Dalla Gestione del Rischi di Compliance alla Governance del Rischi aziendali

a cura di Claudio Ruffini

Conosciamoci

Claudio Ruffini

E-mail: claudio.ruffini@gmail.com

Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Introduzione ai processi aziendali
  - Eventi
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

Indice e scaletta del corso

- **Seconda parte: una metodologia per l'analisi e la gestione del rischio**
  - Risk assessment .
    - Risk Prioritization
    - Risk Identification
    - Risk Evaluation
  - Risk Management
    - Risk Measurement
    - Risk Monitor
    - Risk Mitigation

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Indice e scaletta del corso

- **quarta parte: Aspetti pratici e criticità di un progetto di risk management**
  - Aspetti organizzativi del Risk Management
  - Piani di azione e responsabilità
  - Criticità di progetto

Indice e scaletta del corso

- **quinta parte: esempio di un progetto di Compliance risk management in una banca italiana**
  - Esame delle fasi di un progetto reale in banca
  - Qualche esempio reale di report
  - Analisi di un prodotto di gestione del Rischio

Quali sono le vostre aspettative sul corso ?

Riferimenti

- **Riferimenti bibliografici**
  - Gianpaolo Gabbi, Michele Marsella, Marco Massacesi
    “Il Rischio operativo nelle banche”
    Egea, 2005
  - Thomas H. Davenport
    "Innovazione dei processi"
    Franco Angeli, 1994
  - Comitato di Basilea per la vigilanza bancaria
    “Nuovo accordo di Basilea sui requisiti patrimoniali"
    BIS, 2004
  - Michael G. Silverman
    «Compliance Management»
    Mc Graw Hill, 2008
  - Rupert Limetani, Normanna Tresoldi
    «Compliance Handbook»
    Bancaria Editrice 2012

Premessa

Signori, buongiorno.

Io sono qui per parlare, voi per ascoltare;
se qualcuno di voi termina prima di me, cortesemente me lo faccia sapere!

Anonimo inglese

Prima parte:
Introduzione al rischio

Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

Definizioni di rischio

Qualche domanda di stimolo

Che cosa è un rischio?

Quando si prende un rischio?

Come si misura un rischio?

Che differenza c'è tra rischio di progetto e rischio di processo?

Che rischi corro introducendo un nuovo sistema software in una organizzazione?

Che differenza c'è tra un giocatore d'azzardo e un Risk Manager?

E' possibile vendere un rischio?

E' vero che "chi non risica non rosica"?

Provate voi

…

Definizioni di Rischio

- **Una possibile definizione di Rischio è:**

  "*l'eventualità di subire un danno connessa a circostanze più o meno prevedibili*." (Enciclopedia Treccani)

In questa prima definizione si incontrano dei concetti che ritroveremo in forma più rigorosa:

- Il rischio è in qualche modo connesso alla "**probabilità**" di un evento dannoso
- Il rischio è proporzionale alla "**gravità**" del possibile danno.

- **Una seconda e più rigorosa definizione è:**

  "la variabilità dei possibili risultati intorno ad un valore atteso."

  - Questa seconda definizione estende il concetto di rischio anche a eventi non dannosi ma per esempio profittevoli. In generale si capisce che il rischio è legato allo **scostamento da un valore obiettivo** "target" stimato.

Diversi approcci al rischio

- **Esistono diversi modi di vedere il Rischio in funzione del contesto in cui questi vengono analizzati:**
  - **Aziende strategiche** (Energia, Telecomunicazioni, Militari, unità di crisi etc..): in questo caso un danno o una cattiva gestione dei rischi può avere impatti devastanti; quindi orientamento alla business continuity, alla sicurezza e ai controlli;
    - Errori, malfunzionamenti non sono tollerati, aumento dei controlli; l'imponderabile deve essere diminuito al massimo e bisogna continuare ad operare anche in presenza di emergenze e di eventi indesiderati.
  - **Finanza** (Assicurazioni, Banche, SIM, etc…): fanno della gestione del Rischio un business; orientamento alla valutazione e quindi alla gestione dei rischi;
    - Un certo numero di errori e di malfunzionamenti sono tollerati; si convive con i rischi; in alcuni vengono valutati e misurati e si cerca di comprare e vendere i rischi (opzioni, strumenti derivati, strumenti di copertura, etc…) o di assicurarsi da essi (garanzie, polizze, patrimoni di vigilanza).
  - **Altre Aziende** (Manifatturiere, Commercio, Artigiani, PMI, etc …) vedono il rischio solo come un danno potenziale; Più l'azienda è piccola e più il rischio viene visto come un "non-problema".
    - Nelle PMI e nel mondo artigiano i rischi sono spesso del tutto ignorati; vige un atteggiamento di incauto ottimismo tipico dell'imprenditore; "a me non capiterà mai …";

Diversi approcci al rischio

- **Il settore finanziario è quello che ha analizzato con più rigore il problema del rischio sebbene non sia il settore che "rischi" di più.**
  - L'approccio delle aziende "strategiche" tende a porre l'attenzione sull'analisi della probabilità dei possibili eventi dannosi e tende a neutralizzarli aumentando al massimo il livello di controlli. Ci sono aziende che arrivano ad avere diversi livelli di controllo incastonati uno sull'altro. Questo approccio tende ad ignorare ogni analisi sulla possibile perdita potenziale in caso di evento dannoso.
  - L'approccio delle aziende "Finance" da un punto di vista metodologico è quello che tende ad analizzare tutti gli aspetti del rischio, comprese le valutazioni economiche del danno e dei possibili rimedi in caso di evento dannoso. Non si sottovaluta poi l'approccio ai controlli e all'analisi della probabilità che spesso è portata a livelli di business continuity molto elevata. Una interruzione del servizio può causare molte perdite economiche. Questo è sufficiente per giustificare progetti importanti (come nel caso delle aziende strategiche) di gestione del rischio. La differenza è che il rischio non è più solo visto come evento dannoso ma anche come fonte di business
  - E' per questo motivo che ci appoggeremo alle metodologie tipicamente bancarie e assicurative per analizzare il problema.

Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Oiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

Basilea 2

- **Il Comitato di Basilea (*) nel 1988 ha formulato una proposta recepita dagli organi di vigilanza di più di 150 paesi sviluppati volta a regolamentare il livello di rischio che un intermediario finanziario può assumere. In pratica ha posto dei vincoli sul patrimonio delle banche in funzione del livello di rischio finanziario a cui sono esposte.**
  - Questo ha dato un notevole impulso alla gestione dei rischi e ad una loro valutazione economica
  - Ha migliorato le condizioni di solvibilità delle banche
  - Ha reso più stabili i mercati finanziari
- **I problemi connessi ad alcune distorsioni derivanti da operazioni di arbitraggio ha portato nel 2004 ad una revisione dell'accordo originario noto come "Basilea 2" che ha migliorato l'impianto complessivo originario portando alcune novità significative**

(*) Il **Comitato di Basilea** per la vigilanza bancaria, è un'organizzazione internazionale istituita dai governatori delle Banche centrali dei dieci paesi più industrializzati (G10) alla fine del 1974, che opera sotto il patrocinio della Banca per i Regolamenti Internazionali (Bank for International Settlements: BIS).Il suo scopo è quello di promuovere la cooperazione fra le banche centrali ed altre agenzie equivalenti allo scopo di perseguire la stabilità monetaria e finanziaria.

Struttura dell'accordo di Basilea 2

- **Le novità e la struttura del nuovo accordo sul capitale di Basilea 2 riguardano:**
  - **Pilastro 1**: un nuovo sistema di requisiti patrimoniali che tengano conto non solo dei rischi finanziari di mercato e di credito ma anche dai rischi operativi. Prevede diverse modalità di valutazione del calcolo del patrimonio equivalente in funzione dei rischi assunti dalla banca. Le diverse modalità (standard, AMA) sono applicabili in funzione della complessità e dei requisiti organizzativi che la banca vuole adottare. L'idea base è che più è sofisticato l'approccio (AMA) meno capitale posso mettere a garanzia dei rischi ma maggiore sono i controlli e i requisiti organizzativi richiesti.
  - **Pilastro 2**: Un nuovo processo di revisione da parte degli organi di vigilanza nazionali volto ad assicurare che le banche si dotino di sistemi di misurazione e controllo dei rischi .
  - **Pilastro 3**: Un utilizzo più efficace della disciplina di mercato quale strumento adatto per integrare il ruolo degli organi di vigilanza nel garantire la solvibilità complessiva del sistema; in pratica vuol dire aumentare le regole di trasparenza relative alle condizioni di rischio e di patrimonializzazione delle banche. Questo a tutela del mercato e quindi anche del consumatore.

Esempi tratti da documento Basilea 2

Titolo II Capitolo 5 Sez II

GOVERNO E GESTIONE DEI RISCHI OPERATIVI

Per il conseguimento di un efficace ed efficiente sistema di gestione e controllo dei rischi operativi, un ruolo fondamentale è attribuito agli organi aziendali. Gli organi con funzioni di supervisione strategica, gestione e controllo, ciascuno secondo le rispettive competenze e responsabilità, definiscono le linee generali del sistema, sono responsabili della sua realizzazione, vigilano sul suo concreto funzionamento, verificano la sua complessiva funzionalità e rispondenza ai requisiti previsti dalla normativa.

REQUISITI ORGANIZZATIVI

La banca istituisce una funzione di controllo dei rischi operativi.I compiti che spettano a tale funzione attengono alla progettazione, sviluppo e manutenzione dei sistemi di gestione e di misurazione dei rischi operativi; tali attività riguardano, tra l'altro, il sistema di raccolta e conservazione dei dati, il sistema di reporting nonché la valutazione del profilo di rischio operativo;

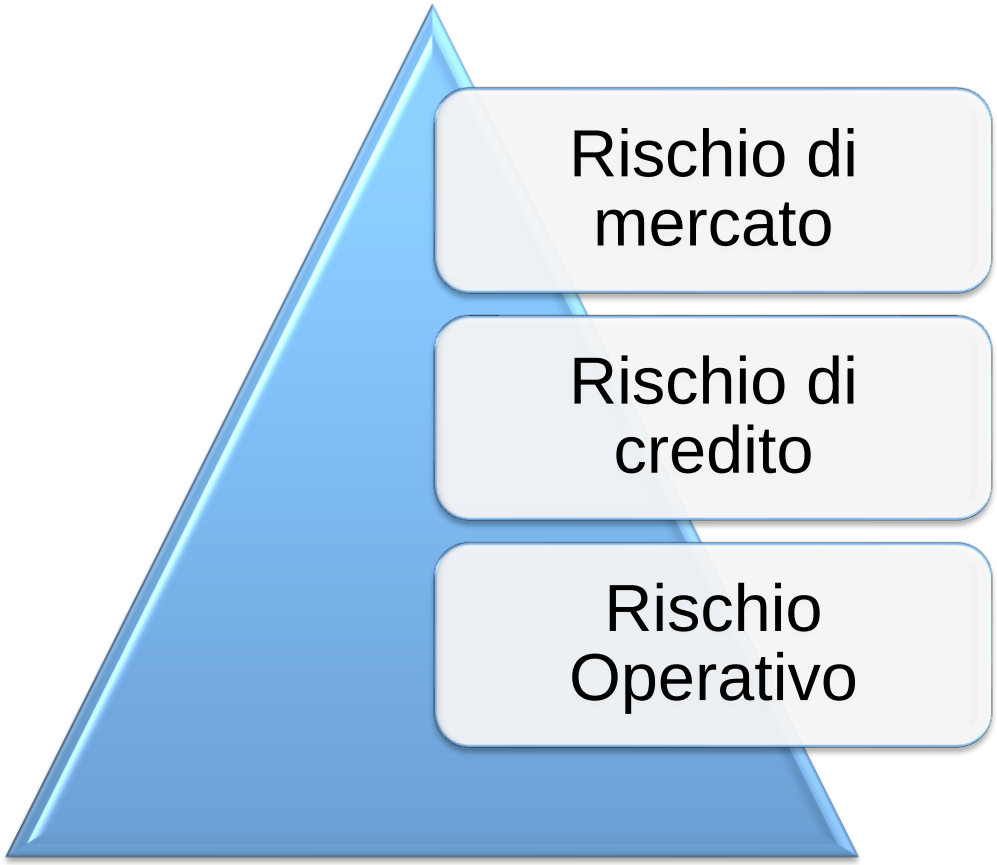
Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

Il Rischio in una Banca

Torniamo alla nostra definizione di rischio come

"la variabilità dei possibili risultati intorno ad un valore atteso."



Rischio di mercato

- **Il Rischio di mercato è inteso come il rischio di fluttuazioni del valore delle posizioni connesse a variazioni inattese dei fattori di mercato quali tassi di cambio, prezzi di titoli azionari, tassi di interesse, prezzi di commodities.**
  - Esempio 1: Acquisto un titolo azionario FIAT a Euro 13,96 nella speranza che il titolo nei prossimi 6 mesi salga del 3%. Il Rischio che corro è che il titolo rimanga sotto il valore target che mi sono fissato.
  - Esempio 2: Acquisto un BTP a 2 anni (tasso fisso del 5%) nella speranza che che i tassi scendano nel periodo. Il rischio è che i tassi non scendano del valore che mi sono prefissato.
- **Da notare che nel caso del rischio di mercato il rischio è simmetrico rispetto al target desiderato. Se il prezzo del titolo sale oltre il 3% io non solo non ho danni ma ho un profitto. Anzi più rischio più ho profitto. Criterio di proporzionalità diretta rispetto al rendimento. Non sempre sarà così!**

Rischio di Credito

- **Il Rischio di Credito è rappresentato dalla possibilità di fluttuazioni del valore di mercato del portafoglio di attività connesse a variazioni del merito creditizio (Es. Rating) delle controparti delle operazioni di impiego o di posizioni fuori bilancio**
  - L'esempio più semplice è il rischio di insolvenza connesso ad operazioni di prestito (mutui) effettuato nei confronti di aziende o privati. Ovvero il danno che ha una banca derivante dalla dichiarazione di insolvenza di un debitore. La stessa cosa può essere detta relativamente al rischio per una azienda o un privato derivante dalla impossibilità di regolare il corrispettivo dovuto a causa di fallimento o situazione di crisi di una azienda cui ho effettuato prestazioni professionali.
  - Più complesso e raffinato il rischio derivante dal deterioramento del merito creditizio (rating) di una società o di una intera nazione di cui posseggo titoli o obbligazioni.
- **Anche il rischio di credito è simmetrico e rispetta una logica di proporzionalità diretta rispetto al rendimento.**

Rischio Operativo

- **Il rischio Operativo è quello più difficile da definire. In una prima e più facile definizione può essere definito in negativo come l'insieme di tutti i rischi di una banca non riconducibili a nessuno dei due rischi precedenti (mercato, credito).**
- **Ecco di seguito alcune definizioni proposte da alcune grandi banche:**
  - "*The potential of any activity to damage the organization, including physical, financial, legal risks and risks to business relationships*"
  - *"The risk that deficiencies in information systems or internal controls will result in financial loss, failure to meet regulatory requirements or an adverse impact on the bank's reputation."*
  - *"The risk of loss through inadeguate systems, controls and procedures, human error or management failure."*
- ***Il Rischio operativo è in sintesi il rischio che comportamenti illegali o inappropriati delle risorse umane, carenze tecnologiche, errori o carenze nei processi produttivi e fattori esterni possano generare perdite nello svolgimento dell'attività dell'impresa.***

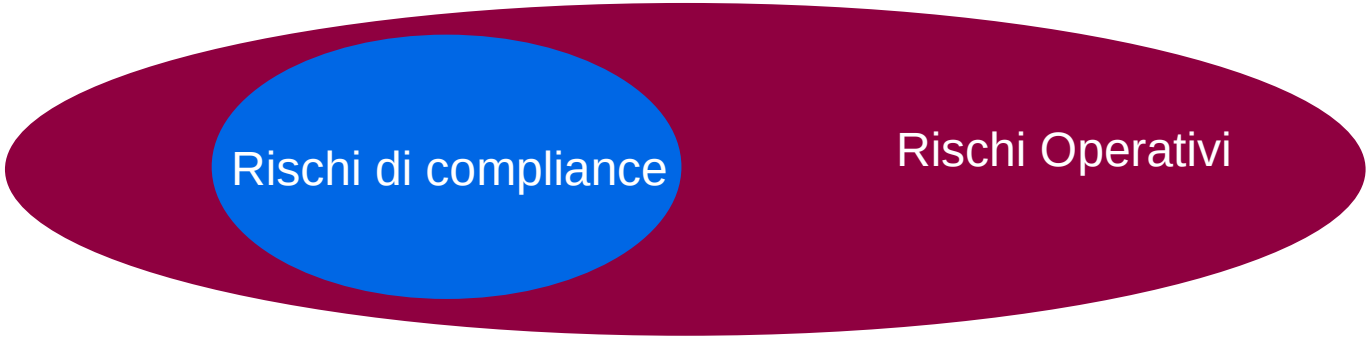
Caratteristiche del Rischio Operativo

- **Alcune caratteristiche peculiari del RO**
  - Il Rischio Operativo può essere assunto involontariamente: come semplice conseguenza delle attività operative svolte dalla istituzione. In particolare se ritengo troppo rischioso comprare un certo tipo di opzione o altro strumento finanziario posso sempre non comprarlo oggi, in quel mercato, con quella controparte. Non mi esporrò a rischi di mercato o di credito. Oppure posso metter in atto operazioni di copertura di rischio con strumenti derivati. Per il RO è più difficile farlo. Il solo fatto di operare, di esistere come banca, azienda mi espone a dei rischi.
  - Il RO si configura principalmente come Rischio Puro. Posso solo perdere o il guadagno involontario è completamente coperto da gli effetti negativi reputazionali. In questo senso è asimmetrico e viene a mancare la proporzionalità diretta tipica degli altri rischi per cui maggior rischio corrisponde a maggior profitto.
  - E' difficile misurarli e gestirli ed è ancor più difficile valutarli economicamente.

Rischio Compliance Vs Rischi operativo

Più rigorosamente (definizione di Basilea 2) è il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni;

<u>è compreso il rischio legale (o di compliance)</u> ovvero il rischio derivante da violazione di leggi o regolamenti, da responsabilità contrattuale o extra-contrattuale ovvero da altre controversie.



Rischio di compliance

- **Il rischio di compliance è il rischio per una organizzazione di non essere adempiente agli obblighi normativi imposti dalle leggi o da regolamenti interni.**
- **Una organizzazione ha il dovere di rispettare le leggi e di fare in modo che tutte le persone che lavorano per conto di essa rispettino le leggi e «il codice etico» scritto o implicito nell'organizzazione stessa.**
- **Ha quindi implicitamente l'obbligo di formare, informare e controllare relativamente al rispetto delle leggi**
- **Per la mancanza di adeguato controllo su alcuni tipi di reati, da qualche anno, la legge punisce l'azienda direttamente sul proprio capitale con sanzioni anche importanti (231/01)**

Rischio Compliance

- **DEFINIZIONE**

Le Istruzioni di vigilanza di Banca d'Italia definiscono il rischio di Compliance come il Rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni da reputazione in conseguenza di violazioni di norme imperative, di legge, di regolamenti ovvero di norme di autoregolamentazione (statuti, codici da autocondotta/autodisciplina)

Rischio di compliance

- **Esempi di leggi che hanno rilevanza per la compliance aziendale**
  - Legge sulla Privacy
  - Legge sulla responsabilità degli enti
  - Legge sulla sicurezza sul lavoro
  - Antiriciclaggio
  - Codice del consumatore
  - Etc...
- **Il danno derivante da un rischio di compliance può essere sia la sanzione determinata dalla legge, sia una conseguenza penale per chi ha avuto la responsabilità della violazione, sia un danno reputazionale se il delitto o la violazione hanno conseguenze che possono incidere sull'immagine dell'azienda stessa.**

Fattori che possono causare eventi dannosi

- **Il Comitato di Basilea propone la seguente classificazione in 4 fattori causali:**
  - **Risorse Umane:** sono fattori che fanno riferimento ad eventuali errori, frodi, violazioni di regole e procedure interne e, in generale, a problemi di incompetenza o negligenza del personale:
    - Esempio: nel Maggio del 2001 un dealer di una grande banca inglese ha erroneamente inserito una negoziazione di 300 Milioni di dollari nel mercato azionario invece dell'importo desiderato di 3 milioni, causando una riduzione dell'indice FTSE 100 di 120 punti.
  - **Processi**: sono fattori relativi ai processi produttivi, includono eventi quali la violazione della sicurezza informatica connessi ad insufficienti controlli, (security risk); errori nel regolamento di operazioni con la controparte (settlement risk); errori di contabilizzazione, registrazione o documentazione delle transazioni (transaction risk); errori nei sistemi di misurazione dei rischi derivanti da problemi sul metodologie utilizzate (model risk)

Rischi

- **Fattori esterni:** eventi che sfuggono al controllo della banca (esempio cambiamento di un contesto politico fiscale, o legislativo che arrecano danno alla redditività della banca(Rischio Ambientale); atti criminali compiuti da soggetti esterni alla banca come furti, atti vandalici o terrorismo; eventi naturali come terremoti, inondazioni (rischio fisico)
- **Tecnologia**: i fattori legati alla tecnologia comprendono i problemi relativi ai sitemi informativi, agli errori di programmazione nelle applicazioni, interruzione nella struttura di rete, fino a includere eventuali fallimenti nei sistemi di telecomunicazioni;

Alcune altri tipi di rischio

- Rischio reputazionale
  - Il danno derivante dalle conseguenze economiche dell'alterazione del giudizio e del rapporto fiduciario percepito dalla clientela della azienda,
- Rischio di strategico
  - È definito come una contrazione dei margini non dovuti ai rischi di mercato, credito ed operativo e deriva da inattesi cambiamenti del contesto competitivo, comportamenti dei clienti, o dal mancato riconoscimento delle tendenze in atto nel settore bancario oppure in errate conclusioni riguardo queste tendenze. Questo può portare a decisioni che risultano svantaggiose per gli obiettivi di lungo periodo e possono risultare irreversibili o difficili da recuperare..
- Rischio immobiliare ("*real estate risk*")
  - È definito come le potenziali perdite derivanti dalle fluttuazioni del portafoglio immobiliare di proprietà della banca, che siano detenute dalle società, trust immobiliari e "*special-purpose vehicle*" mentre sono esclusi gli immobili dati a garanzia da parte della clientela.
- Rischio di investimenti azionari ("*financial investment risk*")
  - Rappresenta le potenziali perdite di valore degli investimenti finanziari non speculativi in società esterne al Gruppo, secondo la definizione di gruppo ai fini di consolidamento contabile. Non sono quindi considerate le posizioni appartenenti al trading book.

Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

La visione “per processi” permette una migliore conoscenza del funzionamento di un’azienda / 1

- **Un processo aziendale può essere definito come:**
  - Un insieme di attività strutturate,
  - Collegate tra loro e misurate,
  - Progettate per trasformare un *input* in un *output*, aggiungendo valore,
  - Compiute da attori ben definiti

- **Un processo permette quindi ad un’organizzazione di compiere ciò che è necessario per produrre valore per i propri clienti**

- **La definizione dei processi di un’area aziendale è presupposto indispensabile per la progettazione e la realizzazione di un sistema informativo a supporto**

La visione “per processi” permette una migliore conoscenza del funzionamento di un’azienda / 2

- **Analizzare un azienda (od un sistema informativo) utilizzando un approccio per processi significa adottare il punto di vista del “cliente” del processo stesso**
  - Questi può essere un nuovo processo, una funzione aziendale oppure un utente esterno all’azienda (ad es. un fornitore, un cliente, un partner)

- **Una misura di valutazione del processo è, quindi, la soddisfazione del “cliente” nei confronti del risultato del processo stesso**

La visione “per processi” permette una migliore conoscenza del funzionamento di un’azienda / 3

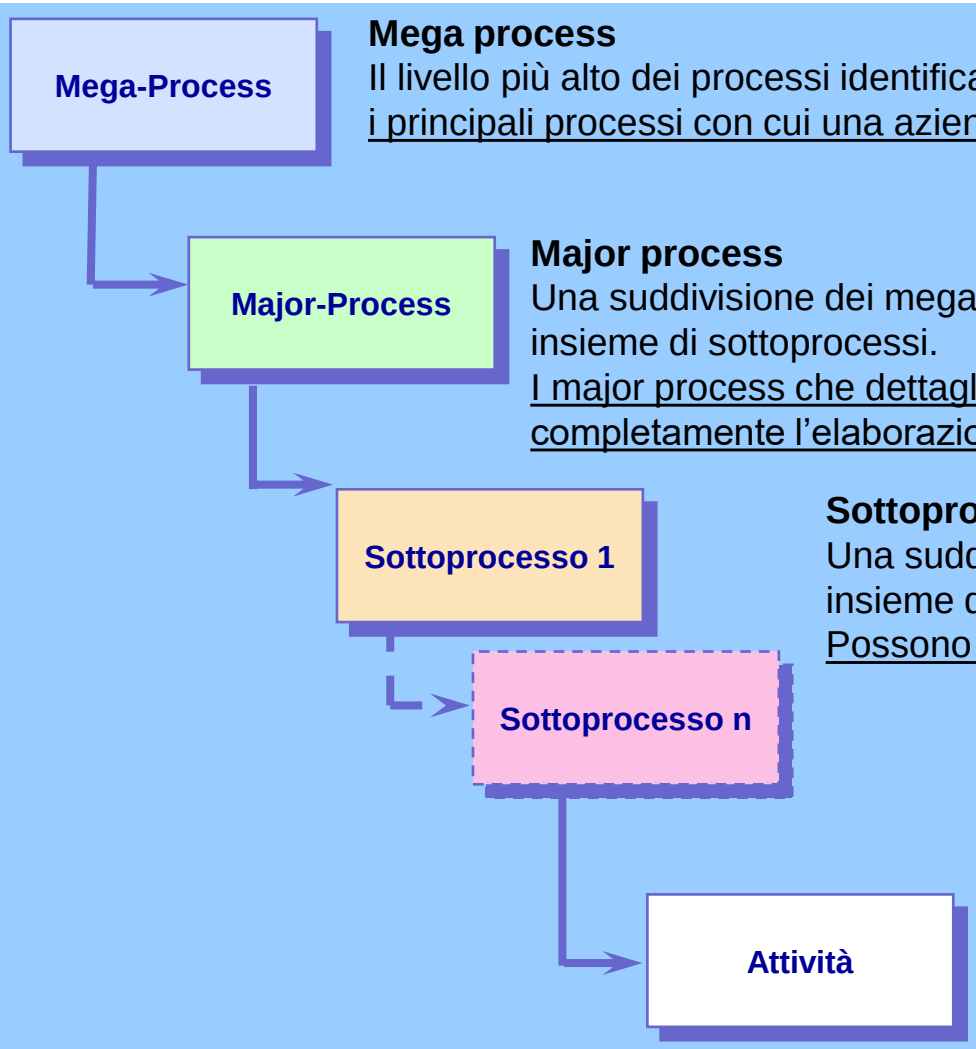
- **Il vantaggio fondamentale di una visione per processi è l’<u>incremento del valore per il cliente finale</u>, ottenuto grazie a:**
  - Una chiara visione delle attività da svolgere per trasformare un input in output
  - Una chiara definizione dei ruoli e delle responsabilità
  - Un miglior controllo sui prodotti / servizi finali
  - Una migliore gestione delle interrelazioni funzionali

- **La visione per processi permette infatti di evidenziare prontamente eventuali errori (*nelle attività, dati, ruoli…*) e di procedere quindi alla loro eliminazione mediante riallineamento (*delle attività, dati, ruoli…*) agli obiettivi di processo**

La modalità di strutturazione tradizionale delle aziende è spesso causa di inefficienze

- Le aziende sono generalmente strutturate per funzioni separate (“*verticali*”)
- I flussi di lavoro sono invece interfunzionali (“*orizzontali*”)
- Questo genera vuoti o sovrapposizioni di responsabilità che peggiorano l’efficienza e l’efficacia complessiva.

Gerarchia del modello dei processi



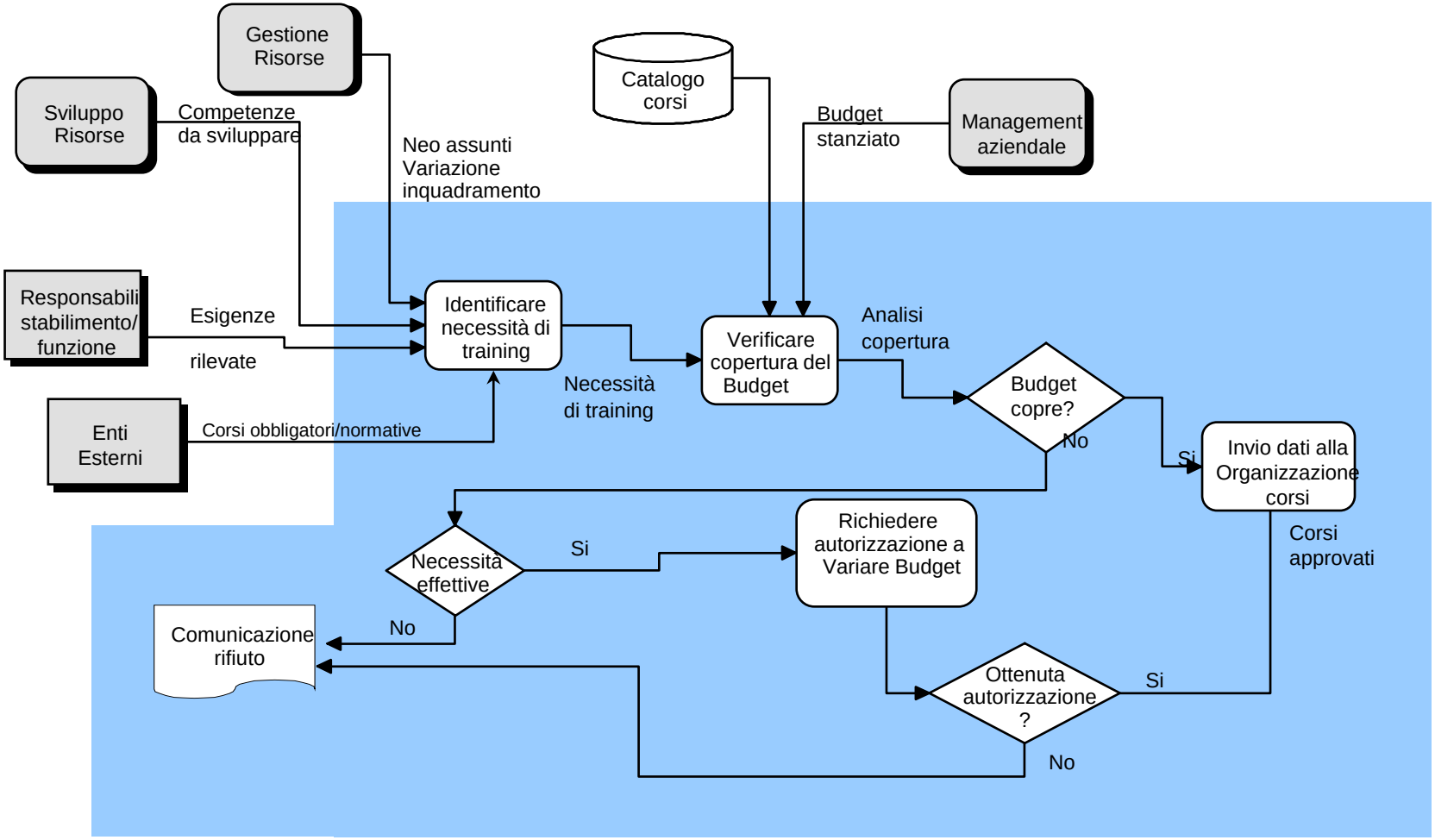
Mega process
Il livello più alto dei processi identificato da una impresa:
i principali processi con cui una azienda svolge la propria missione

Major process
Una suddivisione dei mega process, che rappresenta a sua volta un insieme di sottoprocessi.
I major process che dettagliano un mega process ne svolgono completamente l'elaborazione.

Sottoprocesso
Una suddivisione dei major process che rappresenta un insieme di altri sottoprocessi o delle relative attività.
Possono esistere più livelli di sottoprocessi

Attività
Una porzione di lavoro elementare che trasforma un input in un output per un cliente interno od esterno.
È eseguita in un arco temporale breve (in un giorno o meno) ed all'interno di una sola unità organizzativa

Un esempio di scomposizione di sottoprocesso in attività: "Raccogliere necessità di training"



Basilea 2

- **La banca deve classificare le attività aziendali nelle otto linee e di business regolamentari elencate nella tavola precedente con precise regole**
  - Tutte le attività devono essere mappate
  - Nei casi di attività che fanno capo a più linee di business si assegna secondo il criterio del business prevalente
  - È possibile usare prezzi interni di trasferimento per allocare le attività
  - I criteri di classificazione e mappatura devono essere rivisti in funzione dei cambiamenti aziendali e sottoposte a revisioni interne

Linee di *Business Elenco delle attività Basilea 2*

1. Corporate finance	2. Trading and sales	3. Retail banking	4. Commercial banking
• *Fusioni, Acquisizioni, Attività di collocamento (OPA, OPV, collocamenti privati – c.d. blocchi, emissioni obbligazionarie). Investment Banking in equity e capitale di debito (IPO, privatizzazioni, syndications, piazzamenti privati secondari, sottoscrizioni, etc.). Valutazioni d'azienda. Cartolarizzazioni per conto terzi. Gestione traordinaria di finanza d'impresa. Aumenti di capitale (solo come lead manager). Servizi di consulenza e ricerca (struttura di capitale, strategia industriale, undertakings, ristrutturazione, etc.). Consulenza d'investimento come business specifico.*	• *Negoziazione in conto proprio del portafoglio di trading. Gestione della tesoreria e funding in conto proprio (Asset & Liability Management, etc.). Cartolarizzazioni in conto proprio. Ricezione/trasmissione ed esecuzione di ordini verso clienti corporate e clienti professionali 2. Attività di consulenza, assunzione a fermo, collocamento di strumenti finanziari/prodotti assicurativi (bancassurance, fondi, GPM, GPF, equity, bond, derivati, etc) verso clienti corporate e clienti professionali.*	• *Prestiti/Depositi (anche a clienti "private" e SME). Garanzie e impegni finanziari (anche a clienti "private" e SME). Credito al consumo per clienti retail. Leasing/Factoring. Altri tipi di transazioni con controparti retail non allocati in altre "linee di business". Servizi ancillari ad attività retail come servizi di incasso e pagamento (carte di debito e di credito, trasferimento fondi ed altri pagamenti per conto di clienti, cambio valuta, etc.) e custodia ed amministrazione titoli.*	• *Prestiti/Depositi. Garanzie e impegni finanziari. Leasing/Factoring. Finanziamenti all'esportazione e al commercio. Altri tipi di transazioni con controparti corporate non allocati in altre "linee di business". Servizi ancillari ad attività corporate come servizi di incasso e pagamento (trasferimento fondi ed altri pagamenti per conto di clienti, cambio valuta, etc.) e custodia ed amministrazione titoli. Reddito netto (ad esempio cedole e dividendi) su portafogli non di trading.*

Linee di *Business Elenco delle attività Basilea 2*

5. Payment and settlement	6. Agency services	7. Asset management	8. Retail brokerage
• *Sistemi di pagamento (EBA, BIREL, TARGET, CLS, SWIFT, etc.). Sistema di compensazione e regolamento carte di credito (MASTERCARD, VISA, AMEX, etc.). Trasferimento fondi (come business specifico). Banca Corrispondente. Servizi di compensazione e regolamento.*	• *Banca depositaria. Custodia e servizi correlati (gestione contante e garanzie reali, depositi presso terzi, etc.) come business specifico. Servizi di esattoria. Servizi di tesoreria Enti. Banca Fiduciaria.*	• *Gestione Portafogli ed altre forme di gestione del risparmio (fondi comuni di investimento, fondi di pensione, GPM, GPF, hedge fund, etc.). Si intende solo la produzione e non la distribuzione di prodotti di risparmio gestito; fa eccezione l'attività di collocamento a clienti professionali effettuata da società dedicate.*	• *Ricezione/trasmissione ed esecuzione di ordini verso clienti retail, "private" e SME. Attività di consulenza, assunzione a fermo, collocamento di strumenti finanziari/prodotti assicurativi (bancassurance, fondi, GPM, GPF, equity, bond, derivati, etc.) verso clienti retail, private e SME.*

Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

Eventi dannosi

- **Per dirla con Aristotele**
  - Il Rischio è una danno in potenza
  - L'Evento è una danno in atto
- **In altre parole**
  - Il Rischio è una misura ex-ante
  - La Perdita è una misura ex-post

Eventi dannosi

- **La banca deve predisporre un sistema di raccolta e conservazione dei dati sugli eventi dannosi che comprendano almeno le perdite significative avvenute e gli eventuali recuperi**
  - La raccolta e classificazione degli eventi di perdita o eventi dannosi sono un modo opportuno di valutare nel passato l'effetto di un dato evento e quindi valutare per il futuro il valore del rischio del medesimo effetto.
  - Statisticamente "se nel passato un certo tipo di evento mi ha provocato un danno di gravità X ed è avvenuto Y volte in un anno (e questo dato è costante anche negli anni precedenti) posso affermare con un certo livello di confidenza che nel prossimo anno accadrà con la stessa frequenza qualche evento dannoso che mi provocherà danni di gravità nota e prevedibile."
  - Per Perdita operativa si intende un valore economico certo e misurabile. Basilea 2 addirittura dice che deve essere un dato contabilizzato e inequivocabile.

Eventi di perdita Basilea 2

Frode interna	• Perdite dovute ad attività non autorizzata, frode, appropriazione indebita o violazioni di leggi, regolamenti o direttive aziendali che coinvolgano almeno una risorsa interna dell'ente creditizio.
Frode esterna	• Perdite dovute a frode, appropriazione indebita o violazione/elusione di leggi da parte di soggetti esterni all'ente creditizio.
Rapporto di impiego e sicurezza sul lavoro	• Perdite derivanti da atti non conformi alle leggi o agli accordi in materia di impiego, salute e sicurezza sul lavoro, dal pagamento di risarcimenti a titolo di lesioni personali o da episodi di discriminazione o di mancata applicazione di condizioni paritarie.

Eventi di perdita Basilea 2

Clientela, prodotti e prassi professionali	• Perdite derivanti da inadempienze relative a obblighi professionali verso clienti ovvero dalla natura o dalle caratteristiche del prodotto/servizio prestato.
Danni da eventi esterni	• Perdite derivanti da eventi esterni, quali catastrofi naturali, terrorismo, atti vandalici.
Interruzioni dell'operatività e disfunzioni dei sistemi	• Perdite dovute a interruzioni dell'operatività o a disfunzioni/indisponibilità dei sistemi.
Esecuzione, consegna e gestione dei processi	• Perdite dovute a carenze nel perfezionamento delle operazioni o nella gestione dei processi, nonché perdite dovute alle relazioni con controparti commerciali, venditori e fornitori.

Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

Una metodologia generale per analizzare i propri rischi

- **Una definizione qualitativa generica di rischio. Se ripensiamo alla definizione di rischio "*la variabilità dei possibili risultati intorno ad un valore atteso.*" un modo per identificare i rischi non in forma generale ma specifico per l'ambito/processo in cui si fa l'analisi è quello di**

Identificare le deviazioni

rispetto agli obiettivi di processo

- *Questo ci permette di poter analizzare i rischi calati sulla realtà aziendale che stiamo considerando. Non è una analisi teorica, ipotetica dei rischi che potrebbero succedere in generale. E' una analisi sui possibili scostamenti rispetto agli obiettivi reali. Se gli obiettivi sono oggettivi e misurabili anche gli scostamenti risulteranno tali.*
- *Questa è l'idea base su cui si basa la metodologia che affronteremo nelle prossime slides.*

Indice e scaletta del corso

- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

Esempio

- **Prendiamo in considerazione una Banca Italiana di medie dimensioni**
- **All'interno della banca prendiamo in considerazione per esempio l'attività di negoziazione di divisa (Forex);**
  - L'operatore di una banca che per comodità chiameremo Ruffini's Bank compra $ 1.000.000 con una controparte (JP Morgan) al cambio di 0,62976 USD/EUR.
  - Vediamo cosa succede all'interno delila nostra ipotetica banca facendo attenzione ai processi bancari e ai sistemi informatici e proviamo a fare una analisi dei possibili rischi derivanti da questa operazione.

Operazione in FOREX

Vende €

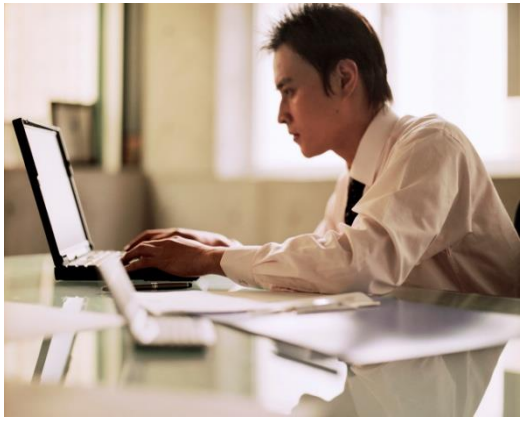
JPMorgan

Ruffini's Bank

Compra $

Fase 0: valutazione operazione

- **L'operatore di Front Office tramite gli strumenti messi a disposizione controlla i dati di mercato, valuta le operazioni da fare , decide di effettuare una operazione con una certa controparte, verifica i limiti suoi e della banca, verifica disponibilità per la valuta, conclude l'operazione (spesso al telefono)**



Fase 1 del processo Front Office

Registrazione manuale dell'operazione telefonica

CTP JP Morgan
Buy 1M USD SPOT
0,62976 USD/EUR
Jsihh osokk

Fase 2: Front Office support

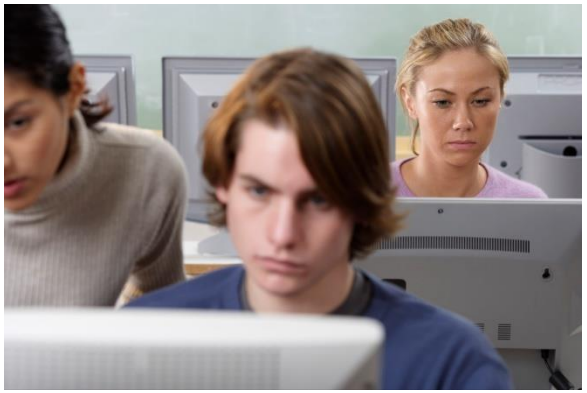
Registrazione sui sistemi di Front Office della operazione manuale per poter avere posizioni aggiornate e valutazione dell'esposizione del portafoglio

Fase 3: Comunicazione F.O verso B.O.

- **Comunicazione dell'operazione dal Front Office all'ufficio Back Office per effettuare il completamento delle informazioni per il regolamento e le conferme**
  - Sono coinvolte diverse persone e spesso più sistemi che devono comunicare tre di loro le informazioni.

Fase 4: completamento delle operazioni per il regolamento

- **Sulla base delle informazioni cartacee scritte dall'operatore di Front Office (dealer) l'ufficio di Back Office completa le istruzioni per il regolamento**
  - Controparte: verifica le banche di appoggio per ciascuna delle divise (USD e EUR) e i relativi metodi di pagamento e conferma
  - Valute di regolamento: verifica se per la data valuta SPOT (+2gg) c'è la disponibilità e in ogni caso l'operazione movimenterà la posizione di cassa per valuta Spot.
  - Controlli limiti ex post (controparte, operatore, rischi cambio, etc…): vengono verificate le esposizioni per quella determintata controparte, i limiti dell'operatore che ha fatto l'operazione, l'esposizione complessiva nella divisa che non deve superare quella voluta dal Risk Manager.



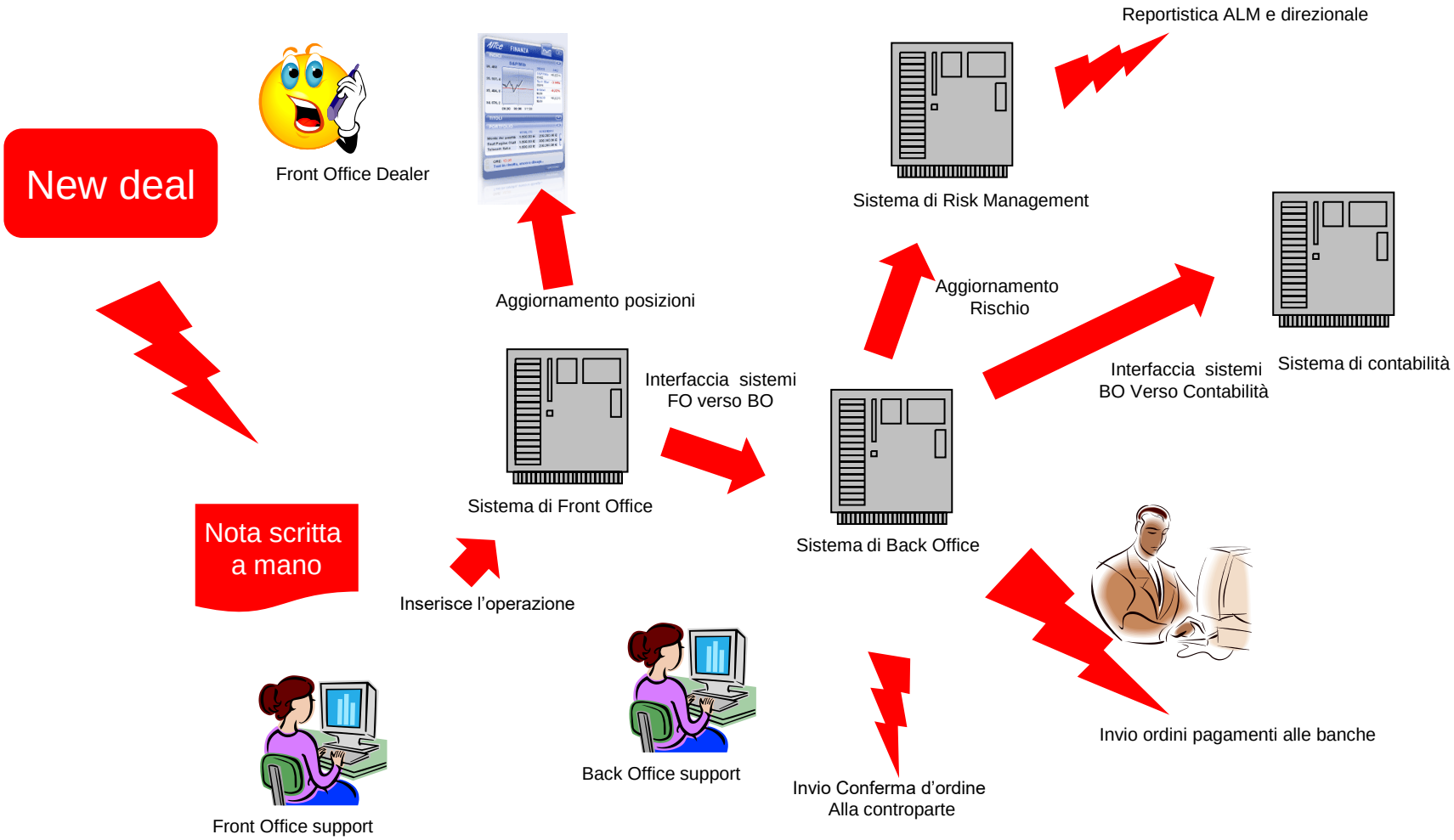
Fase 5: riscontro con la controparte

- **Dopo l'effettuazione dei controlli necessari viene inviata alla controparte una conferma scritta (via fax, messaggi SWIFT, Lettera, etc…) dell'operazione effettuata**
  - E' la conferma ufficiale dell'operazione, si verifica che ciò che si aspetta la controparte sia ciò che ci aspettiamo noi. In caso contrario scattano delle procedure di contestazione.

