Cyber Risk e Resilienza: è necessario un cambio di approccio

Andrea Buzzi
Senior Director | NTT DATA | Cybersecurity Banking

13 Giugno 2024

The most important Business Risks - Europe

Source: ALLIANZ COMMERCIAL - Allianz Risk Barometer Identifying the major business risks for 2024

Convergenza nella gestione del Rischio

1 Enterprise Risk

2 Cyber Risk

3 Operational Risk

- STRATEGIA
- TERZE PARTI
- COMPLIANCE
- DATI
- TECNOLOGIA

Anche le normative sono Risk-Driven

DATI

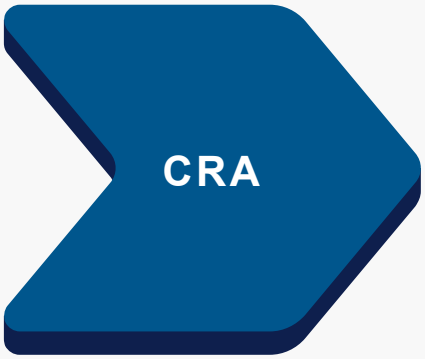
Si applica a tutte le **istituzioni finanziarie che trattano dati personali** di cittadini dell'Unione Europea e **impone standard** rigorosi per la **protezione e la gestione dei dati personali**

SISTEMI INFRASTRUTTURE

Aggiornamento della versione precedente, questa normativa riguarda **la sicurezza delle reti e dei sistemi informativi** e impone alle istituzioni finanziarie di garantire un **elevato livello di sicurezza delle informazioni**

GOVERNANCE

Specifica per il settore finanziario, nelle aree di sovrapposizone è una **lex specialis rispetto alla NIS2**



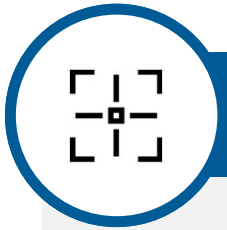
PRODOTTI

Ultimo in ordine temporale, è un **framework per la valutazione del livello di sicurezza «by design»** di tutti i prodotti **HW/SW**

Una nuova Vision per il Settore Finanziario

PERIMETRO

I requisiti normativi impongono di non focalizzarsi più solo verso l'interno dell'organizzazione, ma di considerare ***l'intero ecosistema***



OBIETTIVO

Gli stessi requisiti richiedono di spostare maggiormente l'attenzione sul ***cliente finale*** *e in generale su tutta la* ***filiera*** *di erogazione del servizio*

La classica vista del Digital Operational Resilience Act

Governance End-to-End

Adozione e mantenimento di sistemi e strumenti per la gestione dei rischi ICT, con particolare focus sulle critical functions, ed evoluzione della Business Continuity Policy e del Disaster Recovery Plan come parte integrante del sistema di risposta.

01

ICT Risk Management

Articles from 5 to 16

Armonizzazione dei requisiti di classificazione e segnalazione degli incidenti rilevanti con tempi rapidi di notifica (entro il giorno stesso dell'evento) all'Autorità nazionale competente degli incidenti ICT rilevanti, e applicazione delle capacità di Threat Intelligence.

02

ICT Incident Management

Articles from 17 to 23

Standardizzazione dei requisiti per i test di resilienza (annuali) secondo un approccio risk-based e proporzionato alle dimensioni e al business. Conduzione di test basati sul TLPT (Tiber EU), per le entità significative e con un livello adeguato di maturità cyber, con frequenza triennale

03

Digital Operational Resilience Testing

Articles from 24 to 27

Garantire un monitoraggio completo delle terze parti, dall'ingaggio fino all'exit strategy, anche attraverso elementi contrattuali. La gestione delle terze parti deve essere integrata nei processi di monitoraggio del rischio di gestione degli incidenti ed esecuzione dei test.

