Deloitte.

III Conferenza Cyber Security
Digital Transformation: il ruolo del CISO e la valutazione del Cyber Risk

Roma, 20 Gennaio 2020

Digital Transformation e Rischi Cyber

Il percorso di trasformazione digitale intrapreso dalle organizzazioni determina un espansione del profilo di rischio e strumenti aggiornati di gestione del rischio

Espansione Profilo Rischio

*90% of organizations in North America that are engaged in Digital Transformation acknowledge their **Risk profiles have expanded** due to their **digital initiatives**.*

*Managing **Cybersecurity** Risks is the **top Risk management** objective for decision makers at organizations engaged in **Digital Transformation**[1]*

Deloitte's 2019 Future of Cyber Survey

*For nearly **half of organizations (49%), Cybersecurity** is on the board's agenda, at least quarterly[2]*

Aggiornamento Strumenti di Gestione del Rischio

One of the foundational drivers behind the update of the **COSO ERM Framework** was the need to address the **evolution of risk management** in the **cyber age**, and the need for organizations to improve their approach to managing cyber risk

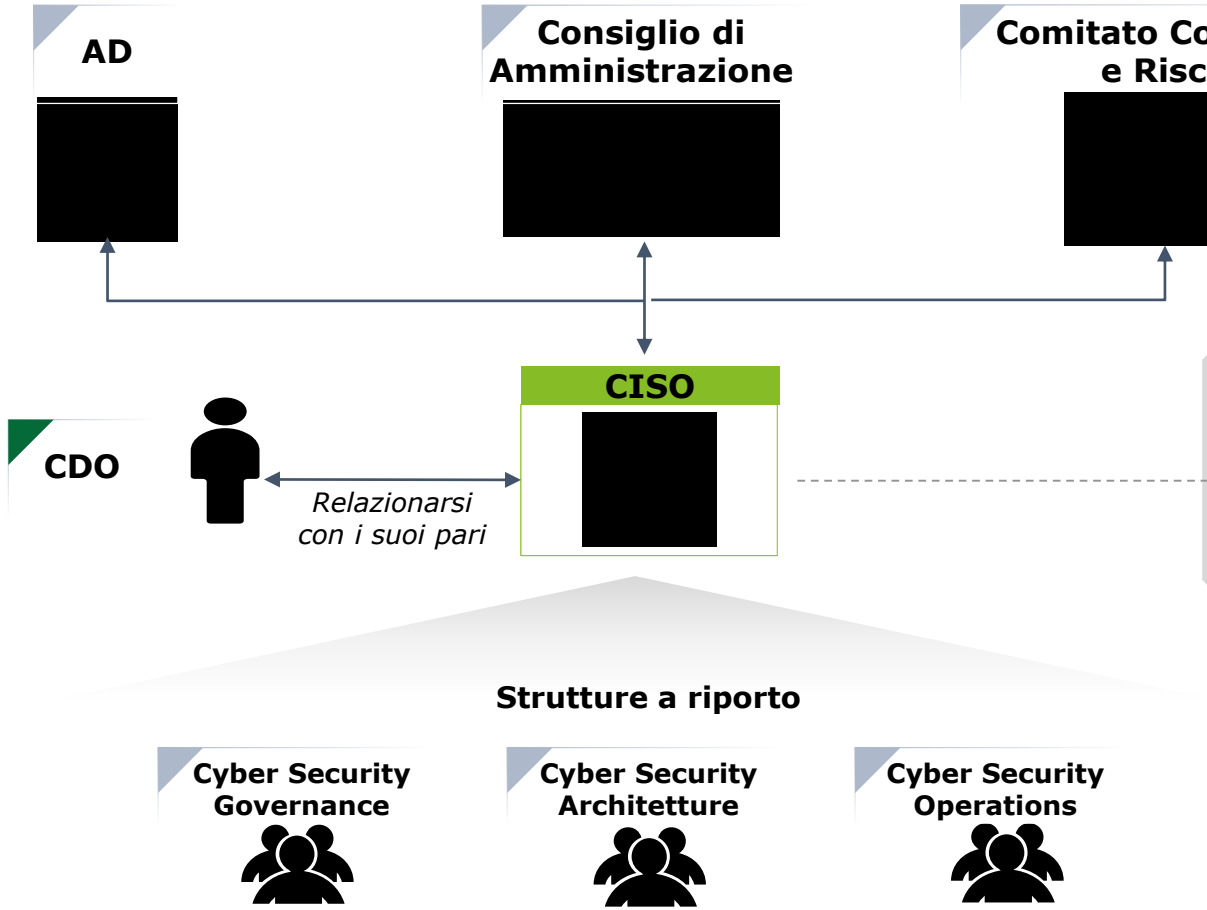
Risk Management Components

Sources: 1) RSA Digital Risk Study 2019; 2) Deloitte's 2019 Future of Cyber Survey; 3) COSO "Managing Cyber Risk in a Digital Age"

