



IBM Première

La stagione esclusiva IBM di arte, musica e innovazione.

**Conoscere il rischio, gestirlo
e coglierne le opportunità**

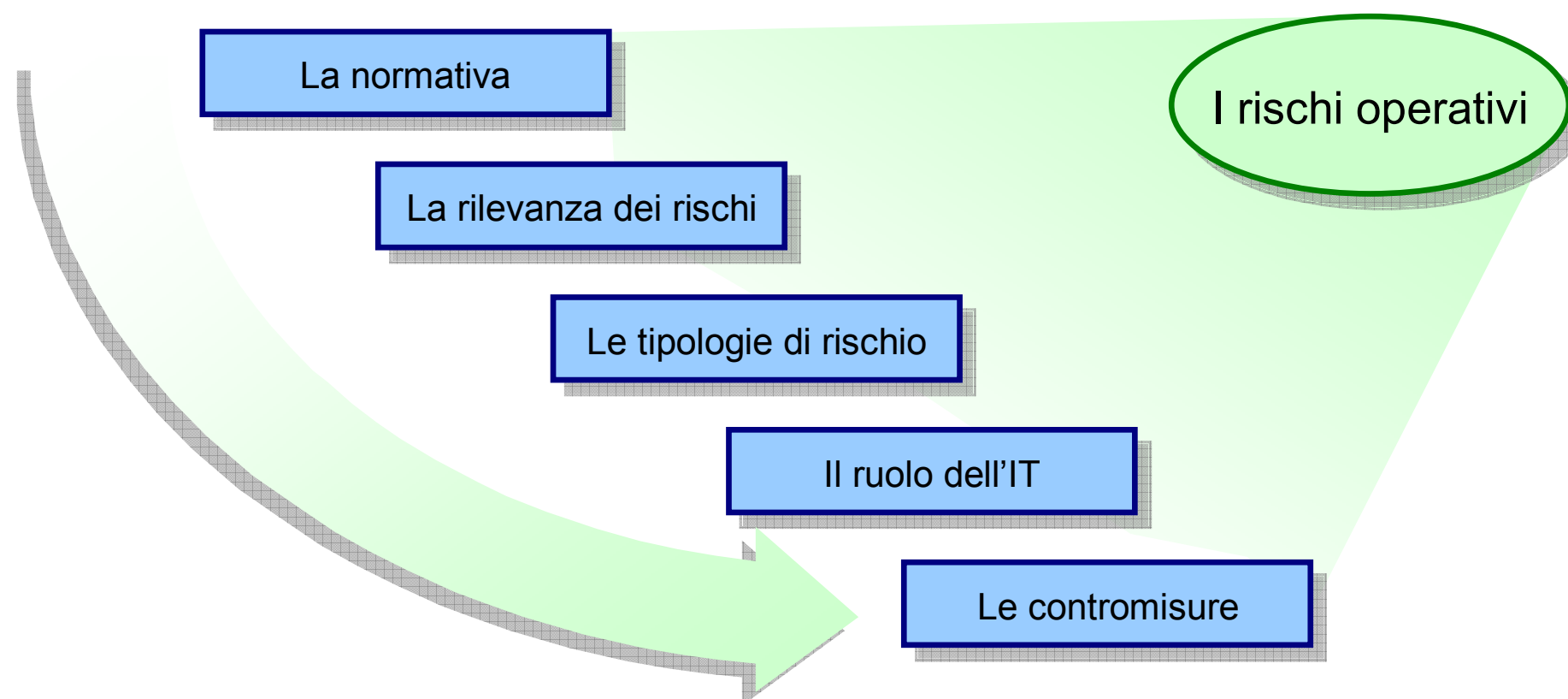
Costantino Gualano

Business Resiliency Principal, IBM Italia





L'evoluzione dei processi di business espone le aziende a nuove minacce o a conseguenze più gravi: questa presentazione si propone di descrivere questi rischi, la loro rilevanza e le possibili contromisure.