04

ICT third-party risks management

Articles from 28 to 30

Promuovere lo scambio

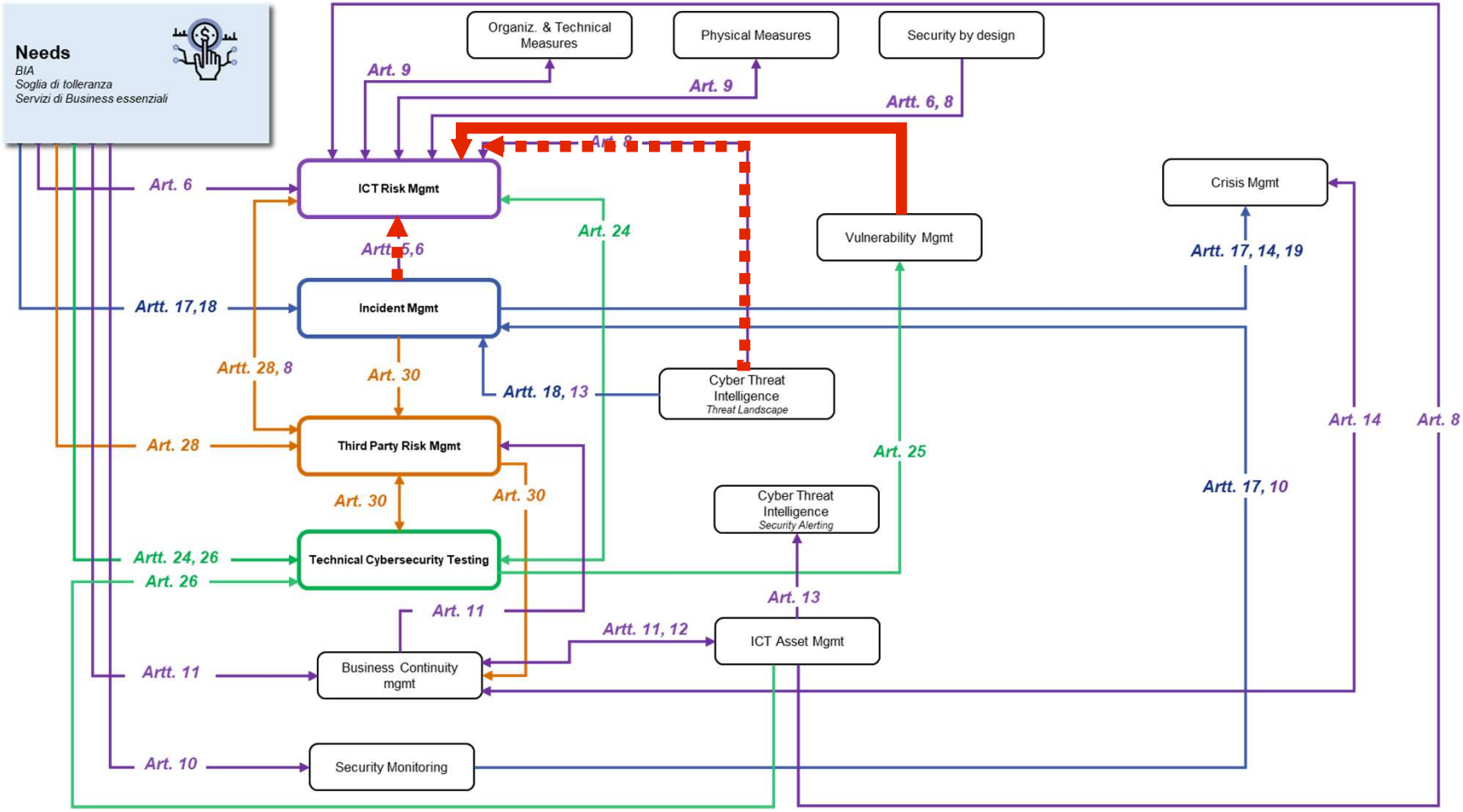
delle informazioni relative alle minacce ICT a livello di sistema, per rafforzare la prevenzione e risposta alle minacce connesse al continuo evolversi del contesto

