Il rischio fornitori e soggetti terzi tra Regolamento DORA, ISO/IEC 27001:2022 e GDPR

compet-e

Pisa, 25 maggio 2023 - AULA WORKSHOP 28 – ore 11.30

RELATORE: Piermaria Saglietto – CEO Compet-e

Piermaria Saglietto

- CEO di **Compet-e Srl**, il “centro di competenza” di **TESISQUARE®** su tematiche di compliance e RegTech.
- Laureato in matematica presso l’Università degli studi di Torino
- Esperienza pluriennale in ambito privacy e Information Security maturata in media e grandi realtà fin dall’anno 2000 (consulenza e formazione)
- Consulente della Privacy e Privacy Officer certificato TUV secondo lo Schema CDP al n° Registro “CDP_077”
- Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni - ISO/IEC 27001:2022
- Lead Auditor per i Sistemi di Gestione per la Continuità Operativa ISO 22301:2012.
- Progettista di corsi per la certificazione dei profili privacy secondo la norma Profili Privacy UNI 11697:2017

Compet-e

«L'anno scorso, quando è arrivato il 2000, erano tutti convinti che fosse l'alba di una nuova era.
Ma quando non è finito il mondo e non sono atterrati i marziani, e il Millennium Bug non ha fatto spegnere neanche una lampadina, avrebbero dovuto capire che era solo un numero sul calendario.»
(Star Trek: Voyager)

Per Compet-e, però, il **2000** non è solo un numero sul calendario, ma la data della propria nascita.

Questa è Compet-e

- Un'azienda che non solo è presente quando c'è da risolvere un problema, ma è sempre al vostro fianco come partner
- Vive e respira il connubio tra tecnologia e adempimenti normativi
- Guarda senza riserve al futuro
- La sua più grande forza è ogni singolo collaboratore

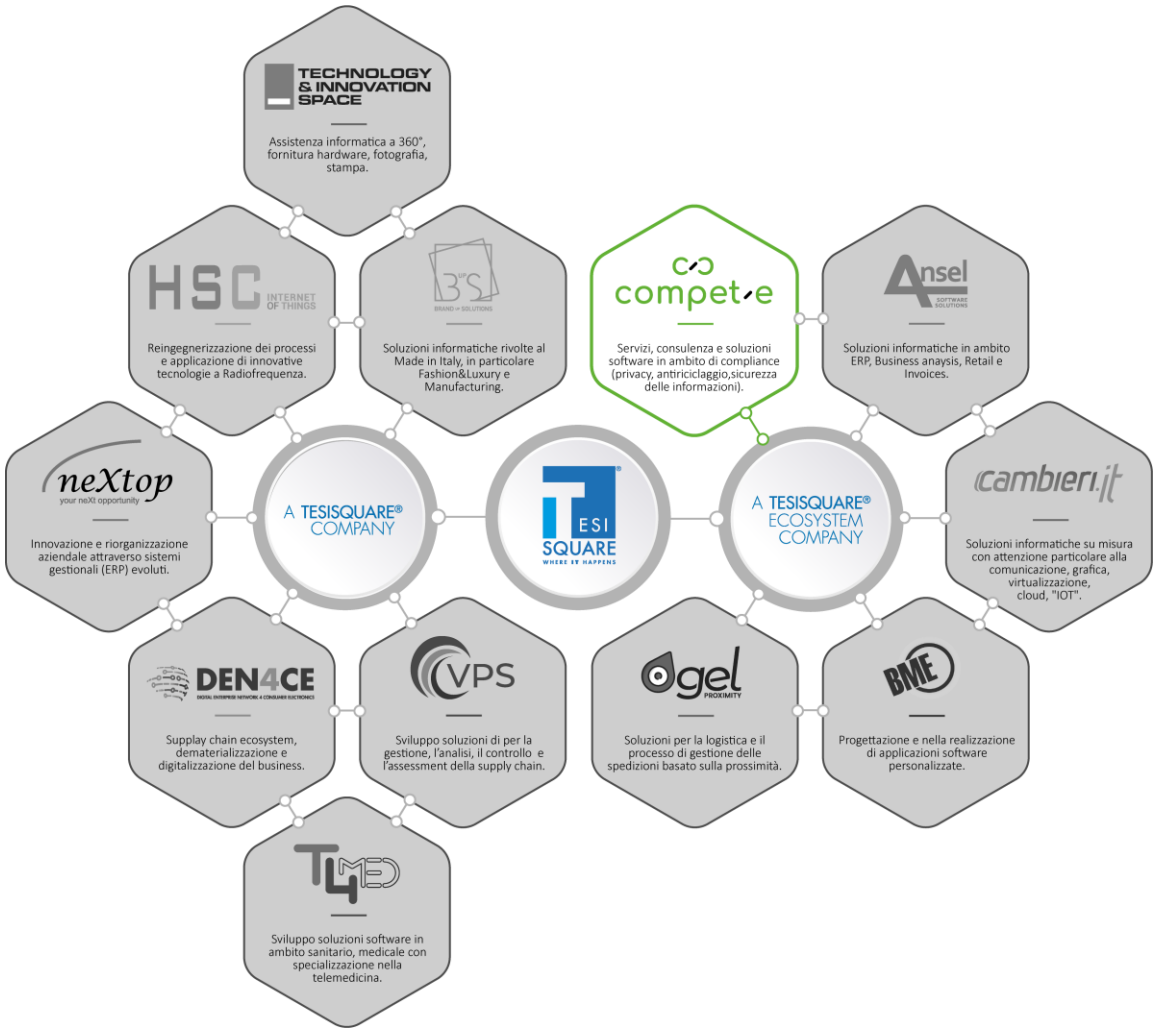
Fondata in Italia, fra le colline e i monti Piemontesi, nel marzo del 2000, da allora abbiamo dedicato il nostro tempo a costruire il futuro. Non solo il nostro, ma anche dei nostri clienti, quando c'è bisogno di servizi tecnologici e di compliance, Compet-e è sempre lì in soccorso, al fianco dei nostri clienti, anzi partner.