Il Ruolo Chiave del CISO

Il Ruolo Chiave del CISO

Il percorso di Digital Transformation intrapreso dalle organizzazioni implica nuove responsabilità per il CISO e la funzione di Cyber Security



Informare sui Rischi Cyber

Realizzare il programma Cyber

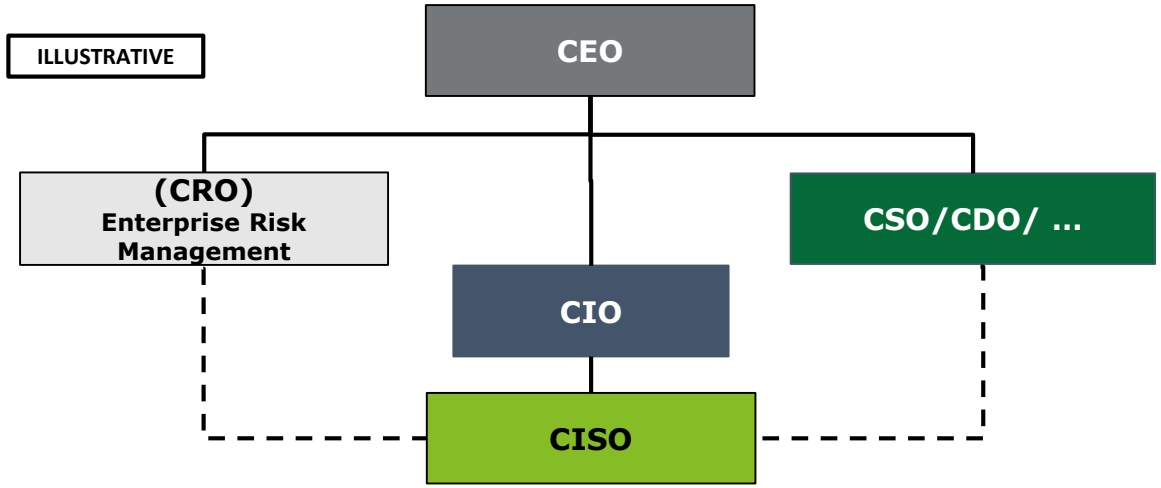
Responsabilità del CISO

- **Interagire** con il **Top Management**, presenziando ai tavoli decisionali
- **Aumentare** la **consapevolezza** dell'azienda su **Rischi** e **minacce** Cyber
- **Parlare** la **lingua** del **Business**
- **Rappresentare** il livello di **Rischio Cyber** e **supportare** la sua **gestione**

- **Definire** ed **implementare** il **programma** pluriennale di Cyber Security
- Definire **piani** e **metodi** per la **valutazione** dei **Rischi** Cyber
- Presidiare **adempimenti** di **Privacy** e **Compliance**
- **Presidiare** il **cambiamento**
- **Gestire** e **coordinare** la **prevenzione** e **risposta** a minacce ed incidenti

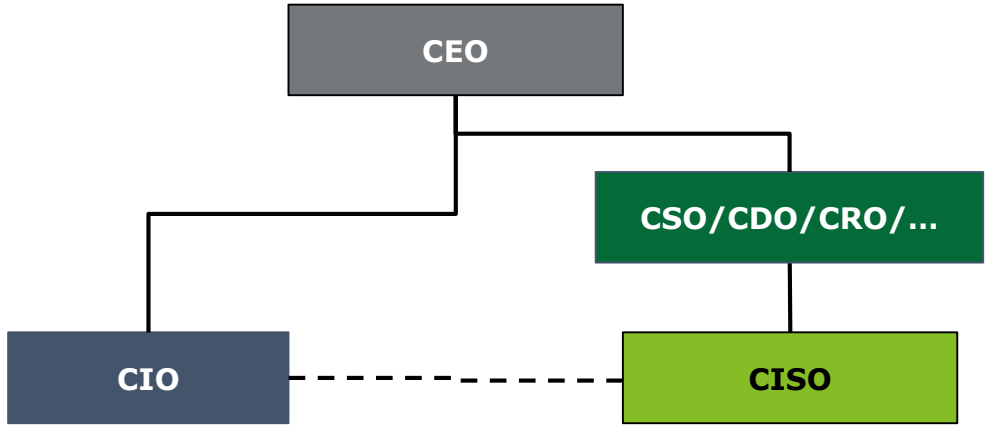
Il ruolo chiave del CISO – Modelli Organizzativi