Il rischio operativo è stato definito dal Comitato di Basilea, incaricato di pervenire a una convergenza internazionale sulle revisioni delle normative di vigilanza che disciplinano l'adeguatezza patrimoniale delle banche.

DEFINIZIONE DI RISCHIO OPERATIVO

“Il rischio operativo è definibile come il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. Tale definizione include il rischio legale, ma non quelli strategico e di reputazione.”

RIFERIMENTI

- “Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali - Nuovo schema di regolamentazione” Giugno 2004
- “Prassi corrette per la gestione e il controllo del rischio operativo” Febbraio 2003



La normativa Basilea 2 definisce i nuovi parametri per la gestione dei rischi di credito, di mercato e operativi per gli istituti finanziari.

FINANCE

- Si applica direttamente a tutti gli istituti finanziari dei paesi appartenenti al G10.
- Ha valenza indiretta per gli istituti finanziari degli altri paesi.

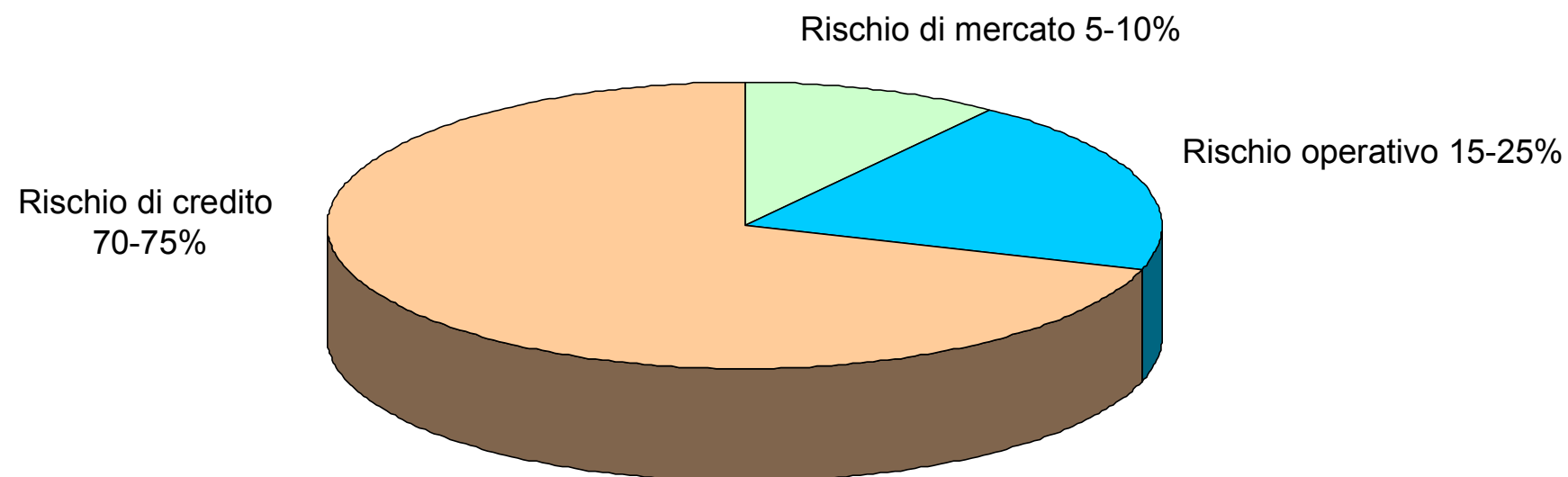
CROSS INDUSTRY

- Introduce il ranking per i rischi di credito (accesso al credito da parte delle imprese).
- Tra i parametri di ranking dei rischi di credito è stata introdotta anche una valutazione relativa ai rischi operativi.
- Costituisce alla data la "best practice" per la misurazione, il controllo, la mitigazione e la gestione dei rischi operativi.



I rischi operativi sono considerati rilevanti, tanto che le previsioni sulla applicazione della normativa Basilea 2 indicano che peseranno in misura superiore ai rischi di mercato.