Come fa Compet-e a distinguersi dagli altri?
Il nome Compet-e sottintende "Centro di Competenza" e sin dalla nascita, l'obiettivo è stato quello **di creare soluzioni e offrire consulenza** specializzandosi sui temi della privacy e la sicurezza delle informazioni e a seguire su tutto l'ambito **RegTech**.
Con competenze tecnologiche e di dominio, condite da un sano entusiasmo che ci contraddistingue, siamo determinati ad aiutare le aziende ad affrontare le esigenze del settore **compliance** ora comunemente chiamato **RegTech**.
L'evoluzione naturale del settore ci ha portato oggi a formare un team costituito da risorse specializzate sui temi della Privacy, Risk Management, Sicurezza delle Informazioni, Antiriciclaggio, Anticorruzione, Sicurezza sul lavoro, 231, ecc.. in grado di supportare le aziende in ambito legale ed operativo.

L'ecosistema

Nel **2022** nasce ufficialmente l'ecosistema **TESISQUARE** che ha portato ad una importante **riorganizzazione**, con l'obiettivo di definire, per ogni legal entity del gruppo, il **perimetro di azione** in base al core business e alle **competenze specifiche** in un determinato ambito.

Compet-e srl è stato quindi identificato come **Centro di Competenza** per le tematiche di **Reg tech (compliance)**.



Agenda

- Cos’è il rischio delle terze parti
- Il rischio delle terze parti: il punto di vista di alcune normative
- Il rischio delle terze parti: evoluzione culturale
- Il rischio delle terze parti: organizzazione, processi
- Il rischio delle terze parti: processo di valutazione del rischio
- Il rischio delle terze parti: possibili strumenti
- Conclusioni

Cos'è il rischio delle terze parti

Definizione: Le terze parti

La **Terza Parte (3P)** è un **fornitore esterno di servizi e/o prodotti**. La 3P mette a disposizione dell'azienda e dell'organizzazione la propria expertise e le best practice del settore in cui opera, spesso integrandosi **efficacemente e completamente** all'interno dei processi produttivi e/o di erogazione di prodotti/servizi dell'organizzazione stessa.