Le differenti strutture organizzative permettono al CISO di focalizzarsi su ruoli tipicamente di indirizzo e controllo o anche di carattere tecnico



Modello CIO-Driven

- Cyber Security supporta l'agenda del CIO, focalizzandosi tipicamente sulla **progettazione** ed **implementazione** di soluzioni di sicurezza
- Ambiti operativi: definire, mantenere e applicare **policy**, implementare la **security** nelle **architetture** dei nuovi progetti, assicurare il rispetto della **Compliance** nei soluzioni tecnologiche. Non sono escluse attività comunque di **valutazione del rischio**
- Possibile «**dotted-line relationship**» con **ERM**



Modello CISO-Driven

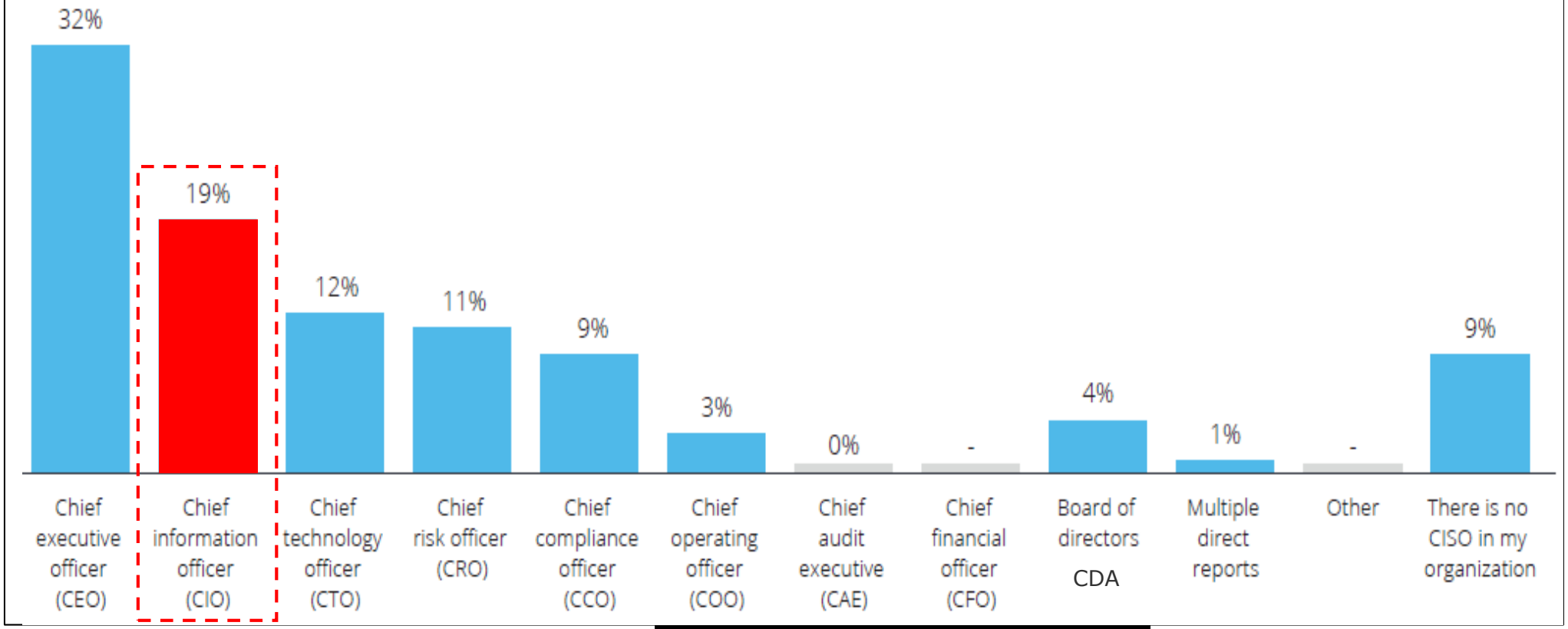
- **Focalizzazione** tipicamente sulle attività di **indirizzo** e **controllo**, sulla **gestione** dei **rischi**, la Compliance e l'enforcement delle policy
- Ambiti operativi**:** alta accountability per la **gestione** dei **Rischi** Cyber, **compliance**, **controllo** e applicazione delle **policy** aziendali
- Richiede **integrazione** con la struttura del **CRO** e **Architetture IT**
- L'implementazione e gestione delle tecnologie di sicurezza può essere delegata ad altre funzioni come ICT, permettendo al **CISO** di **focalizzarsi** sulla gestione dei **rischi** e **compliance**,