Evoluzione dell'assorbimento di patrimonio per tipologia di rischio del sistema bancario



Fonte: elaborazione di A.T. Keamey su "The 2002 Loss Data Collection Exercise for Operational Risk"



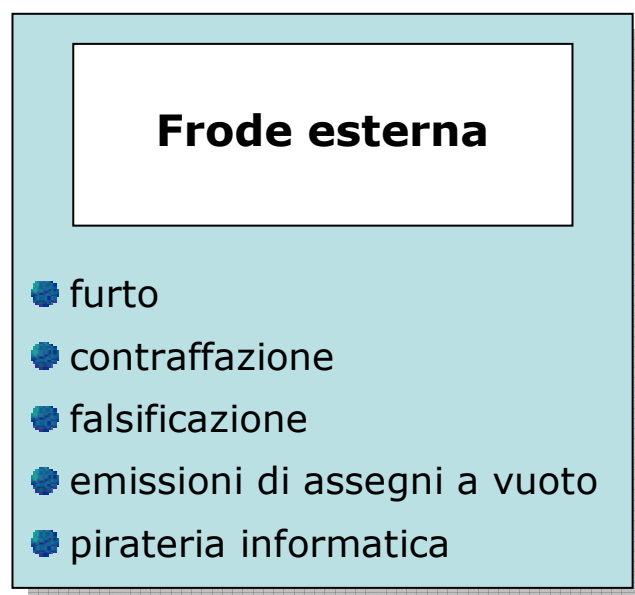
Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.

Frode interna

- alterazione intenzionale di dati
- sottrazione di beni e valori
- operazioni in proprio basate su informazioni riservate

- **Frode interna**
- **Frode esterna**
- **Rapporto di impiego e sicurezza sul posto di lavoro**
- **Pratiche connesse con la clientela, i prodotti e l'attività**
- **Danni a beni materiali**
- **Disfunzioni e avarie di natura tecnica**
- **Conformità esecutiva e procedurale**

Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.



- **Frode interna**
- **Frode esterna**
- **Rapporto di impiego e sicurezza sul posto di lavoro**
- **Pratiche connesse con la clientela, i prodotti e l'attività**
- **Danni a beni materiali**
- **Disfunzioni e avarie di natura tecnica**
- **Conformità esecutiva e procedurale**



Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.

Rapporto di impiego e sicurezza sul posto di lavoro

- risarcimenti richiesti da dipendenti
- violazione delle norme a tutela della salute e sicurezza personale
- attività sindacale
- pratiche discriminatorie
- responsabilità civile

- **Frode interna**
- **Frode esterna**
- **Rapporto di impiego e sicurezza sul posto di lavoro**
- **Pratiche connesse con la clientela, i prodotti e l'attività**
- **Danni a beni materiali**
- **Disfunzioni e avarie di natura tecnica**
- **Conformità esecutiva e procedurale**

Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.

**Pratiche connesse
con la clientela, i
prodotti e l'attività**

- violazione del rapporto fiduciario
- abuso di informazioni confidenziali
- transazioni indebite effettuate per conto della banca
- riciclaggio di denaro di provenienza illecita
- vendita di prodotti non autorizzati

- **Frode interna**
- **Frode esterna**
- **Rapporto di impiego e sicurezza sul posto di lavoro**
- **Pratiche connesse con la clientela, i prodotti e l'attività**
- **Danni a beni materiali**
- **Disfunzioni e avarie di natura tecnica**
- **Conformità esecutiva e procedurale**



Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.

Danni a beni materiali

- atti di terrorismo
- atti di vandalismo
- terremoti
- incendi
- inondazioni

- **Frode interna**
- **Frode esterna**
- **Rapporto di impiego e sicurezza sul posto di lavoro**
- **Pratiche connesse con la clientela, i prodotti e l'attività**
- **Danni a beni materiali**
- **Disfunzioni e avarie di natura tecnica**
- **Conformità esecutiva e procedurale**



Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.

Disfunzioni e avarie di natura tecnica

- anomalie di infrastrutture e applicazioni informatiche
- problemi di telecomunicazione
- interruzione nell'erogazione di utenze.

