Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
STREAMING EDITION

ASTREA Advanced Security, Training Research, Events Agency

Rischio di sicurezza e compliance relativo alle terze parti

Alessandro Vallega e Cesare Gallotti, CLUSIT COMMUNITY FOR SECURITY

9 – 10 novembre 2022 orario 16.20 – 17.20

Clusit Community For Security

Clusit Community for Security

c4s.clusit.it

Libro sulla supply chain security (ETA marzo 2023)

Fase 7: i nostri 94 autori, organizzati in piccoli gruppi di 3-5 persone, hanno consegnato i 96 componenti previsti

D61 | IVASS - REGOLAMENTO N. 38/2018 - Capo VIII

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	ID	Sezione	Nome componente	Descrizione componente. ATTENZIONE se non vedi tutti i componenti potrebbe essere attivo un filtro. Lo puoi rimuovere o modificare nel menu Dati	Note indicative/facoltative per gli autori in fase di stesura	Autori assegnati	Pagine attese	Status consegna	Team Leader di Riferimento	Abeti Riccardo	Agostinello Davide	Arena Orlando	Ariu Davide	Arrigoni Andrea
58	5500	Compliance	Normative di riferimento - DORA	DORA		4	0,5	consegnato	Valeria Lazzaroli					
59	5600	Compliance	Normative di riferimento - 285	Banca d'Italia - Circ. 285 - SEZIONE VI – L'ESTERNALIZZAZIONE DEL SISTEMA INFORMATIVO		4	0,5	Consegnato	Fabrizio Bulgarelli					
60	5700	Compliance	Normative di riferimento - regolatori UE	Orientamenti ESMA (European Securities and Markets Authority), EBA (European Central Bank) e EIOPA (assicurazioni)	https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_it.pdf https://www.eba.europa.eu/documents/10180/2	3	0,5	consegnato	Valeria Lazzaroli					
61	5800	Compliance	Normative di riferimento - IVASS	IVASS - REGOLAMENTO N. 38/2018 - Capo VIII		5	0,5	consegnato	Valeria Lazzaroli					
62	5900	Compliance	Normative di riferimento - MDR	MDR (regolamento sui dispositivi medici).		3	0,5	consegnato	Silvia Stefanelli	1				
	6000	Compliance	Principi comuni e accettati	principi generali del nostro ordinamento sulla culpa in		3	1	consegnato	Silvia Stefanelli					

Le sezioni principali del prossimo libro

- Introduzione
- L’outsourcing e gli scenari
- I rischi della supply chain
- Incidenti e statistiche
- Settori specifici
- Normative di riferimento
- I contratti
- Le misure di sicurezza
- Interviste
- Case study
- Conclusioni