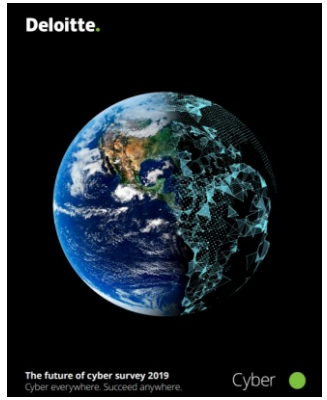
Sources: Forrester Report 2019 Build your security organization, Deloitte elaborated

Il ruolo chiave del CISO – Livello di reporting

Il livello di reporting del CISO non presenta un approccio comunemente adottato nelle diverse organizzazioni. Il reporting al CIO sussiste ma non è l'unico

1. "To whom does the CISO typically report in your organization?"





The Deloitte 2019 Future of Cyber Survey

I Trend per la Valutazione dei Rischi Cyber

Responsabilità del Top Management in ambito Cyber Risk

Il Top Management deve bilanciare crescita e profittabilità di mercato con la tutela dell'azienda, la mitigazione dei Rischi Cyber e l'adempimento agli obblighi normativi

Leggi, Regolamenti e Best Practice di riferimento

Cyber Security Framework Nazionale
(applicazione volontaria - 2016)

Direttiva NIS[1]
(applicazione entro 9 Maggio 2018)

General Data Protection Regulation
(applicazione entro 25 Maggio 2018)

Obblighi e Raccomandazioni di Sicurezza

FOCUS

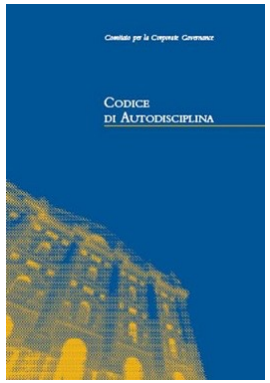
1. Coinvolgimento del Top Management/CDA nei processi di **valutazione e gestione dei Rischi Cyber**
2. Definizione e assegnazione dei **ruoli** e delle **responsabilità** di Cyber Security (CSO, CISO, ecc.)
3. Sviluppo **capacità CERT**, con obiettivi preventivi e di adeguata **reazione agli incidenti di sicurezza**
4. Applicazione degli **obblighi di protezione dei dati** come le misure Privacy by Design e Privacy by Default
5. Definizione di programmi per **promuovere** la **consapevolezza** e la **cultura della Cyber Security** a tutti i livelli aziendali

Il ruolo del CDA in ambito Cyber Risk

Analogamente il Consiglio di Amministrazione è chiamato a identificare, misurare, gestire e monitorare tutti i Rischi dell'azienda inclusi quelli Cyber

Il comitato di **Corporate Governance** di Borsa Italiana ha rilasciato un **Codice di Autodisciplina** per le **società quotate**. Il codice parla chiaramente degli **obblighi** del **Consiglio di Amministrazione** in merito ai "Principali Rischi afferenti all'emittente"

Codice di Autodisciplina
(Luglio 2018)



Art. 7 – Sistema di controllo interno e di gestione dei Rischi

"Il consiglio di amministrazione, previo parere del comitato controllo e Rischi:

- *definisce le linee di indirizzo del **sistema di controllo interno** e di **gestione dei Rischi**, in modo che i **principali Rischi** afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre il **grado di compatibilità** di tali Rischi con una gestione dell'impresa coerente con gli **obiettivi strategici** individuate"*

Le aziende quotate sono chiamate a rilasciare ogni anno una dichiarazione di conformità