- **Frode interna**
- **Frode esterna**
- **Rapporto di impiego e sicurezza sul posto di lavoro**
- **Pratiche connesse con la clientela, i prodotti e l'attività**
- **Danni a beni materiali**
- **Disfunzioni e avarie di natura tecnica**
- **Conformità esecutiva e procedurale**

Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.

Conformità esecutiva e procedurale

- errata immissione dei dati
- gestione inadeguata delle garanzie
- documentazione legale incompleta
- indebito accesso consentito a conti di clienti
- inadempimenti di controparti non clienti
- controversie legali con fornitori.

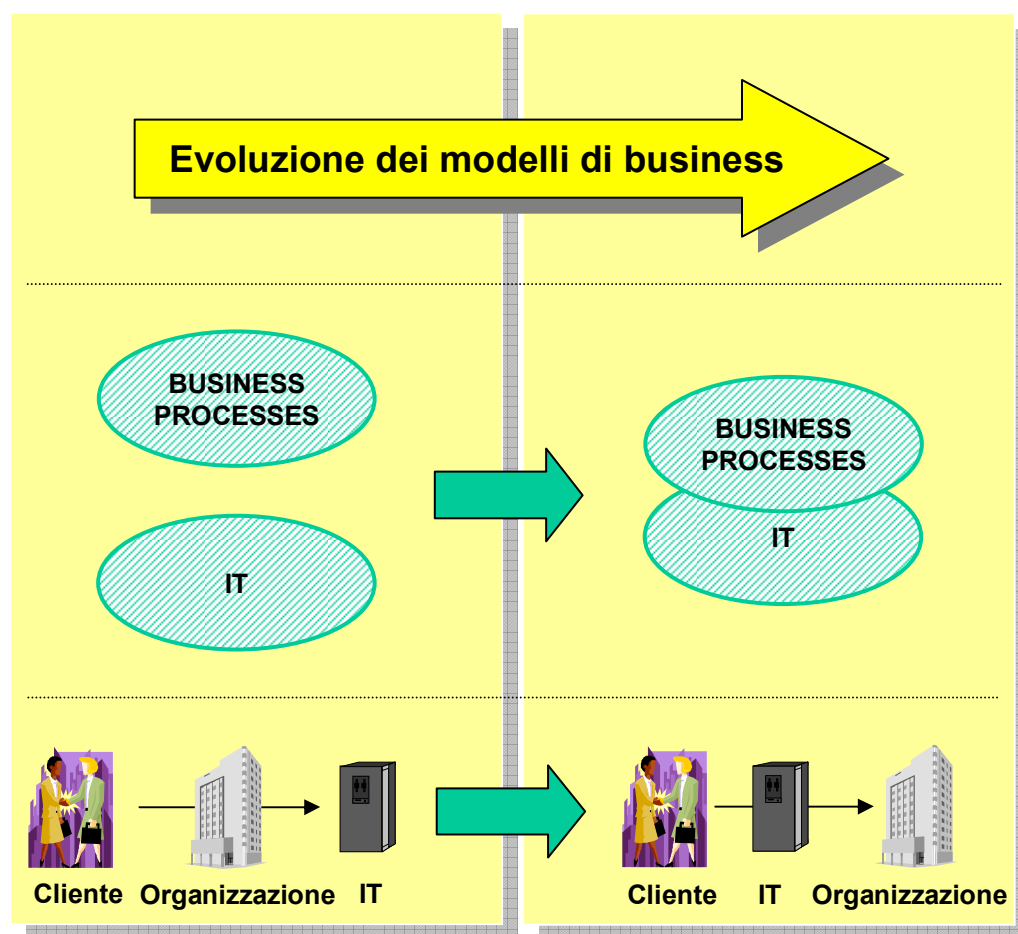
- **Frode interna**
- **Frode esterna**
- **Rapporto di impiego e sicurezza sul posto di lavoro**
- **Pratiche connesse con la clientela, i prodotti e l'attività**
- **Danni a beni materiali**
- **Disfunzioni e avarie di natura tecnica**
- **Conformità esecutiva e procedurale**



Alcuni esempi mostrano le conseguenze di questi rischi sul business di diversi settori di industria, quando non adeguatamente preparati alla mitigazione e controllo.