05

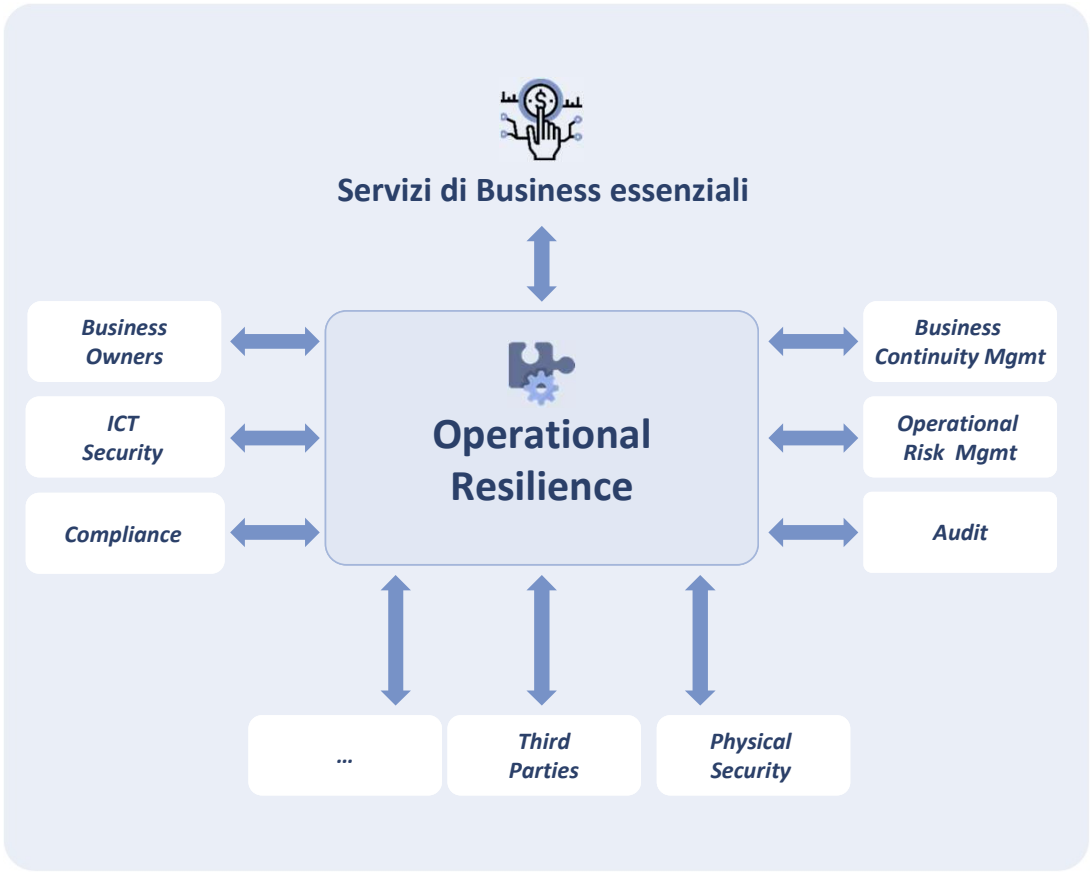
Information Sharing

Article 45

La forza dell'integrazione



Cambio di approccio\1: la resilienza operativa come orchestratore

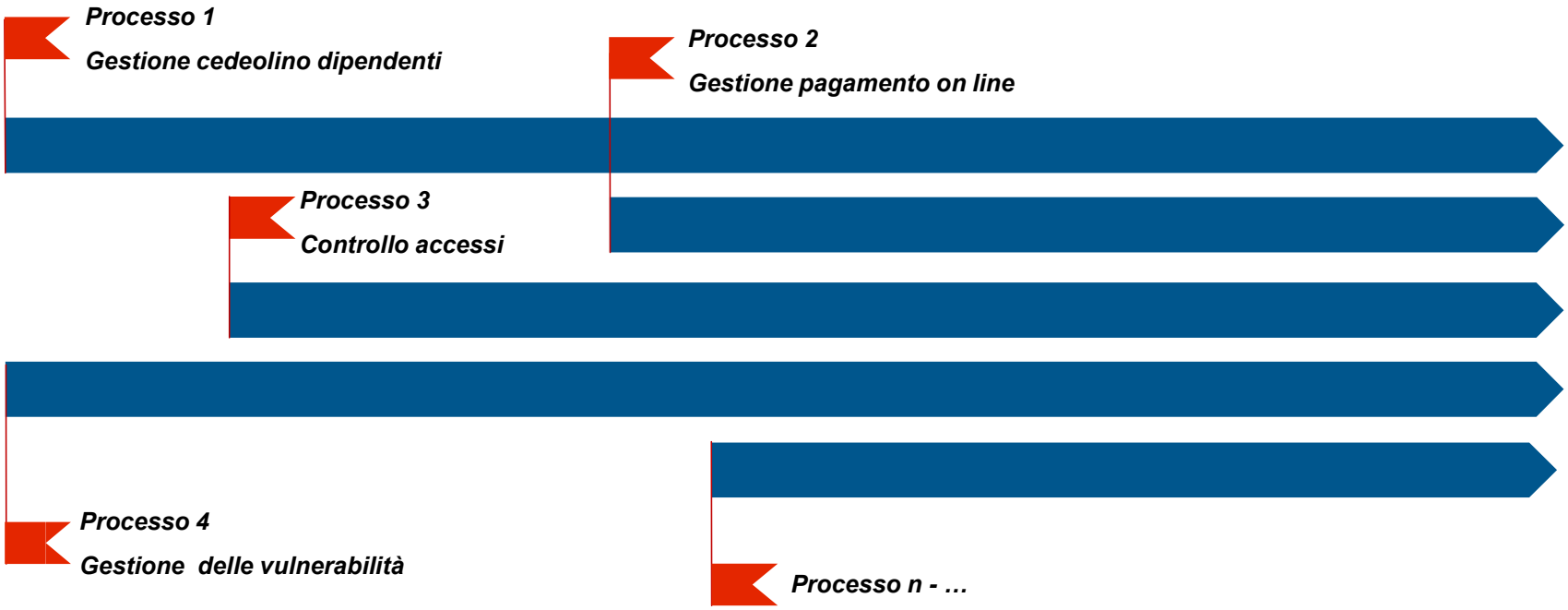


La Resilienza Operativa digitale agisce come **orchestratore**:

definisce gli obiettivi e stabilisce nuovi requisiti, raccogliendo e integrando gli input provenienti da altre Funzioni al fine di guidare le decisioni aziendali e garantire la resilienza dei Servizi di Business importanti