Fase 6: Regolamento della operazione e invio Contabilità

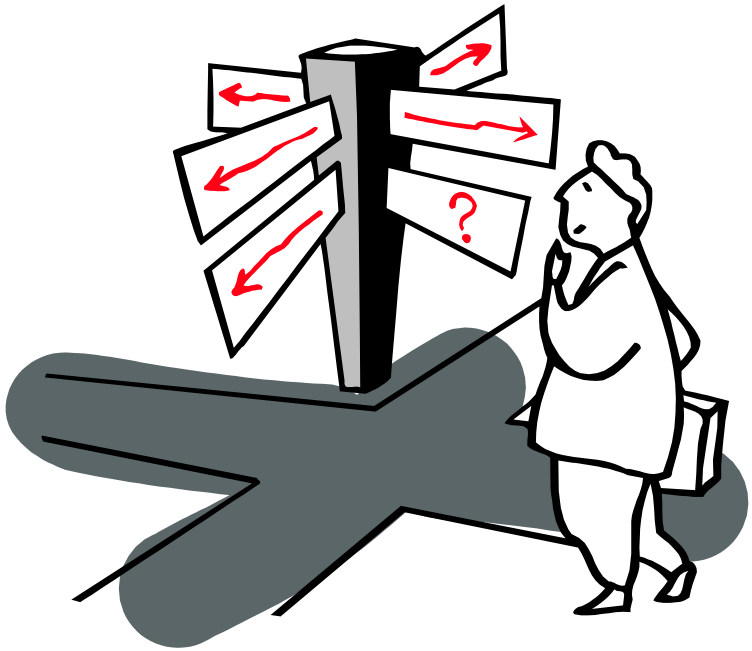
- **Predisposizione degli ordini di pagamento alle banche di appoggio o ai circuiti per il regolamento dell'operazione e invio alla contabilità.**
  - Aggiornamento delle posizioni per i report di direzione
  - Invio alla contabilità

Flusso di un ordine



Tocca a Voi

- **Dove possono essere i rischi?**



Indice e scaletta del corso

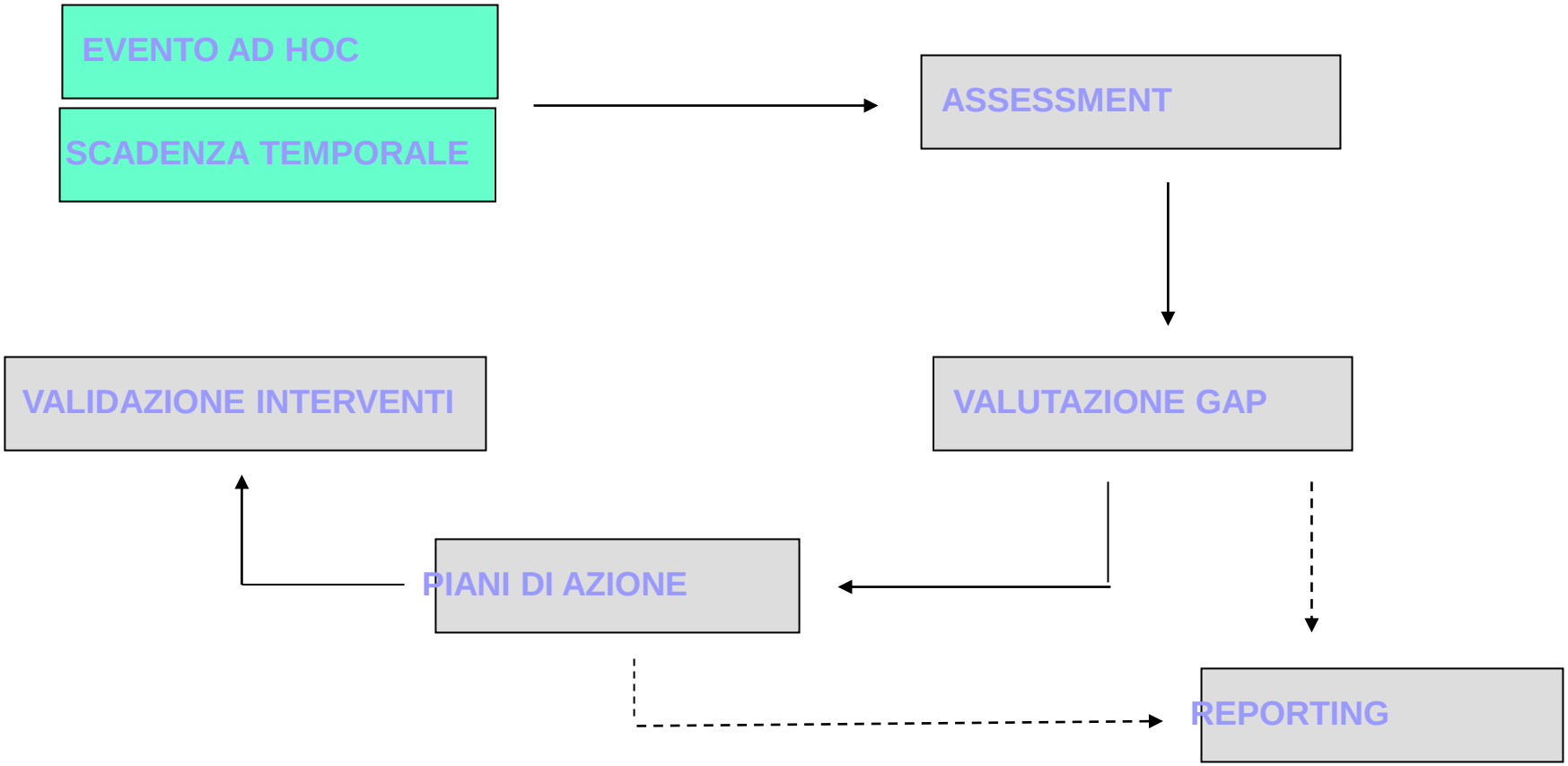
- **Prima Parte: Introduzione al rischio**
  - Definizioni di rischio
  - Introduzione a Basilea II
  - Le diverse categorie di rischio
  - Introduzione ai processi aziendali
  - Eventi di perdita
  - Obiettivi, processi, rischi
  - Un esempio di analisi dei processi in una banca
  - La funzione di Compliance in Banca

La Funzione di Compliance in banca

La Funzione Compliance deve avere la possibilità di gestire in modo integrato:

- **Disposizioni normative** sia di fonte aziendale che esterna
- **Processi** operativi (attività) sui quali impattano le disposizioni normative, descritti ad un sufficiente grado di dettaglio
- **Rischi di non conformità,** intesi come l'incrocio tra un determinato disposto normativo e uno specifico processo aziendale, incrocio che determina un rischio da censire e sottoporre a valutazione
- **Sanzioni** ed altri elementi caratterizzanti il rischio (frequenza, etc.)
- **Strutture organizzative** e ruoli/responsabilità che sono chiamati a presidiare nel continuo la conformità

Per un ciclo di attività che prevede …



Il vero problema: la gestione della complessità

Alcuni numeri:

- **Disposizioni normative:** le normative presenti in ABICS prevedono oltre 800 disposizioni cogenti, che associate ai processi determinano oltre 4.000 rischi di violazione. Inoltre occorre considerare le normative aziendali e i codici di comportamento…
- **Processi** operativi: la tassonomia ABILab è composta da circa 400 elementi, molti alberi dei processi aziendali ne hanno più di mille, le singole attività elementari possono superare le 10.000 …
- **Rischi di non conformità:** Sono oltre 4.000 in ABICS, solo molti di più nella singola Banca, con più disposizioni, più processi, le attività …
- **Sanzioni:** ogni disposizione normativa può comportare sanzioni di diversa natura e/o rischi reputazionali
- **Strutture organizzative:** i rischi devono essere associati, attraverso i processi, alle strutture organizzative e ai singoli soggetti che le presidiano.

Le esigenze della funzione …

- Gestione di un **numero elevato di informazioni**: 10.000, 20.000 ?
- Necessità di adottare approcci standard a livello **di Gruppo**
- Efficienza nell'esecuzione periodica degli **assessment**
- **Standardizzazione del processo** di gestione degli adempimenti
- Sicurezza dei dati e **storicizzazione** delle informazioni
- Efficaci **strumenti di analisi e reportistica**
- Capacità di **monitorare** la realizzazione delle **azioni correttive** individuate
- **Tracciabilità** degli interventi realizzati dalla funzione nei diversi ambiti

L’aiuto da parte di tool dedicati …

- **Collegabilità** a repository esterni o ad altri repository aziendali (tool di Business Process Management) per garantire efficienza manutentiva e integrazione con gli strumenti già disponibili
- Gestione di un **numero elevatissimo** di oggetti favorendone la gestione selettiva, la memorizzazione (storicizzazione) e …
- …..

Ufficio marketing progetta un nuovo prodotto per la Ruffini's Bank

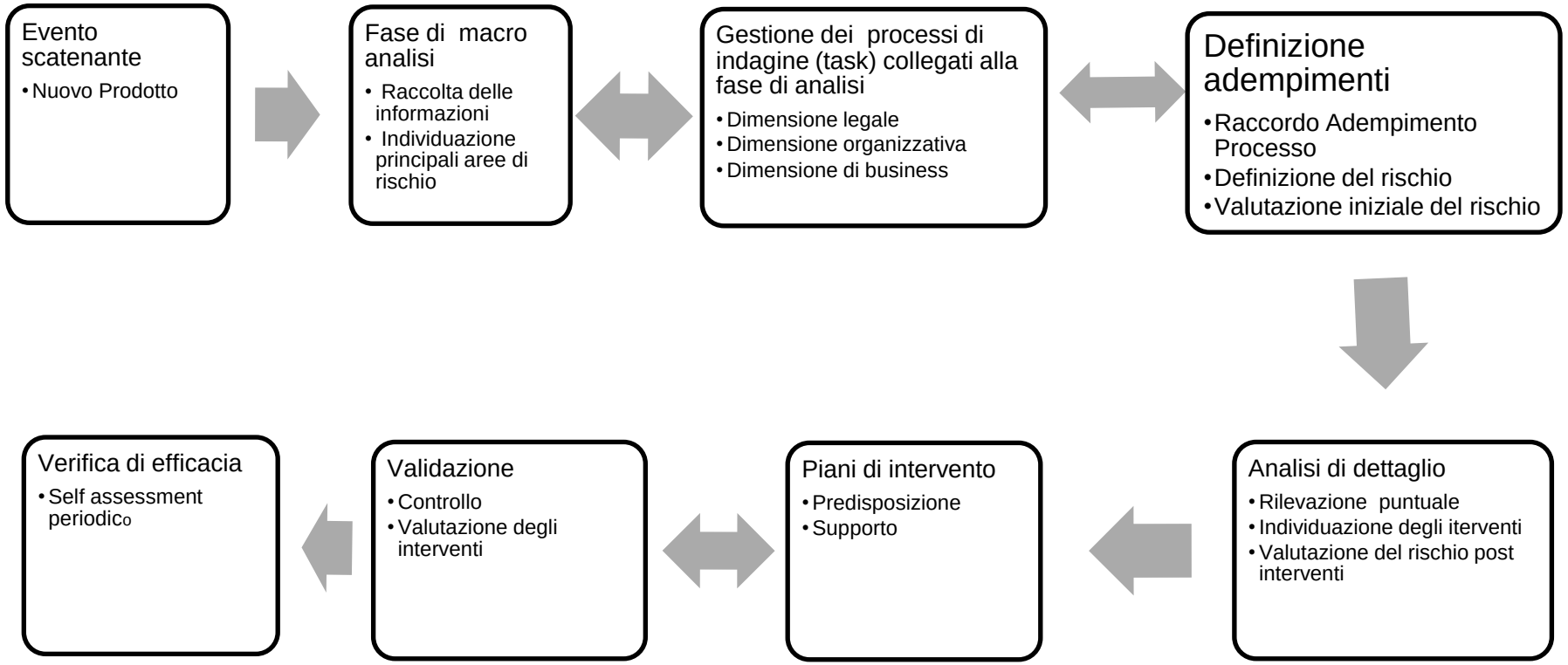
Viene predisposto un primo documento di valutazione con i vari macro impatti adempimenti e rischi

Chiede il parere dell'ufficio compliance per la valutazione degli impatti normativi

Inizia una fase di intenso scambio di informazioni, pareri e valutazioni tra uffici diversi per una prima formulazione degli ambiti di impatto, di focalizzazione delle norme interessate, di macro valutazione degli impatti

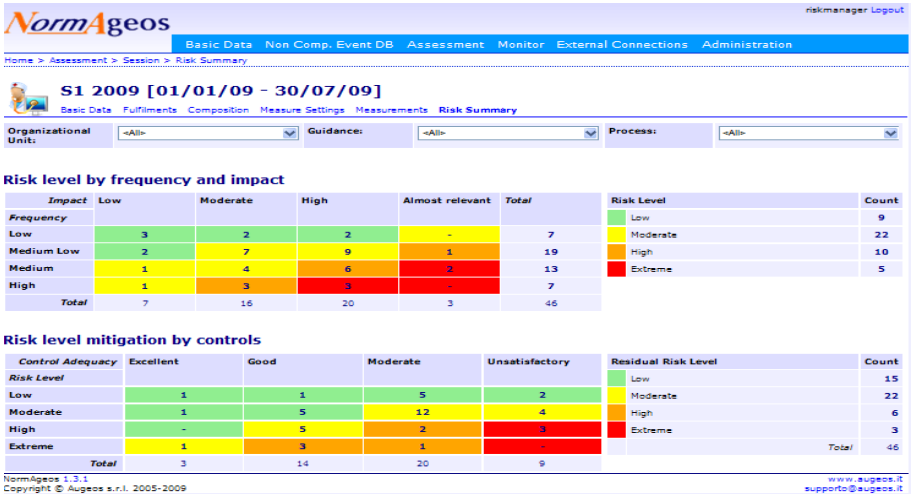
Si appronta un dossier con tutta la doc necessaria atta a supportare e giustificare il parere. Tali informazioni serviranno anche in seguito per seguire domande spot di approfondimenti specifici

Esempio di attività dell'ufficio di compliance a fronte di una richiesta di valutazione di conformità per un nuovo prodotto



Assessment

Successivamente verranno predisposte analisi più approfondite, degli adempimenti necessari e dei controlli da effettuare per una più attenta valutazione dei rischi



Criticità

- **Metodologia consolidata per analisi impatti, rischi normativi, adempimenti**
- **Grande mole di dati non strutturati e difficoltà nell'analizzare legami tra informazioni di diverso tipo (legali, organizzative, procedurali, ...)**
- **Processi autorizzativi complessi tra aree organizzative diverse**
- **Difficoltà nel ricostruire giudizi o valuazioni effettuate. Giustificabilità delle valutazioni di impatto e di rischio**

Le funzionalità ICT di supporto alla compliance

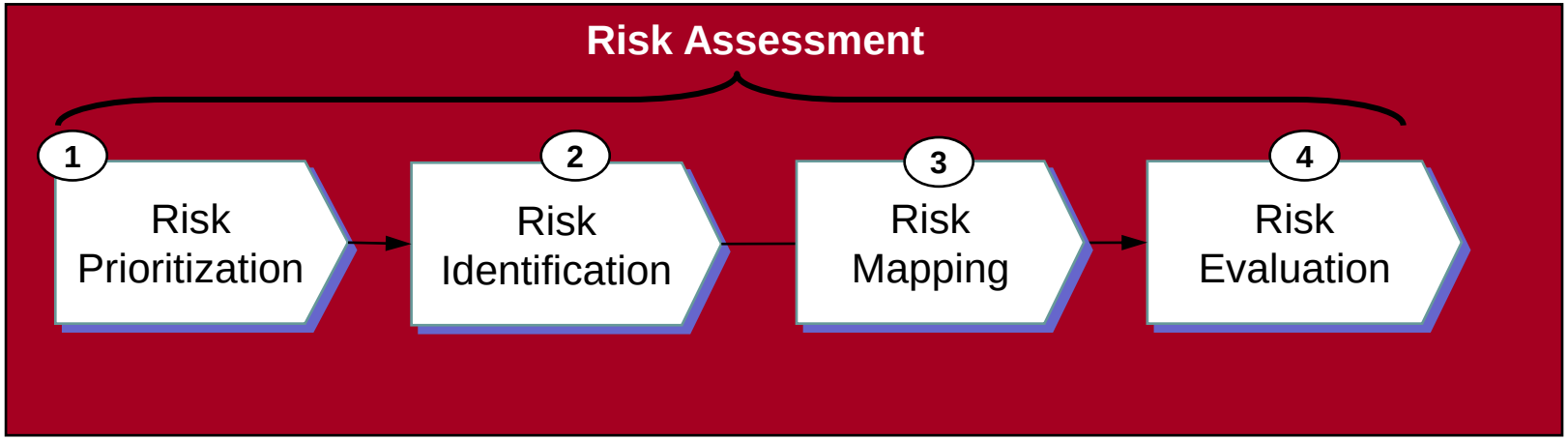
Funzioni base	Funzioni di supporto analisi di conformità ex-ante	Funzioni di supporto analisi di conformità ex-post	Funzioni per la raccolta segnalazioni di non conformità	Funzioni per il monitoraggio	Funzioni di collegamento verso sistemi esterni
gestione degli utenti, dei ruoli e dell'accesso al sistema	Ambiente definizione scenari	**Ambiente di suporto al test di efficacia degli interventi effettuati e all'analisi ex-post**	Inserimento e gestione degli Eventi di non conformità	Cruscotto per analisi dei dati a livello aggregato con possibilità di drill-down al singolo dettaglio	Interfaccia ARIS: import da ARIS delle informazioni relative a Processi, Risk Unit,Controlli e Rischi
Gestione Anagrafiche e configurazioni riguardanti Processi, Risk Unit, Controlli e Rischi	Strumenti per gestione degli adempimenti		Definizione e gestione del workflow di approvazione segnalazione	Report	Interfaccia ABICS: import tassonomia disposizioni normative
Gestione gruppi o multi società	Gestione del processo e work flow				

- **Pausa?**

Seconda parte:
una metodologia per l’analisi e la gestione del rischio

La soluzione: approccio metodologico

Metodologia



1. **Definisce, seleziona e prioritizza le "aree di rischio":** unità di riferimento potenzialmente in grado di generare eventi sfavorevoli. Questa fase, supportata da un'analisi costi/benefici, ha l'obiettivo di individuare le aree di rischio su cui intervenire.

2. **Identifica i Rischi potenziali e specifici** e le condizioni che favoriscono o impediscono il verificarsi del rischio.

3. **Identifica i Rischi potenziali e specifici** e le condizioni che favoriscono o impediscono il verificarsi del rischio.

4. **Definisce le metriche del sistema di monitoraggio e le modalità di misurazione** dei rischi identificati nella fase precedente.

Indice e scaletta del corso

- **Seconda parte: una metodologia per l'analisi e la gestione del rischio operativo**
  - Risk assessment .
    - Risk Prioritization
    - Risk Identification
    - Risk Mapping
    - Risk Evaluation
  - Risk Management
    - Risk Monitor
    - Risk Mitigation
-

Perché la fase di prioritizzazione

- **La fase di prioritizzazione è molto importante per poter avere una bussola e una metodologia condivisa per poter discernere sulla base delle priorità dell'azienda che si sta analizzando**
  - Un rischio ed un processo possono essere più o meno prioritari a seconda dell'azienda e in maniera più specifica a seconda degli obiettivi di una certa area.
  - La percezione dell'importanza dei rischi e dei danni è spesso molto soggettiva. Se la ancoriamo agli obiettivi aziendali riusciamo ad avere un metro oggettivo contestualizzato dell'importanza

Risk Prioritizazion

L'obiettivo: definire "cosa si vuole valutare", ovvero le Aree di Rischio principali

Le Aree di Rischio

- ✓ **le Aree di Rischio rappresentano entità organizzative che possono essere soggette ad eventi sfavorevoli; spesso possono essere legate a degli obiettivi o sono degli obiettivi stessi.**

Contenuti della fase

- ✓ **questa fase porta all'identificazione delle aree/unità organizzative/obiettivi sulle quali concentrare l'analisi successiva di identificazione e misurazione dei rischi**

- ✓ **la scelta delle Aree di Rischio sulle quali concentrare l'attenzione è supportata da un'analisi costi/benefici che consente all'azienda di effettuare una scelta secondo criteri di economicità dell'intervento**

La soluzione: la fase di risk prioritization

La matrice processi/Aree di Rischio

- ✓ la matrice delle Aree di Rischio rappresenta le relazioni con la catena del valore e costituisce la base del sistema di misurazione

MATRICI DELLE AREE DI RISCHIO

Processi aziendali (Macroprocessi)	Aree di rischio 1	2	3	4	n
1		X			
2	X			X	
3			X	X	X
4	X		X		
5					X
	KRI A	KRI B	KRI C	KRI D	KRI E

⇦ **Fase di Risk Evaluation**

La soluzione: la fase di risk Prioritization

Processo aziendale	Obiettivi di processo	Obiettivi aziendali		
		A	B	C
X	1			
	2			
Y	1			
	2			

Esempio: la fase di risk prioritization

Riprendiamo l'esempio della Ruffini's Bank

Strategia aziendale

AREE DI RISCHIO

Obiettivi strategici di business

1. Ottimizzazione dell'impiego delle risorse finanziarie
2. Incrementare la redditività aziendale
3. Massimizzare la soddisfazione del cliente

Obiettivi strategici di governo

4. Rispetto normative esterne
5. Incrementare qualità e sicurezza dei dati
6. Efficacia dei processi aziendali di supporto

Altri obiettivi aziendali

7. Migliorare la struttura finanziaria
8. Migliorare l'efficienza interna

Potenza della prioritizzazione

- La prioritizzazione a partire dagli obiettivi è uno strumento estremamente potente ed efficace che può essere utilizzato anche per identificare le entità più importanti in un sistema anche molto complesso
- E' un faro che ci permette di dirigere l'azione su i nodi importanti
- Altri ambiti in cui è possibile utilizzare la prioritizzazione
  - Ricerca delle unità organizzative più strategiche in una azienda
  - Ricerca degli archivi o base di dati con le informazioni più importanti di una azienda
  - Ricerca del personale critico per una azienda
  - Prioritizzazione delle nostre azioni

Indice e scaletta del corso

- **Seconda parte: una metodologia per l'analisi e la gestione del rischio operativo**
  - Risk assessment .
    - Risk Prioritization
    - Risk Identification
    - Risk Mapping
    - Risk Evaluation
  - Risk Management
    - Risk Monitor
    - Risk Mitigation

Risk Identification

Obiettivo: identificare che cosa, come, dove e quando un evento o una situazione potrebbe ostacolare il raggiungimento di un obiettivo chiaramente definito o degradarne la qualità o ritardarne l'attività.

Contenuti della fase

- **l'identificazione dei rischi indaga:**
  - Obiettivi, norme, vincoli, adempimenti
  - le minacce, ossia le tipologie di eventi dannosi a cui l'impresa è esposta
  - le condizioni agevolanti e frenanti, ossia i fattori di controllo specifici dai quali dipende se la minaccia troverà o no realizzazione e, se si, con quali conseguenze
  - Luoghi, processi, aree, uffici, persone, macchine o beni strumentali, prodotti
  - Eventi, storie, situazioni

Identification: Obiettivi, norme, adempimenti

1. **Recuperare gli obiettivi aziendali, di processo, di area o degli uffici**
2. **Recuperare le norme di riferimento, le prassi aziendali, i regolamenti**
3. **Scomporre le norme in adempimenti e elaborare un elenco di adempimenti e di obiettivi**

Es. Ruffini's Bank

❑ Obiettivo processo compravendita divisa

- Massimizzare gli utili
- Correttezza, completezza nel processo di contabilizzazione
- Minimizzare i costi del processo
- Massimizzare la velocità
- Rispettare i limiti imposti dalla direzione
- Rispettare le norme di settore
- Massimizzare gli effetti fiscali

Recuperare le norme di riferimento

- **Definizione del contesto normativo di riferimento**

  sulla base del business, dell'organizzazione, dei mercati e della localizzazione vengono definiti i domini normativi di riferimento, ovvero l'insieme dei documenti normativi di riferimento che definiscono il perimetro normativo entro cui ci si muove:

Esempio in ambito bancario:

- Antiriciclaggio
- Privacy
- Sicurezza informatica
- MIFID
- Trasparenza bancaria
- Servizi di pagamento PSd
- Antiusura
- Credito al consumo
- Market abuse

Recuperare le norme di riferimento

- Le norme di riferimento sono una parte dei vincoli con cui vengono definiti gli obiettivi
- Occorre studiare la normativa del dominio di riferimento e analizzare il contesto
- Verificare per ogni normativa in ambito se è applicabile al processo che sto analizzando

l'adempimento di compliance

- **Adempimenti per ruolo aziendale**

  Per ciascuno degli argomenti trattati occorre definire gli adempimenti normativi a cui ciascuna persona con qualche ruolo aziendale responsabile deve attenersi. Si individuano quindi le regole di prescrizione, i reati di riferimento, le sanzioni in caso di violazione.

Esempio in riferimento all'argomento «modalità di accesso alle informazioni» si definisce un adempimento di tipo:

> «A pena del riconoscimento di una responsabilità civile per danni derivanti dall'esercizio di attività pericolose, la banca deve prevenire accessi non autorizzati a informazioni contenute in sistemi applicativi.»
>
> «A pena del riconoscimento di una responsabilità civile per danni derivanti dall'esercizio di attività pericolose, la banca deve prevenire accessi non autorizzati ai servizi di rete.»