Il rischio inerente le terze parti

Lavorare con una terza parte può introdurre dei rischi importati in una azienda o organizzazione. Esempi:

- Se le 3P hanno accesso a dati «**strategici**» esiste un **rischio per la sicurezza**;
- Se le 3P hanno accesso a **dati personali** ad esempio «**sensibili o particolari**» la cui titolarità è della organizzazione esiste un **rischio in ambito protezione dei dati**
- Se le 3P forniscono un **componente o un servizio essenziale** per l'azienda esiste un **rischio operativo**
- Etc..

La **gestione del rischio di terze parti** permette alle organizzazioni di monitorare e valutare il rischio derivante da terze parti per individuare in quali casi esso supera la soglia stabilita dall'azienda «**risk appetite**». Questo permette alle organizzazioni di **prendere decisioni** tenendo conto del rischio che corrono e di ridurre il rischio stesso posto dalle parti fornitrici a **un livello accettabile**.

Il rischio terze parti

Punto di attenzione di varie norme

GDPR

GDPR art.. 28 par. 1): il titolare "…ricorre unicamente a **responsabili** del trattamento che presentino **garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato….";

ISO 27001

Annex A ISO 27001:2022

- 5.19 **Information security in supplier relationships**
- 5.20 Addressing information security within **supplier agreements**
- 5.21 Managing information security in the information and communication technology (ICT) **supply chain**

NIS2

Articolo 21 comm2 lettera d NIS2 «Misure di gestione dei rischi di cybersicurezza»: «sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i **rapporti tra ciascun soggetto e i suoi fornitori**»

DORA

Uno dei *6 pillar* di DORA: Rischio Terze Parti (*art. 1 comma1 lettera a*) adozione di «misure relative alla solida gestione dei **rischi informatici derivanti da terzi**».

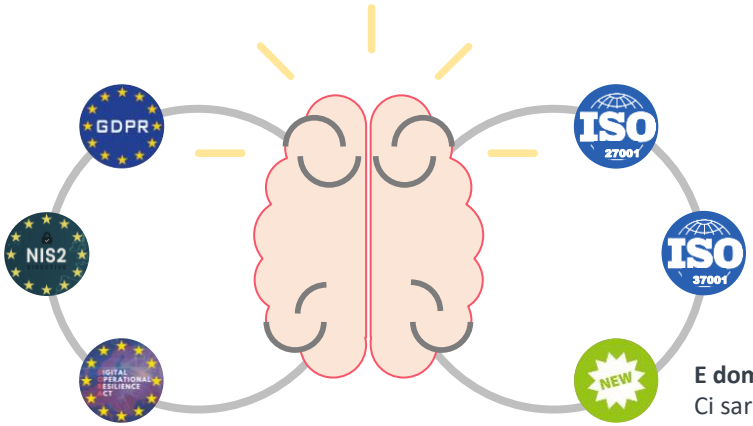
Il rischio terze parti

Evoluzione culturale

1. Evoluzione culturale

Dalla compliance di settore alla compliance integrata

Non solo non è più efficiente, ma nemmeno più efficace una gestione compartimentata per settore normativo del rischio delle terze parti: le norme stanno convergendo.



E domani?
Ci saranno nuove norme...