Contesto

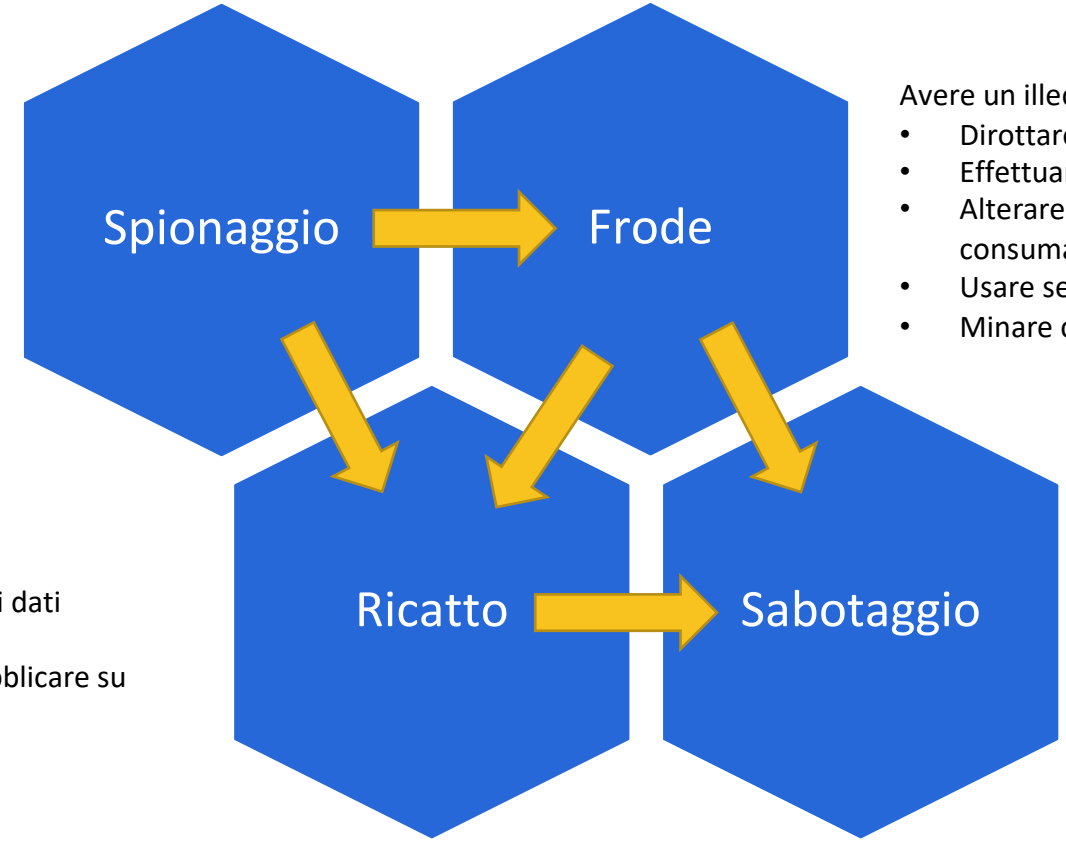

Rapporto
Clusit
2022
sulla sicurezza ICT
in Italia
SECURITY SUMMIT


Panoramica sull'evoluzione del cyber crime in Italia e nel mondo – Edizione marzo 2022
Di seguito una rappresentazione sintetica delle medie mensili negli ultimi 4 anni.
Media mensile 2018 - 2021
175
165
155
145
135
125
130
139
156
171
2018
2019
2020
2021
© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia


dreamstime

Motivazioni e percorsi degli attaccanti

Rubare e usare o rivendere
- informazioni commerciali, documenti contabili, piani e progetti di sviluppo …
- segreti industriali, software, configurazioni, mappe installazione …
- dati relativi a clienti come credenziali, carte di credito, dati sanitari ...



Avere un illecito vantaggio economico
- Dirottare i pagamenti esistenti
- Effettuare versamenti (CEO fraud)
- Alterare informazioni (es. riattivare crediti consumati)
- Usare servizi telefonici altrui
- Minare cryptovalute

Ottenere il pagamento di un riscatto
- Per riavere la disponibilità dei propri dati (ransomware)
- Per impedire altre ritorsioni (es. pubblicare su Internet le informazioni rubate)

Creare danno
- Impedire l'operatività
- Distruggere le infrastrutture
- Distogliere l'attenzione
- Aumentare le proteste
- Danneggiare l'avversario

Il pericolo arriva anche tramite la catena di fornitura

24%

delle organizzazioni dichiara di aver subito un **incidente di sicurezza legato alle terze parti** negli ultimi 12 mesi

Campione: 151 grandi imprese

Fonte: Ricerca "Supply Chain Security" degli Osservatori del Politecnico di Milano

- Le grandi imprese sono meglio protette e più si possono accorgere prima dell'incidente di sicurezza
- Le aziende medie e piccole sono realmente alla mercé dei criminali e spesso non si accorgono nemmeno di essere attaccate

Tutti sono un bersaglio

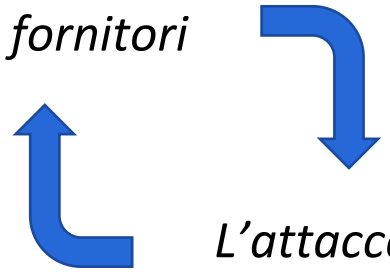
Grandi imprese

- Normalmente meglio protette ma più capienti
- L'attacco inizia con una ricognizione tecnica e sociale

Piccole imprese

- Tecnicamente impreparate
- L'attacco inizia a fronte di vulnerabilità scoperte automaticamente

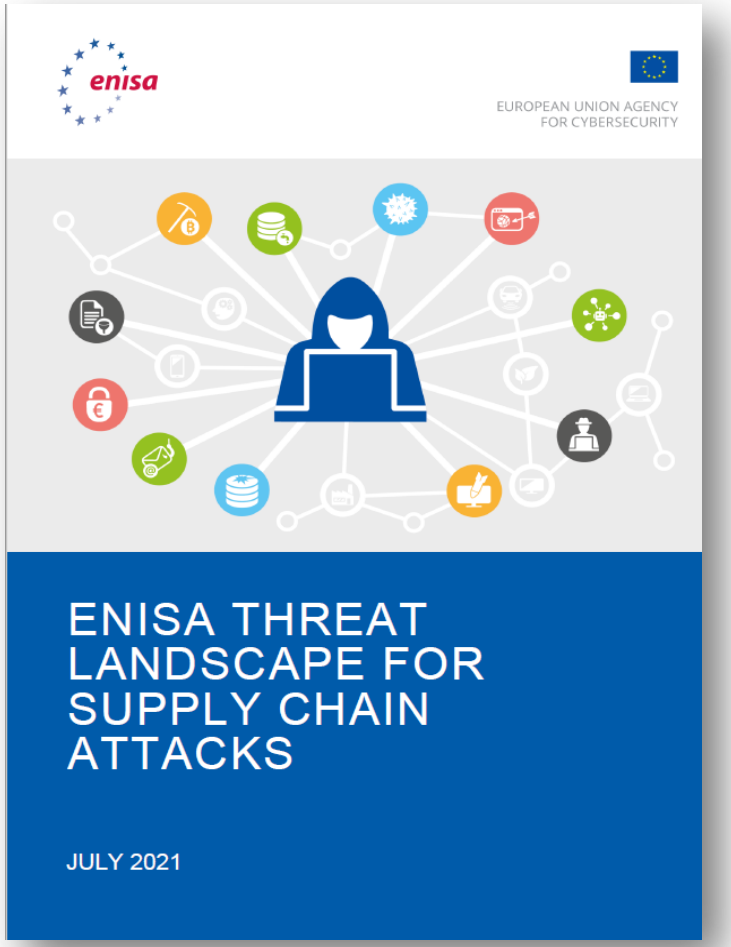
L'attaccante sceglie la grande impresa e studia i suoi fornitori (piccoli)