Numerosità e priorità degli adempimenti: La numerosità degli adempimenti per dominio è elevata. Si contano circa una media di 200 adempimenti per dominio tipo.

Adempimento normativo

- **Schema logico di un adempimento:**
  - Ruoli attivi
  - Ruoli passivi
  - Reato, violazione
  - Sanzioni o conseguenze in caso di inadempienza
  - Situazioni aggravanti
  - Oggetti, persone, luoghi inerenti, Nozioni correlate

Esempio Decreto Legislativo 81/2008

Prendiamo un comma della norma relativa Sicurezza sul luogo del lavoro:

Art. 18 Obblighi del datore di lavoro e del dirigente

Comma 1. Il datore di lavoro, che esercita le attività di cui all' articolo 3 , e i dirigenti, che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, devono:

a) nominare il medico competente per l'effettuazione della sorveglianza sanitaria nei casi previsti dal presente decreto legislativo; …. omissis

Art. 55. (Sanzioni per il datore di lavoro e il dirigente)

Comma 1. E' punito con l'arresto da tre a sei mesi o con l'ammenda da 2.500 a 6.400 euro il datore di lavoro:

a) per la violazione dell' articolo 29, comma 1 ;

b) che non provvede alla nomina del responsabile del servizio di prevenzione e protezione ai sensi dell' articolo 17, comma 1, lettera b) , o per la violazione dell'articolo 34, comma 2.

….. omissis ….

c) con l'arresto da due a quattro mesi o con l'ammenda da 1.200 a 5.200 euro per la violazione dell' articolo 18, comma 1 , lettere c), e), f) e q), 36, commi 1 e 2, 37, commi 1, 7, 9 e 10, 43, comma 1, lettere d) ed e-bis), 46, comma 2;

……

Riscriviamolo sotto forma di adempimento

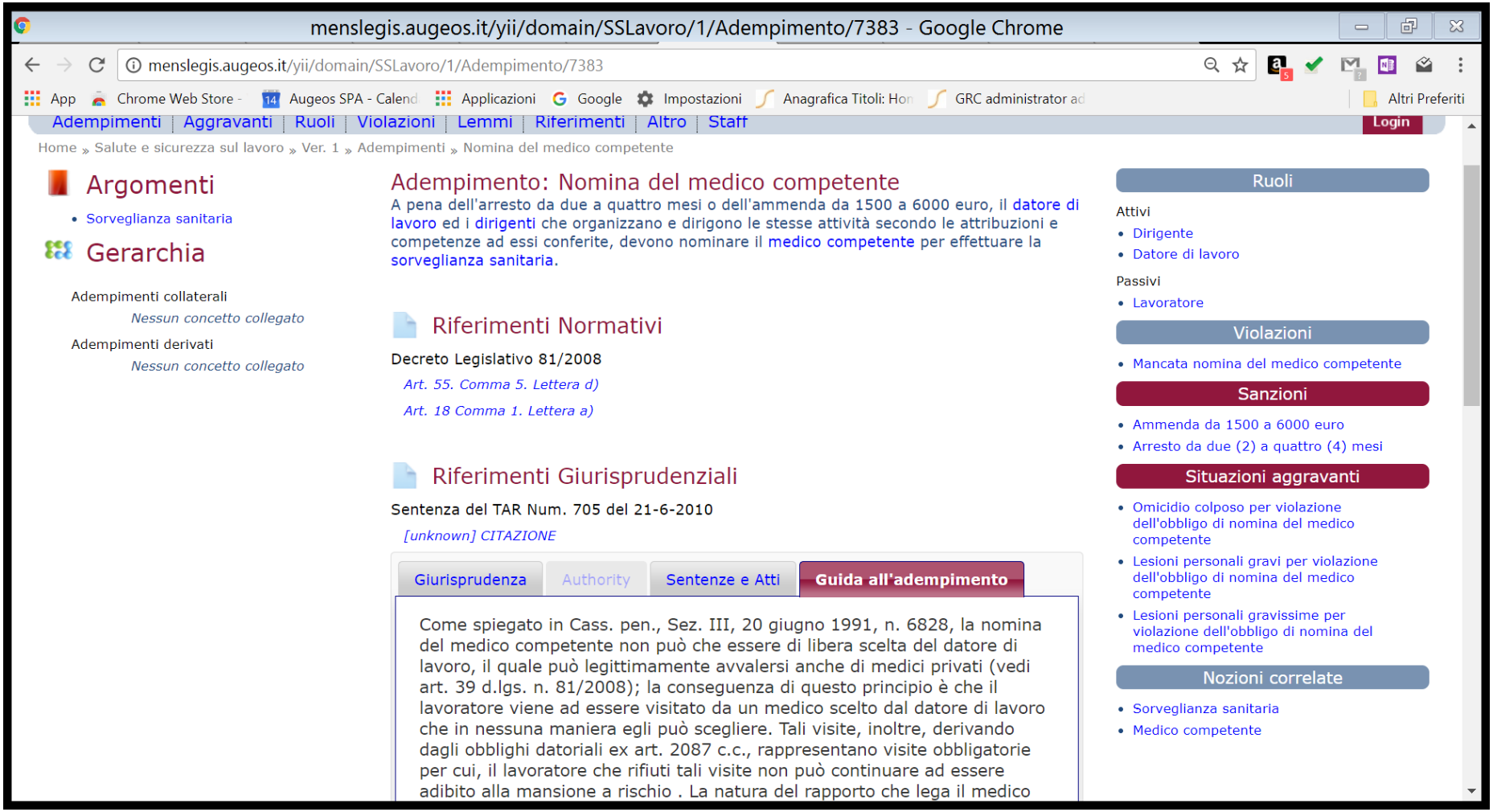
Adempimento: Nomina del medico competente

A pena dell'arresto da due a quattro mesi o dell'ammenda da 1500 a 6000 euro, il datore di lavoro ed i dirigenti che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, devono nominare il medico competente per effettuare la sorveglianza sanitaria.

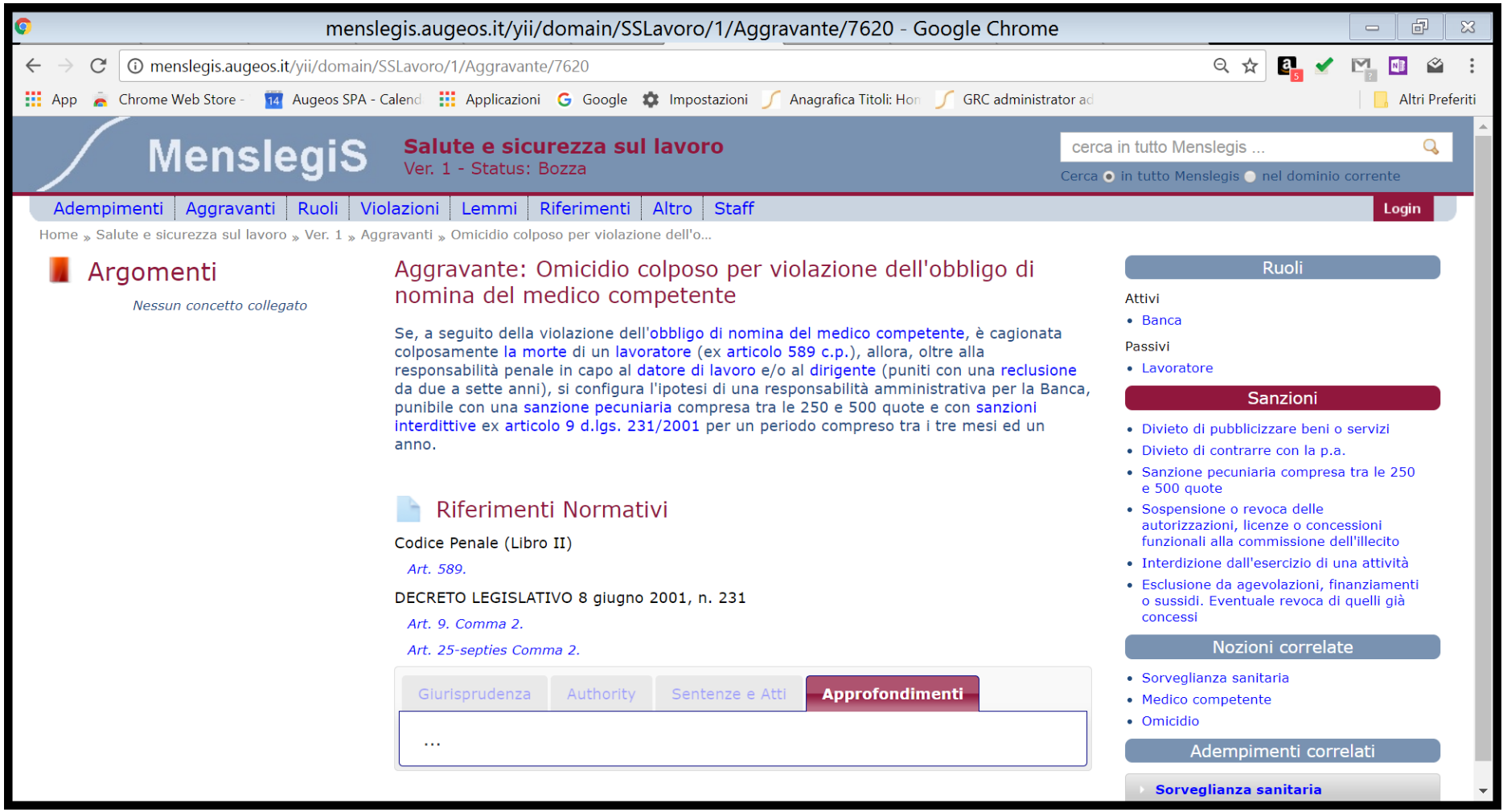
Sono stati individuati secondo il nostro schema:

- **Ruoli attivi**: Datore di lavoro e dirigenti
- **Ruoli passivi**: Lavoratore
- **Reato, violazione**: Mancata nomina del Medico Competente
- **Sanzioni o conseguenze in caso di inadempienza**: arresto da due a quattro mesi o dell'ammenda da 1500 a 6000 euro
- **Situazioni aggravanti**: vedi 231
- **Oggetti, persone, luoghi inerenti**: medico competente, sorveglianza sanitaria

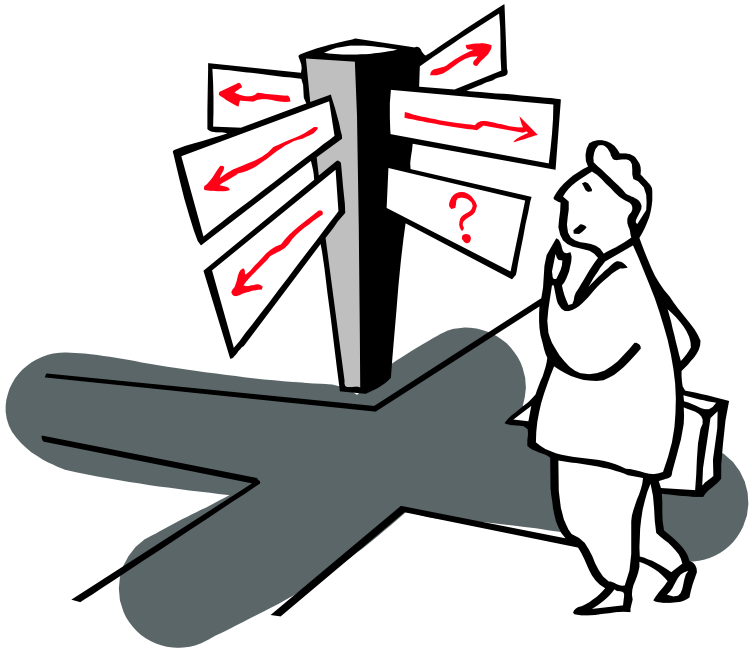
Adempimento scomposto



Aggravante


menslegis.augeos.it/yii/domain/SSLavoro/1/Aggravante/7620 - Google Chrome
menslegis.augeos.it/yii/domain/SSLavoro/1/Aggravante/7620
MenslegiS
Salute e sicurezza sul lavoro
Ver. 1 - Status: Bozza
cerca in tutto Menslegis ...
Cerca in tutto Menslegis nel dominio corrente
Adempimenti Aggravanti Ruoli Violazioni Lemmi Riferimenti Altro Staff
Login
Home » Salute e sicurezza sul lavoro » Ver. 1 » Aggravanti » Omicidio colposo per violazione dell'o...
Argomenti
Nessun concetto collegato
Aggravante: Omicidio colposo per violazione dell'obbligo di nomina del medico competente
Se, a seguito della violazione dell'obbligo di nomina del medico competente, è cagionata colposamente la morte di un lavoratore (ex articolo 589 c.p.), allora, oltre alla responsabilità penale in capo al datore di lavoro e/o al dirigente (puniti con una reclusione da due a sette anni), si configura l'ipotesi di una responsabilità amministrativa per la Banca, punibile con una sanzione pecuniaria compresa tra le 250 e 500 quote e con sanzioni interdittive ex articolo 9 d.lgs. 231/2001 per un periodo compreso tra i tre mesi ed un anno.
Riferimenti Normativi
Codice Penale (Libro II)
Art. 589.
DECRETO LEGISLATIVO 8 giugno 2001, n. 231
Art. 9. Comma 2.
Art. 25-septies Comma 2.
Giurisprudenza Authority Sentenze e Atti Approfondimenti
...
Ruoli
Attivi
Banca
Passivi
Lavoratore
Sanzioni
Divieto di pubblicizzare beni o servizi
Divieto di contrarre con la p.a.
Sanzione pecuniaria compresa tra le 250 e 500 quote
Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito
Interdizione dall'esercizio di una attività
Esclusione da agevolazioni, finanziamenti o sussidi. Eventuale revoca di quelli già concessi
Nozioni correlate
Sorveglianza sanitaria
Medico competente
Omicidio
Adempimenti correlati
Sorveglianza sanitaria

Tocca a Voi



Articolo 174

1. Il datore di lavoro, all'atto della valutazione del rischio di cui all' articolo 28 , analizza i posti di lavoro con particolare riguardo:

a)ai rischi per la vista e per gli occhi;

b)ai problemi legati alla postura ed all'affaticamento fisico o mentale;

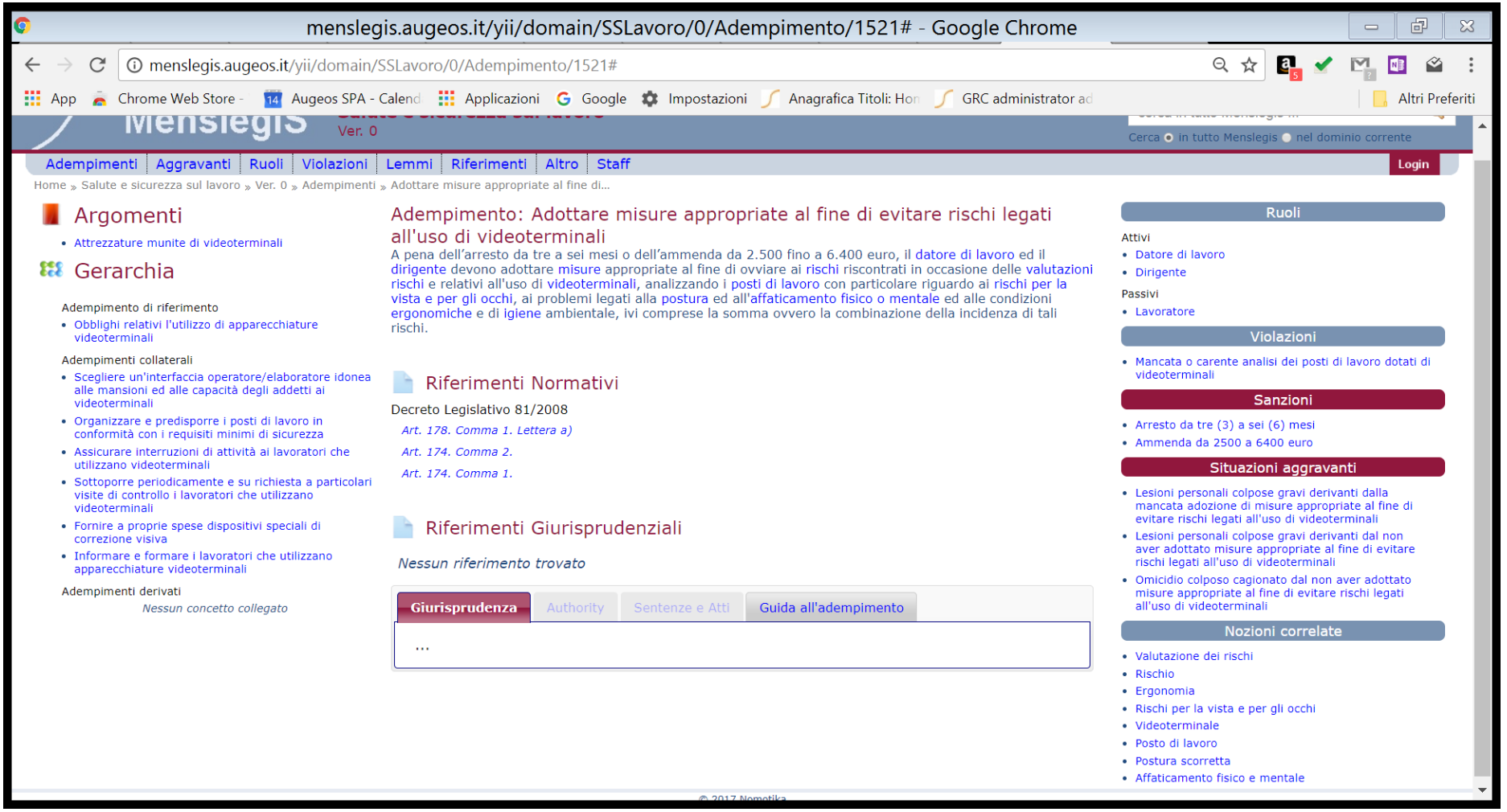
c)alle condizioni ergonomiche e di igiene ambientale.

2. Il datore di lavoro adotta le misure appropriate per ovviare ai rischi riscontrati in base alle valutazioni di cui al comma 1 , tenendo conto della somma ovvero della combinazione della incidenza dei rischi riscontrati.

….Omissis …. Verrà punito ….Omissis ….

a)con l'arresto da tre a sei mesi o con l'ammenda da 2.500 fino a 6.400 euro per la violazione degli articoli 174, comma 2 e 3, 175, commi 1 e 3, e 176, commi 1, 3, 5;

Soluzione


menslegis.augeos.it/yii/domain/SSLavoro/0/Adempimento/1521# - Google Chrome
menslegis.augeos.it/yii/domain/SSLavoro/0/Adempimento/1521#
App
Chrome Web Store
Augeos SPA - Calend
Applicazioni
Google
Impostazioni
Anagrafica Titoli: Hon
GRC administrator ad
Altri Preferiti
Menslegis
Ver. 0
Cerca in tutto Menslegis nel dominio corrente
Adempimenti
Aggravanti
Ruoli
Violazioni
Lemmi
Riferimenti
Altro
Staff
Login
Home » Salute e sicurezza sul lavoro » Ver. 0 » Adempimenti » Adottare misure appropriate al fine di...
Argomenti
Attrezzature munite di videoterminali
Gerarchia
Adempimento di riferimento
Obblighi relativi l'utilizzo di apparecchiature videoterminali
Adempimenti collaterali
Scegliere un'interfaccia operatore/elaboratore idonea alle mansioni ed alle capacità degli addetti ai videoterminali
Organizzare e predisporre i posti di lavoro in conformità con i requisiti minimi di sicurezza
Assicurare interruzioni di attività ai lavoratori che utilizzano videoterminali
Sottoporre periodicamente e su richiesta a particolari visite di controllo i lavoratori che utilizzano videoterminali
Fornire a proprie spese dispositivi speciali di correzione visiva
Informare e formare i lavoratori che utilizzano apparecchiature videoterminali
Adempimenti derivati
Nessun concetto collegato
Adempimento: Adottare misure appropriate al fine di evitare rischi legati all'uso di videoterminali
A pena dell'arresto da tre a sei mesi o dell'ammenda da 2.500 fino a 6.400 euro, il datore di lavoro ed il dirigente devono adottare misure appropriate al fine di ovviare ai rischi riscontrati in occasione delle valutazioni rischi e relativi all'uso di videoterminali, analizzando i posti di lavoro con particolare riguardo ai rischi per la vista e per gli occhi, ai problemi legati alla postura ed all'affaticamento fisico o mentale ed alle condizioni ergonomiche e di igiene ambientale, ivi comprese la somma ovvero la combinazione della incidenza di tali rischi.
Riferimenti Normativi
Decreto Legislativo 81/2008
Art. 178. Comma 1. Lettera a)
Art. 174. Comma 2.
Art. 174. Comma 1.
Riferimenti Giurisprudenziali
Nessun riferimento trovato
Giurisprudenza
Authority
Sentenze e Atti
Guida all'adempimento
...
Ruoli
Attivi
Datore di lavoro
Dirigente
Passivi
Lavoratore
Violazioni
Mancata o carente analisi dei posti di lavoro dotati di videoterminali
Sanzioni
Arresto da tre (3) a sei (6) mesi
Ammenda da 2500 a 6400 euro
Situazioni aggravanti
Lesioni personali colpose gravi derivanti dalla mancata adozione di misure appropriate al fine di evitare rischi legati all'uso di videoterminali
Lesioni personali colpose gravi derivanti dal non aver adottato misure appropriate al fine di evitare rischi legati all'uso di videoterminali
Omicidio colposo cagionato dal non aver adottato misure appropriate al fine di evitare rischi legati all'uso di videoterminali
Nozioni correlate
Valutazione dei rischi
Rischio
Ergonomia
Rischi per la vista e per gli occhi
Videoterminale
Posto di lavoro
Postura scorretta
Affaticamento fisico e mentale
© 2017 Nomotika

Esempi di adempimenti

Titolo	Descrizione	Dominio legale / Argomento	Normativa
Adottare adeguati mezzi di prevenzione incendi sul luogo di lavoro	A pena dell'arresto da due a quattro mesi o dell'ammenda da 1200 a 5200 euro, il datore di lavoro ed i dirigenti che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, devono adottare ogni misura per prevenire gli incendi e tutelare l'incolumità dei lavoratori sul luogo di lavoro.	Salute e sicurezza sul lavoro *Gestione delle emergenze*	DECRETO LEGISLATIVO 9 aprile 2008, n. 81
Adottare disposizioni miranti ad eliminare o ridurre i rischi di esposizione dagli agenti fisici	A pena dell'arresto da tre a sei mesi dell'ammenda da 2.000 a 4.000 euro, il datore di lavoro e il dirigente devono adottare disposizioni affinché i lavoratori non vengano esposti a valori superiori a quelli limite di esposizione agli agenti fisici (definiti nei capi II, III, IV e V) o, in caso di superamento, devono adottare misure immediate per riportare l'esposizione al di sotto di tali valori limite, individuandone le cause del superamento e adeguando di conseguenza le misure di protezione e prevenzione per evitare un nuovo superamento.	Salute e sicurezza sul lavoro *Agenti fisici*	DECRETO LEGISLATIVO 9 aprile 2008, n. 81
Adottare il documento di valutazione rischi previa consultazione del rappresentante dei lavoratori	A pena di una ammenda da 2000 euro a 4000 euro, è compito del datore di lavoro effettuare la valutazione dei rischi ed adottare il relativo documento, anche se su supporto informatico, previa consultazione del rappresentate dei lavoratori per la sicurezza.	Salute e sicurezza sul lavoro *Valutazione dei rischi connessi all'attività*	DECRETO LEGISLATIVO 9 aprile 2008, n. 81
Adottare le misure di primo soccorso, di prevenzione incendi e di evacuazione	A pena dell'arresto da due a quattro mesi o dell'ammenda da 750 a 4000 euro, è compito del datore di lavoro e del dirigente adottare tutte le misure di prevenzione degli incendi e di evacuazione dai luoghi di lavoro organizzando i necessari rapporti con i servizi pubblici in materia di primo soccorso, salvataggio, lotta antincendio e gestione delle emergenze. Il datore di lavoro deve, inoltre, designare i lavoratori preposti a tali funzioni, informando tutti gli altri circa i comportamenti da adottare in caso di pericolo e prendendo ogni provvedimento necessario affinché le misure preventive siano adeguate a qualsiasi contesto.	Salute e sicurezza sul lavoro *Gestione delle emergenze*	DECRETO LEGISLATIVO 9 aprile 2008, n. 81

Esempi di minacce informatiche

Accesso non autorizzato a basi dati o archivi	Si considera un "Accesso non autorizzato a basi dati o archivi" una delle seguenti minacce:Interrogazione non autorizzata a basi dati o archivi in ambiente di produzione, Accesso non autorizzato ai sistemi e librerie di backup, Accesso non autorizzato agli ambienti di sviluppo, test e produzione, Privilege escalation, Accesso a dati di produzione durante attività di manutenzione, Copia non autorizzata dei dati di produzione, Modifica non autorizzata flussi dati alimentanti (es, staging area, share di scambio,…), Modifica non autorizzata dei dati sulle basi dati in esercizio, Modifica non autorizzata delle basi dati sugli archivi di backup
Attacchi informatici	Hackitivm (es. defacing, netstrike, …), Distributed Denial Of Service, Modifica degli instradamenti geografici, Malware, Danneggiamento volontario di un apparato hardware, Attacchi sul provider di servizi di connettività, Danneggiamento volontario sistemi (applicazioni,server, ..), Sql injection, Phishing, Smishing, Tampering dei sistemi di conservazione delle chiavi di crittografia dei dati
Errata/inefficace gestione di un incidente informatico	Mancata identificazione della causa degli incidenti, Incapacità di gestire gli incidenti informatici

Famiglie di controlli

- ACCESS CONTROL
  - ACCESS CONTROL POLICY AND PROCEDURES
  - REMOTE ACCESS
  - USE OF EXTERNAL INFORMATION SYSTEMS
  - ACCESS CONTROL DECISIONS
  - ACCESS ENFORCEMENT
  - SEPARATION OF DUTIES
  - LEAST PRIVILEGE
- AUDIT AND ACCOUNTABILITY
- AWARENESS AND TRAINING
- CONFIGURATION MANAGEMENT
- CONTINGENCY PLANNING
- IDENTIFICATION AND AUTHENTICATION
  - "IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)"
  - AUTHENTICATOR MANAGEMENT
  - AUTHENTICATOR FEEDBACK
  - CRYPTOGRAPHIC MODULE AUTHENTICATION
- INCIDENT RESPONSE
- MAINTENANCE

Esempi di controlli

Famiglia «Access Control»

0	Nome	Descrizione	Tipologia	Stato di attivazione
☐	A.11.2.6	Sicurezza delle attrezzature e degli asset fuori sede		Attivo
☐	A.5.1.1	Policy per la sicurezza informatica	ISO	Attivo
☐	A.5.1.2	Revisione delle policy per la sicurezza informatica	ISO	Attivo
☐	A.6.1.1	Ruoli e Responsabilità per la sicurezza informatica	ISO	Attivo
☐	A.6.1.2	Segregazione dei compiti	ISO	Attivo
☐	A.6.2.1	Policy per i dispositivi mobili	ISO	Attivo
☐	A.6.2.2	Telelavoro	ISO	Attivo
☐	A.9.1.2	Accesso alla rete e ai servizi di rete	ISO	Attivo
☐	A.9.4.1	Limitazione delle informazioni di accesso	ISO	Attivo

Processi, Unità organizzative, persone

Elementi 5

Unità di rischio

Ricerca libera...