I trend per la valutazione dei rischi Cyber

L’analisi dei rischi Cyber seppur considerata come pratica consolidata sta vedendo un evoluzione guidata principalmente dal ruolo strategico ricoperto

Key Driver

Valutare i **rischi Cyber** come rischi **operativi** alla stessa stregua degli altri rischi aziendali

Individuare modalità di valutazione **flessibili**, che tenga conto di fenomeni **dinamici**

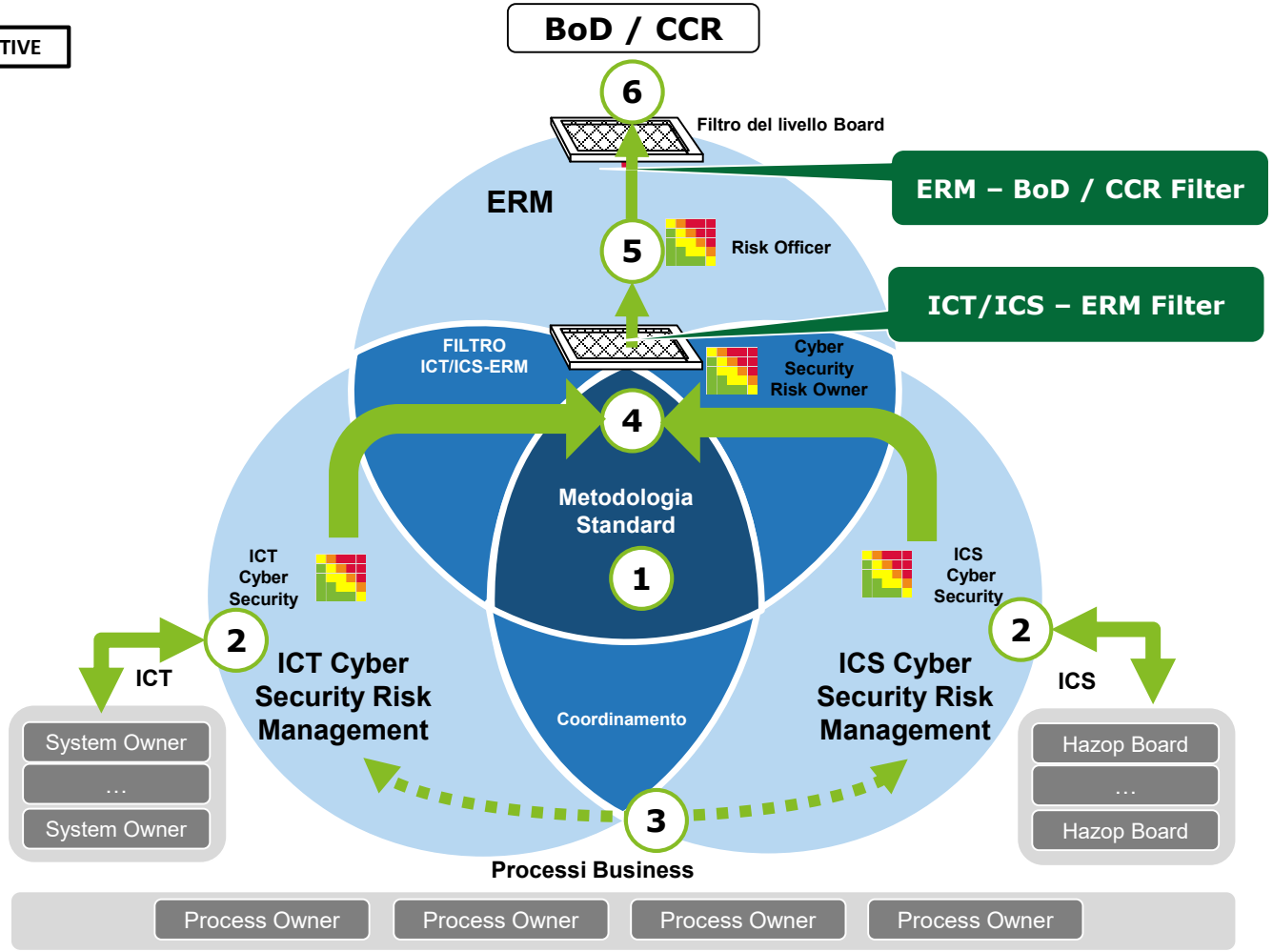
Rappresentare il livello di rischio cyber con un **linguaggio** comprensibile dal **business**

