



# CYBER RISK: MODELLI DI GESTIONE E MISURAZIONE

## PRINCIPALI PRASSI E SFIDE FUTURE

SESSIONE PARALLELA 3.3

*23 giugno 2021*



**accenture**

# AGENDA



## STATUS QUO SUL RISCHIO CYBER & ICT



## MODELLI ORGANIZZATIVI PER LA GESTIONE DEL RISCHIO CYBER & ICT



## MISURAZIONE DEL RISCHIO CYBER & ICT



## SFIDE FUTURE

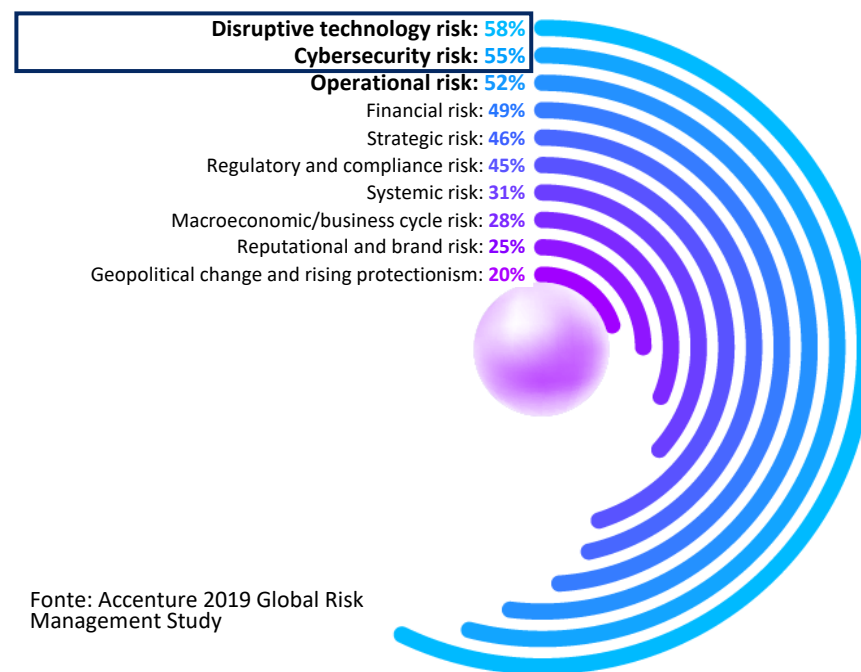
# STATUS QUO SUL RISCHIO CYBER & ICT

## OVERVIEW SU RISCHI CYBER & ICT PER FS

- Le aziende hanno fatto **progressi significativi nella cybersecurity** negli ultimi anni<sup>1</sup>, tuttavia le **minacce informatiche stanno crescendo in complessità e precisione**, portando ad una **perdita di valore stimata globalmente di \$5,2 trillioni** entro il 2025, di cui \$347 miliardi in ambito bancario e \$305 in quello assicurativo<sup>2</sup>
- Normative**, come le linee guida EBA e il DORA Framework della Commissione Europea, stanno spingendo le imprese ad **accelerare il loro percorso verso la resilienza operativa digitale**
- Maggiori investimenti sono in quest'ottica dedicati al **rafforzamento dei framework di gestione del rischio** e al **ridisegno delle funzioni** che gestiscono questi rischi (e.g., Risk, Security), come passo necessario per migliorare l'efficacia del processo di gestione del rischio Cyber & ICT

## IMPATTO DEI RISCHI CYBER & ICT SUI FS

Le percentuali si riferiscono agli executive che affermano che il rischio ha ora un impatto maggiore o un impatto significativamente maggiore sulla propria organizzazione rispetto a due anni fa



Fonte: Accenture 2019 Global Risk Management Study

**Per far fronte alle crescenti minacce cyber, le aziende stanno investendo sempre più su competenze di cybersecurity nella seconda linea di difesa**