0	Acronimo	Nome	Team	Stato di attivazione
☐	U.O.P.	Direzione Amministrativa	Team Direzione Amministrativa	Attivo
☐	U.O.P.	Direzione Commerciale	Team Direzione commerciale	Attivo
☐	U.O.P.	Direzione Crediti	Team Crediti	Attivo
☐	U.O.P.	Direzione Generale	Team Direzione Generale	Attivo
☐	RM	Risk Management	ORM - Operational Risk Management	Attivo

Elementi 4

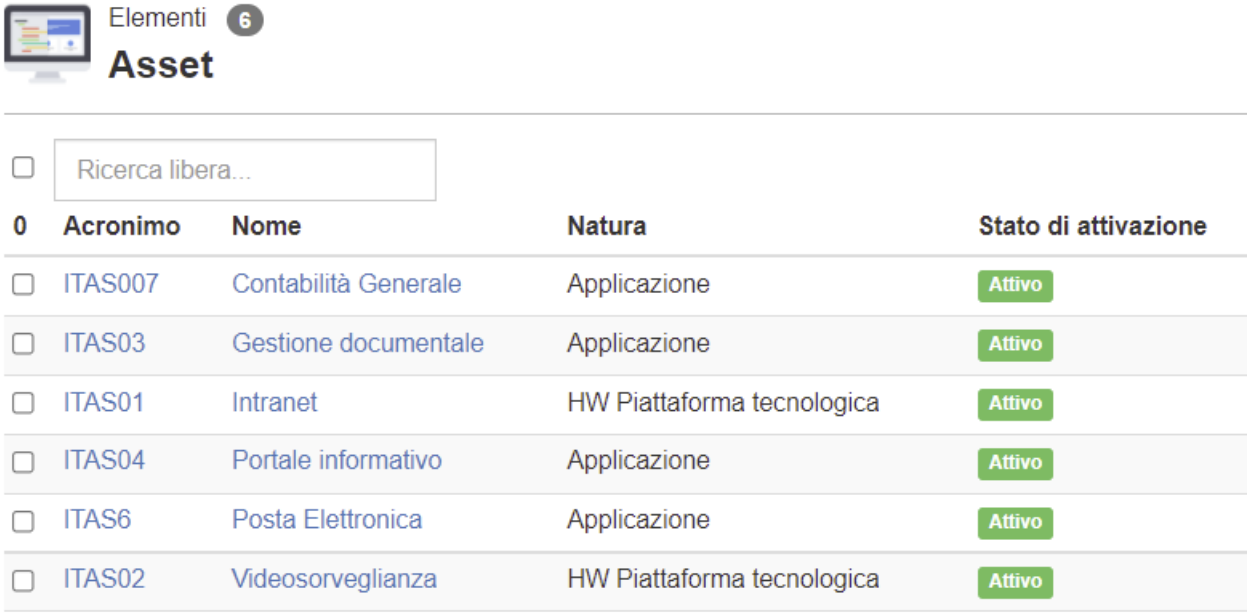
Processi

+

Ricerca libera...

0	Acronimo	Nome	Tipologia	Unità organizzativa	Stato di attivazione
☐	02.01.01	Definizione delle linee strategiche e coerenza delle stesse con l'orizzonte previsivo considerato	INTERNA	Direzione Amministrativa	Attivo
☐	01.01.02	Pianificazione strategica	INTERNA	Direzione Generale	Attivo
☐	01.01.01	Pianificazione ed Organizzazione	INTERNA	Direzione Generale	Attivo
☐	02.01.02	Valutazione sullo stato di conformità ai fini ICAAP	INTERNA	Risk Management	Attivo

Asset informatici



Identification: Eventi

In questa fase si raccolgono gli eventi che sono successi che possono essere catalogati come

- Eventi di rischio operativo
- Incidenti informatici
- Reclami
- Multe e procedimenti amministrativi
- Etc…

Esempio di evento di perdita

Informazioni di registrazione

Nome pratica	Risarcimento per errati prelievi
Data di rilevazione	26/10/18
Data di accadimento	09/10/18
Descrizione dell'evento	L'amministratore di sostegno della cliente chiede il risarcimento di euro 3.000 per l'errato prelievo. La Sig.ra Tizia non ha la capacità di intendere e volere, ed il cassiere ha proceduto ugualmente alla consegna del denaro richiesto senza nulla osta dell'amministratore di sostegno.
Note	

Dettaglio

Protocollo	LE000003
Id esterno	
Stato	Certificato
Data inserimento	26/10/18
Assegnato a	Rossi, Mario [MAT01]
Id di gruppo	
Evento padre	

Indice e scaletta del corso

- **Seconda parte: una metodologia per l'analisi e la gestione del rischio operativo**
  - Risk assessment .
    - Risk Prioritization
    - Risk Identification
    - Risk Mapping
    - Risk Evaluation
  - Risk Management
    - Risk Monitor
    - Risk Mitigation

Risk Mapping

- **E’ la fase più di studio e di analisi delle informazioni raccolte per poter individuare i punti di analisi.**
  - Si incrociano informazioni sui processi con i rischi potenziali
  - Asset con i processi e con le minacce
  - Adempimenti con i processi con i controlli
  - Scenari di rischio con minacce
  - Eventi con rischi nei processi.

Il Rischio di compliance

- **Il rischio di compliance**

  Per ogni processo aziendale occorre valutare accuratamente se le attività svolte nel processo aziendale sono nel perimetro di impatto dell'adempimento. In altre parole occorre valutare se esiste una prescrizione specifica o un controllo che deve essere fatto per assicurarsi che non si violi la regola normativa sottostante il singolo adempimento. Il Rischio di Compliance è il rischio che in un determinato processo aziendale l'azienda non sia adempiente rispetto ad una prescrizione/regola imposta dalla legge. .

Esempio in riferimento all'adempimento di prima relativo all'argomento «modalità di accesso alle informazioni» si definisce un Rischio nel processo specifico di gestione conti correnti la possibilità che siano eseguiti da persone non autorizzate accessi a dati e documenti riservati.

Il valore del danno potenziale può essere esplicitato nel valore della sanzione, nell'effetto reputazionale o danno di immagine se il cliente lo viene a sapere e rende pubblico l'accaduto.

Il rischio di compliance

- **Giurisprudenza:**

è utile andare a vedere come ha sentenziato un giudice o un'autorità di settore relativamente agli adempimenti o agli argomenti analizzati:

Tribunale Asti, 03 settembre 2012

Non è condizione di per sé stessa sufficiente per escludere la possibilità di intrusioni indebite da parte di terzi nei conti correnti altrui il semplice rispetto da parte del cliente delle norme di sicurezza sulla custodia delle credenziali di accesso al servizio di home banking.

È infatti plausibile che tali intrusioni siano causate non tanto dal comportamento del cliente, quanto da un basso livello di protezione del servizio offerto dalla banca. Di conseguenza, se la banca non è in grado di dimostrare al contempo la sua completa idoneità tecnica nella prestazione del servizio di home banking e la negligenza del comportamento del cliente nella custodia delle credenziali di accesso, è responsabile e deve essere condannata alla rifusione delle somme sottratte.

Provvedimento del Garante per la protezione dei dati personali del 28 maggio 2009

La banca è tenuta a dare attuazione a misure di sicurezza idonee a contenere il rischio di accesso non autorizzato mediante tempestiva disattivazione di credenziali di autenticazione attribuite alla clientela.

Compliance Risk Mapping

Il rischio di compliance è identificato con l'incrocio tra l'adempimento e il processo in cui ci potrebbe essere l'inadempimento.

	Ademp. 1	Ademp 2	Ademp 3	...	Ademp N
Processo n. 1					X
Processo n. 2		X			
Processo n. 3	X		X		
...					
Processo n. N			X		

Esempio di Rischio di Complance

Id	36		
Acronimo	Rapp Cont No Adeg verifica		
Nome	Mancata adeguata verifica della clientela quando si instaura un nuovo rapporto continuativo		
Descrizione	Mancata adeguata verifica della clientela quando si instaura un nuovo rapporto continuativo		
Dominio legale	Antiriciclaggio		
Normativa	DECRETO LEGISLATIVO 21 novembre 2007, n. 231		
Adempimento	Adeguata verifica quando si instaura un rapporto continuativo		
Tipo di rischio			
Applicabilità	Applicabile		
Stato	Attivo (dal 14/05/2012)		
Fattori di rischio	Fattore umano Prodotti	**Rischi impattati**	Sanzione Reputazionale Crimine Frode
Natura del rischio	Esterna	**Strategia di trattamento**	Evitare
Unità organizzativa	Antiriciclaggio		
Sottoprocesso	Adeguata verifica		
Sottoprocessi secondari			

Operational Risk Mapping

Le categorie di rischio possono essere un semplice albero tassonomico a più livelli (Es. Tassonomia di Basilea 2). Ognuno degli incroci individua un particolare rischio nel singolo processo

	Risk Cat 1	Risk Cat 2	Risk Cat 3	...	Risk Cat N
Processo n. 1					x
Processo n. 2		x			
Processo n. 3	x		x		
...					
Processo n. N			x		

Esempio di Rischio Operativo

Caratteristiche

Protocollo	RSK00002
Titolo	Indisponibilità sistema informativo
Descrizione	Indisponibilità del sistema informativo
Processo	P 01 - Processi società Capogruppo P 01.80 - Sistema informativo P 01.80.02 - Gestione del sistema informativo
Sottofase	
Unità organizzativa	IT e Back Office
Responsabile rischio	Follis, Sempronio [MAT19]
Responsabile sostitutivo rischio	Azzurro, Bigulo [MAT20]
Tipologie	RO - Operativo

Controlli

Categorie di rischio 1

I Liv.	II Liv.	III Liv.
F - 6 Interruzioni dell'operatività e disfunzioni dei sistemi	F-1 - Sistemi	F-1-1 - Indisponibilità di sistemi

Indice e scaletta del corso

- **Seconda parte: una metodologia per l'analisi e la gestione del rischio operativo**
  - Risk assessment .
    - Risk Prioritization
    - Risk Identification
    - Risk Mapping
    - Risk Evaluation
  - Risk Management
    - Risk Monitor
    - Risk Mitigation

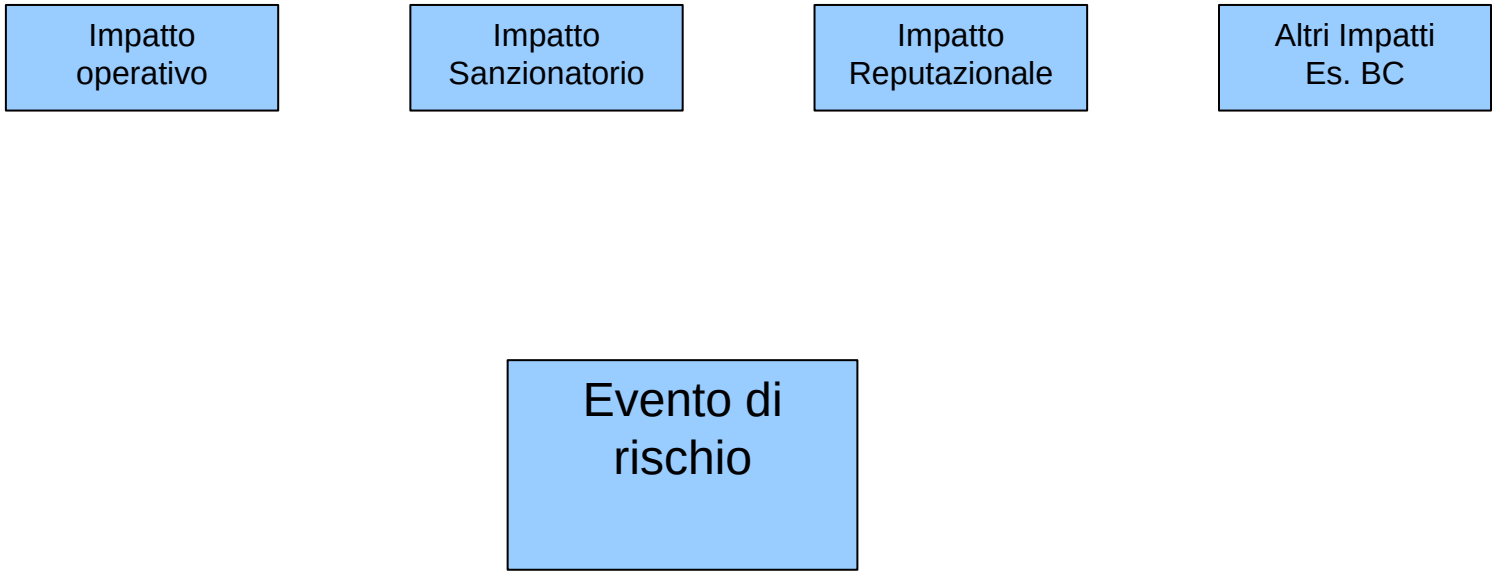
Esempio di eventi di rischio

- A causa di un passaggio a sofferenza tardivo (da parte dell'ufficio gestione sofferenze) è stato concesso il rinnovo del fido al cliente Tizio
- A causa di una errata immissione dei dati da parte della addetta amministrativa è stato fatto un pagamento di 100.000 euro anziché 10.000 Euro.
- Il direttore centrale dell’area Nord Ovest è stato incriminato per associazione mafiosa.

Come faccio a valutare questi eventi?

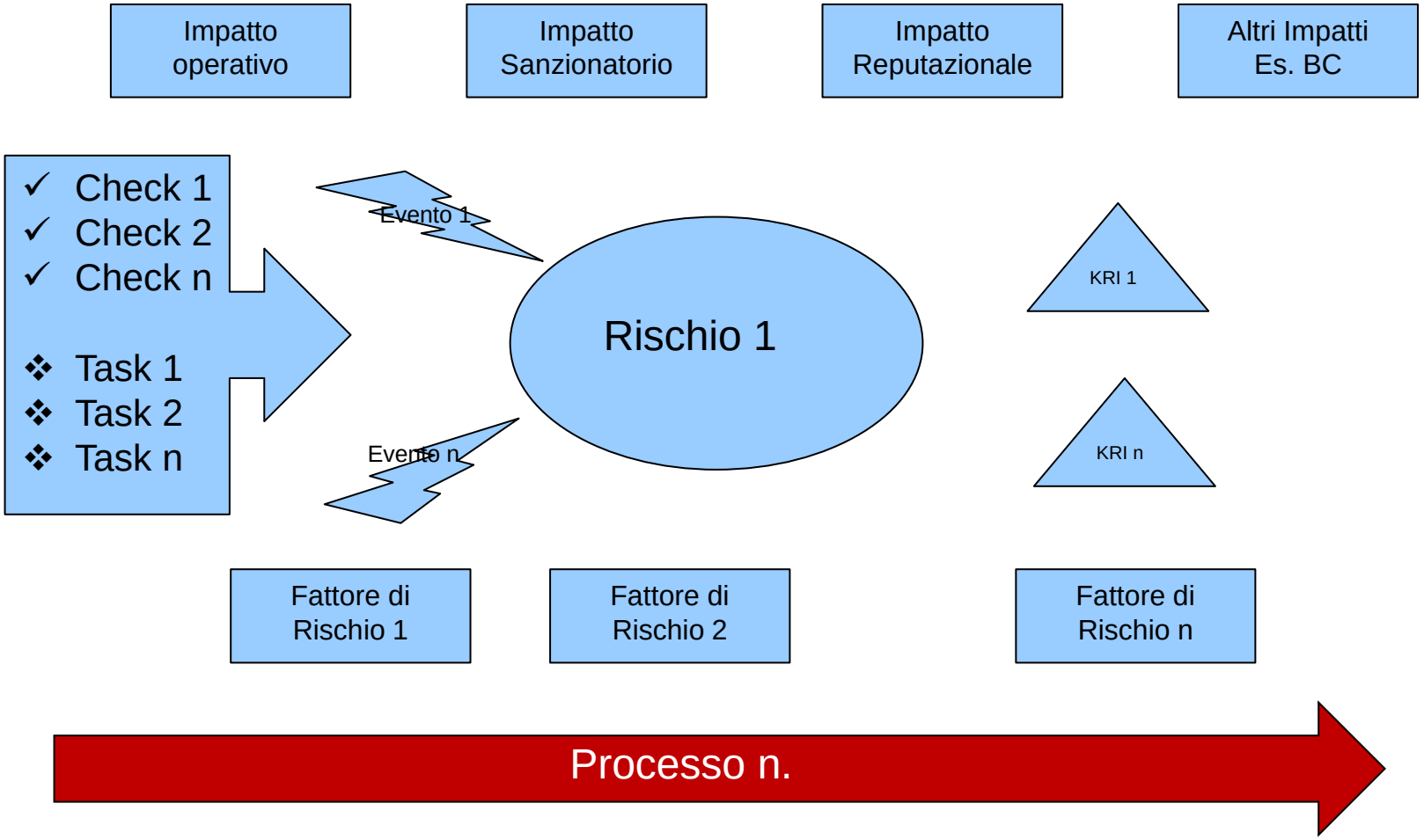
Tocca a voi

Diversi tipi di Impatti



Proviamo a valutare gli impatti di qualcuno degli eventi che abbiamo definito e trovato prima.

Generalizziamo il concetto



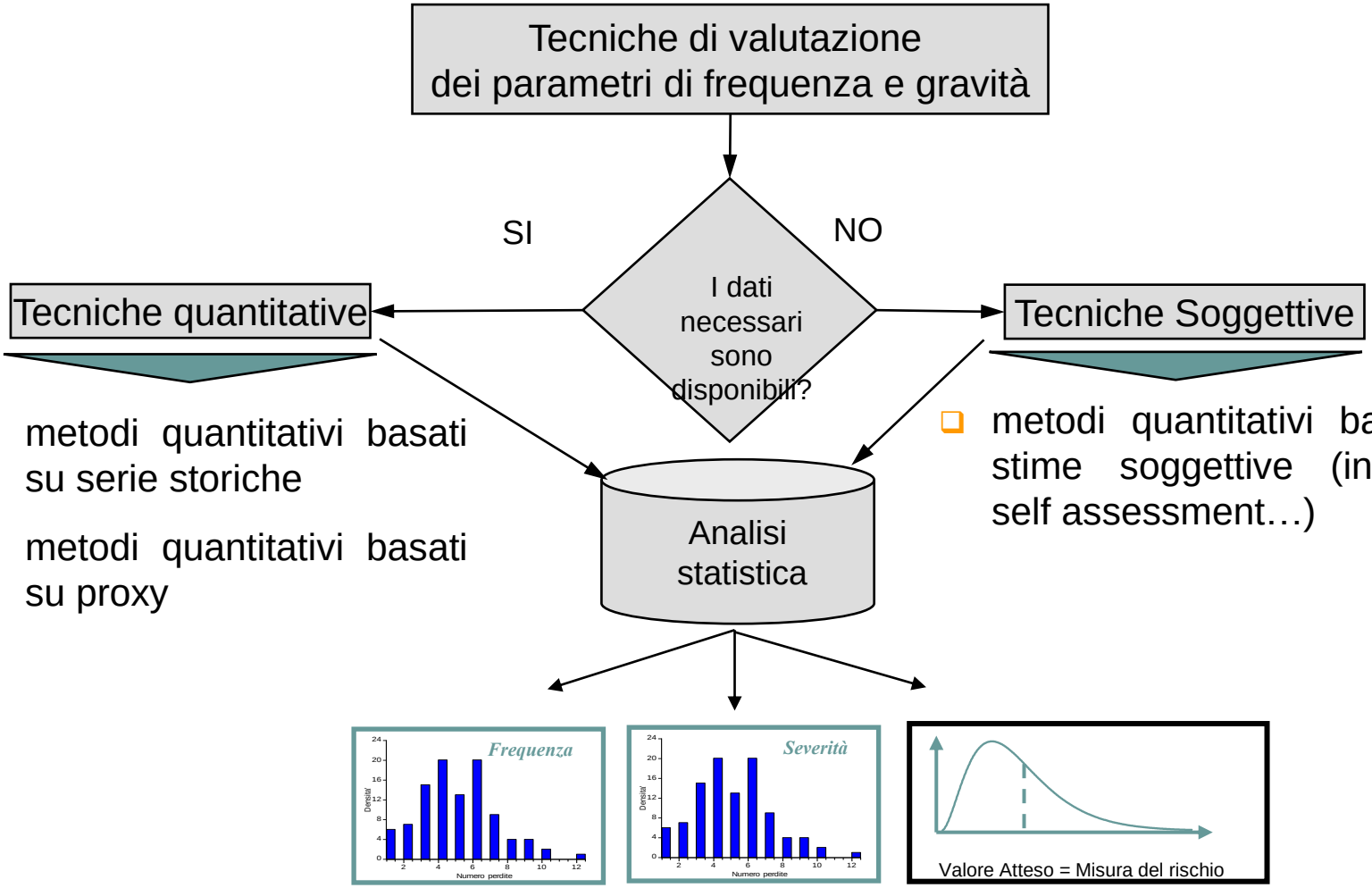
Risk measurement: una definizione

- il rischio operativo è il mancato o parziale conseguimento di un obiettivo dell'impresa
- il mancato o parziale conseguimento di un obiettivo dell'impresa comporta una perdita che può essere espressa sia in termini economici che non. Nel primo caso identifica la perdita economica stimata, mentre nel secondo il danno (in senso lato: perdita di immagine, ad esempio). In termini rigorosi, essendo la probabilità un numero puro, la Perdita ha le stesse dimensioni della Severità
- Il rischio identificabile come perdita è funzione di due componenti: frequenza, severità della perdita. Tali componenti si suppone siano indipendenti tra di loro.