L'attaccante scopre una piccola impresa e risale alla grande impresa

Il tema è importante e all'attenzione delle autorità

- Le imprese non possono esimersi dal verificare l'affidabilità dei propri fornitori
- Inoltre, potrebbero essere loro stesse sottoposte alle verifiche dei loro clienti



Fonte: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Cosa può capitare

Rischio di sicurezza

- A causa di un fornitore, può avvenire un incidente di sicurezza alla disponibilità dei sistemi, alla loro riservatezza e alla loro integrità

Rischio di compliance

- A causa di un fornitore, si possono violare norme, leggi e regolamenti
- Ciò può anche capitare nella relazione con un fornitore (culpa in eligendo e culpa in vigilando)

- Perdita di profitto, danni diretti/indiretti, costi e spese
- Multe, sanzioni, obblighi e divieti
- Cause, class action, perdita di immagine, perdita di clienti

Crescenti obblighi normativi

I regolamenti europei e le leggi Italiane richiedono di farsi carico del livello di sicurezza e di conformità dei fornitori e dei subfornitori:

- Dimostrando la propria responsabilizzazione (**accountability**) nel processo di scelta e nel processo di monitoraggio
- A protezione dei **diritti di terzi** (le persone fisiche, il mercato, la società)
- Utilizzando criteri di priorità basati sull'**analisi del rischio**
- Con crescenti **obblighi di segnalazione** alle autorità e/o al pubblico

Crescenti obblighi normativi e il buon senso

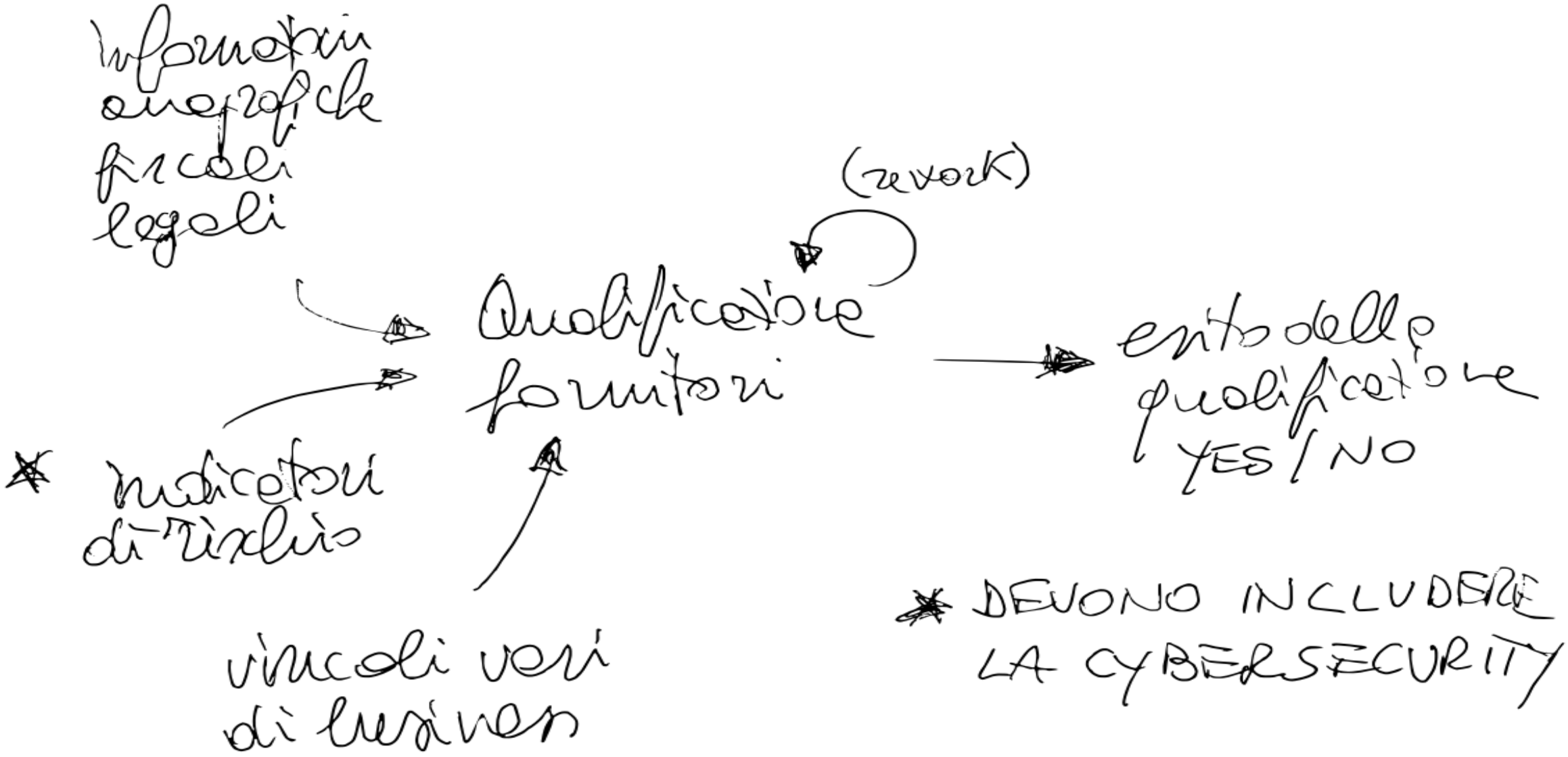
Le aziende devono:

- Essere responsabili
- Essere in grado di dimostrare la responsabilità.

La responsabilità passa attraverso la capacità di:

- Scegliere correttamente i propri fornitori
- Controllare regolarmente il loro operato

Come si affronta questa situazione?

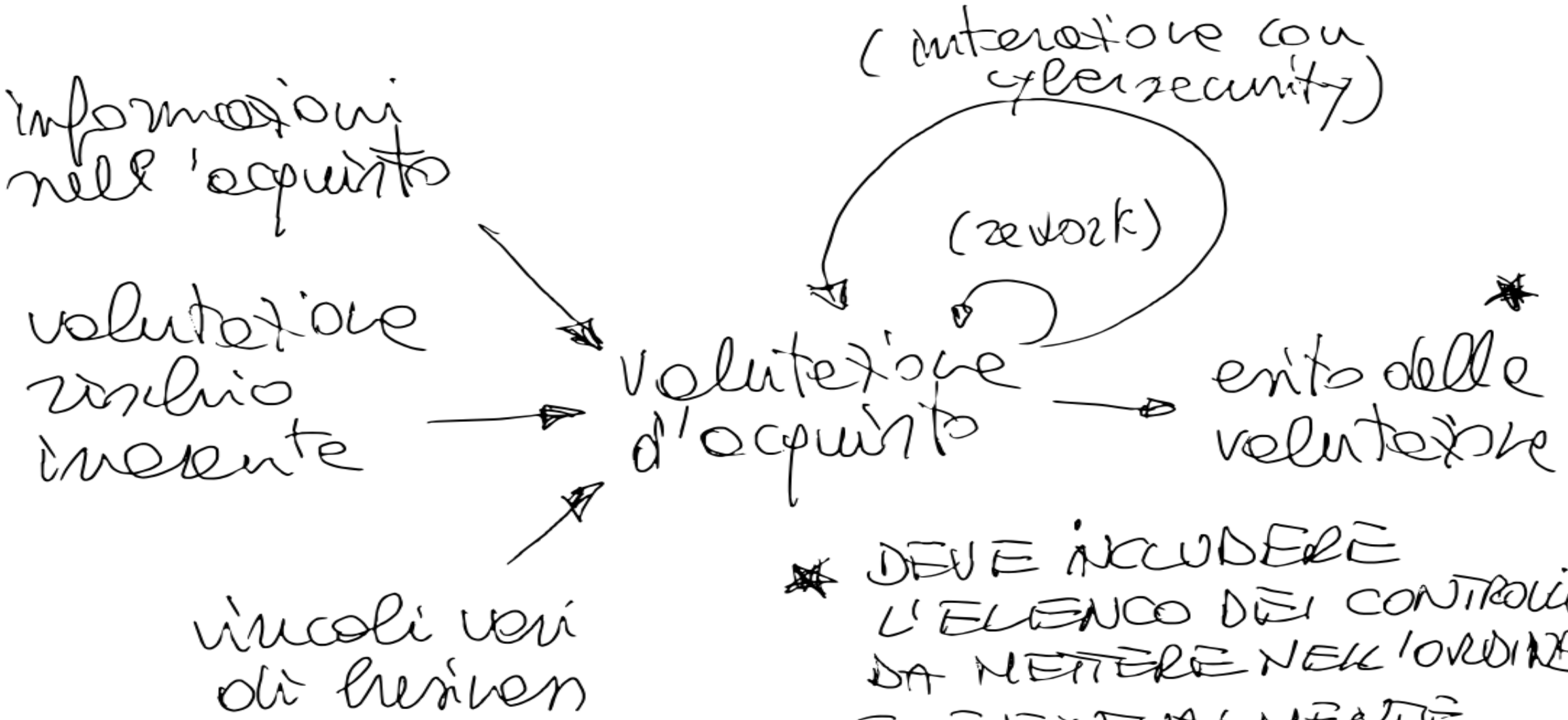

informazioni energetiche fisiche legali
(rework)
qualificazione fornitori
esito della qualificazione YES / NO
indicatori di rischio
vincoli veri di business
DEVONO INCLUDERE LA CYBERSECURITY

Elementi di complessità / opportunità

Bisogno di estendere gli attuali processi di qualificazione del fornitore

- Anticipare i controlli generali di cybersecurity e compliance
- Integrare le informazioni raccolte nel sistema informativo
- Cooptare ufficio acquisti e funzione data protection (GDPR)