# AGENDA



STATUS QUO SUL RISCHIO CYBER & ICT



**MODELLI ORGANIZZATIVI PER LA GESTIONE DEL RISCHIO  
CYBER & ICT**



MISURAZIONE DEL RISCHIO CYBER & ICT



SFIDE FUTURE

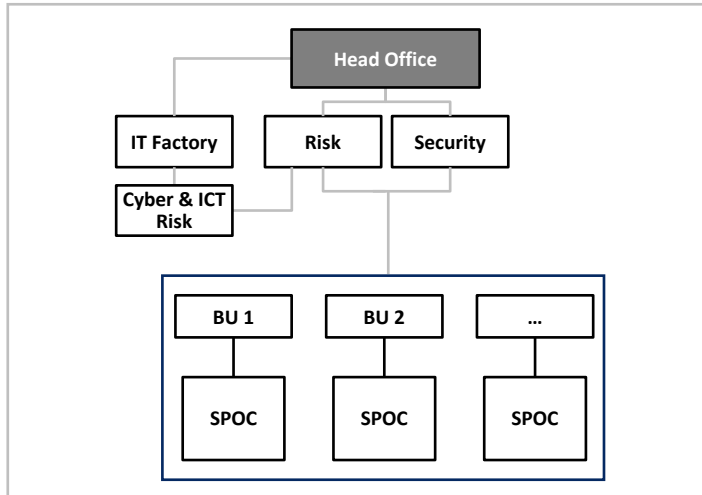


# MODELLI ORGA. PER LA GESTIONE DEL RISCHIO CYBER & ICT

I PLAYER FS POSSONO ADOTTARE DIVERSE STRUTTURE ORGANIZZATIVE PER GESTIRE I RISCHI CYBER & ICT

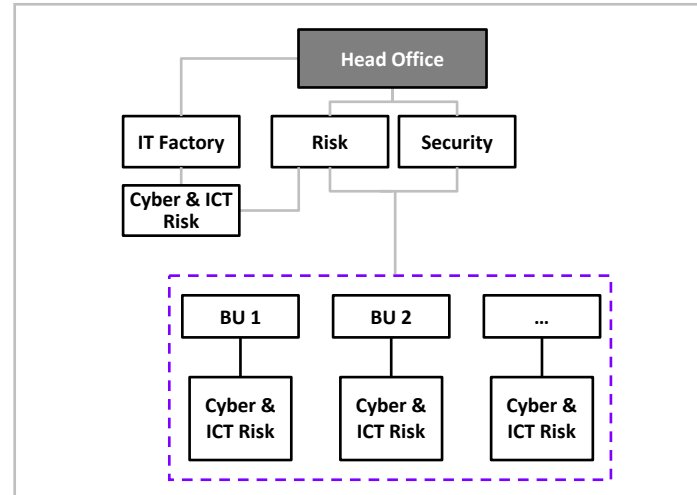
LEGENDA — Centralizzato  
- - - Decentralizzato

## Approccio centralizzato



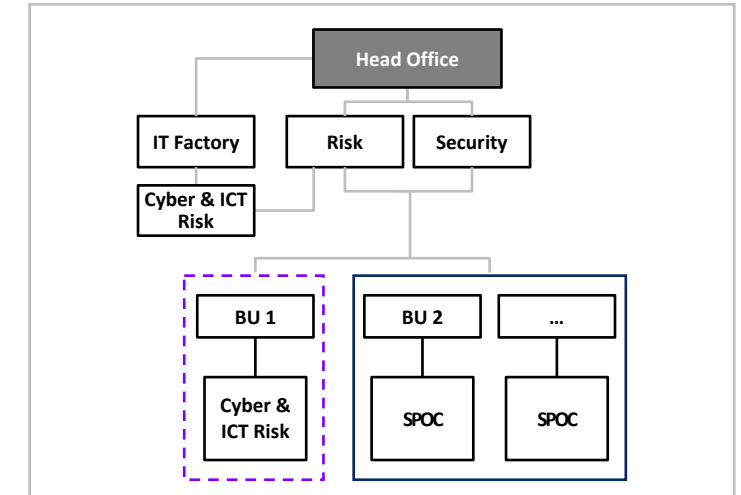
- **Implementazione e governance** del modello di misurazione del rischio Cyber & ICT **centralizzato nel Risk di Head Office** e nella **IT Factory**, a supporto di **tutte le BU**, sfruttando un **panorama IT integrato ed omogeneo**
- **Le BU forniscono Single Points of Contact (SPOC)**, di solito situato all'interno dell'OpRisk (Seconda linea) e Security (Prima linea), che supporta le funzioni di Risk e Security di Head Office ad alimentare il modello