- **Integrazione** con **ERM**
- **Analisi dinamica** del Rischio
- Metodologie e strumenti di **valutazione quantitativa**

Integrazione con l'Enterprise Risk Management (ERM)

Per includere il rischio cyber nella valutazione dei rischi aziendali (ERM), è necessario un modello comune che permetta una corretta rappresentazione del livello di rischio

ILLUSTRATIVE



Legenda

1	Metodologia Comune
2	Dominio del profile di Rischio Cyber
3	Coordinamento se necessario
4	Profilo di Rischio Cyber
5	Profilo di Rischio aziendale
6	Top Risks

ERM e Analisi per Scenari di Rischio

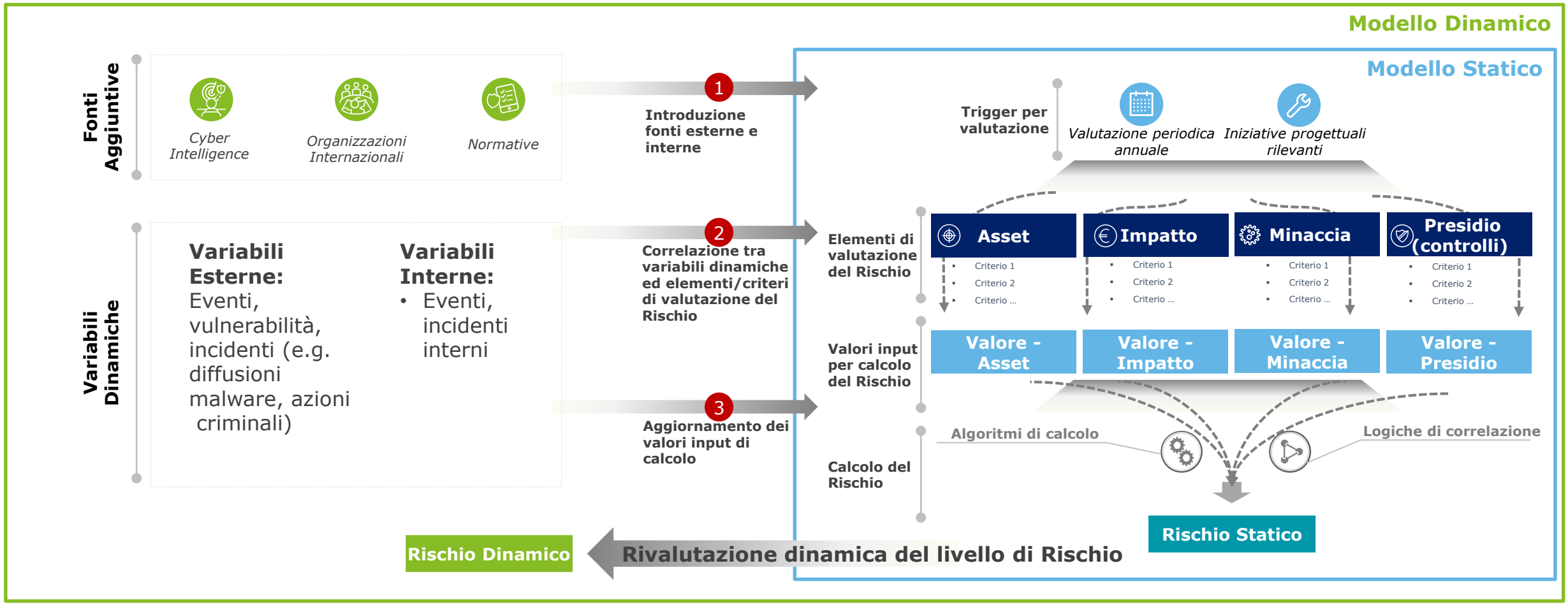
L'integrazione prevede un approccio basato sulla scenari di rischio, costituito dalla combinazione di Minaccia, Asset interessato ed effetto determinato

Evento di Perdita

Minaccia	**Asset**	**Effetto**
Qualsiasi entità, attore o agente, in grado di **danneggiare** un bene in modo che possa **provocare perdite**. E.g. Cyber criminali, utenti privilegiati	Qualunque **entità di valore** che può essere influenzata in modo tale che si possa **tradurre in perdita**. E.g. informazioni non pubbliche presenti in database, Applicazioni	In che modo una **perdita si materializza** su un determinato Asset: • **Confidentiality** • **Integrity** • **Availability**