- Los Angeles County Pension Fund ha perso 1.2 miliardi di dollari in 20 anni a causa di errori di programma.
- Il Mars Orbiter, costato 125 milioni di dollari, è stato perso perchè il team di ingegneri ha usato il sistema metrico inglese invece che il sistema metrico decimale per le principali operazioni di controllo.
- Circa la metà delle banche norvegesi sono andate offline dopo che per un errore operativo è stato cancellato il data warehouse invece di inizializzare 280 nuovi dischi.
- Volkswagen ha perso 250 milioni di euro per una frode sui cambi valuta basata su computers.
- Tre olandesi di 19, 22 e 27 anni sono stati arrestati perchè controllavano circa un milione e mezzo di computer come parte di una botnet mondiale.
- Solo nel mese di agosto 2005 sono stati rilevati 13,776 attacchi (phishing) verso circa 900 aziende.

L'IT costituisce una "utility" indispensabile a sostegno della crescita ed evoluzione del business, ma rappresenta allo stesso tempo una significativa fonte di rischi.



In assenza di adeguati controlli, il crescente impiego di tecnologie altamente automatizzate può trasformare il rischio di errori manuali di trattamento dei dati in rischio di disfunzioni sistemiche, dato il sempre maggiore ricorso a sistemi globalmente integrati.

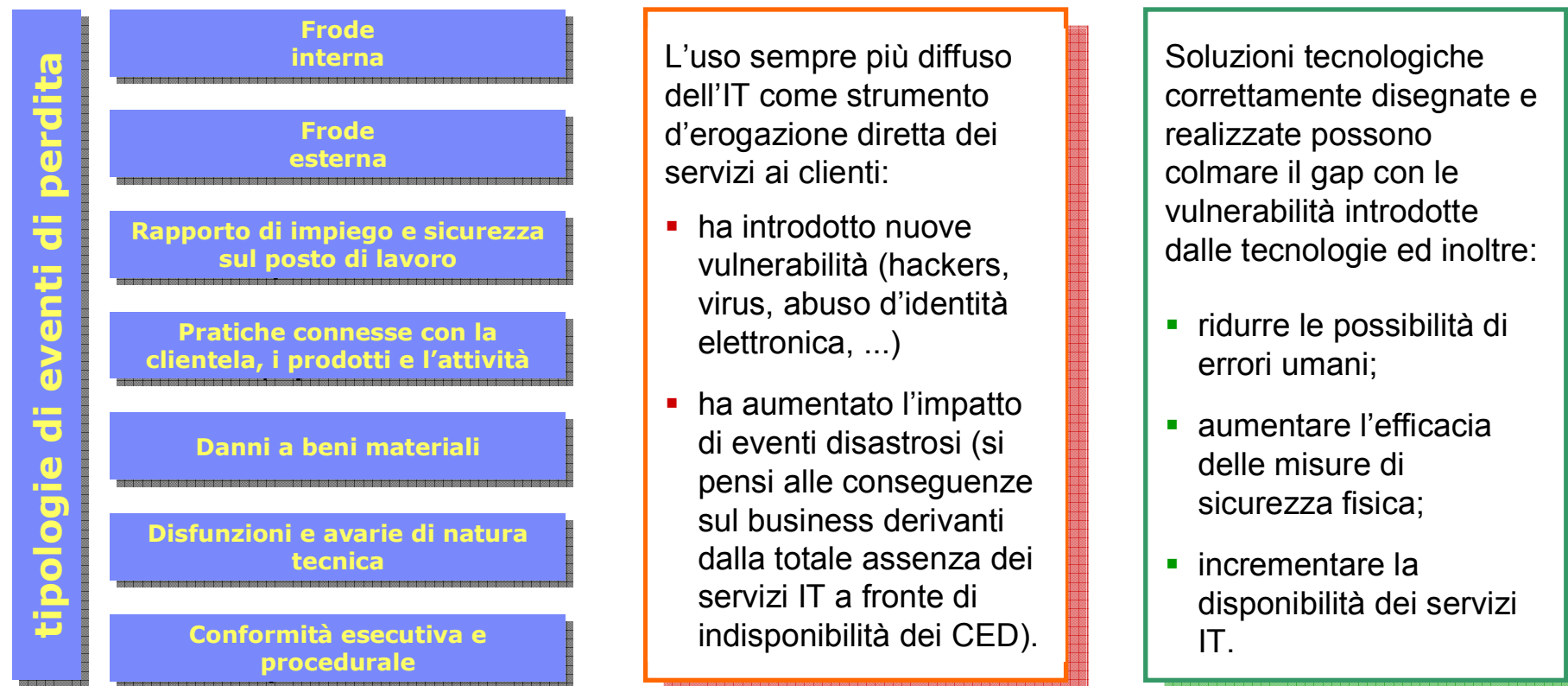
L'espansione del commercio elettronico comporta rischi potenziali (ad esempio, frodi interne ed esterne, sicurezza dei sistemi) di cui non si ha ancora completa padronanza.