## Approccio decentralizzato



- **Implementazione** del modello di misurazione del rischio Cyber & ICT **decentralizzato nelle BU**, che dispongono di un **team dedicato al Cyber & ICT Risk** per l'operatività
- Le funzioni **Risk e Security di Head Office** svolgono solo **attività di governance e reporting**

## Approccio ibrido



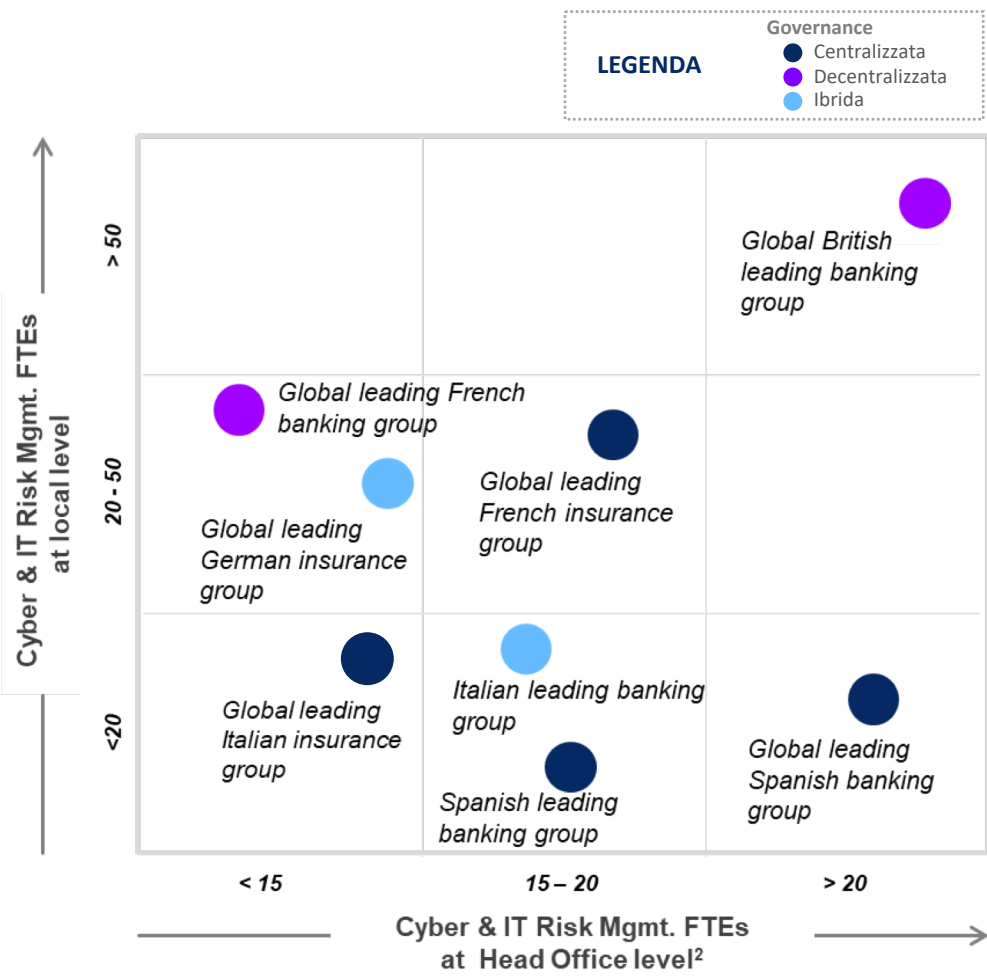
- **Implementazione e governance** del modello di misurazione del rischio Cyber & ICT **centralizzato nelle funzioni di Risk e Security di Head Office** e nella **IT Factory**, a supporto delle **principali BU**
- **Decentralizzazione** del modello nelle **BU minori**, per le quali le funzioni **Risk e Security di Head Office** svolgono solamente attività di **governance e reporting**