Ragionare in logica di rischio aumentando l'importanza della cybersecurity ma accettando i vincoli del business


informazioni nell'acquisto
valutazione rischio inerente
vincoli vari di business
valutazione d'acquisto
(interazione con cybersecurity)
(rework)
esito della valutazione
* DEVE INCLUDERE L'ELENCO DEI CONTROLLI DA METTERE NELL'ORDINE E, EVENTUALMENTE, IL PIANO DI AUDIT
* T+1

Elementi di complessità / opportunità

Definire dei criteri per calcolare il rischio inerente di un prodotto/servizio

Predisporre dei cataloghi di misure adeguate al livello di rischio inerente

- Il catalogo deve essere pertinente alle caratteristiche del prodotto/servizi e riferirsi a standard internazionali

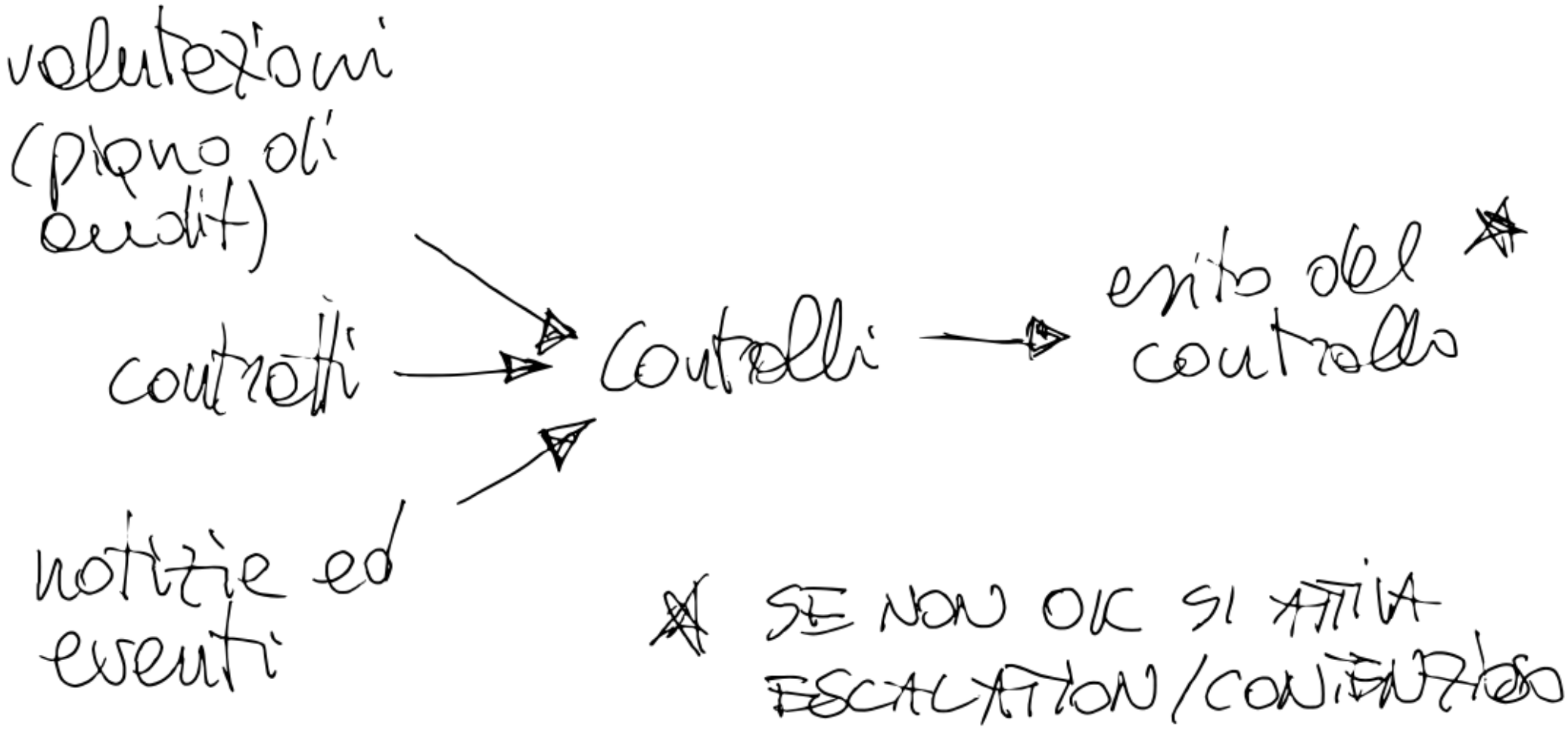
Collaborando con il fornitore, valutare l'adeguatezza delle stesse e la presenza di misure compensative