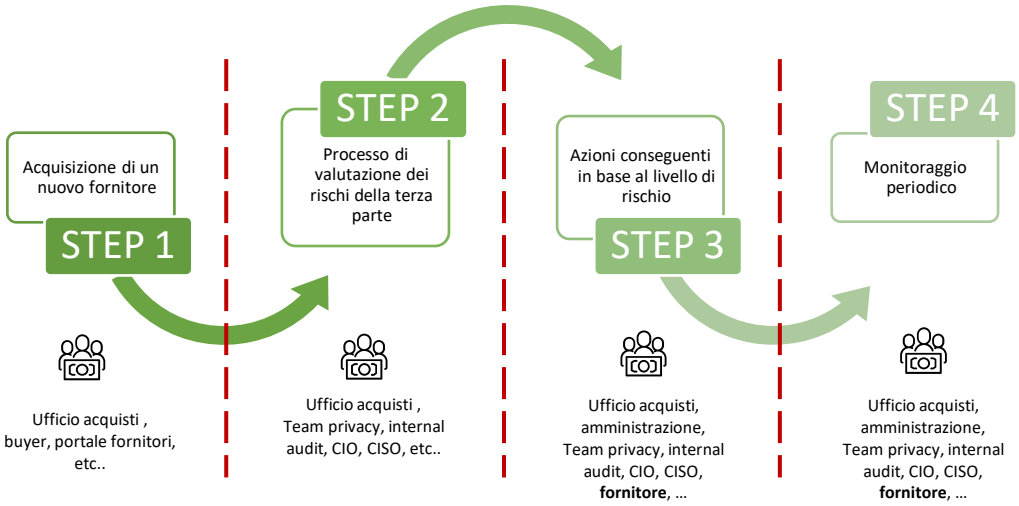
Il rischio terze parti

Organizzazione, processi

2. Revisione/ristrutturazione dell'organizzazione e dei processi

L'organizzazione deve cominciare a strutturarsi per seguire le tematiche di compliance in maniera integrata. I processi devono essere ridisegnati per poter gestire al meglio le nuove esigenze.

Esempio:



Il rischio terze parti

Processo di valutazione del rischio

3. Definizione e attuazione del processo di valutazione del rischio

L'organizzazione deve definire il processo e gli algoritmi per la valutazione del rischio e i criteri per l'accettazione/non accettazione del rischio stesso.

- **External survey**
  Questionari/interviste di valutazione/autovalutazione devono essere somministrati alle terze parti
- **Internal survey**
  Questionari/interviste di valutazione/autovalutazione devono essere somministrati ai soggetti interni che presidiano determinati temi (acquisiti, team privacy, Security, etc…)
- **Internal database**
  Devono essere «scandagliati» database e archivi interni per scoprire se esistono già evidenze sulla parte terza
- **External database**
  Devono essere interrogate eventuali fonti dati esterne che riportano informazioni sulla parte terza

Il rischio terze parti

Possibili strumenti

4. Scelta e acquisizione degli strumenti utili a supportare i processi di valutazione

- L'organizzazione deve scegliere ed eventualmente acquisire gli strumenti in grado di supportare gli algoritmi di valutazione, i processi collaborativi per lo scambio di informazioni e per il presidio di tali aspetti nel tempo.
- A seconda del livello di complessità dell'organizzazione, dei processi e del numero delle terze parti da gestire si possono intraprendere due strade.

Strumenti di office

Tool dedicato

Possibili strumenti

Costi di acquisizione

Strumenti di office

★☆☆☆☆

Spesso non necessitano di acquisizione, al limite qualche licenza aggiuntiva.

Tool dedicato

★★★☆☆

Spesso non sono già disponibili in azienda. Occorre fare una *software selection* ed operare un nuovo acquisto nella modalità «on premise» o in Saas.

Possibili strumenti

Costi di implementazione

Strumenti di office

L'implementazione degli algoritmi spesso è demandata alla creazione/parametrizzazione di fogli di calcolo Excel.

Tool dedicato

L'implementazione, a seconda del grado di parametrizzazione del tool, può necessitare sia di fasi di sviluppo sul prodotto che di azioni di configurazione dello strumento.

Possibili strumenti

Facilità di rimodulazione degli algoritmi e dei processi

Strumenti di office

★★☆☆☆

Gli strumenti di office non hanno funzionalità avanzate e guidate di revisione delle formule e degli algoritmi.

Tool dedicato

★★★★☆

Su questi aspetti normalmente il tool è più performante in quanto appositamente progettato per gestire e governare i cambiamenti (tramite opportune funzionalità di configurazione/riconfigurazione).

Possibili strumenti

Facilità nella gestione degli aspetti collaborativi

Strumenti di office

Gli strumenti di office non hanno solitamente funzionalità avanzate per la gestione degli aspetti collaborativi. Gli aspetti collaborativi possono essere gestiti ma in maniera destrutturata e senza un unico strumento.