Operazioni di acquisizione, fusione, scorporo e consolidamento di notevole entità mettono alla prova la funzionalità dei sistemi nuovi o di quelli di recente integrazione.

(tra le motivazioni del Comitato di Basilea)



La tecnologia è tra le principali cause di incremento del rischio operativo ma, allo stesso tempo, è mezzo fondamentale per la riduzione dei rischi entro soglie accettabili.

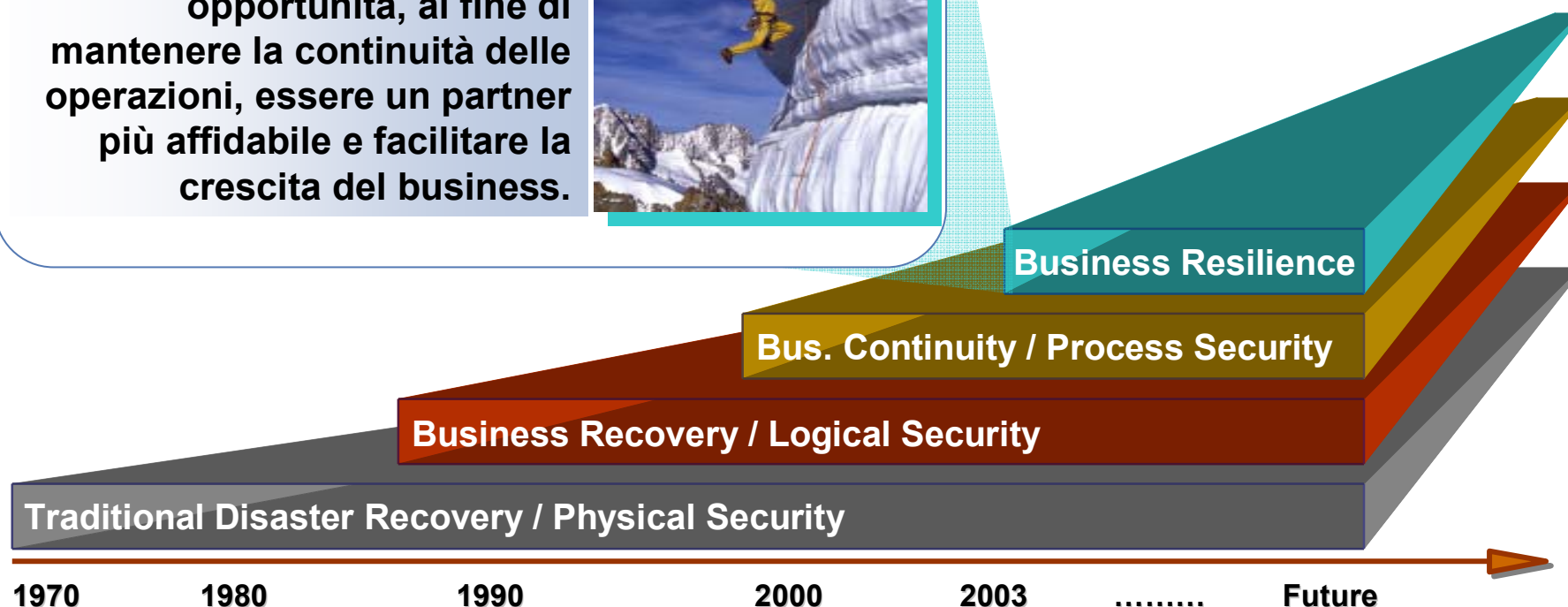




La IBM ha sviluppato un framework chiamato Business Resilience con l'obiettivo di valutare il livello complessivo di resilienza delle infrastrutture dei clienti ed aggregare le soluzioni in grado di aumentarla.

Business resilience è la capacità di...