Analisi Dinamica del Rischio Cyber

Le organizzazioni devono poter disporre di processi di Cyber Risk Management che tengano in considerazione la natura dinamica del panorama di Rischio



Divulgazione delle informazioni di Rischio

La valutazione quantitative del rischio Cyber inizia ad essere promossa in particolare negli Stati Uniti

La nuovo **Direttiva SEC** per le quotate americane richiede la quantificazione del Rischio Cyber in termini **economici**

MERE ENUMERATION OF CYBER RISK FACTORS NO LONGER ACCEPTABLE

CYBERSECURITY RISKS AND INCIDENTS TO BE REPORTED IF "MATERIAL" TO THE FINANCES OF THE COMPANY

- Disclosures to include:
  - Frequency of Cyber events
  - Probability and magnitude of incidents **(costs, in financial terms)**
  - Adequacy of controls
  - Potential reputational harm
  - Potential fines and judgements

"Controls and procedures should enable companies to

- *identify Cybersecurity Risks and incidents,*
- *assess and analyze their impact on a company's business,*
- *evaluate the significance associated with such Risks and incidents,*
- *provide for open communications between technical experts and disclosure advisors, and*
- *make timely disclosures regarding such Risks and incidents."*

SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures – Feb. 26, 2018

Metodologia Quantitativa di Cyber Risk Management

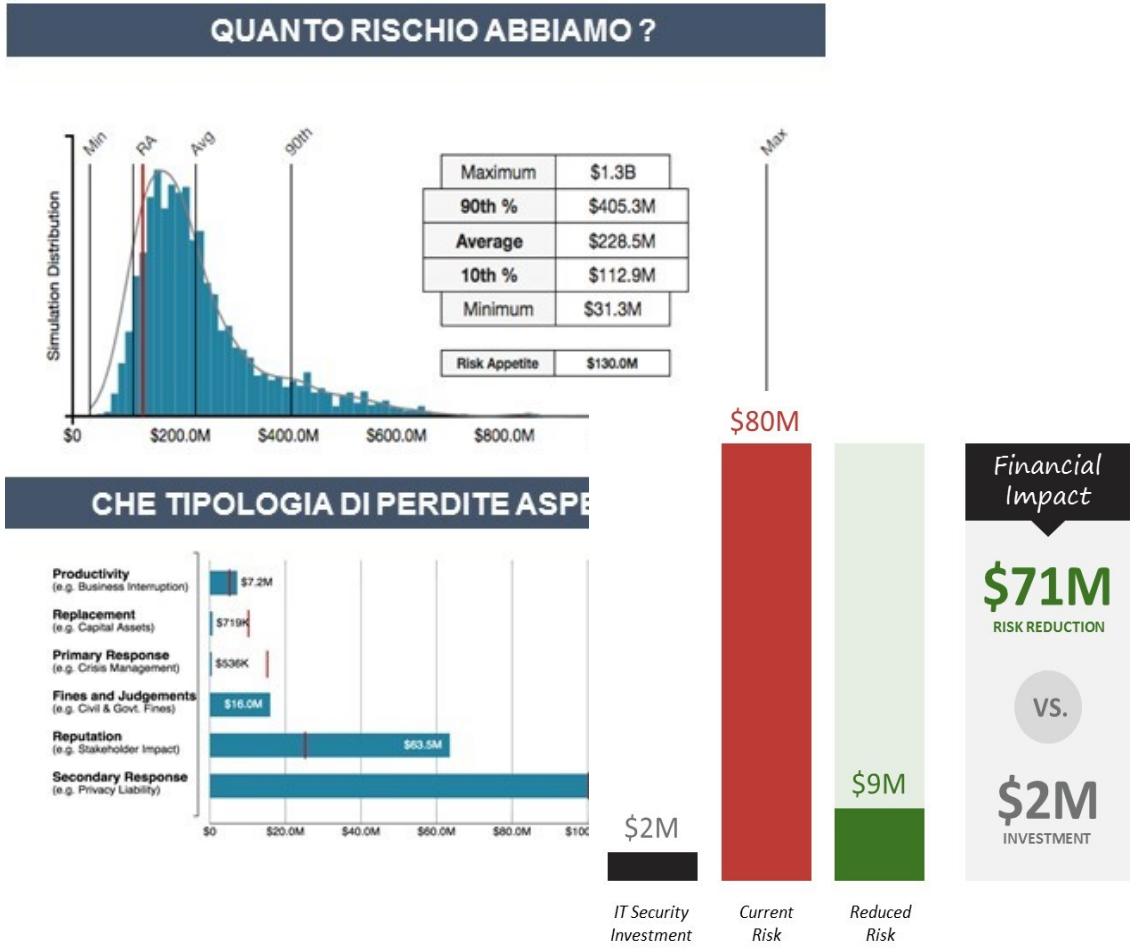
Recentemente le organizzazioni stanno avviato iniziative di valutazione quantitativa a complemento di quelle qualitative