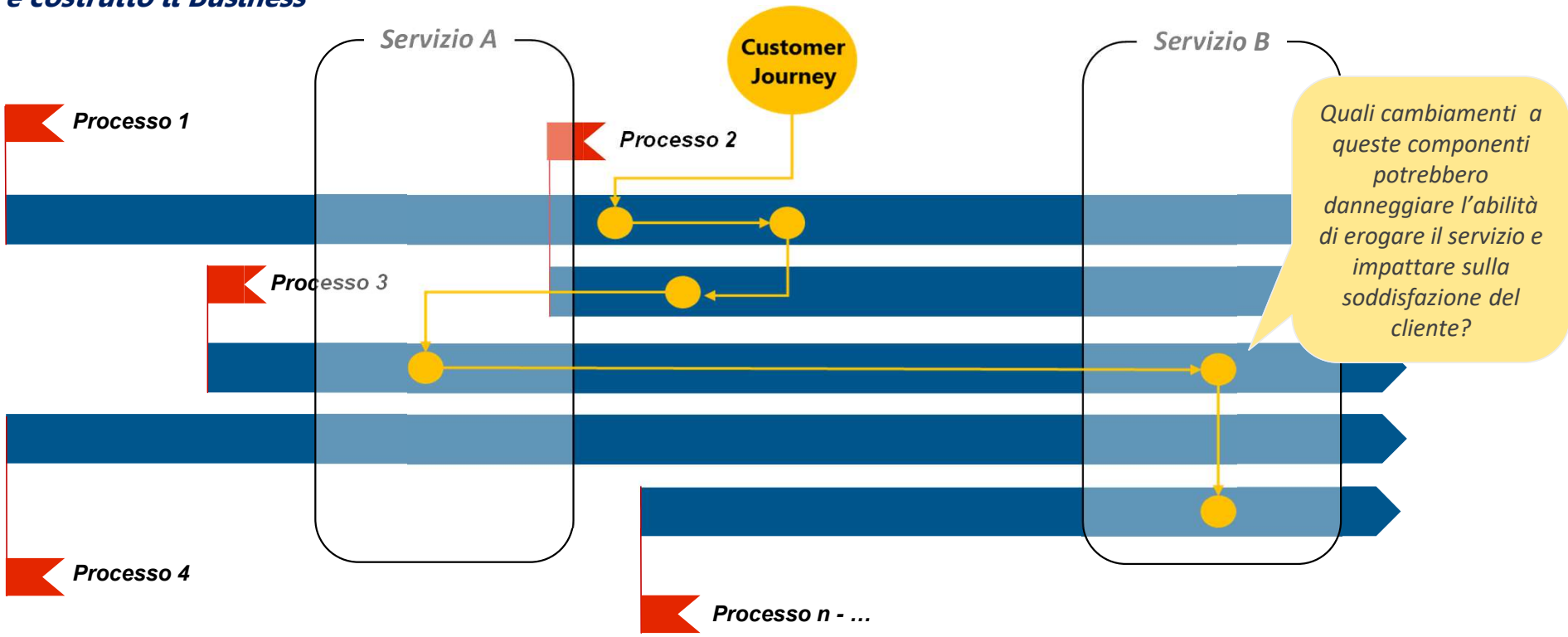
Cambio di approccio\2: dalla vista per processi…