Le misure concordate diventano allegati al contratto

Definire dei criteri / procedure per

- Gestire i fornitori non collaborativi ma non sostituibili
- Ridurre / automatizzare i controlli per acquisti poco rischiosi
- Non dover frequentemente valutare acquisti molto simili dallo stesso fornitore

- Rischio come funzione di probabilità e impatto
- Rischio inerente + misure tecniche / organizzative = rischio residuo
- Rischio residuo <= rischio accettabile?

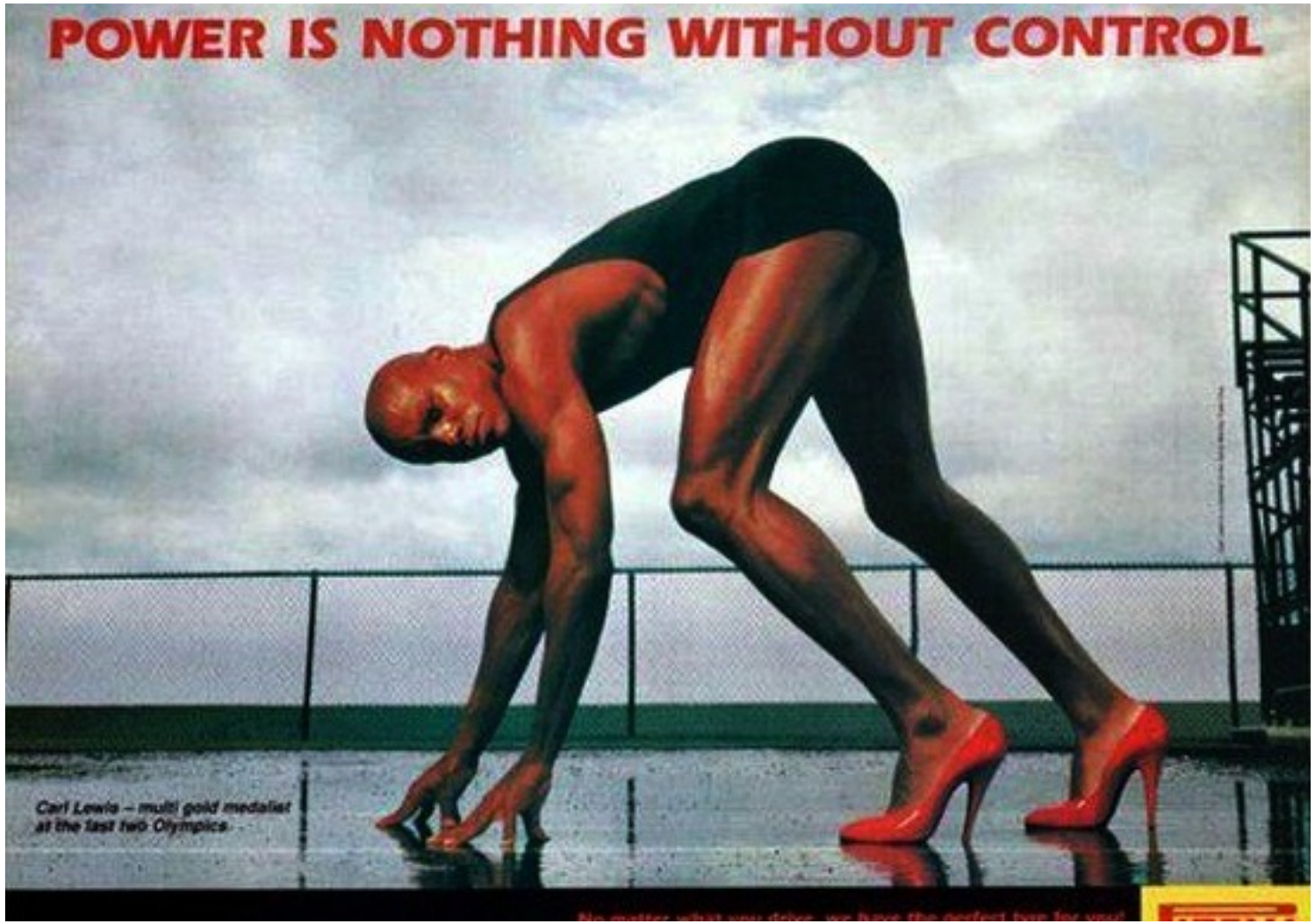

valutazioni (piano di audit)
controlli
notizie ed eventi
controlli
esito del controllo
SE NON OK SI ATTIVA ESCALATION/CONTENZIOSO

Elementi di complessità / opportunità

I fornitori non sono dei nemici. La responsabilità sociale d’impresa deve valorizzare la maturazione della relazione anche in logica cybersecurity

Tecnologie a supporto

Premesso che



Fonte: https://www.automoto.it/news/pirelli-25-anni-fa-lo-spot-la-potenza-e-nulla-senza-controllo.html

E quindi prima servono i processi poi si completa con la tecnologia….

Accenniamo ai prodotti…

Componente: 8200 - Che fare - Prodotti per l'analisi del rischio di fornitura

Versione: 1

Autori: Giuseppe Cusello, Franco Marconcini, Angelo Bosis, Luca Zammarchi

TLR: Alessandro Vallega

Prodotto	URL	Forrester	Gartner
Allgress	https://allgress.com/	Not rated	Aspiring
Aravo	https://aravo.com/	Strong Performers	Strong Performer
Archer	https://www.archerirm.com/	Strong Performers	Aspiring
BitSight	https://www.bitsight.com/	Not rated	Customer's Choice
Black Kite	https://blackkite.com/	Not rated	Customer's Choice
Coupa	https://www.coupa.com/	Contenders	Not rated
CyberGRX	https://www.cybergrx.com/	Not rated	Strong Performer
Cyber Quant (MasterCard)	https://www.mastercard.ca/en-ca/business/large-enterprise/safety-security/cyber-solutions/cyber-quant.html	Not rated	Not rated
Diligent (Galvanize)	https://www.diligent.com/	Strong Performers	Strong Performer