... adattarsi rapidamente e reagire ai rischi, come alle opportunità, al fine di mantenere la continuità delle operazioni, essere un partner più affidabile e facilitare la crescita del business.





La tipologia delle situazioni alle quali l'infrastruttura deve sapersi adeguare senza generare impatti significativi spazia da eventi tecnologici a eventi sociali e naturali con una sostanziale coincidenza con quelli previsti nell'ambito del rischio operativo.

Ambientali

- Natural Disasters
- Workplace Issues
- Contaminations / Fuel Spills

Tecnologiche

- IT Infrastructure
- Technology Adoption
- Innovation and Trends
- 24x7 Expectations



Sociali

- Terrorism
- Cyber Attacks
- Biological Threats
- Employee Sabotage
- Industrial Espionage

Politiche

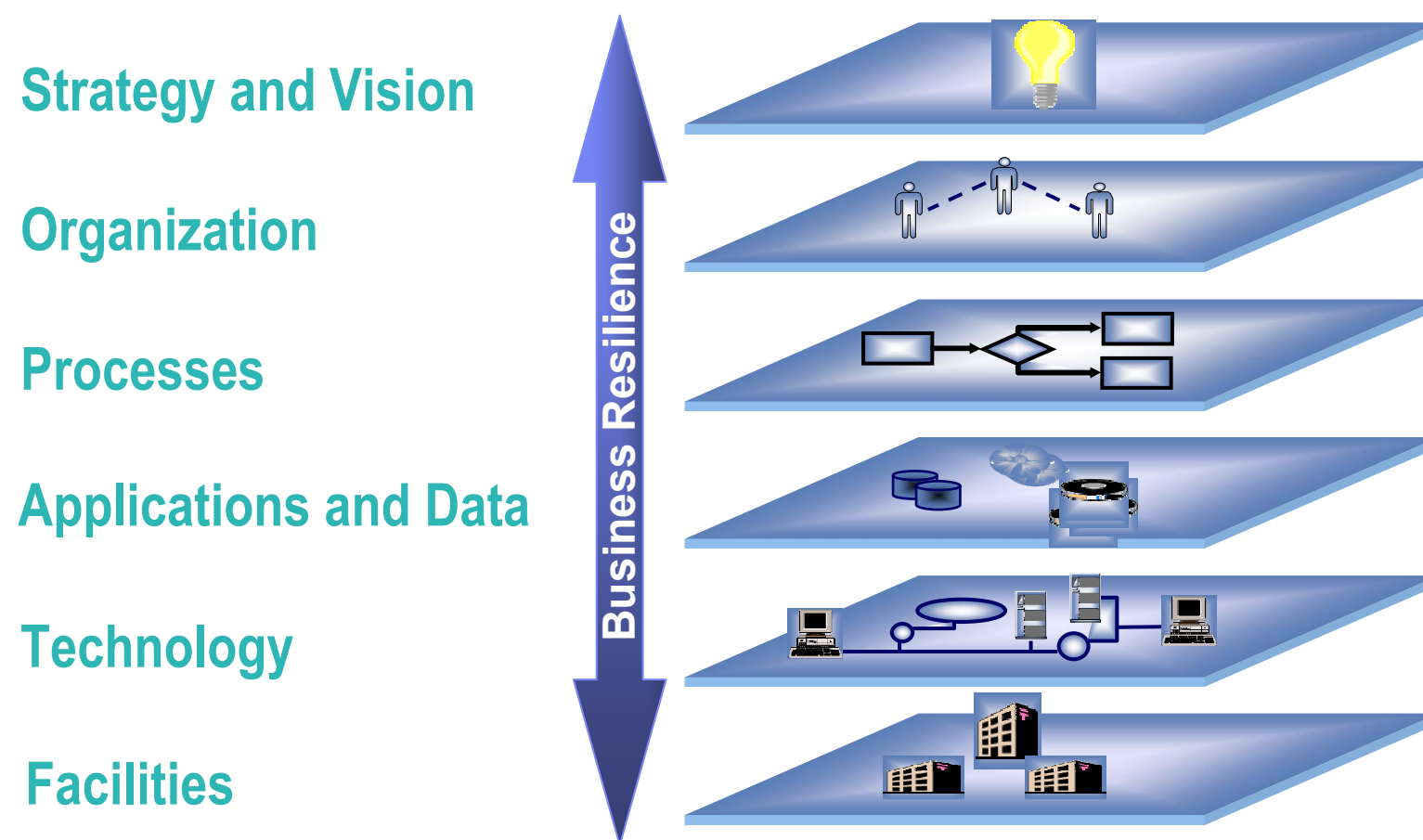
- Regulation
- Deregulation
- Incentives
- Legal