Rischio ≡ Perdita = F(frequenza, severità)

Risk measurement: la stima

- le distribuzioni di frequenza si possono ricavare con diverse tecniche



- metodi quantitativi basati su serie storiche
- metodi quantitativi basati su proxy

- metodi quantitativi basati su stime soggettive (interviste, self assessment…)

Rilevazione dei parametri m,s attraverso l'utilizzo di serie storiche

Rilevazione e Correzione della serie storica

- rilevazione della serie storica sui database aziendali
- correzione dei dati

Anno	Importo (€)
1985	100.000
	421.000
	50.000
	200.000
	329.000
	80.000
1986	600.000
	523.000
1987	90.000
	450.000
	210.000
	100.000
	160.000
	800.000
1988	50.000
	140.000
	340.000
	410.000
	420.000
1989	160.000
	80.000
1990	200.000
	320.000
1991	700.000
	510.000
	50.000
	360.000
	210.000
1992	430.000
	90.000
1993	100.000
	860.000
	480.000
	100.000
	250.000
	60.000
	390.000
	710.000
1994	470.000
	380.000
	100.000
	630.000

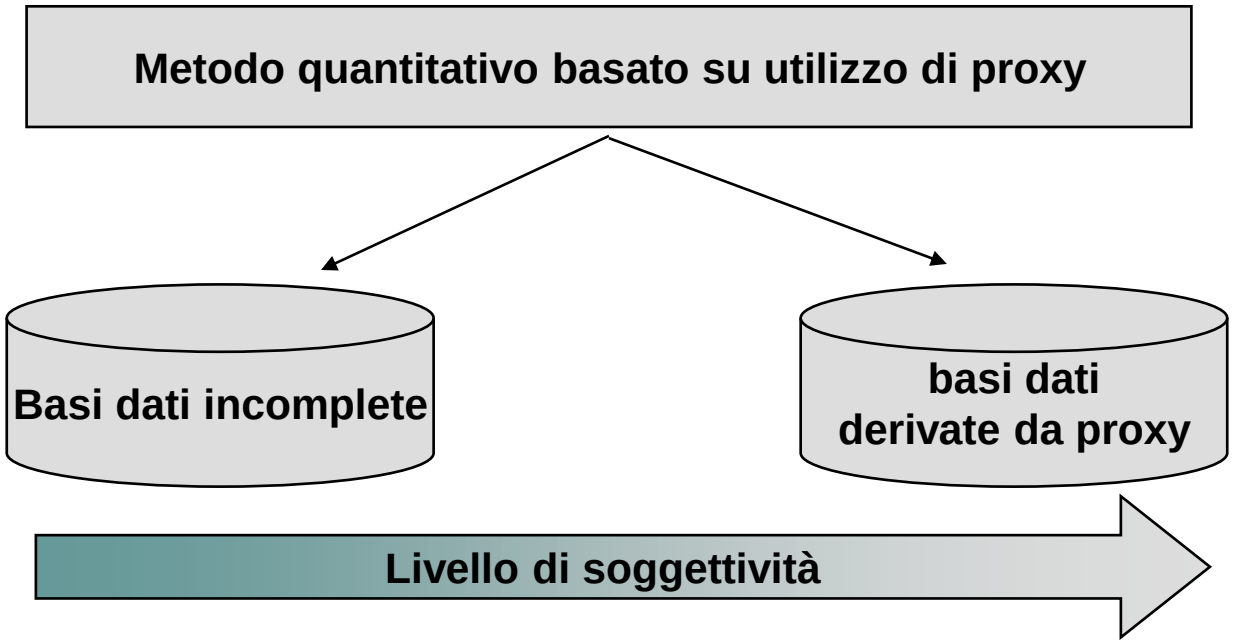
Parametrizzazione delle distribuzioni

- calcolo di media e deviazione std per la distribuzione della frequenza per ogni classe di severità

Media (**m**)	4,2
Deviazione Std (**s**)	2,1
Livello min	90.000
Livello Max.	200.000

Risk measurement: misurazione quantitativa basata su proxy

- si utilizzano quando i dati sono parzialmente o per nulla disponibili



I fattori critici identificati nel processo di Risk Identification possono essere utilizzati come base per determinare quali possono essere le principali variabili esplicative (proxy)

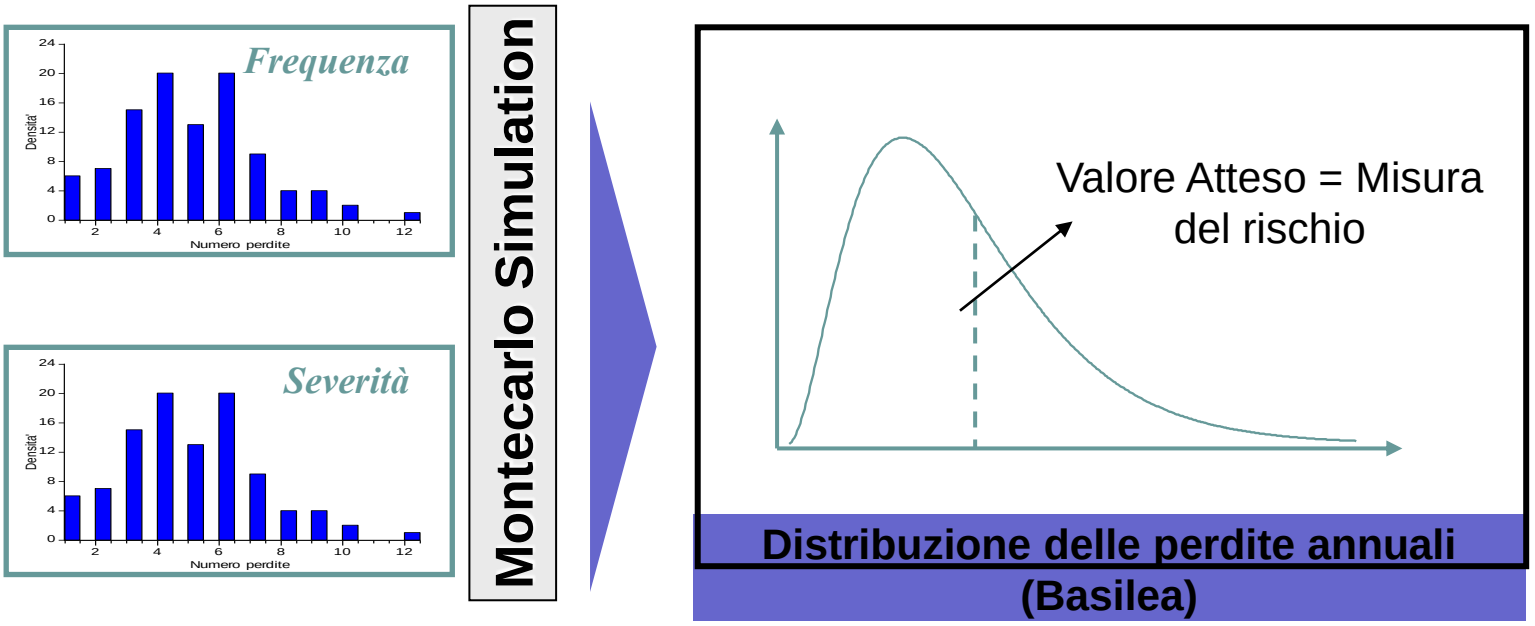
Rilevazione dei parametri m,s attraverso l'utilizzo di stime soggettive

ILLUSTRATIVE

N.	Domanda		Risposta
1	Quante volte in un anno si verifica che i dati su lettera di conferma sono diversi da quelli che risultano alla controparte?	A	Molto raramente (circa 2 volte l'anno)
		B	Raramente (circa 6 volte l'anno)
		C	Spesso (circa 12 volte l'anno)
		D	Molto spesso (circa 30 volte l'anno)
2	Tale frequenza è costante o si rilevano notevoli differenze da anno ad anno?	A	I valori sono molto simili di anno in anno
		B	I valori sono differenti di anno in anno
		C	I valori sono molto differenti di anno in anno
3	Un evento di questo tipo provoca, di solito, un danno…	A	Trascurabile, l'operatività dell'UP non viene compromessa
		B	Lieve, l'operatività dell'UP viene lievemente ridotta
		C	Rilevante, l'operatività dell'UP viene compromessa
		D	Grave, l'operatività dell'UP viene interrotta
4	Il danno provocato è sempre quello indicato nel punto 3?	A	Sì, il danno provocato è molto spesso simile
		B	No, varia di anno in anno
		C	Il fenomeno è molto variabile

Risk measurement: Analisi Montecarlo

- Per una analisi più completa occorrerebbe stimare la probabilità della frequenza e la probabilità della severità e, dopo aver individuato i parametri (media e deviazione standard) di ciascun Risk Driver, con il metodo Montecarlo ottenere una stima della distribuzione della perdita attesa legata a quel determinato evento rischioso



Indice e scaletta del corso

- **Seconda parte: una metodologia per l'analisi e la gestione del rischio operativo**
  - Risk assessment .
    - Risk Prioritization
    - Risk Identification
    - Risk Mapping
    - Risk Evaluation
  - Risk Management
    - Risk Monitor
    - Risk Mitigation
-

Monitor

- **L’idea chiave è che nel Risk Assessment faccio una fotografia statica della mia situazione del rischio, con il monitor invece metto in piedi uno strumento e un processo per il monitoraggio continuo del mio rischio operativo per poter … volare verso i miei obiettivi**

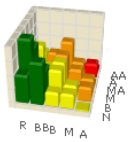
Esempio di monitor

Risks

Sub process: Cartolariz. 1 **Assessment:** Q1 2009 **Risk category:** All **Show top:** 5

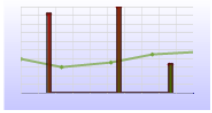
Risk	Risk Level	Loss Events		KRIs	Tasks
		Count	Amount		
MFT_F.1.3_2: Informazioni assenti	Extreme	2	2.123,00€	3	-
MFT_A.2.2_1: Azioni Volontarie	Extreme	1	1.936,20€	1	-
MFT_A.2.6_2: Reato di Corruzione	Moderate	-	-	2	1
MFT_G.1.7_1: Tenuta documentazione	Moderate	-	-	1	-
MFT_F.1.1_1: Rischi IT	Low	-	-	5	2

1 2 3



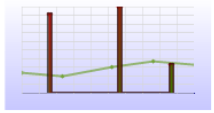
KRI

Tentativi di accesso non autorizzati



Media giornaliera: 43

Contratti con informazioni insufficienti



Percentuale su totale: 10%

Tasks

Assigned to	Description	Status	Due date	Reference
mmarino	Riorganizzazione controlli su rischi di corruzione	Completed	20/02/2009	Risk: MFT_A.2.6_2
mmarino	Esaminare sistemi autenticazione portale	Completed	10/01/2009	L.E.: Furto di informazioni
mmarino	Riorganizzare sistema di gestione informazioni	In progress (20%)	-	Risk: MFT_F.1.1_1

1

Risk Shelter 1.2 p3
Copyright © Augeos s.r.l. 2005-2009
www.augeos.it
supporto@augeos.it

Done Local intranet 100%

Esempio di scheda di assessment

Informazioni generali | LDC 1 | Indicatore di rischio 1 | Analisi dei Livelli di Rischio | Informazioni addizionali | Note | Allegati 0

Scheda di valutazione del rischio

Caratteristiche

Assessment	Assessment 2018
Rischio	Contratti firmati dai clienti erroneamente o parzialmente
Categorie di processo	• P 01 - Processi società Capogruppo • P 01.02 - Intermediazione assicurativa • P 01.02.04 - Stipula dei contratti
Tipologia	
Unità organizzativa	Agenzia
Responsabile rischio	
Responsabile sostitutivo rischio	
Stato attivazione	Attivo

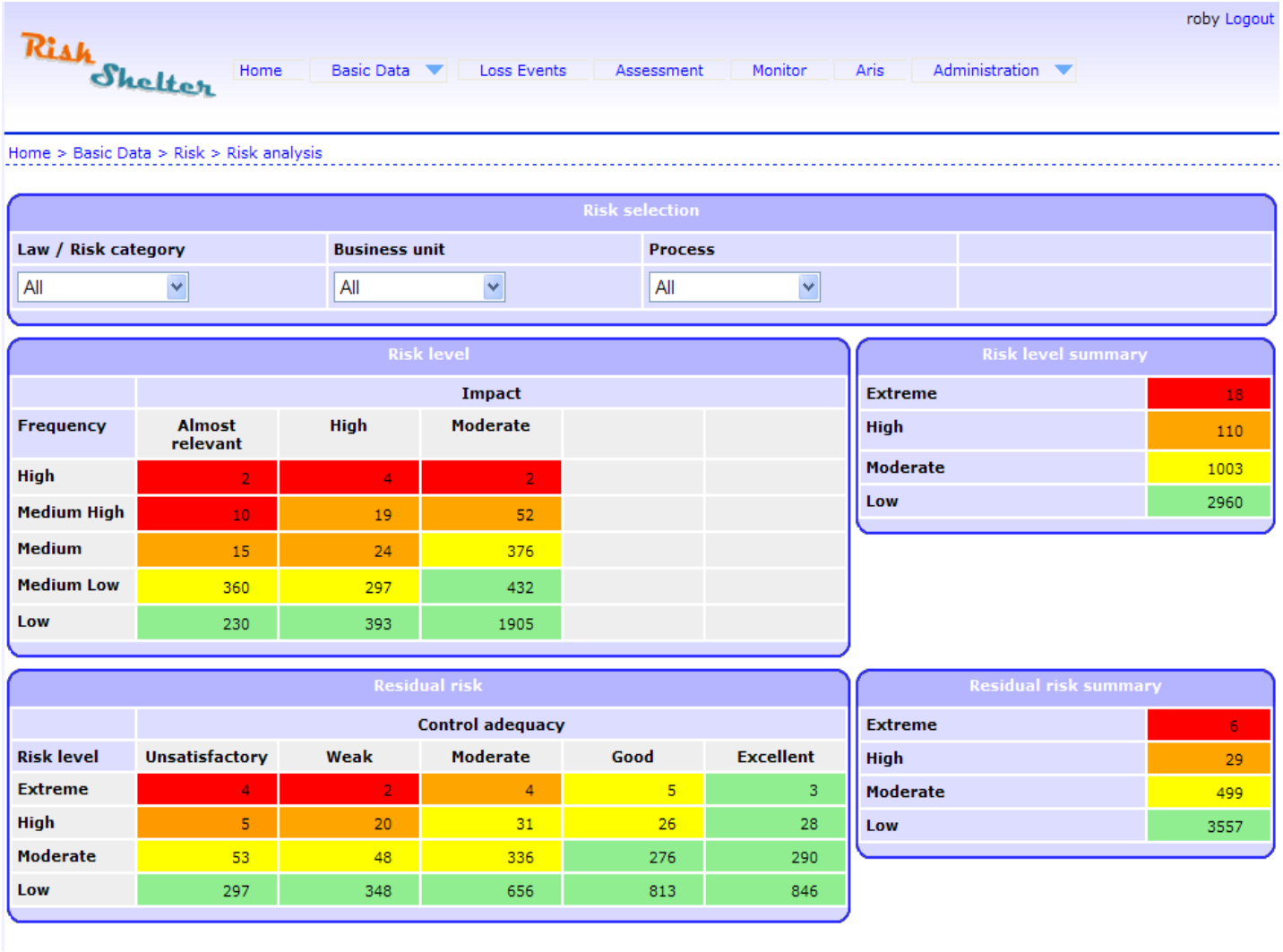
Dettaglio delle valutazioni

	Rischio lordo	Rischio netto
Base Case Scenario	Medio	Medio
Worst Case Scenario	Alto	Alto

Per l'analisi dei livelli di rischio, si rinvia alla relativa tab.
(*) indica se il livello rischio è quello di override inserito dal Risk Manager

Frequenza attività - COMPLIANCE	Medio
Impatto reputazionale (qualitativo)	Basso

Esempio sintesi del Risk Assessment



roby Logout

Risk Shelter

Home | Basic Data | Loss Events | Assessment | Monitor | Aris | Administration

Home > Basic Data > Risk > Risk analysis

Risk selection

Law / Risk category	Business unit	Process
All	All	All

Risk level

Frequency	Impact: Almost relevant	High	Moderate
High	2	4	2
Medium High	10	19	52
Medium	15	24	376
Medium Low	360	297	432
Low	230	393	1905

Risk level summary

Extreme	18
High	110
Moderate	1003
Low	2960

Residual risk

Risk level	Control adequacy: Unsatisfactory	Weak	Moderate	Good	Excellent
Extreme	4	2	4	5	3
High	5	20	31	26	28
Moderate	53	48	336	276	290
Low	297	348	656	813	846

Residual risk summary

Extreme	6
High	29
Moderate	499
Low	3557

Risk Apetite Framework

E’ stato introdotto nell’ordinamento di vigilanza italiano il concetto di **risk appetite framework** (**RAF**). E’ contenuto nella Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013 (si applica alle Banche e non alle finanziarie ex 106 e 107 TUB, almeno sino a che non è completato il riordino della disciplina di vigilanza di queste ultime).

> ***«risk appetite framerwork***» – “RAF” (sistema degli obiettivi di rischio): il quadro di riferimento che definisce – in coerenza con il massimo rischio assumibile, il *business model* e il piano strategico – la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli (cfr. Allegato C).

RAF

di seguito, le definizioni dei concetti rilevanti ai fini del RAF:

*risk capacity (**massimo rischio assumibile**)*: il livello massimo di rischio che una banca è tecnicamente in grado di assumere senza violare i requisiti regolamentari o gli altri vincoli imposti dagli azionisti o dall'autorità di vigilanza;

r*isk appetite (**obiettivo di rischio** o **propensione al rischio**)*: il livello di rischio (complessivo e per tipologia) che la banca intende assumere per il perseguimento dei suoi obiettivi strategici;

*risk tolerance (**soglia di tollerenza**)*: la devianza massima dal *risk appetite* consentita; la soglia di tolleranza è fissata in modo da assicurare in ogni caso alla banca margini sufficienti per operare, anche in condizioni di stress, entro il massimo rischio assumibile. Nel caso in cui sia consentita l'assunzione di rischio oltre l'obiettivo di rischio fissato, fermo restando il rispetto della soglia di tolleranza, sono individuate le azioni gestionali necessarie per ricondurre il rischio assunto entro l'obiettivo prestabilito;

*risk profile (**rischio effettivo**)*: il rischio effettivamente assunto, misurato in un determinato istante temporale;

*risk limits (**limiti di rischio**)*: l'articolazione degli obiettivi di rischio in limiti operativi, definiti, in linea con il principio di proporzionalità, per tipologie di rischio, unità e o linee di *business*, linee di prodotto, tipologie di clienti;

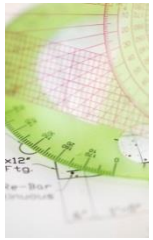
La soluzione: la fase di risk evaluation

Misurazione dei fattori critici o Key Risk Indicator

- i fattori critici possono essere misurati con delle specifiche sonde, che ne misurano il valore con delle scale numeriche. Ad una variazione del valore del fenomeno che la sonda rileva corrisponde una variazione del rischio.






Fattori critici di controllo: sono quelli che possono essere controllati attraverso il processo di mitigation

Fattori critici fuori controllo: sono quelli che non possono essere controllati attraverso il processo di mitigation (normalmente variabili esogene)

Esempio sonda qualità dei processi

APRILE 2007	lun	mar	mer	gio	ven	lun	mar			REFERENTE: DR. XXXXXXX	
TABELLA N° 4	2	3	4	12	13	16	17				
RISCONTRI E REGOLAMENTI											
Non coincidenza tra poteri di firma/limitanti interne e lettere di conferma inviate alle controparti terze	**COMPILATO CON DATI FORNITI DA XXXXXX**										
								0	0,0	0,2	0,0
Numero totale operazioni PORTALE+M.P.	**300**	**255**	**254**	**338**	**332**	**347**	**328**	**6973**			
Non coincidenza tra le condizioni applicate e quelle concordate:	**COMPILATO CON DATI FORNITI DA XXXXXX**										
.. conto finanziamento Società								0	0,0	0,2	0,0
Numero totale operazioni PORTALE+M.P.	**300**	**255**	**254**	**338**	**332**	**347**	**328**	**6973**			
Disallineamento tra i sistemi Middle Officee Sap-FI:	**COMPILATO CON DATI FORNITI DA XXXXXX**										
..modulo securities								0	0,0	0,1	0,0
Numero totale operazioni PORTALE+M.P.	**300**	**255**	**254**	**338**	**332**	**347**	**328**	**6973**			
.. modulo derivatives								0	0,0	0,1	0,0
Numero totale operazioni PORTALE+M.P.	**300**	**255**	**254**	**338**	**332**	**347**	**328**	**6973**			
.. modulo forex								0	0,0	0,1	0,0
Numero totale operazioni PORTALE+M.P.	**300**	**255**	**254**	**338**	**332**	**347**	**328**	**6973**			
Disallineamento delle anagrafiche tra i sistemi Middle Officee Sap-FI:	**COMPILATO CON DATI FORNITI DA XXXXXX**										
.. tempi di aggiornamento in Front Office /Middle Office > di 3 gg. rispetto alla data di richiesta								0	0,0	0,1	0,0
Numero totale anagrafiche censite	**0**	**18**	**0**	**2**	**2**	**2**	**2**	**211**			
.. tempi di aggiornamento in Tieffe > di 3 gg. rispetto alla data di richiesta								0	0,0	0,1	0,0
Numero totale anagrafiche censite	**0**	**18**	**0**	**2**	**2**	**2**	**2**	**211**			
Numero scarti di operazioni non conluite correttamente da Front Office a TIEFFE:				**COMPILATO CON DATI FORNITI DA XXXXXX**							
.. tempi di aggiornamento in Tieffe > di 3 gg. rispetto alla data di richiesta								0	0,0	0,2	0,0
Numero totale anagrafiche censite	**0**	**18**	**0**	**2**	**2**	**2**	**2**	**211**		**1,00**	
									0,0		**100%**

Esempio KRI

Indicatore di rischio

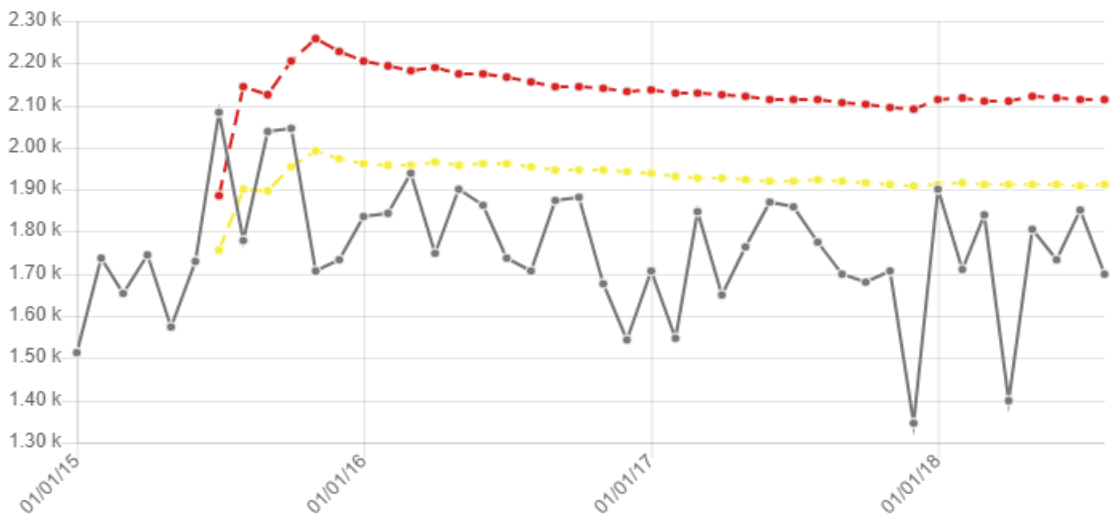
Aperture NDG (adattivo - crescente)

Informazioni Generali | Classificazione | Configurazioni | Misurazioni 44 | Allegati 0

Caratteristiche

Acronimo	2
Descrizione	Aperture NDG
Area	Direzione Commerciale
Funzione di riferimento	RM - Funzione Risk Management
Unità organizzativa	Direzione Commerciale
Asset	
Processo	
Rischio	N.N
Attivo	Attivo
Tags	

Trend Map



Esempio KRI Misurazini e trend

Record delle misurazioni

Ricalcola soglie | Import

Data	#	Soglia gialla	Soglia rossa	Extra-soglia	Test sul trend	Variazione	Tags	Note
01/08/18	1.698,00	1.910,32	2.113,19		▼	⌄		
01/07/18	1.852,00	1.909,20	2.113,56		▼	⌃		
01/06/18	1.734,00	1.911,59	2.118,44		▼	⌄		
01/05/18	1.804,00	1.912,17	2.121,40		▼	⌃		
01/04/18	1.398,00	1.912,26	2.109,48		–	⌄		
01/03/18	1.841,00	1.911,67	2.110,80		–	⌃		
01/02/18	1.709,00	1.914,90	2.116,44		–	⌄		
01/11/15	1.707,00	1.990,44	2.257,21		▲	⌄		
01/10/15	2.044,00	1.952,06	2.205,46	Alert	▲	⌃		
01/09/15	2.039,00	1.897,41	2.124,43	Alert	–	⌃		
01/08/15	1.778,00	1.902,35	2.145,72		–	⌄		
01/07/15	2.082,00	1.756,48	1.886,65	Risk Tolerance		⌃		
01/06/15	1.730,00					⌃		

Un KRI molto importante: la qualità dei dati

- In una società in cui l'informazione dematerializzata è sempre più determinante per lo svolgimento del core business di una impresa, **la qualità dei dati** e delle informazioni è diventato **un fattore chiave per il suo successo**.