LogicManager	https://www.logicmanager.com/	Contenders	Not rated
LogicGate	https://www.logicmanager.com/	Strong Performers	Not rated
MetricStream	https://www.metricstream.com/	Strong Performers	Not rated
NAVEX	https://www.navex.com/	Strong Performers	Not rated
OneTrust	https://www.onetrust.com/	Leaders	Customer's Choice
Panorays	https://panorays.com/	Not rated	Strong Performer
Prevalent	https://www.prevalent.net/	Strong Performers	Customer's Choice
ProcessUnity	https://www.processunity.com/	Leaders	Customer's Choice
Red Piranha	https://redpiranha.net/	Not rated	Strong Performer
RiskRecon	https://www.riskrecon.com/	Not rated	Aspiring
SCORE (Rexilience)	https://score.rexilience.eu/	Not rated	Not rated
SecurityScorecard	https://securityscorecard.com/	Not rated	Customer's Choice
ServiceNow	https://www.servicenow.com/	Leaders	Established
Swascan	https://www.swascan.com/it	Not rated	Not rated
UpGuard	https://www.upguard.com/	Not present	Established

La tabella sintetizza quanto indicato nei report 2022 sul Third-Party Risk Management di Forrester Research (1) e di Gartner (2).

Il report di Forrester Research valuta i top vendor presenti sul mercato usando le quattro classificazioni decrescenti: **Leaders, Strong Performers, Contenders e Challengers**. L'analisi è svolta utilizzando 21 indicatori che valutano Offerta Corrente, Strategia e Presenza di Mercato.

Il report "Voice of the Customer" di Gartner aggrega le recensioni dei decisori IT sui vari prodotti. Le recensioni sono riclassificate come:

- **Customer's Choice**: soddisfa o supera sia la valutazione complessiva media del mercato sia l'interesse e l'adozione medi degli utenti del mercato.
- **Established**: soddisfa o supera la media di mercato dell'interesse e dell'adozione degli utenti, ma non soddisfa la media di mercato della valutazione complessiva

(1) "The Forrester Wave™: Third-Party Risk Management Platforms, Q2 2022. The 12 Providers That Matter Most and How They Stack Up", May 16, 2022.

