Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

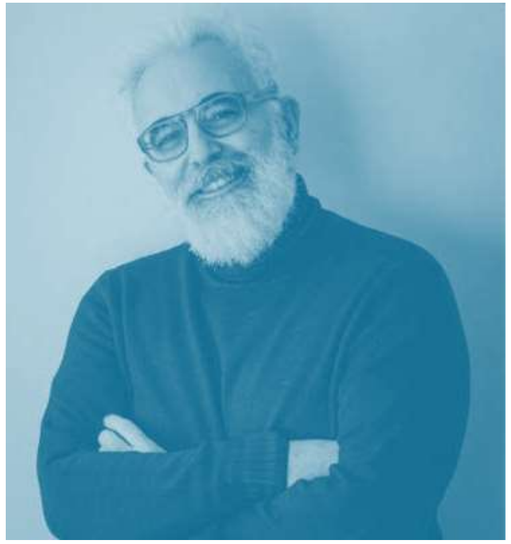
# Sicurezza delle informazioni e protezione dei dati personali verso i fornitori e la supply chain

*Roberto DE SORTIS, Fabio GUASCONI*

*Partners @* ***Bl4ckswan*** *S.r.l.*

19 marzo 2024 15.00-15.40

# RELATORI



**Roberto DE SORTIS**
Partner @ Bl4ckswan

**Fabio GUASCONI**
Partner @ Bl4ckswan

# AGENDA

- Premessa
- Gestione dei fornitori – best practices
- Questionario CLUSIT
- Soluzioni pratiche – Supplier³
- Conclusioni

# AGENDA

**Premessa**

**Gestione dei fornitori – best practices**

**Questionario CLUSIT**

**Soluzioni pratiche – Supplier³**

**Conclusioni**

# PREMESSA

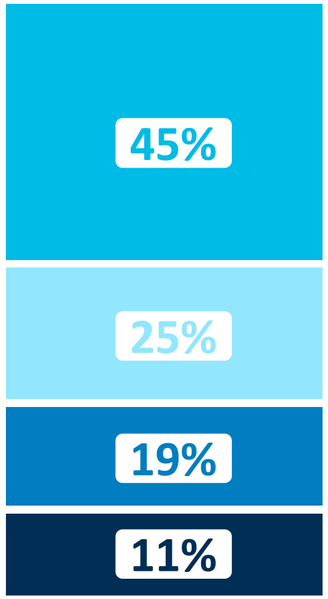
Negli ultimi anni, soprattutto a partire dall'introduzione del **GDPR** (v. in particolare articolo 28), si sono moltiplicati i casi in cui vengono richieste informazioni specifiche sulle misure di sicurezza informatica e di protezione dei dati personali dirette ai fornitori.

Queste informazioni vengono spesso richieste attraverso la compilazione di questionari, addendum contrattuali o survey online, più raramente sono al momento oggetto di audit/intervista.

Posto che la motivazione è incontestabile, la gestione di questo fenomeno, soprattutto per chi ha molti Clienti, può diventare estremamente onerosa, **per fornire le stesse informazioni molteplici volte ma in forma diversa**.

# PREMESSA

Effort per la valutazione del livello di **sicurezza** e della **compliance** alla normativa sui **dati personali** del fornitore




Meno di 2 g/u

Tra 2 e 6 g/u

Tra 8 e 16 g/u

Oltre 16 g/u

**Giornate uomo** complessive impiegate dalle aziende per le valutazioni

**31.000 – 34.000**

destinate alle attività di valutazione della compliance e della sicurezza di fornitori e subfornitori ogni anno