Risultati Qualitativi

Business Impact					
5	Medium	High	High	Very High	Very High
4	Low	Medium	High	High	Very High
3	Low	Low	Medium	High	High
2	Very Low	Very Low	Low	Medium	High
1	Very Low	Very Low	Very Low	Low	Medium
	Very Low	**Low**	**Medium**	**High**	**Very High**

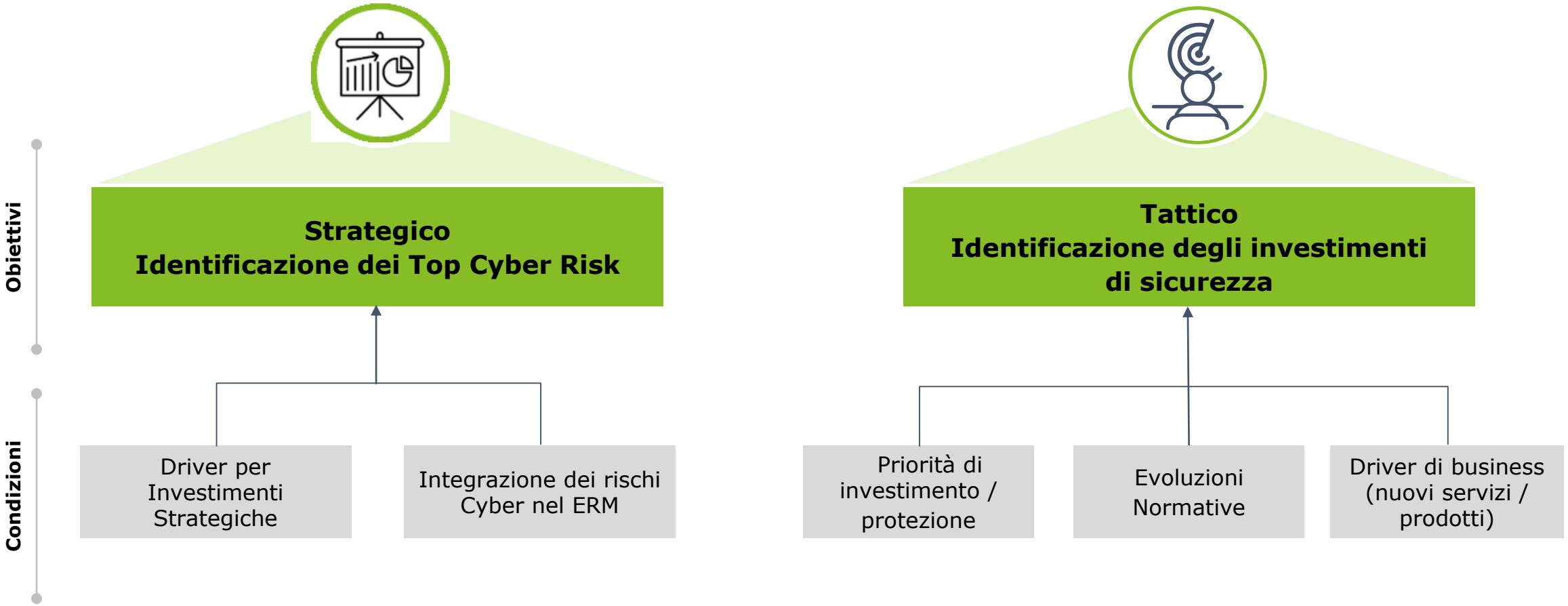
Level of Occurency

Risultati Quantitativi



Metodologia Quantitativa di Cyber Risk Management

L'analisi quantitativa può essere applicata ad esempio per l'identificazione dei Top Cyber Risk di un organizzazione e/o a supporto di decisioni di investimento di sicurezza



Grazie per l'attenzione