**Una struttura organizzativa centralizzata può garantire una forte gestione dei rischi Cyber & ICT, facendo leva anche sulla creazione di un Centro di Eccellenza dedicato**

# MODELLI ORGA. PER LA GESTIONE DEL RISCHIO CYBER & ICT

BENCHMARK SU CYBER & ICT RISK GOVERNANCE<sup>1</sup> – IL CAMPIONE INTERVISTATO INCLUDE 8 DELLE PRINCIPALI ISTITUZIONI FINANZIARIE

## STRUTTURA DEL RISK MANAGEMENT NEI FS



## PUNTI CHIAVE

### APPROCCIO DI GOVERNANCE PER GESTIRE IL RISCHIO CYBER & ICT

- **4 player FS hanno adottato una governance centralizzata** con risorse localizzate principalmente al livello di Head Office per garantire una veloce messa a terra del framework di rischio Cyber & ICT, una visione più chiara delle problematiche e una più veloce escalation verso il Board
- **2 player FS hanno adottato una governance decentralizzata** con risorse dedicate a livello locale che gestiscono task chiave in ambito Cyber & ICT risk, al fine di far leva sulla loro conoscenza del contesto locale per l'applicazione del framework definito centralmente
- **2 players FS hanno adottato una governance ibrida** con risorse localizzate sia all'interno degli Head Office, che a livello locale, che fanno leva sul supporto dell'IT Factory per velocizzare la raccolta di dati e l'esecuzione degli assessment per le principali BUs

# AGENDA



STATUS QUO SUL RISCHIO CYBER & ICT



MODELLI ORGANIZZATIVI PER LA GESTIONE DEL RISCHIO  
CYBER & ICT



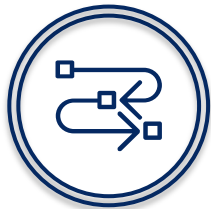
**MISURAZIONE DEL RISCHIO CYBER & ICT**



SFIDE FUTURE

# MISURAZIONE DEL RISCHIO CYBER & ICT

QUANTIFICAZIONE ECONOMICA DEL RISCHIO DIGITALE, BASATA SU FORTI ELEMENTI STRATEGICI



## CENTRALITA' DEGLI ASSET IT E DEI PROCESSI

Identificazione del **contesto tecnologico dell'azienda** tramite la produzione di un **elenco di asset IT centralizzato** direttamente **collegato ai processi di business** che riporta le principali **info sulle tecnologie utilizzate** (e.g., esposizione Internet, classificazione dei dati...)



## MODELLO DI COLLABORAZIONE CROSS FUNZIONE

Definizione di **standard driver IT** (e.g., incidenti di indisponibilità dei sistemi, change d'emergenza, vulnerabilità), basati su una forte **collaborazione tra funzioni di Risk, IT e Security** per la realizzazione della metodologia e per la sua implementazione



## APPROCCIO DATA DRIVEN PER LA QUANTIFICAZIONE ECONOMICA

**Raccolta dati, data quality e analisi dei dati** provenienti da fonti informative fornite dalla **funzioni IT & Security** relative agli standard driver IT definiti, al fine di quantificare una **perdita economica (€)** che viene poi usata per valutare il **Digital risk**

MAIN ISSUES  
ADDRESSABLE

- *Assenza di un inventario degli asset IT*
- *Informazioni frammentarie su diversi sistemi / repository*
- *Mancanza di informazione sulle tecnologie utilizzate per gli asset IT*