**154** **FTE**
di 3318 aziende

***Fonte**: Osservatorio Cybersecurity & Data Protection*

# AGENDA

**Premessa**

**Gestione dei fornitori – best practices**

**Questionario CLUSIT**

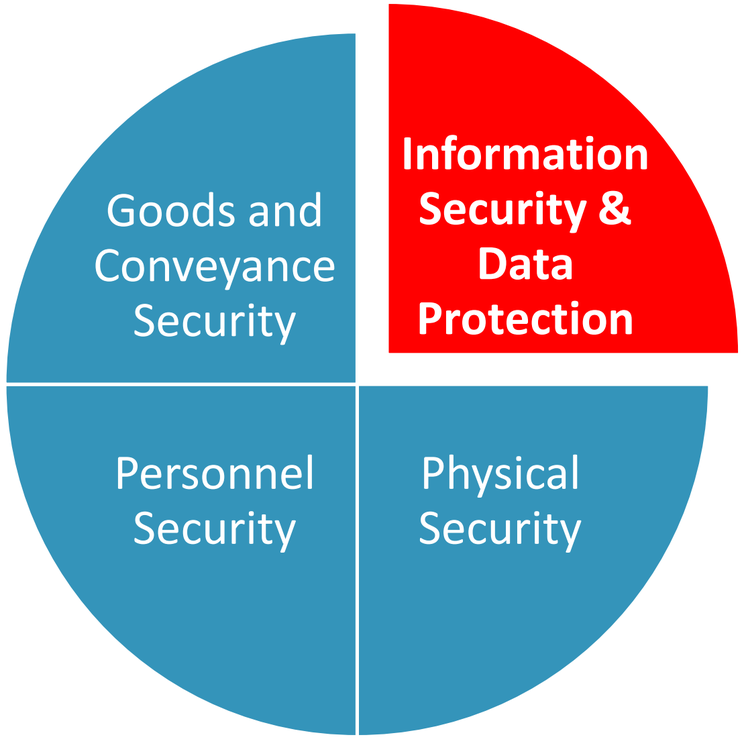
**Soluzioni pratiche – Supplier³**

**Conclusioni**

# GESTIONE DEI FORNITORI - BEST PRACTICES

La norma internazionale di riferimento per la sicurezza della catena della fornitura è la ISO 28000 "Security management systems - Requirements".

La sicurezza delle informazioni e la protezione dei dati personali sono solo due degli ambiti i cui rischi sono indirizzati dalla norma ma sono indubbiamente tra i più rilevanti.