(2) "Gartner Peer Insights 'Voice of the Customer': IT Vendor Risk Management Tools", March 2, 2022 - ID G00763741


Swascan
TINEXTA GROUP
SERVIZI
CYBER ACADEMY
PARTNERS
BLOG
ABOUT
CONTATTI
EN IT
SOTTO ATTACCO
European Cyber Research Team
La piattaforma di Security Testing - Threat Intelligence & Cyber Competence Center di
Swascan per il Cyber Security Framework Aziendale.
Sicurezza Predittiva. Sicurezza Preventiva. Sicurezza Proattiva.
PROVA IL FREE TRIAL
CSA cloud security alliance®
ISO 9001
ISO 27017
ISO 27001
ISO 27018

SCORE
Security and Compliance
Overall Risk Evaluation

Terms and conditions Privacy Policy About Us Italiano

SCORE Me!

Entra con SPID

What is SCORE

SCORE means Security and Compliance Overall Risk Evaluation

It is a service delivered in SaaS from the cloud that enables cyber risk assessment of small and medium-

Un’esperienza sul campo

Processo

A. Il cliente valuta il rischio intrinseco

B. Il cliente identifica i controlli di sicurezza (determinati dalla classe e dalla criticità di prodotto o servizio) e li sottopone ai potenziali fornitori

   i. i fornitori analizzano i controlli di sicurezza e rispondono al cliente (eventualmente indicando i controlli compensativi)

   ii. il cliente verifica le risposte, calcola il rischio residuo e seleziona il fornitore

C. Il cliente conduce eventuali verifiche ulteriori, a seconda del livello di rischio residuo, al fine di verificare l'effettiva adozione dei controlli di sicurezza indicati

D. Il cliente stipula i contratti

E. Il cliente, periodicamente, con il supporto dei referenti dei fornitori, valuta i fornitori

Rischio intrinseco

Elementi che determinano il rischio intrinseco

- tipo di fornitura (prodotti sviluppati ad hoc, prodotti a pacchetto, servizi, servizi cloud,…);
- criticità dei dati trattati in termini di riservatezza e integrità e disponibilità;
- tipologia di dati personali trattati (anagrafica, dati particolari, dati particolari e sanitari, dati giudiziari, profilazione con elementi di intelligenza artificiale);
- l'ambiente in cui sarà usato il prodotto o servizio (disponibile solo internamente allo staff, tutti o alcuni docenti, al pubblico,…);
- complessità del prodotto o servizio e quindi anche la possibilità o meno di cambiare più o meno velocemente fornitore;
- eventuale necessità di un passaggio di consegne (rischio contingente e operativo).
- dipendenze da misure tecniche di sicurezza (se la fornitura include misure tecniche di sicurezza con impatto su più prodotti e servizi);

Controlli di Sicurezza

- Politiche e regole e procedure di sicurezza
- Assegnazione di ruoli e responsabilità
- Formazione, aggiornamento e controllo del personale
- Sicurezza fisica (p.e. per i data center)
- Gestione delle utenze, dei meccanismi di autenticazione (p.e. password) e delle autorizzazioni
- Sicurezza dei sistemi (p.e. antivirus, monitoraggio, backup, log)
- Sicurezza della rete (p.e. ridondanze, firewall, VLAN)
- Processo di sviluppo delle applicazioni e verifiche di sicurezza
- Gestione degli incidenti
- Continuità operativa
- Rispetto della normativa (p.e. GDPR)
- Esecuzione di vulnerability assessment e penetration test.
- …..

Controlli di Sicurezza (ulteriori elementi)

Oltre ai controlli tecnologici, elementi da considerare sono:

- locazione dei dati (presso Il cliente, presso il fornitore);
- fornitore italiano o estero (con diversità culturali);
- fornitore con competenze nel settore del cliente o meno;
- se è previsto un piano di continuità da parte del fornitore o è in carico al cliente;
- se la soluzione ha il rischio di vendor lock in (ossia la difficoltà di cambiare fornitore o per la tecnologia usata che non permette migrazioni verso altre tecnologie o per le competenze accumulate non condivise con altri);
- se garantisce un adeguato passaggio di consegne.

Rischio Residuo

Il modello deve prevedere il calcolo di un rischio residuo inerente al fornitore, in base a quanto da lui dichiarato rispetto ai controlli di sicurezza ed a eventuali eccezioni. Il rischio residuo potrà:

- risultare (1) **basso**, (2) **medio/medio-alto** (3) **alto**,
- evidenziare una mitigazione rispetto al rischio intrinseco,
- essere accettato (ancorché, ad esempio, **alto**) dal top management, attraverso un processo di deroga
- determinare l'attivazione di approfondimenti ulteriori pre-contrattuali (p.e. audit di persona, audit da remoto, colloquio, niente),
- portare all'introduttore di clausole speciali (p.e. durata del contratto, clausole risolutive espresse, penali, ecc.).


The End