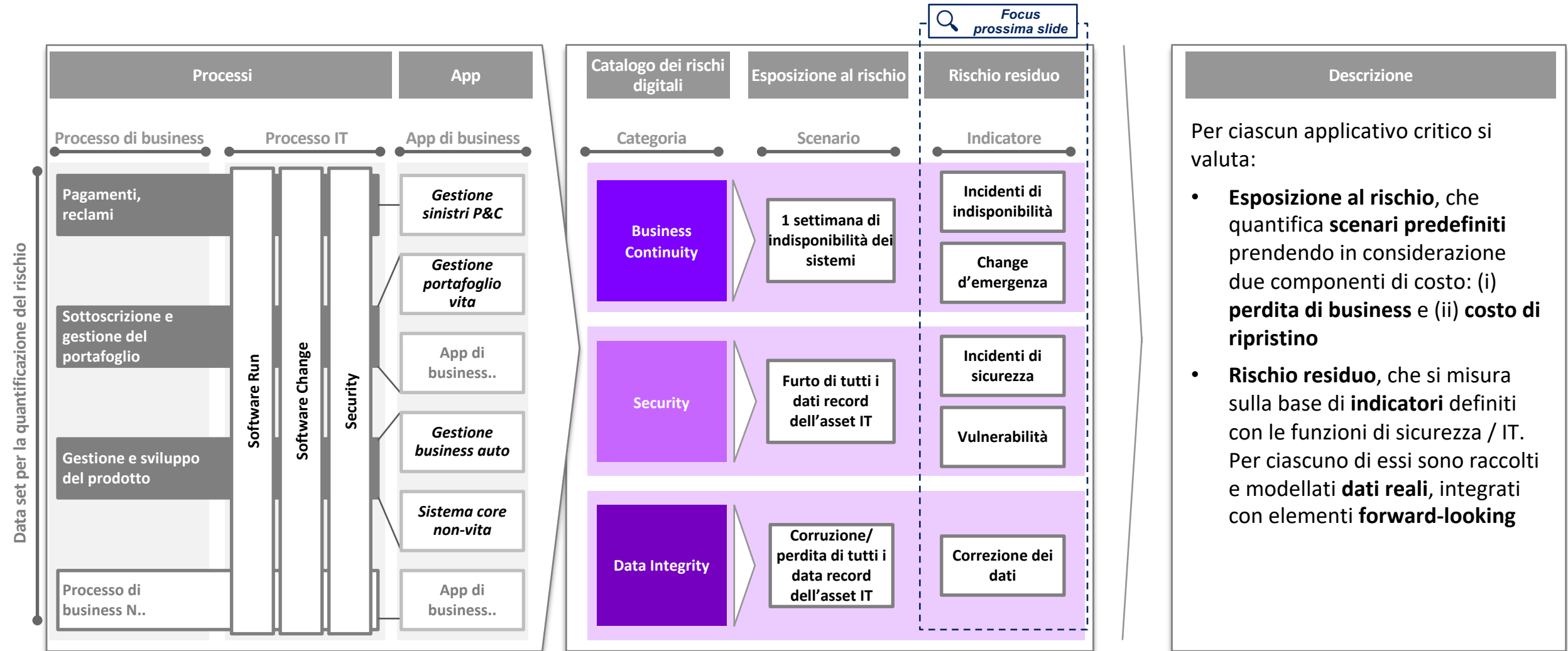
- *Disallineamento tra differenti funzioni che gestiscono / richiedono le stesse informazioni*
- *Mancanza di una fonte unica di informazioni relative agli IT asset*

- *Nessun allineamento sulla raccolta dati*
- *Nessun check sulla data quality / consistency*
- *Diversi livelli di granularità dei dati tra diversi dipartimenti IT*



# MISURAZIONE DEL RISCHIO CYBER & ICT

PANORAMICA DELLA METODOLOGIA PER UNA MISURAZIONE ASSET-CENTRICA DEL RISCHIO BASATA SUI DATI



Focus prossima slide





Descrizione

Per ciascun applicativo critico si valuta:

- Esposizione al rischio**, che quantifica **scenari predefiniti** prendendo in considerazione due componenti di costo: (i) **perdita di business** e (ii) **costo di ripristino**
- Rischio residuo**, che si misura sulla base di **indicatori** definiti con le funzioni di sicurezza / IT. Per ciascuno di essi sono raccolti e modellati **dati reali**, integrati con elementi **forward-looking**

# MISURAZIONE DEL RISCHIO CYBER & ICT

## SINTESI DEI RISULTATI DI MISURAZIONE DEL DIGITAL RISK A LIVELLO DI SINGOLO PAESE

RISCHI RESIDUALI	COMMENTI	PRINCIPALI ASSET IT CRITICI COINVOLTI	PRINCIPALI INDICATORI
<div>(€ Milioni)</div> <div>17 €</div> <div>Business Continuity</div>	<div>Diversi incidenti di indisponibilità riguardanti in particolare <b>sistemi agenziali</b> si sono verificati a seguito di <b>attività di migrazione</b> ed implementazione di <b>requisiti legislativi</b> (e.g. GDPR, IDD), per un totale di <b>57 ore</b> di indisponibilità</div>	<div> <b>Applicazione 1:</b> app dedicate alla vendita di polizze vita in agenzia e via mobile<ul style="list-style-type: none"><li>27 ore di indisponibilità</li><li>4 cambi di emergenza</li></ul></div>	<div>50 Incidenti di indisponibilità totali, per <b>57 ore</b> di indisponibilità</div> <div>16 Cambi di emergenza totali</div>
<div>10 €</div> <div>Security</div>	<div>La gestione delle problematiche di sicurezza è stata influenzata da <b>architettura IT obsoleta</b> delle app e da <b>codici di bassa qualità</b> con processi business maggiormente impattati relativi a <b>pagamenti</b> e <b>stipulazioni</b> di polizze</div>	<div> <b>Applicazione 2:</b> sistema di gestione sinistri.<ul style="list-style-type: none"><li>14 incidenti sulla sicurezza</li></ul></div> <div> <b>Applicazione 3:</b> Sistema integrato attuariale<ul style="list-style-type: none"><li>13 vulnerabilità aperte</li></ul></div>	<div>45 Incidenti sulla sicurezza totali</div> <div>76 Vulnerabilità totali (aperte e chiuse)</div>
<div>5 €</div> <div>Data Integrity</div>	<div>I bug nei software che hanno impattato <b>l'integrità dei dati</b> sono stati pochi (solo <b>36</b> in un anno), principalmente causati da procedure manuali di gestione dei dati</div>	<div> <b>Applicazione 4:</b> front office delle agenzie<ul style="list-style-type: none"><li>8 fix di dati</li></ul></div>	<div>36 Fix di dati totali</div>

# AGENDA



STATUS QUO SUL RISCHIO CYBER & ICT



MODELLI ORGANIZZATIVI PER LA GESTIONE DEL RISCHIO CYBER & ICT



MISURAZIONE DEL RISCHIO CYBER & ICT



**SFIDE FUTURE**

# SFIDE FUTURE



## REVISIONE ORGANIZZATIVA

- **Evoluzione del modello organizzativo verso un approccio centralizzato** in modo da armonizzare processi, controlli e procedure per la gestione del Cyber & ICT risk



## CENTRALITÀ DEL DATO

- **Utilizzo del dato come elemento chiave per identificare nuovi pattern di rischio** e fornire una vista prospettica dell'esposizione al rischio Cyber & ICT



## EVOLUZIONE DEL MODELLO

- **Revisione del modello di misurazione passando da un'ottica process based a customer based** in modo circoscrivere il rischio Cyber & ICT a livello di cliente e disegnare azioni di mitigazione specifiche





**NICASIO MUSCIA**

**MANAGING DIRECTOR  
ACCENTURE RISK & COMPLIANCE**

**MILAN OFFICE (IT)**

[nicasio.muscia@accenture.com](mailto:nicasio.muscia@accenture.com)

+39 335 7365157