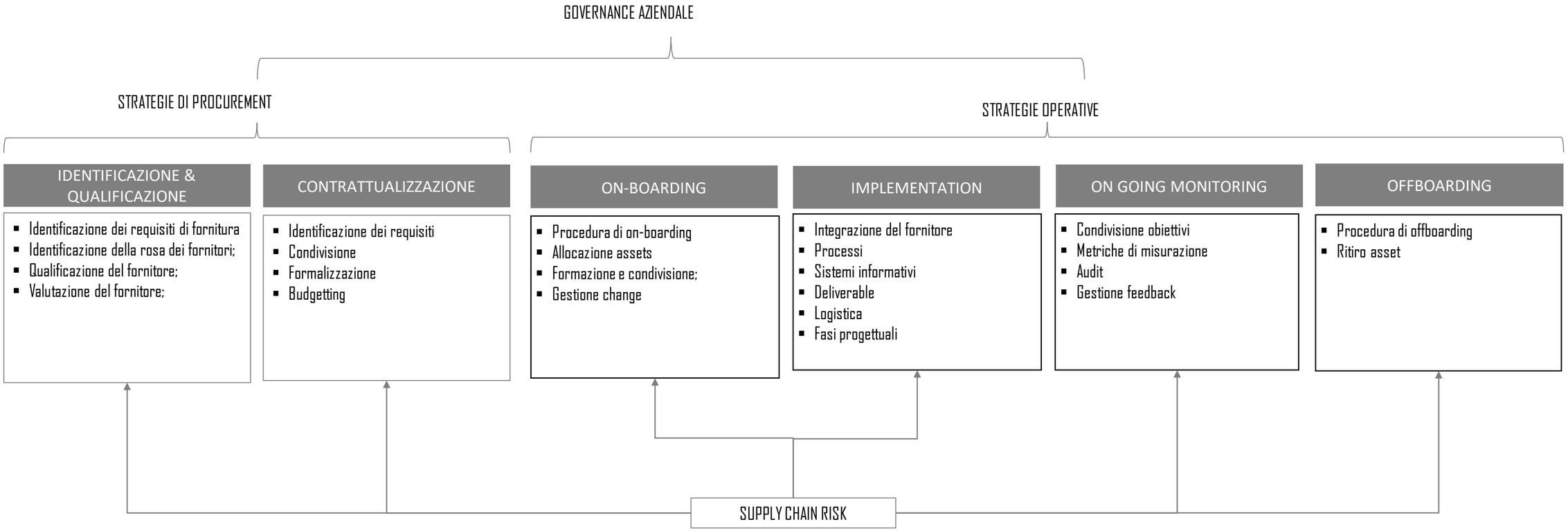


# GESTIONE DEI FORNITORI - BEST PRACTICES

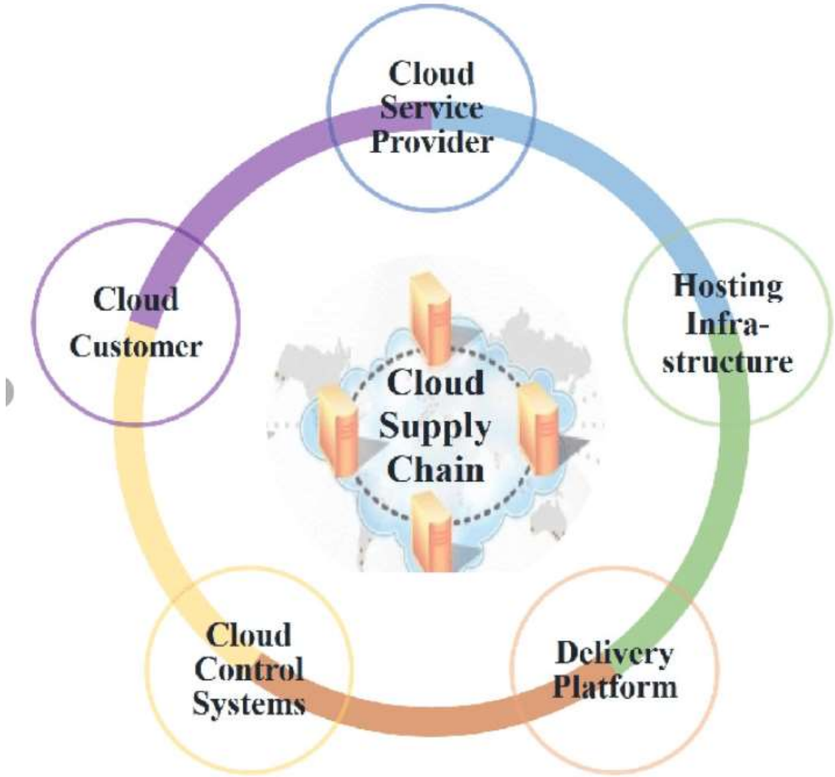
Sempre in ambito ISO, la ISO/IEC 27001 pubblicata nel 2022 ha diversi controlli che sono direttamente collegati con la gestione dei fornitori, tra cui:

- **5.19 Information security in supplier relationships**
- **5.20 Addressing information security within supplier agreements**
- **5.21 Managing information security in the ICT supply chain**
- **5.22 Monitoring, review and change management of supplier services**