Economiche

- Global Marketplace
- Partners/Suppliers
- Demand Elasticity



La soluzione è stata strutturata in sei livelli di intervento e circa 130 componenti, tutti da indirizzare per misurare le esposizioni e raggiungere il livello di business resilience coerente con le esigenze dell'azienda.





La soluzione è stata strutturata in sei livelli di intervento e circa 130 componenti, tutti da indirizzare per misurare le esposizioni e raggiungere il livello di business resilience coerente con le esigenze dell'azienda.

Strategy and Vision

- Governance strategy
- Financial strategy
- Security strategy
- Availability strategy
- Communications strategy
- New product/services strategy
- Risk management

Processes

- Business Process
 - Sales order
 - Finance and accounting
 - Enterprise resource planning
 - Customer relationship management
 - Supply chain management
 - Quality management
 - Research and development
- IT Process
 - Change management
 - Problem management
 - Incident management
 - Availability management

Strategy and Vision

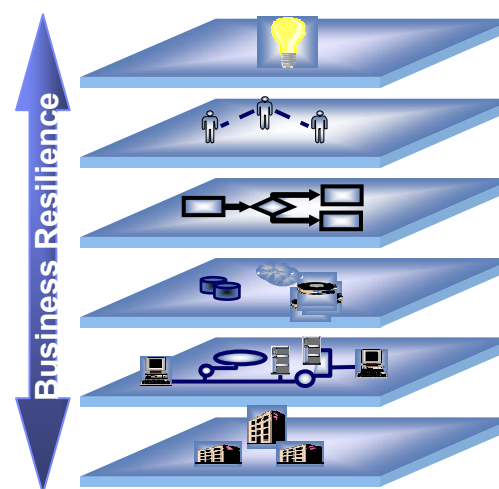
Organization

Processes

Applications and Data

Technology

Facilities



Facilities

- Physical and logical security
- Access controls
- Power protection
- Environmental considerations

Organization

- Roles and responsibilities
- Structures
- Human resource management
- Skills
- Cross-organizational cooperation

Applications and Data

- Data and application security
- Data storage
- Application architecture and design
- Backup and recovery

Technology

- Hardware architectures
- System software
- Middleware
- Networks



La gestione e il controllo dei rischi operativi richiede un approccio multi-disciplinare, che comprende i temi della sicurezza e della business continuity, oggetto dei prossimi interventi.