Come funziona l'azienda oggi



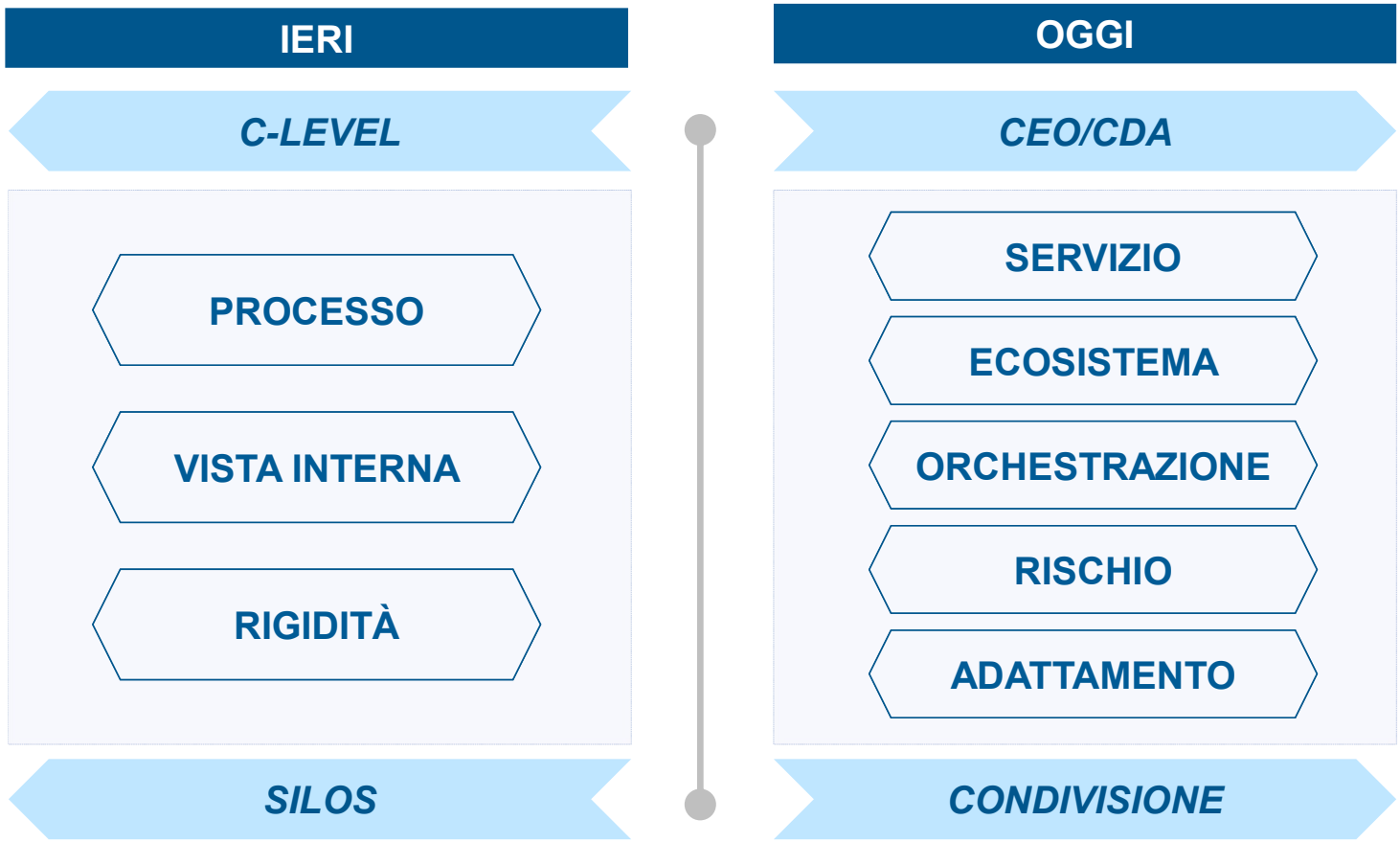
Cambio di approccio\2: …alla vista per Servizio

Come è costruito il Business



La resilienza operativa deve essere progettata tenendo conto del «customer journey»: è necessario visualizzare i propri servizi dal punto di vista del cliente per garantire che il livello di servizio, durante un evento dannoso, soddisfi le sue aspettative.

Per concludere, la normative richiedono un cambio di approccio…



La Cybersecurity Agenda

Ogni organizzazione deve avere una Agenda per decidere il proprio **approccio** per affrontare i rischi Cyber. La immaginiamo come una mappa composta da **tutte le tappe** che possono essere raggiunte affinché possano **orientarsi** e **costruire** la propria strada nella Cybersecurity.

ASSESS

Progetta la tua strategia di cybersecurity sulla base delle necessità attuali e future

PREPARE

Prepara la tua organizzazione a proteggersi dalle minacce del contesto in cui operi

OPERATE

Reagisci in fretta alle minacce con una gestione continua della cybersecurity

INFLUENCE

Rafforza l'ecosistema assicurandoti che i tuoi partner siano attenti alla cybersecurity

FORESEE

Alza il tuo punto di vista per rilevare le nuove minacce e ridurre l'esposizione al rischio

MAKE IT SUSTAINABLE

Monitora le attività per garantire un livello di protezione adeguato alle tue necessità

NTT DATA


NTT DATA