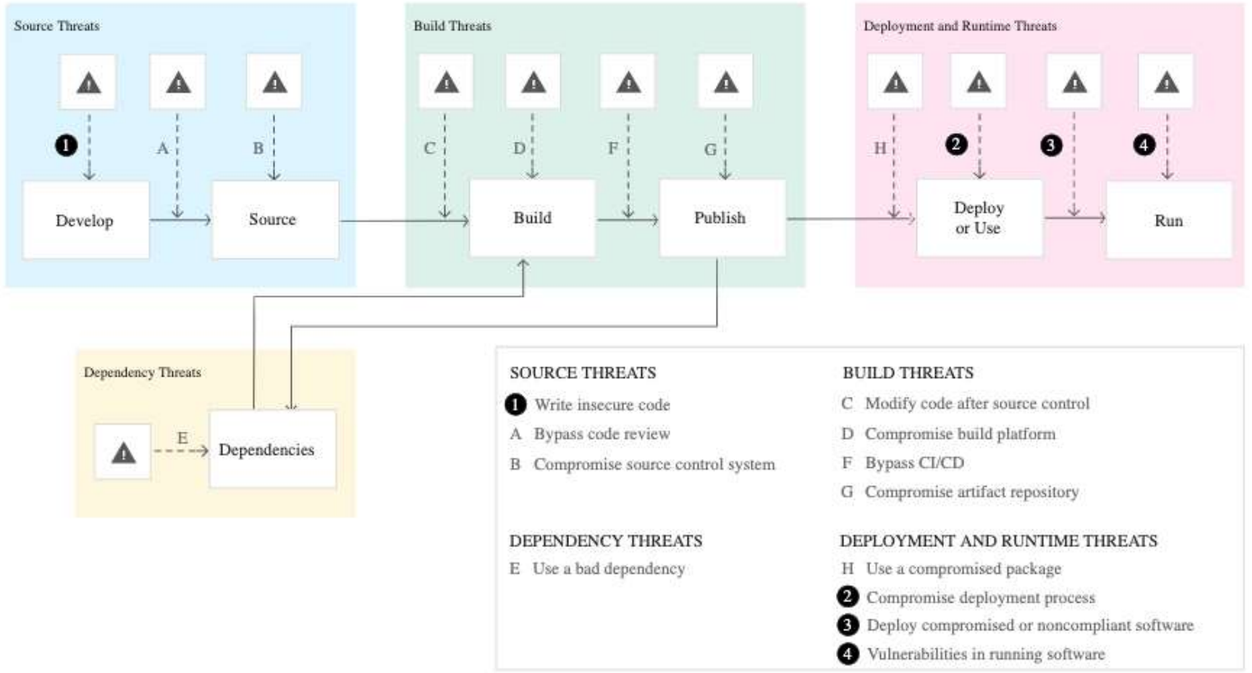
# GESTIONE DEI FORNITORI APPROCCIO INTEGRATO



# GESTIONE DEI FORNITORI – VALUTAZIONE AMBITI DI FORNITURA SPECIFICI




The Cloud Supply Chain



# INTEGRAZIONI DELLE BEST PRACTICES
# CASO PNRR – PROGETTO POLO CONSERVAZIONE DIGITALE - MIC

QUADRO STRATEGICO NAZIONALE SICUREZZA CIBERNETICA

STANDARD ISO

27001

27036

29800

LINEE GUIDA AGID

LG SICUREZZA PROCUREMENT ICT

LINEE GUIDA PER L'ADOZIONE DI UN CICLO DI SVILUPPO DI SOFTWARE SICURO

ALTRE FONTI

NIST

SANS

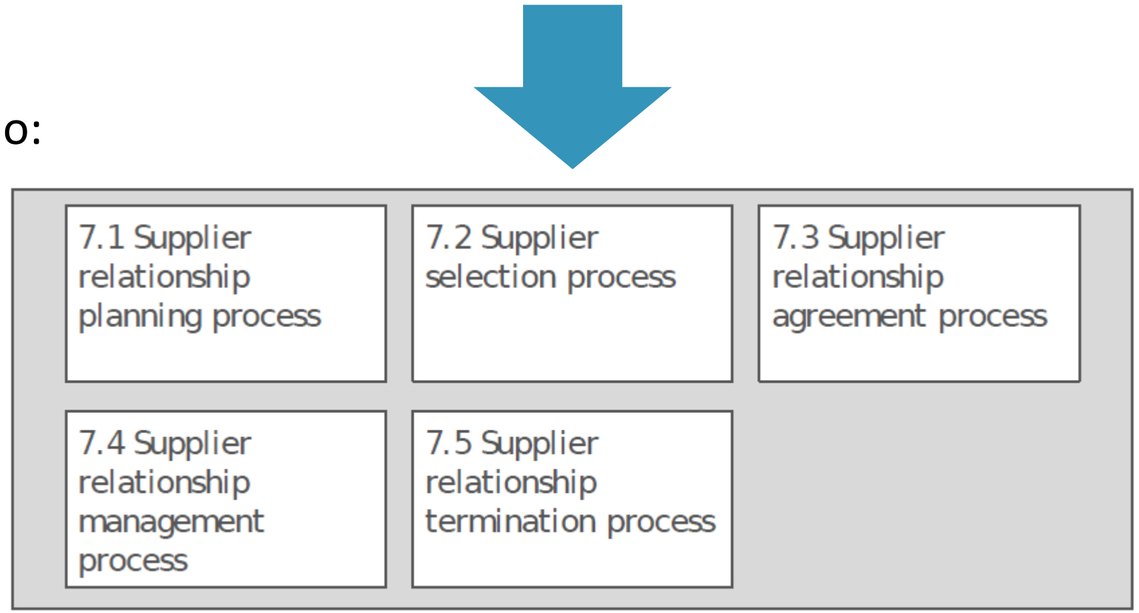
ENISA

# GESTIONE DEI FORNITORI - BEST PRACTICES

La ISO/IEC 27036-2 "Cybersecurity — Supplier relationships — Part 2: Requirements"  si spinge oltre e disegna una vera e propria struttura di governo delle relazioni con le terze parti con processi legati alla gestione dei fornitori (da parte dei clienti) e dei clienti da parte dei fornitori strutturati in attività, passaggi e input / output.