- Molti eventi anche di grande impatto hanno avuto come causa la scarsa qualità dei dati o dei processi di controllo relativi. La tragedia dello shuttle, per esempio, è riconducibile ad un problema qualità di dati.

La centralità ed il valore dell'informazione per le organizzazioni

"Si stima che la scarsa qualità dei dati e delle informazioni comporta per le aziende americane una perdita di 600 bilioni di $ l'anno"

Data Warehousing Institute

"La scarsa qualità dei dati costituisce nel 50% dei casi la causa principale del fallimento delle strategie e dei progetti di CRM"

"Customer Data Quality and Integration: The Foundation of Successful CRM."
Gartner, Inc. 26 November 2001

"…Poiché la qualità e l'affidabilità del sistema di misurazione sono ampiamente in funzione della qualità dei dati e delle varie ipotesi utilizzate dal modello, la direzione della Banca dovrebbe annettere una particolare attenzione a questi aspetti" …

Dagli atti del Comitato di Basilea II

"Nel 2006, la Regione Sicilia ha mandato al macero 400.000 tessere sanitarie elettroniche in quanto stampate con dati errati, altre 21.000 sono state inviate a cittadini che non ne avevano diritto, circa 90.000 tessere risultavano intestate a persone defunte"

La Repubblica, 6 aprile 2007

" Tipicamente le organizzazioni spendono tra il 20% e il 40% del budget per l'ICT nell'aggiornamento delle procedure di migrazione dei dati, di conversione (cambiare i dati in altre forme, stati o prodotti), di gestione (correzione e pulizia)".

John Zachman (Industry pioneer)

Data Quality Dimensions

Le "*Data Quality Dimensions*" rappresentano gli indici base sui quali viene misurata la qualità di un dato

Completezza

Ampiezza, profondità e adeguatezza del dato in relazione agli obiettivi della struttura che lo utilizza

Volatilità

Grado di aggiornamento di un dato o di un'informazione rispetto al suo valore reale più recente

Consistenza

Insieme dei vincoli di integrità, di proprietà logiche e di regole semantiche del patrimonio delle informazioni

Accuratezza

Grado di correttezza, attendibilità e assenza di errori di natura semantica e sintattica

A ciascuna dimensione possono essere associate una o più Metriche

Indice e scaletta del corso

- **Seconda parte: una metodologia per l'analisi e la gestione del rischio operativo**
  - Risk assessment .
    - Risk Prioritization
    - Risk Identification
    - Risk Mapping
    - Risk Evaluation
  - Risk Management
    - Risk Monitor
    - Risk Mitigation

Risk Mitigation

- **Il trattamento del rischio implica l'identificazione di tutte le possibili alternative per contenerlo, la valutazione di tali alternative, la predisposizione di piani di mitigation**
- **I piani di mitigazione spesso comportano una ridefinizione o miglioramento dell'organizzazione esistente, introduzione di processi di controllo, identificazione di figure preposte al controllo**
  - Sono azioni spesso a medio-lungo termine
  - Spesso trovano resistenze al cambiamento

Mitigation: identificazione delle alternative

- **Evitare il rischio non procedendo all'attività (quando questo è possibile)**
  - Questo potrebbe avere come conseguenza l'innalzamento di rischio in altre aree o la riduzione delle opportunità di profitto o di raggiungimento degli obiettivi.
- **Incidere sulla frequenza della manifestazione dell'evento di perdita**
  - Questo comporta l'aumento della probabilità del raggiungimento dell'obiettivo
- **Incidere sulla gravità dell'evento**
  - Significa diminuire l'entità delle conseguenze negative
- **Trasferire il rischio ad altre entità o all'esterno**
  - In genere significa porre in essere dei contratti assicurativi o degli accordi con altre entità dell'azienda.
  - Sono spesso onerose, costose,
  - Dovrebbe essere buona prassi quella di trasferire i rischi alle parti del'azienda che siano maggiormente in grado di controllarli.
- **Ritenere il rischio:**
  - spesso dopo il trasferimento del rischio rimangono comunque dei rischi residuali
  - A volte rimangono dei rischi non identificati in capo ad alcune organizzazioni (errore nel trasferimento)

Valutazione delle azioni di mitigation

- **Tutte le alternative devono essere valutate in funzione degli obiettivi di riduzione delle perdite stesse, occorre inoltre valutare il costo beneficio dell'intervento.**
  - Occorre valutare anche le conseguenze che un controllo potrebbe causare. A volte l'inserimento di un controllo è più dannoso o costoso del lasciare il rischio senza controlli.
  - La scelta deve sempre essere fatta in equilibrio tra questi fattori

Preparazione Piani di progetto

- **I piani di progetto devono**
  - Identificare le responsabilità
  - Identificare i programmi su cui intervenire
  - Definire gli obiettivi dell'intervento
  - Il budget
  - Le misure che devono essere monitorate per valutare i risultati
  - Tempi

Preparazione e gestione Piani di progetto

- **I piani di progetto vengono proposti da**
  - Risk Manager
  - Dirigenza
  - Audit
  - Responsabile della RU
- **Vengono presi in carico da**
  - Responsabile della RU
- **Vengono approvati da**
  - Risk Manager
  - Audit
  - Dirigenza
- **Vengono monitorati da**
  - Risk Manager
  - Dirigenza
  - Audit

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Un po’di vocaboli

Ransomware
Malware che induce limitazioni nell’uso di un dispositivo (ad esempio criptando i dati (crypto-ransomware), o impedendo l’accesso al dispositivo (locker-ransomware).

Malware
Definizione generica di applicazioni finalizzate a arrecare in qualche modo danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili…).

Phishing
Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all’originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.

Dark web
Parte oscura del World Wide Web, sottoinsieme del deep web,accessibile mediante l’uso di apposite applicazioni software.

Un po’ di vocaboli

Hacktivism
Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.

Spyware
Malware che raccoglie informazioni sul comportamento della vittima trasmettendole all’attaccante.

SQL injection
Tecnica di attacco basata sull’uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.

Dos (Denial of Service)
Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie:

- applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti);
- volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse.

DDoS (Distributed Denial of Service)
Attacchi DOS distribuiti, cioè basati sull’uso di una rete di apparati, costituenti in una botnet dai quali parte l’attacco verso l’obiettivo.

Qualche dato

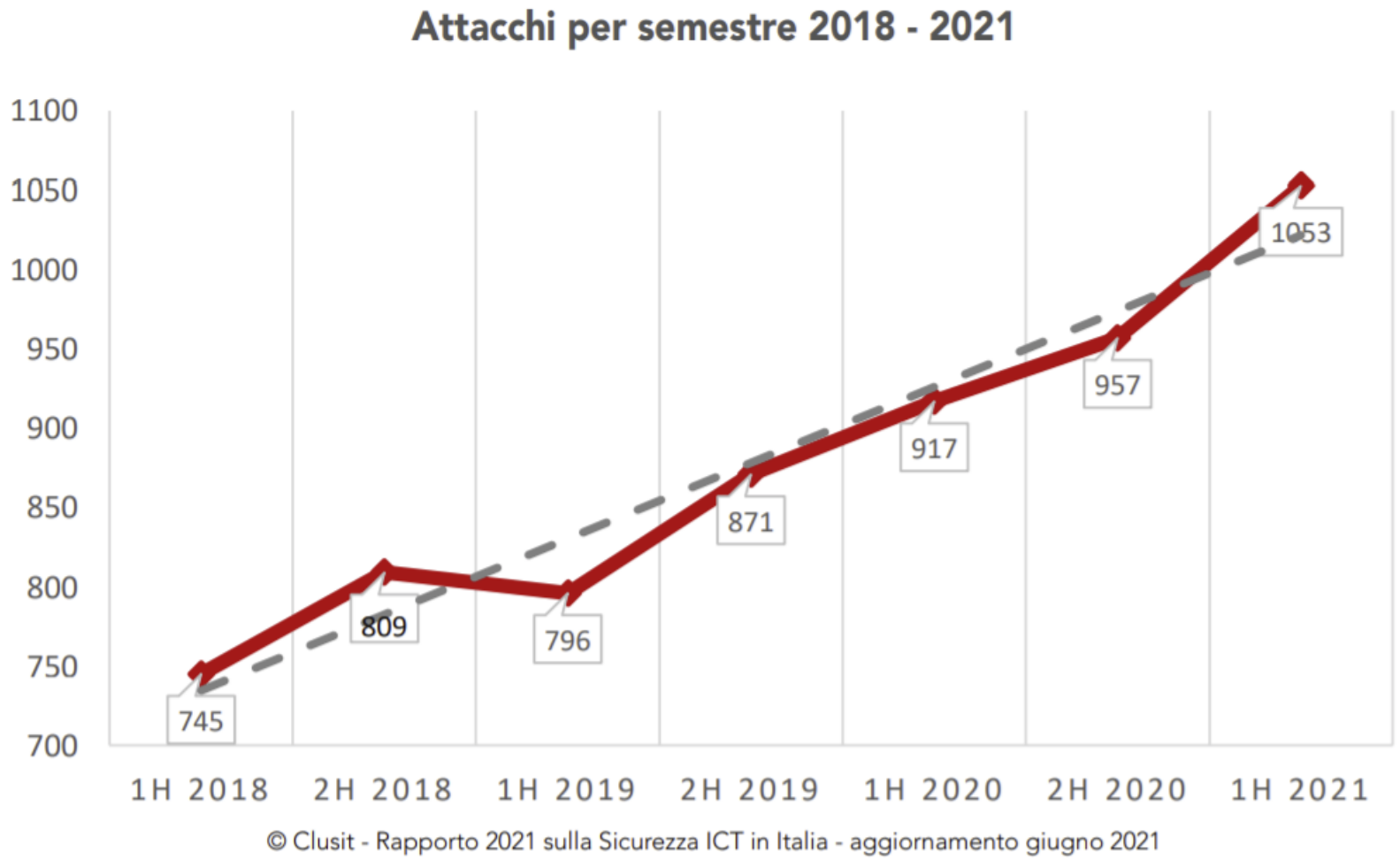
- le perdite derivanti da Cyber Attack sono stimate in **1 trilione di dollari per il 2020 e 6 trilioni per il 2021** in tutto il mondo.
- a la distribuzione geografica delle vittime: nel 1° semestre 2021 la percentuale delle vittime di area americana sono stabili (**dal 45% al 46%),** gli attacchi verso realtà basate in Europa aumentano sensibilmente (**dal 15% al 25%)** mentre rimangono percentualmente quasi invariati quelli rilevati contro organizzazioni asiatiche.

Qualche dato

nella prima metà del 2021 (dal 1°gennaio al 31 agosto), si sono registrati **36 Milioni di eventi malevoli,** in forte aumento rispetto allo stesso periodo dell'anno precedente **(+180%).**

Il fenomeno più preoccupante è l'incremento dell'attività dei **ransomware** con richiesta di riscatto. Infatti, è stata osservata una crescita dell'attività di questo malware di circa **il 350%** rispetto allo stesso periodo dello scorso anno. E le conseguenze causate da questa tipologia di attacchi, sempre più aggressivi, diventano in qualche modo ancora più evidenti. Si vedano ad esempio gli attacchi a danno di strutture pubbliche che hanno bloccato l'operatività quotidiana.

Introduzione IT Risk Management



Rischi

- **Tecnologia**: i fattori legati alla tecnologia comprendono i problemi relativi ai sitemi informativi, agli errori di programmazione nelle applicazioni, interruzione nella struttura di rete, fino a includere eventuali fallimenti nei sistemi di telecomunicazioni;

- Alcune considerazioni generali

Crescente diffusione dei sistemi informatici

Automazione della attività e dei processi produttivi delle aziende

Esigenza di garantire il corretto funzionamento

- Per garantire il medesimo livello di perforamnce precedente

Elementi di rischio dei Sistemi informativi

- **Aumentata numerosità e pervasività degli apparati tecnologici usati nei processi produttivi**
  - Questo comporta una esigenza di continuità di funzionamento e di funzionamento corretto degli apparati. Oggi in molti settori non si potrebbe più fare a meno delle tecnologie che hanno aumentato la produttività e cambiato radicalmente le modalità e le abitudini di lavoro.

- **Il tasso di innovazione tecnologica è mediamente elevato nei paesi industrializzati e rende obsolete rapidamente conoscenze e capacità delle persone che con esse lavorano.**
  - Questo comporta una esigenza di formazione continua e quindi di conseguenza un rischio di osolescenza rapida delle competenze acquisite

Elementi di rischio dei Sistemi informativi

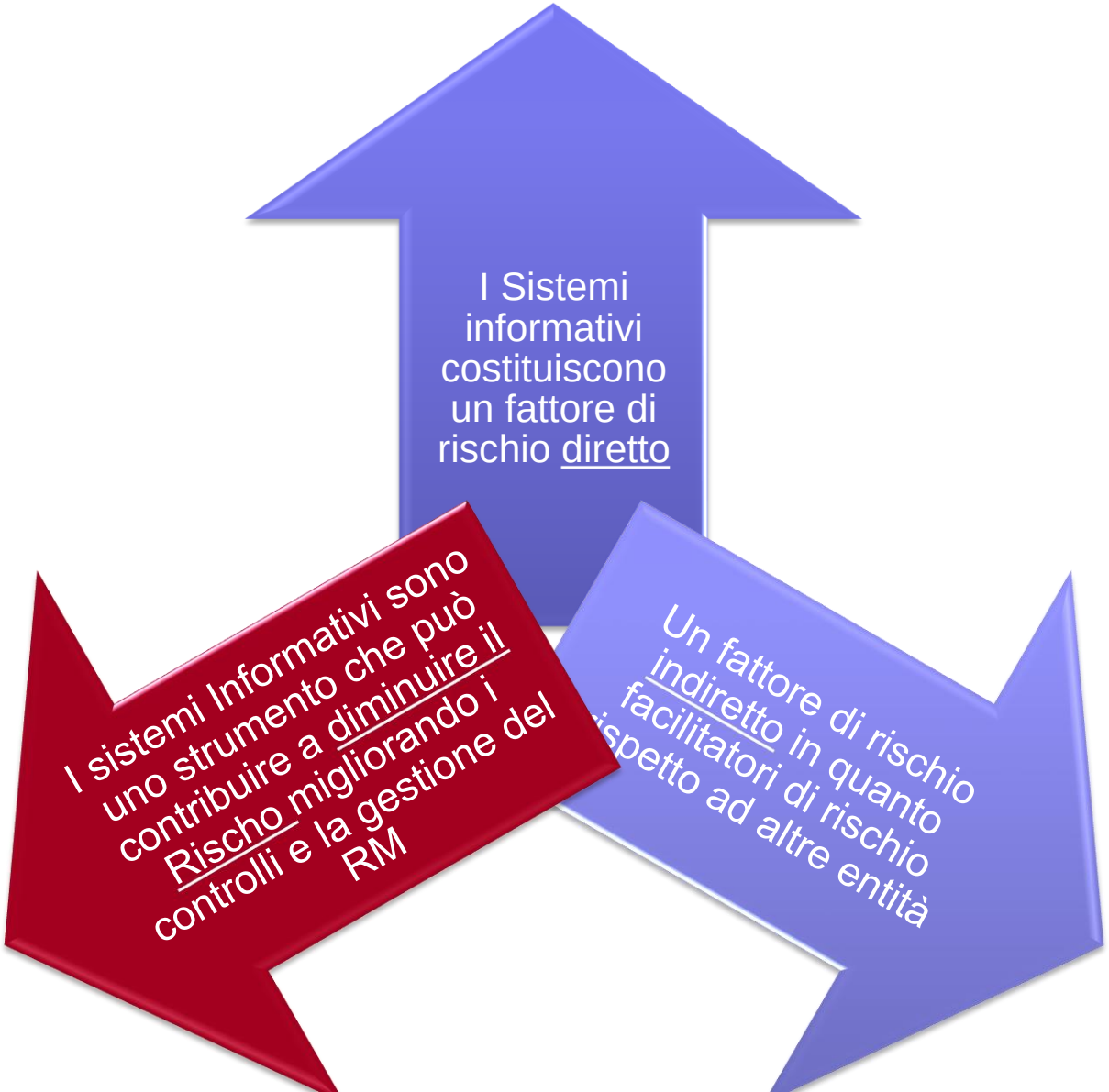
- **Aumentata integrazione tra sistemi informativi interni ed esterni**
  - Questo comporta un aumento del rischio di intrusione anche ai fini di dolo che rende generalmente più vulnerabile il sistema complessivo.
- **Aumentata facilità con cui si possono immagazzinare dati sensibili**
  - Questo comporta un aumento dei rischi di violazione della legge sulla privacy.
- **Il maggiorre utilizzo di fonti di dati diffuse su diversi sistemi o provenienti da fonti esterni può portare ad errori**
  - Questo comporta un aumento dei rischi dovuti ai problemi di integrazioni tra DB diversi o a scarsa qualità dei dati

Considerazioni generali sul rischio dei Sistemi informativi

Aumento della dipendenza da parte delle aziende dall'uso di nuove tecnologie

Aumento delle esigenze di controlli e di tecniche per prevenire eventuali malfunzionamenti o interruzioni di servizio che possano causare danni al ciclo di processo produttivo

Fattori di Rischio e Sistemi Informativi



Fattori di Rischio Diretti dei Sistemi Informativi

- **Sistemi non progettati bene**
  - la mancanza di qualche tassello nel sistema complessivo può causare un danno o una forte riduzione delle performance complessive del sistema
  - La ridondanza di sistemi o di dati può causare analogamente dei problemi. Si pensi alla ridondanza di dati su sistemi paralleli non perfettamente allineati.
- **Sistemi non integrati bene: sono una delle cause principali di malfunzionamento nei sistemi informativi di organizzazioni complesse.**
  - Errori di integrazione dovuta a errori di progettazione delle interfacce
  - Errori di integrazione dovuta ad errori di interpretazione semantica dei dati
    - Codifiche errate
    - Mancanza di trascodifiche
    - Errori di integrazioni dovuta a scarsa qualità dei dati
  - Errori di progettazione di timing di integrazione in relazione alle velocità di comunicazione

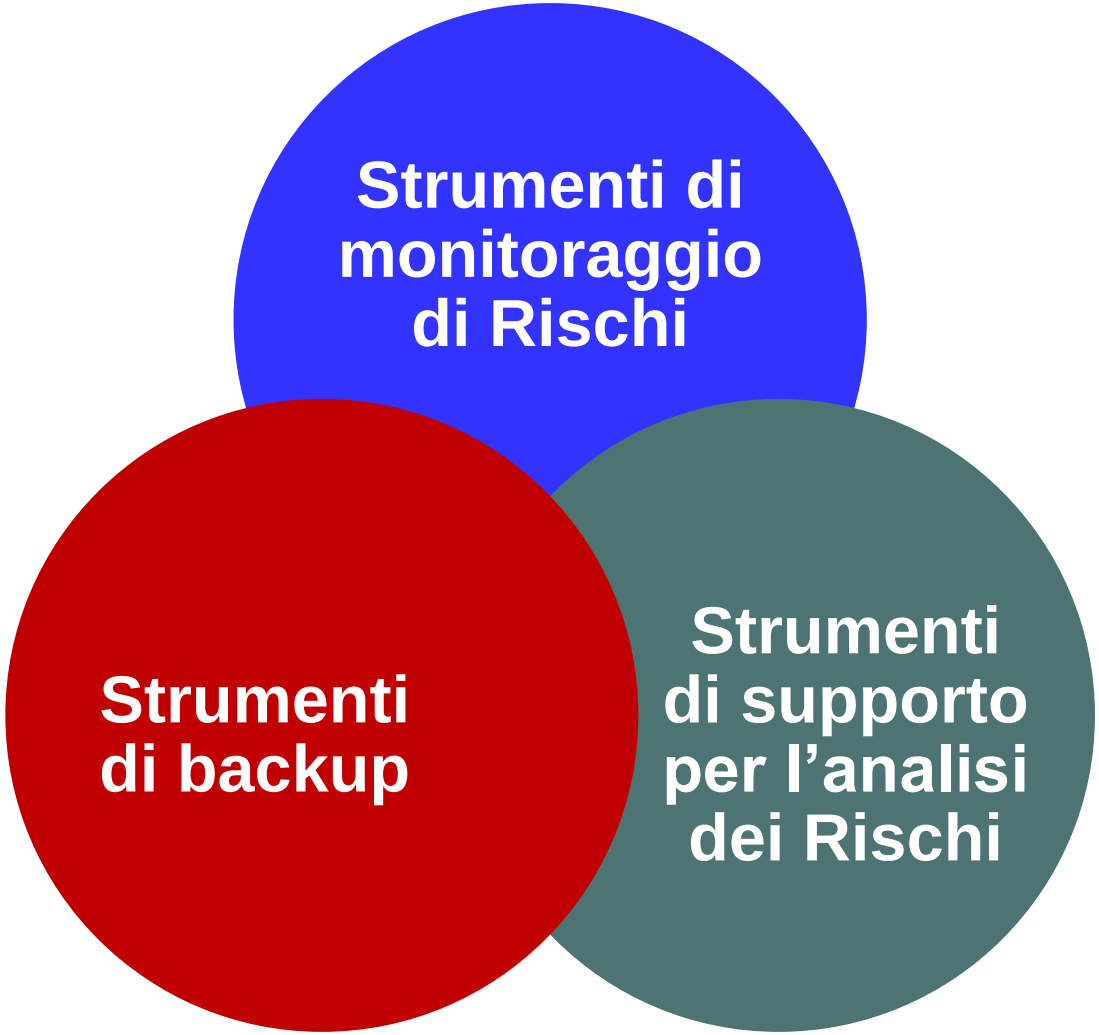
Fattori di Rischio Diretti dei Sistemi Informativi

- **Perdita fisica dei dispositivi hardware:**
  - oggi questo rischio è aumentato molto si pensi alla facilità con cui si possono perdere telefonini, palmari e blackberry con una grande quantità di dati aziendali sensibili inseriti senza grandi protezioni.
- **Attacchi informatici dall'esterno:**
  - È uno dei rischi più temuti dai Responsabili di sistema e non solo. Si è speso molto su questo tema. Rappresenta un'area a se stante nel panorama dei possibili rischi.
  - uso fraudolento di dati sensibili
- **Attacchi informatici dall'interno:**
  - Furto di identità
  - Uso non conforme di dati personali o aziendali per atti fraudolenti da parte del personale dell'azienda

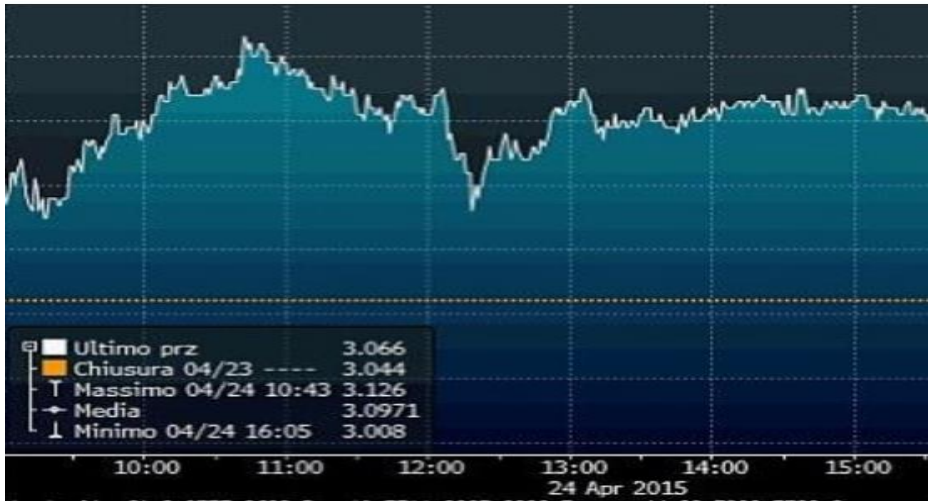
Fattori di Rischio indiretti dei Sistemi Informativi

- **Indirettamente i Sistemi informativi possono essere dei driver che facilitano l'evento di perdita dovuto ad altri fattori**
  - Frode Interna: il personale interno approfitta di qualche situazione contingente per portare una frode o un furto tramite l'uso di tecnologie
  - Incapacità , scarsa preparazione, motivazione del personale addetto all'uso di certe tecnologie
  - Frode esterna: da parte di persone non dell'azienda attraverso l'uso di tecnologia
  - Disfunzioni organizzative che vengono amplificate dall'uso della potenza tecnologica
  - Cadute di immagine (reputazione) dovuta alla lentezza percepita dai clienti relativamente ai sistemi informativi

I Sistemi Informativi come strumento di supporto alla gestione del Rischio



Era un tranquillo pomeriggio di aprile …



24 Aprile 2015 ore 15.40: Intesa Sanpaolo conferma di aver ricevuto oggi **una lettera di dimissioni** dal suo consigliere delegato e CEO, **Carlo Messina** che **ammette di aver falsato la contabilità**, esagerando il risultato netto di 1.920 milioni di euro nel 2014. Considerando queste nuove informazioni, Intesa Sanpaolo riporterebbe **un bilancio in perdita per il 2014**.

