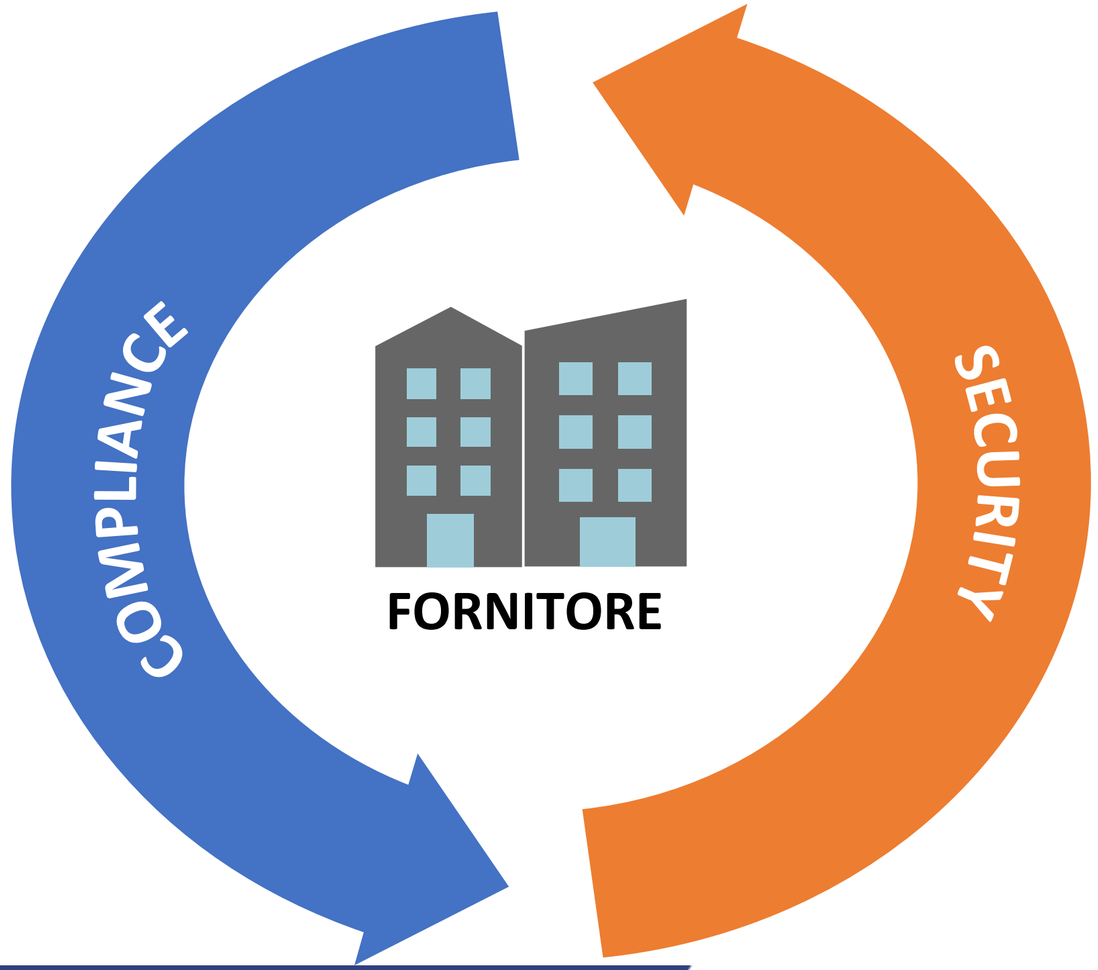


- Serve collaborazione tra entrambe le parti che devono garantire all'organizzazione risultati complementari. Sia il fornitore uscente che quello entrante devono avere chiari gli obiettivi verso il cliente e tra di essi.

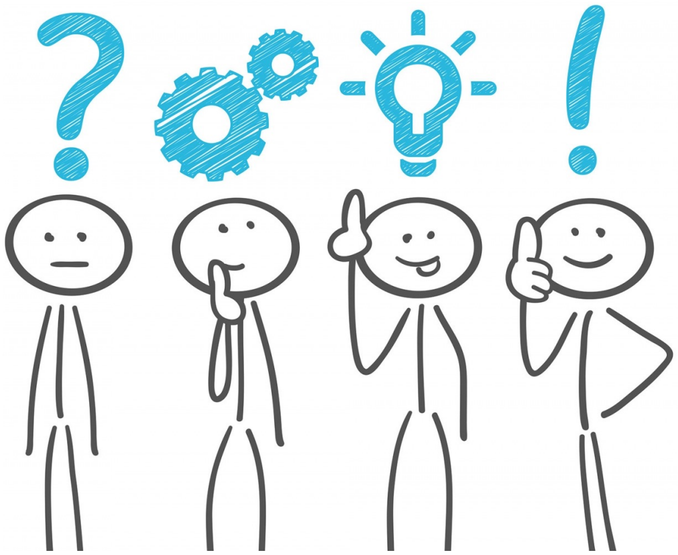
MODELLO INTEGRATO DI SECURITY & COMPLIANCE

Implementare efficace modello di governo e del controllo

- I processi di compliance e sicurezza devono essere integrati e devono muoversi di pari passo
- La sicurezza deve essere verificata/bile, ed il mezzo è la conformità (alle leggi, agli standard, …), non solo formale, ma anche sostanziale
- La trasparenza è realizzata tramite il rilevamento di indicatori e informazioni, condivise mediante strumenti, che l'azienda deve integrare ai dati di esercizio dei servizi nei propri sistemi di performance management, compliance management e security monitoring



Q&A



annamaria.italiano@p4i.it