Gli elementi chiave specificati in questo contesto sono:

- **Strategia di alto livello**
- **Criteri e requisiti**
- **Valutazione dei rischio**
- **Documentazione contrattuale**



# AGENDA

Premessa

Gestione dei fornitori – best practices

**Questionario CLUSIT**

Soluzioni pratiche – Supplier³

Conclusioni

# QUESTIONARIO CLUSIT

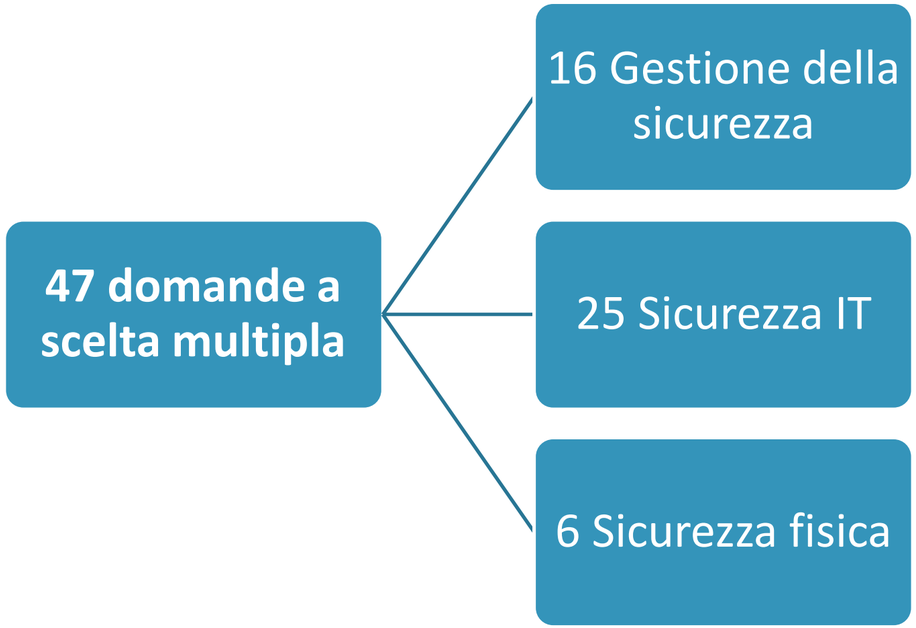
Il Questionario CLUSIT nasce come primo prodotto del gruppo di lavoro per facilitare la convergenza su un insieme di domande definito da esperti in grado di agevolare sia Fornitori che Clienti nella gestione della sicurezza informatica e nella protezione dei dati personali lungo la catena di fornitura.

E' stato progettato come documento da rendere liberamente disponibile al pubblico con le seguenti caratteristiche:

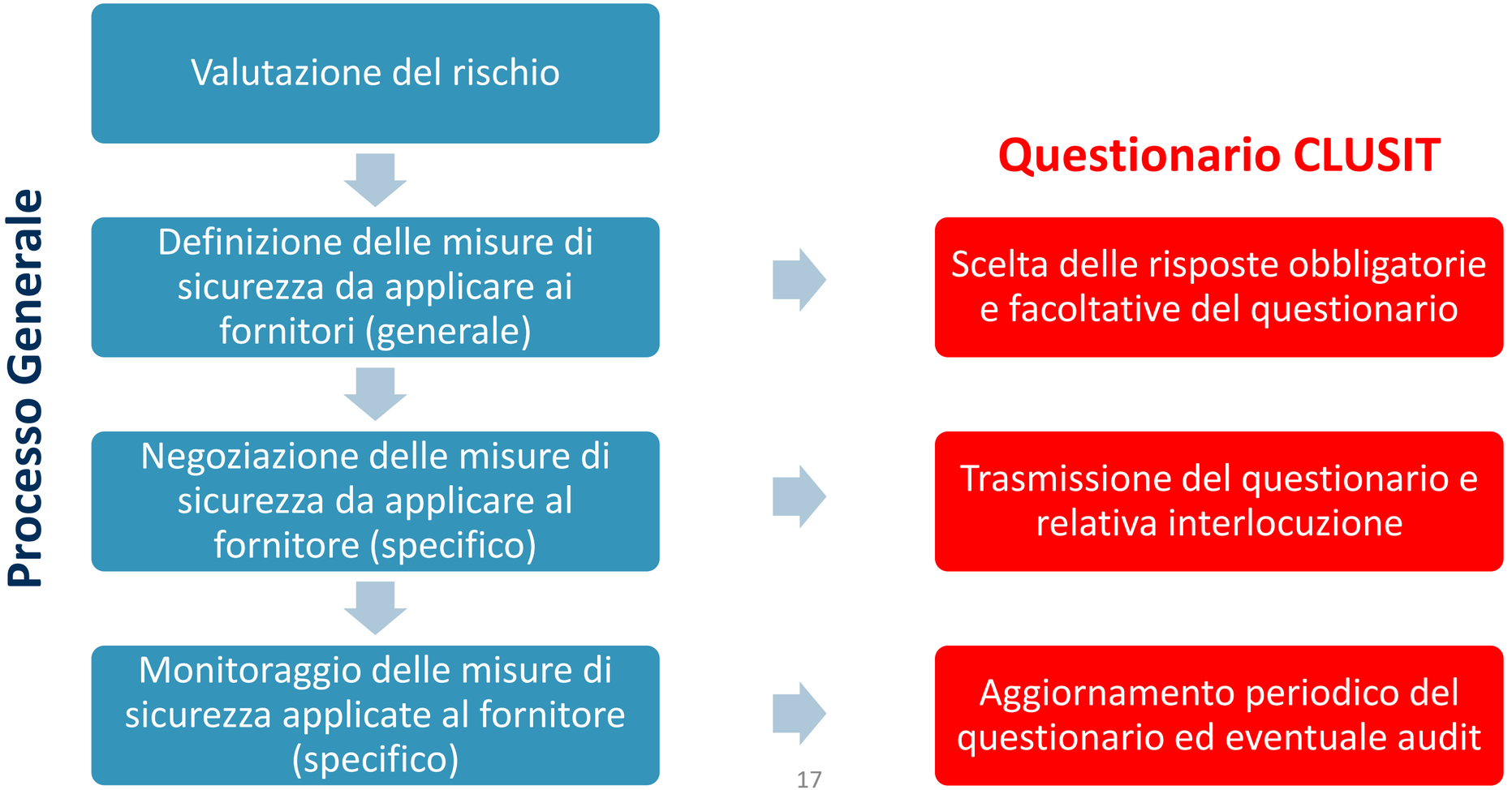
- ✓ **semplicità d'impiego**
- ✓ **rapidità di compilazione**
- ✓ **efficacia di raccolta delle informazioni**
- ✓ **esaustività nella copertura dei "controlli" di base**
- ✓ **flessibilità rispetto ai soggetti compilanti e ai servizi/prodotti forniti**