Tool dedicato

Su questi aspetti normalmente il tool è più performante in quanto appositamente progettato per gestire e governare gli aspetti di collaborazione tramite il disegno di processi, di workflow, di step di approvazione, di reminder e alter di scadenze, tramite processi automatici di sollecito ai vari attori.

Possibili strumenti

Facilità nella gestione delle azioni legate al valore di rischio

Strumenti di office

Gli strumenti di office consentono di gestire check list, documenti contenenti piani di trattamento dei rischi etc… ma senza contemperare in mondo avanzato aspetti di processo.

Tool dedicato

Su questi aspetti normalmente il tool è più performante in quanto appositamente progettato per gestire e governare gli aspetti di presidio dei temi di remediation e, tramite integrazione, colloquio con ulteriori piattaforme aziendali (ex: anagrafica fornitori, albi interni di qualifica, etc…).

Possibili strumenti

Livello di supporto nel «day by day»

Strumenti di office

★★☆☆☆

Gli strumenti di office danno un discreto supporto alle attività «day by day» fornendo modelli e documenti di utilizzo più comune. Spesso lo strumento di office non è ottimale nel governare gli aspetti di processo.

Tool dedicato

★★★★☆

Su questi aspetti normalmente il tool è più performante in quanto appositamente progettato per gestire e governare questi aspetti (Scadenze, reminder, to do list, etc…)

Possibili strumenti

Capacità di conservazione e raffronto dei dati su base storica

Strumenti di office

Gli strumenti di office spesso non sono associati (o facilmente coniugabili) con una base dati che conservi i dati con profondità storica. La conservazione dei dati su base storica è affidata agli utenti che operano opportune copie storiche dei documenti.

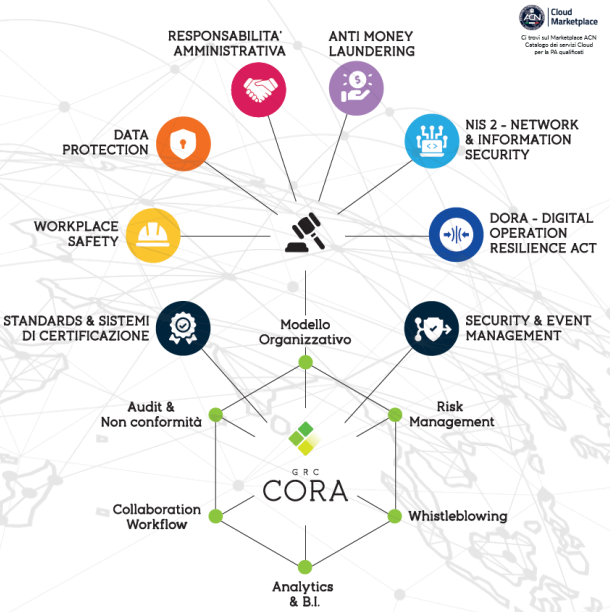
Tool dedicato

Su questi aspetti normalmente il tool è più performante in quanto appositamente progettato per gestire e governare questi aspetti (storicizzazione dei dati esplicite o implicite insite nelle funzionalità o nell'architettura del tool stesso).

Quadro di sintesi finale

	Strumenti di office	Tool dedicato
Costi di acquisizione	★☆☆☆☆	★★★☆☆
Costi di implementazione	★★☆☆☆	★★★☆☆
Facilità di rimodulazione degli algoritmi e dei processi	★★☆☆☆	★★★★☆
Facilità nella gestione degli aspetti collaborativi	★☆☆☆☆	★★★★★
Facilità nella gestione delle azioni legate al valore di rischio	★★★☆☆	★★★★☆
Livello di supporto nel «day by day»	★★☆☆☆	★★★★☆
Capacità di conservazione e raffronto dei dati su base storica	★★☆☆☆	★★★★★

Il rischio fornitori e soggetti terzi tra Regolamento DORA, ISO/IEC 27001:2022 e GDPR



Pisa, 25 maggio 2023 - AULA WORKSHOP 28 – ore 11.30

RELATORE: Piermaria Saglietto – CEO Compet-e