# QUESTIONARIO CLUSIT

Il questionario CLUSIT è liberamente scaricabile qui come foglio di calcolo ed è strutturato come segue:



# QUESTIONARIO CLUSIT



# AGENDA

- Premessa
- Gestione dei fornitori – best practices
- Questionario CLUSIT
- **Soluzioni pratiche – Supplier³**
- Conclusioni

# SOLUZIONI PRATICHE – SUPPLIER³

**SUPPLIER³** è una soluzione innovativa cloud-based per semplificare e velocizzare la valutazione del livello di sicurezza e di protezione dei dati personali dei Fornitori ICT, dalla fase di qualifica all'esecuzione di audit del fornitore, mettendo a disposizione - anche in modalità self-service - il know-how e i servizi dei professionisti di P4I e **Bl4ckswan**

La soluzione si rivolge ad organizzazioni di **medie e grandi imprese del settore Privato** che effettuano o sono coinvolti nella valutazione del livello di sicurezza e protezione dei dati personali dei Fornitori ICT:

Inoltre, alla soluzione possono accedere direttamente anche i **responsabili/referenti commerciali** e i **presidi specialistici dei Fornitori ICT.**

# SOLUZIONI PRATICHE – SUPPLIER³

La soluzione consente di effettuare delle valutazioni dei Fornitori ICT in relazione a **molteplici aspetti legati alla sicurezza e alla protezione dei dati personali**, riconducibili a:

- **Normative trasversali** (es. GDPR)
- **Normative di natura settoriale** (es. Circolare 285, d.lgs. 231/2007, Regolamento DORA, Direttiva NIS2)
- **Norme tecniche e di certificazione** (es. ISO/IEC 27001:2022)

La soluzione, inoltre, consente alle aziende di configurare **ulteriori ambiti ad hoc** in relazione ai quali valutare i propri fornitori (es. 231, Anticorruzione, ESG).

# SOLUZIONI PRATICHE – SUPPLIER[3]

## Funzionalità Principali

| | | | |
|---|---|---|---|
| 1.1. Database Fornitori ICT, Prodotti e Servizi | 1.2. Framework, questionari ed elaborati | 1.3. Valutazione e comparazione dei Fornitori ICT | 1.4. Generazione semi-automatizzata di documenti |
| 1.5. Gestione dell'interazione con i Fornitori ICT | 6. Selezione di uno o più Fornitori ICT | 7. Conservazione di informazioni e documenti | 8. Programmazione e tracciamento degli audit (wip) |

# SOLUZIONI PRATICHE – SUPPLIER[3]

| | | | |
|---|---|---|---|
| **1.1. Database Fornitori ICT, Prodotti e Servizi** | **1.2. Framework, questionari ed elaborati** | **1.3. Valutazione e comparazione dei Fornitori ICT** | **1.4. Generazione semi-automatizzata di documenti** |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | **6. Selezione di uno o più Fornitori ICT** | **7. Conservazione di informazioni e documenti** | **8. Programmazione e tracciamento degli audit (wip)** |

La soluzione consente di censire e classificare i Fornitori ICT a cui l'azienda si rivolge/vorrebbe rivolgersi e i relativi prodotti e servizi di cui intende approvvigionarsi

# SOLUZIONI PRATICHE – SUPPLIER$^3$

| | | | |
|---|---|---|---|
| **1. Database Fornitori ICT, Prodotti e Servizi** | **2. Framework, questionari ed elaborati** | **1.3. Valutazione e comparazione dei Fornitori ICT** | **1.4. Generazione semi-automatizzata di documenti** |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | **6. Selezione di uno o più Fornitori ICT** | **7. Conservazione di informazioni e documenti** | **8. Programmazione e tracciamento degli audit (wip)** |

La soluzione consente di accedere a framework, questionari ed elaborati messi a disposizione da noi o, in alternativa, di configurare framework, questionari ed elaborati specifici.

# SOLUZIONI PRATICHE – SUPPLIER[3]

| | | | |
|---|---|---|---|
| **1. Database Fornitori ICT, Prodotti e Servizi** | **2. Framework, questionari ed elaborati** | **1.3. Valutazione e comparazione dei Fornitori ICT** | **1.4. Generazione semi-automatizzata di documenti** |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | **6. Selezione di uno o più Fornitori ICT** | **7. Conservazione di informazioni e documenti** | **8. Programmazione e tracciamento degli audit (wip)** |

La soluzione consente di somministrare uno o più questionari a uno o più Fornitori ICT per valutare e comparare il livello di Sicurezza e Protezione dei dati personali garantito.

# SOLUZIONI PRATICHE – SUPPLIER[3]

| | | | |
|---|---|---|---|
| **1. Database Fornitori ICT, Prodotti e Servizi** | **2. Framework, questionari ed elaborati** | **3. Valutazione e comparazione dei Fornitori ICT** | **1.4. Generazione semi-automatizzata di documenti** |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | **6. Selezione di uno o più Fornitori ICT** | **7. Conservazione di informazioni e documenti** | **8. Programmazione e tracciamento degli audit (wip)** |

La soluzione consente di generare molteplici tipologie di documenti per regolamentare il rapporto con i Fornitori ICT (es. Allegato tecnico di sicurezza) recuperando direttamente tutte le informazioni utili dai questionari compilati dal fornitore.

# SOLUZIONI PRATICHE – SUPPLIER[3]

| | | | |
|---|---|---|---|
| 1. Database Fornitori ICT, Prodotti e Servizi | 2. Framework, questionari ed elaborati | 3. Valutazione e comparazione dei Fornitori ICT | 1.4. Generazione semi-automatizzata di documenti |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | 6. Selezione di uno o più Fornitori ICT | 7. Conservazione di informazioni e documenti | 8. Programmazione e tracciamento degli audit (wip) |

La soluzione consente di gestire l'interazione con i Fornitori ICT in fase di compilazione del questionario e/o di revisione di un documento, tenendo traccia di tutti i commenti e le osservazioni direttamente all'interno della soluzione.

# SOLUZIONI PRATICHE – SUPPLIER[3]

| | | | |
|---|---|---|---|
| **1. Database Fornitori ICT, Prodotti e Servizi** | **2. Framework, questionari ed elaborati** | **3. Valutazione e comparazione dei Fornitori ICT** | **4. Generazione semi-automatizzata di documenti** |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | **6. Selezione di uno o più Fornitori ICT** | **7. Conservazione di informazioni e documenti** | **8. Programmazione e tracciamento degli audit (wip)** |

La soluzione consente di invitare i Fornitori ICT ad una gara per l'approvvigionamento di specifici prodotti/servizi e selezionare il/i Fornitore/i ICT che offre/offrono un livello di sicurezza e protezione dei dati personali adeguato.

# SOLUZIONI PRATICHE – SUPPLIER[3]

| | | | |
|---|---|---|---|
| **1. Database Fornitori ICT, Prodotti e Servizi** | **2. Framework, questionari ed elaborati** | **3. Valutazione e comparazione dei Fornitori ICT** | **4. Generazione semi-automatizzata di documenti** |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | **6. Selezione di uno o più Fornitori ICT** | **7. Conservazione di informazioni e documenti** | **8. Programmazione e tracciamento degli audit (wip)** |

La soluzione consente di conservare di tutte le informazioni e i documenti necessari (es. contratto, DPA) per regolamentare il rapporto con il Fornitore ICT selezionato, impostando la data di validità e i relativi alert per la revisione.

# SOLUZIONI PRATICHE – SUPPLIER[3]

| | | | |
|---|---|---|---|
| **1. Database Fornitori ICT, Prodotti e Servizi** | **2. Framework, questionari ed elaborati** | **3. Valutazione e comparazione dei Fornitori ICT** | **4. Generazione semi-automatizzata di documenti** |
| **1.5. Gestione dell'interazione con i Fornitori ICT** | **6. Selezione di uno o più Fornitori ICT** | **7. Conservazione di informazioni e documenti** | **8. Programmazione e tracciamento degli audit (wip)** |

La soluzione consentirà di interfacciarsi con la gestione degli audit di seconda parte effettuati verso i fornitori e gestiti anche con strumenti esterni.

# SOLUZIONI PRATICHE – SUPPLIER$^3$

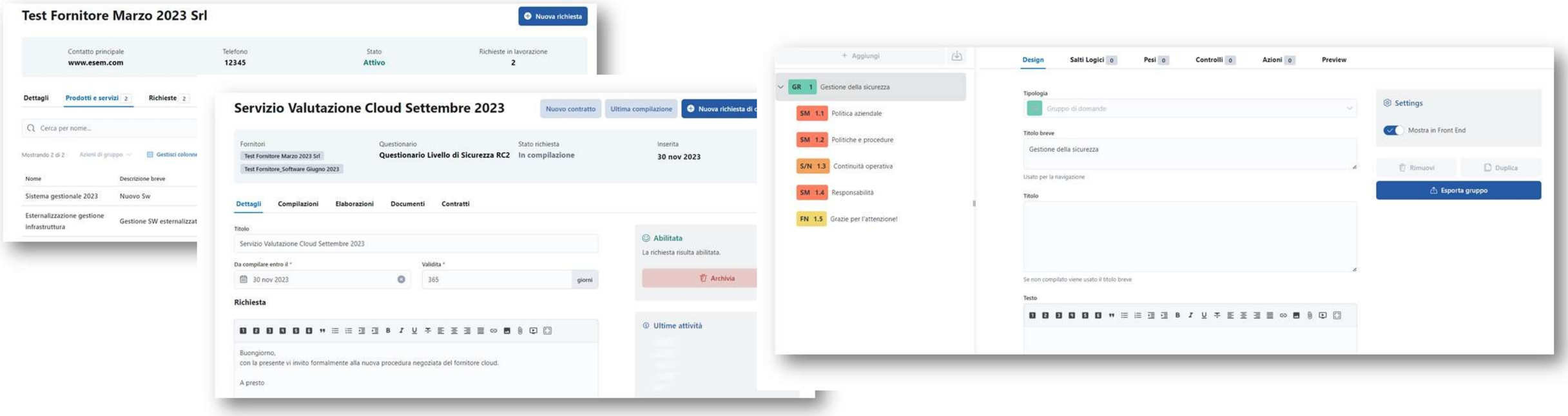
## Altre Funzionalità

1. Censimento e classificazione delle informazioni in merito al fornitore e ai prodotti e servizi che offre
2. Gestione delle richieste delle aziende per entrare a far parte del loro network di fornitori
3. Ricezione, analisi e compilazione dei questionari di valutazione erogati dalle aziende
4. Ricezione, analisi e compilazione dei documenti condivisi dalle aziende per formalizzare il rapporto
5. Gestione dell'interazione con le aziende in fase di compilazione del questionario e/o di revisione di un documento
6. Conservazione di tutte le informazioni e i documenti necessari per regolamentare il rapporto con le aziende
7. Accesso alla programmazione degli audit organizzati dalle aziende in relazione a specifici prodotti/servizi
8. Presa visione e gestione della risoluzione di azioni di remediation derivanti dagli audit delle aziende

# SOLUZIONI PRATICHE – SUPPLIER³

La soluzione è nella fase finale di beta testing ed è aperta a demo senza impegno, basta richiederle a:

**supplier3@bl4ckswan.com**




Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Bl4ckSwan

# AGENDA

**Premessa**

**Gestione dei fornitori – best practices**

**Questionario CLUSIT**

**Soluzioni pratiche – Supplier³**

**Conclusioni**

# CONCLUSIONI

La gestione della sicurezza delle terze parti è sempre più un elemento indispensabile

Soprattutto quando i fornitori iniziano ad essere numerosi è necessaria una gestione dedicata

L'automazione con soluzione specifiche può fare la differenza

# VI ASPETTIAMO AL NOSTRO STAND!