Si cercano conferme …

Tramite google si arriva al sito «ufficiale» di Intesa San Paolo dove si trova conferma della notizia in prima pagina e si rafforza la convinzione che è successo qualcosa di grosso.

INTESA SANPAOLO

CHI SIAMO GOVERNANCE INVESTOR RELATIONS SALA STAMPA SOSTENIBILITA' STUDI E RICERCHE BANCA E SOCIETA' LAVORA CON NOI

Sala stampa

> Home > Sala stampa

aggiorna

INTESA SANPAOLO RICEVE LETTERA DAL SUO CEO CHE SI DIMETTE E DICHIARA IRREGOLARITÀ FINANZIARIE

Milano, 24 aprile 2015 – Intesa Sanpaolo conferma di aver ricevuto oggi una lettera dal suo consigliere delegato e CEO, Carlo Messina. La lettera, datata 24 Aprile 2015, è circolata a tutti i membri del Board ed è stata inviata alla CONSOB. Carlo Messina ha ammesso di aver falsato la contabilità, esagerando il risultato netto di 1.920 milioni di euro nel 2014. Considerando queste nuove informazioni, Intesa Sanpaolo riporterebbe un bilancio in perdita per il 2014. "Siamo sconvolti dal contenuto della lettera. Il management di Intesa Sanpaolo rinnova il suo impegno verso clienti, dipendenti e azionisti. Ci siamo riuniti a Milano per avviare un action plan che ci permetta di superare questo momento di crisi" ha dichiarato Gaetano Micciché, nominato CEO dal Board a titolo provvisorio.

Intesa Sanpaolo ribadisce che le sue priorità immediate sono la difesa degli interessi dei clienti, azionisti e dipendenti. Intesa Sanpaolo crede che le sue prospettive di crescita resteranno solide nonostante le attuali difficoltà finanziarie. La direzione di Intesa Sanpaolo è fiduciosa di poter continuare a fornire eccellenti servizi bancari e finanziari ai suoi clienti producendo valore per i suoi azionisti a medio e lungo termine.

Intesa Sanpaolo si impegna a garantire i massimi standard di trasparenza aziendale e coopererà con le autorità competenti per condurre una inchiesta dettagliata in materia. Intesa Sanpaolo terrà i suoi azionisti regolarmente informati sugli sviluppi. Una conferenza stampa volta a portare chiarezza sui nuovi risvolti sarà tenuta al più presto.

Media Relations
+39.02.21118079
stampa@intesasanpaolo-group.com

intesasanpaolo-group.com

"Siamo sconvolti dal contenuto della lettera. Il management di Intesa Sanpaolo rinnova il suo impegno verso clienti, dipendenti e azionisti. Ci siamo riuniti a Milano per avviare un action plan che ci permetta di superare questo momento di crisi" ha dichiarato Gaetano Micciché, nominato CEO dal Board a titolo provvisorio".

Smentita e conseguenze

"Intesa Sanpaolo rende noto che oggi è stato diffuso un comunicato stampa, apparentemente attribuito alla Banca stessa ma in realtà totalmente falso e infondato, nel quale si annunciano le dimissioni del Consigliere Delegato e CEO Carlo Messina"

-3% nel giro di una decina di minuti con scambi intensi

Alla sera stessa l'attacco è rivendicato da gruppi NO TAV

Alcune considerazioni

«Abbiamo passato un brutto quarto d’ora – dichiara il resp. Sicurezza di Banca Intesa - ma i nostri sistemi non sono stati violati. Le nostre difese hanno retto»

La Consob apre un’inchiesta

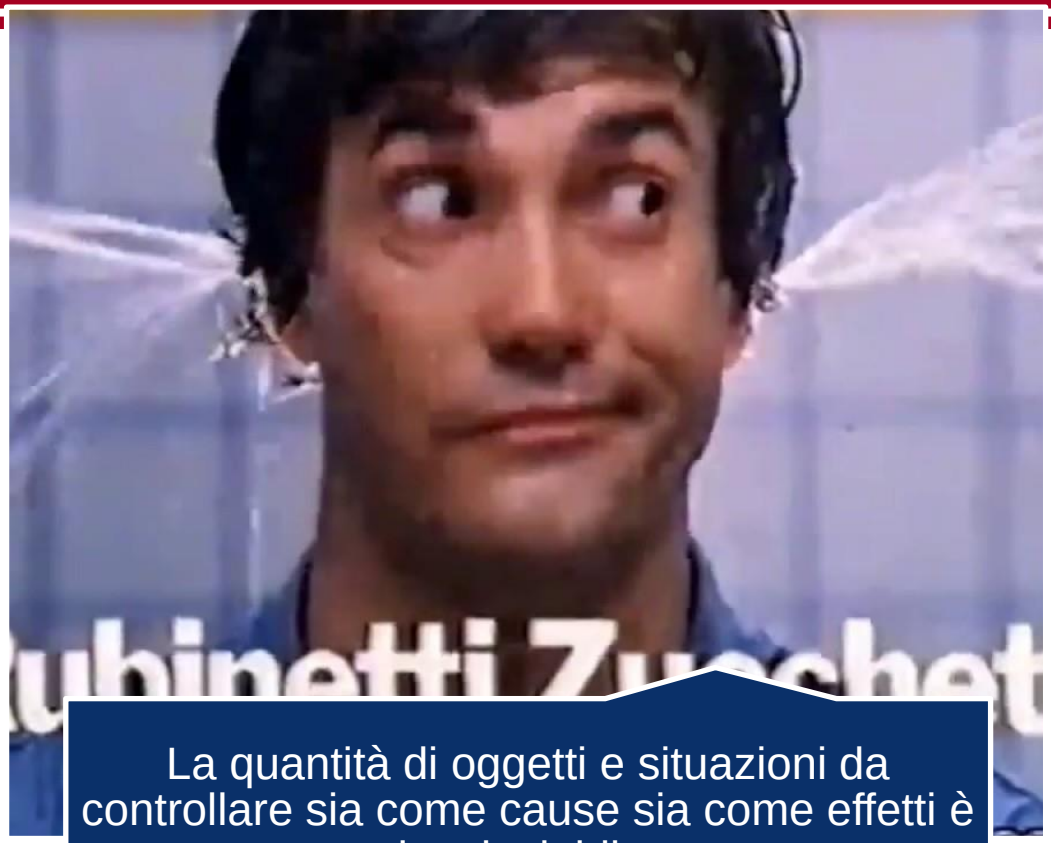
Qualche mese dopo circola la notizia che a guadagnarci furono dei fondi esteri collegati a Cyber team orientali

Cosa sta cambiando?

Il livello di **interconnessione** di dati tra banche, clienti, fornitori e pubblica amministrazione è aumentato a dismisura

Si alza l'asticella **della sfida**: le conseguenze nella sfida tra attaccanti e difensori possono essere sempre più dannose

Cosa sta cambiando?



La quantità di oggetti e situazioni da controllare sia come cause sia come effetti è incalcolabile.

E’ sempre più difficile **chiudere tutti i buchi**

Cosa sta cambiando?

L’obiettivo dell’attacco potrebbe essere anche altrove e il bersaglio stesso può essere utilizzato come elemento intermedio per qualche obiettivo più grande

Non basta **difendere i confini** con un muro perché i confini non sono più definibili in maniera netta. Il nemico sta dentro o fuori?

Banche e Assicurazioni

In questa categoria invece il rischio **è valutato in ogni suo aspetto**: dal grado di probabilità all'impatto economico e all'efficacia dei controlli.

E' gestito il concetto di **grado di accettabilità** del rischio in base ad un fattore di propensione al rischio stesso.

Qualche volta il rischio viene venduto o comprato speculando sulla diversa valutazione. Il rischio è trasformato in una **fonte di guadagno**

Chi non risica non rosica.

Aziende strategiche e sistemiche

non è ammesso lo sbaglio prevedibile

non possono esserci vulnerabilità troppo esposte ad azioni ostili.

In caso di eventi di rischio esistono procedure codificate che devono essere assunte con responsabilità chiare.
Evidenza in ogni momento del livello di emergenza.

Scenario

È in atto un cambiamento strutturale: le banche, in quanto aziende inserite in una catena di relazioni vitali per uno stato o per la vita del cittadino, si stanno trasformando sempre più in aziende sistemiche.

Considerazione

Sempre più numerosi sono gli eventi di rischio che diventano «**inaccettabili**».

Stato di guerriglia

- **Una nuova guerra verrà sicuramente combattuta su un fronte cybernetico (anzi è probabile che ne sarà il fronte principale)**
- **Oggi siamo già in uno stato di «guerriglia» non dichiarata in cui squadre al soldo di governi si fronteggiano in modo non ufficiale quotidianamente.**
- **Il sistema Bancario nel suo complesso (banche, reti, dati e fornitori) è un nodo cruciale di uno stato da un punto di vista della difesa.**

FRANCESCO VESTITO
Comando Militare Interforze per le Operazioni Cibernetiche (CIOC)

Le domande a cui diamo già una risposta

quanto vale questo rischio oggi? Quanto vale domani se faccio queste scelte?

quanto capitale devo mettere a riserva?

questo rischio è accettabile? quale è l'impatto sul RAF?

Le altre domande da porsi

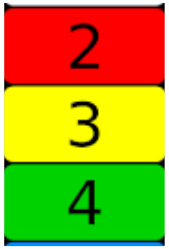
Quali sono i controlli più efficaci per **evitare** questo rischio?

I miei attuali controlli sono **adeguati**? Possono essere **potenziati**?

Quanto costano i miei controlli in relazione all'efficacia e al rischio che vogliono coprire?

Sto **concentrando l'attenzione** e gli sforzi sulle minacce giuste? Non è che c'è già uno scimmione in casa e manco me ne sono accorto?

Le altre domande da porsi

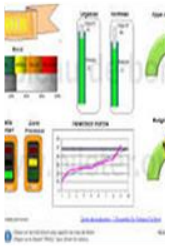


Ho un **sistema di detection** che mi permette di dire che sono sotto attacco o in una situazione di allarme (Giallo, Rosso, Critico) per eccesso di vulnerabilità di risorse?

Chi dichiara la gravità di allarme?

Ho **un piano di azioni** chiaro e conosciuto da attuare in situazione di allarme grave? Ho un kit di emergenza preparato?

Come posso **contenere le conseguenze** o i danni quando vengono «violate le mura difensive»?



Quali **risorse sono collegate** e in che stato di vulnerabilità si trovano?

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Cenni su ISO 27001

ISO/IEC 27001: specifies the requirements for establishing, implementing, maintaining and continually improving an **information security management system** within the context of the organization.

SGSI **Sistema per la Gestione della Sicurezza delle Informazioni**

ISO/IEC 27001

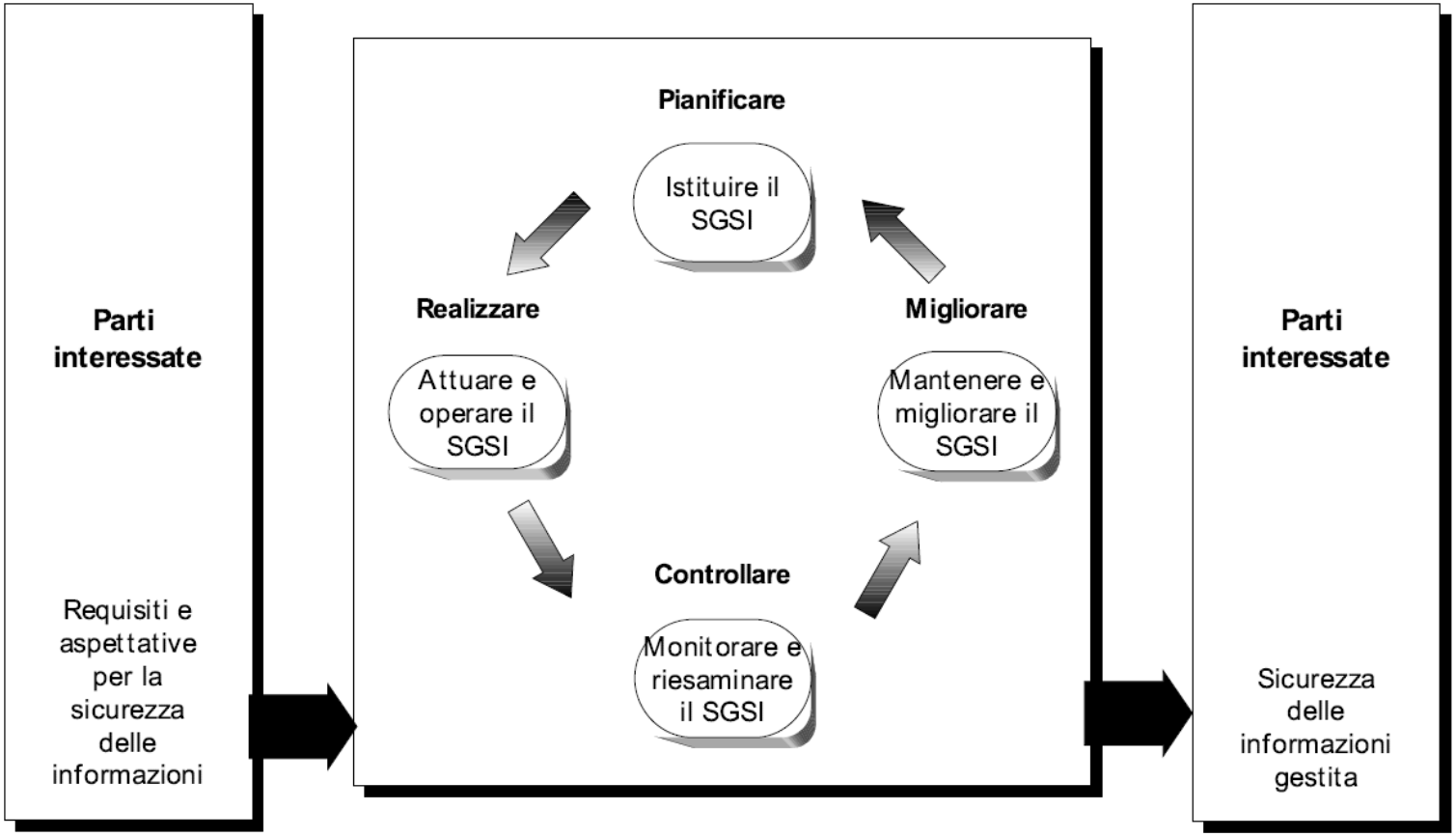


Figura 1 – modello PDCA applicato ai processi del SGSI

Un processo in quattro fasi

Pianificare (istituire il SGSI)	Istituire la politica per il SGSI, gli obiettivi, i processi e le procedure per la sicurezza pertinenti per la gestione del rischio e il miglioramento della sicurezza delle informazioni per conseguire risultati in armonia con le politiche e gli obiettivi globali dell'organizzazione.
Realizzare (attuare e operare il SGSI)	Attuare e operare la politica per il SGSI, i controlli, i processi e le procedure.
Controllare (monitorare e riesaminare il SGSI)	Valutare e, ove applicabile, misurare le prestazioni dei processi a fronte della politica per il SGSI, degli obiettivi e dell'esperienza pratica, e fare rapporto alla direzione sui risultati per un riesame.
Migliorare (mantenere e migliorare il SGSI)	Intraprendere azioni correttive e preventive basandosi sui risultati degli audit interni del SGSI e del riesame da parte della direzione o su altre informazioni pertinenti per conseguire il miglioramento continuo del SGSI.

In pratica ….

L’organizzazione deve:

1. Definire ampiezza del SGSI in funzione del contesto aziendale di riferimento
2. Definire una politica della Sicurezza delle informazioni e del SGSI (definizione degli obiettivi di sicurezza, principi generali, crteri con cui si stimano i rischi)
3. Definire l’approccio alla valutazione del rischio (metodologia e criteri di accettazione dei rischi)

4. Identificare elementi del rischio: Asset, responsabili, Minacce, vulnerabilità, impatti in termini di scenari di rischio di perdita di
   - **R**iservatezza
   - **I**ntegrità
   - **D**isponibilità
5. Valutare i rischi in termini di Impatto, Probabilità e Rischio e determinazione se il rischio è accettabile in funzione dei criteri stabiliti

7. Identificare le opzioni per il trattamento del rischio:
   - Applicare i controlli appropriati
   - Accettare i rischi
   - Evitare i rischi
   - Trasferire i rischi
8. Scegliere i controlli e gli obiettivi di controlli secondo l'appendice A
9. Ottenere l'approvazione per i rischi residui
10. Ottenere l'autorizzazione per attuare l'SGSI
11. Preparare un documento Dichiarazione di applicabilità

Allegato A

A.9.2 User access management		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change

La Sicurezza informatica

- ISO/IEC
- Codice Penale (Libro II)
- DECRETO LEGISLATIVO 8 giugno 2001, n. 231
- DECRETO LEGISLATIVO 30 giugno 2003,

Sicurezza informatica - argomenti

- Accesso ai sistemi operativi
- Attività crittografica
- Controllo degli accessi
- Crimini informatici
- Gestione degli incidenti
- Gestione della continuità aziendale
- Gestione delle informazioni
- Gestione e controllo del sistema informativo
- Gestione e riesame dei diritti di accesso Informazioni personali
- Misure minime di sicurezza
- Modalità di accesso alle informazioni
- Modalità di accesso dell'utenza
- Organizzare la sicurezza delle informazioni, delle attrezzature e delle aree
- Procedure di ripristino dei dati
- Protezione di dati sensibili e giudiziari
- Salvataggio dei dati
- Sistema di autorizzazione informatico
- Software e codici pericolosi
- Strumenti e supporti removibili
- Trattamento dei dati personali attraverso strumenti elettronici
- Tutela della Privacy

Indice e scaletta del corso

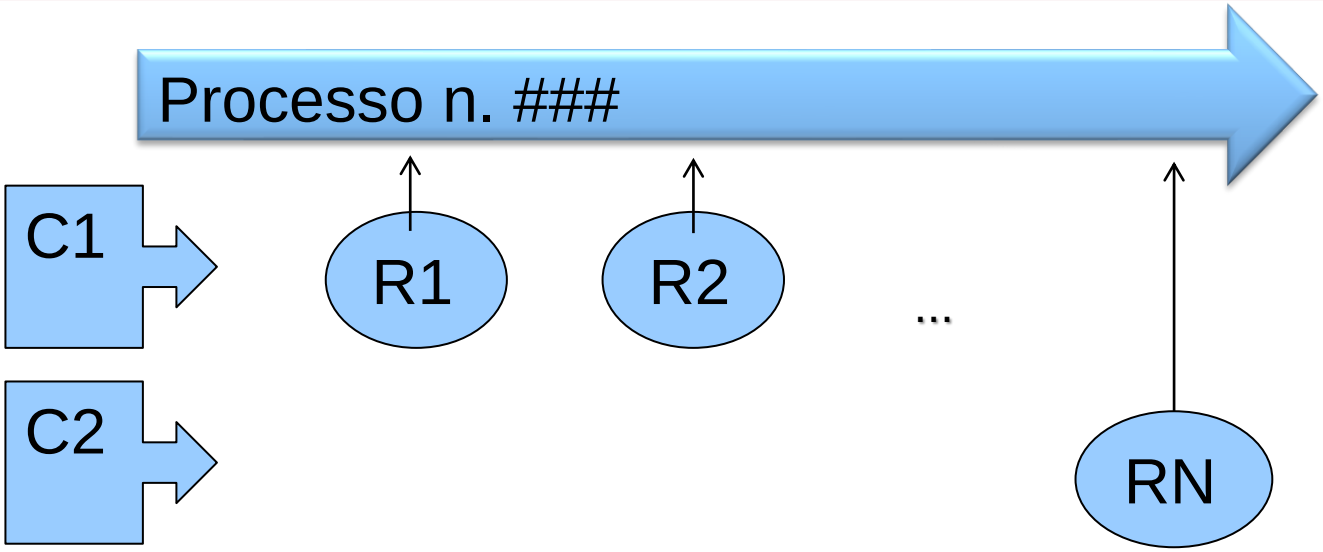
- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Compliance Risk Mapping

L’analisi del rischio IT è focalizzata sulle vulnerabilità degli asset informatici e le possibili minacce correlate per formare uno scenario di rischio potenziale;

	Ademp. 1	Ademp 2	Ademp 3	...	Ademp N
Processo n. 1					X
Processo n. 2		X			
Processo n. 3	X		X		
...					
Processo n. N			X		

Approccio per funzione Compliance



Il compliance Management è orientato ai controlli. Il rischio è definito dall'incrocio tra adempimento normativo e processo in cui questo si colloca.

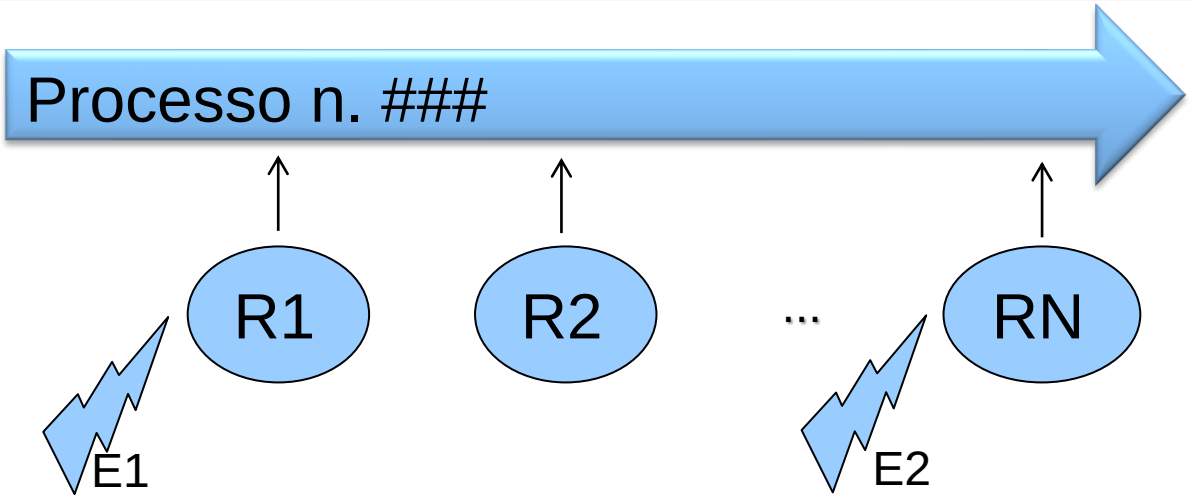
Focalizzazione su adempimenti e controlli

Operational Risk Mapping

Le categorie di rischio possono essere un semplice albero tassonomico a più livelli (Es. Tassonomia di Basilea 2). Ognuno degli incroci individua un particolare rischio nel singolo processo

	Risk Cat 1	Risk Cat 2	Risk Cat 3	...	Risk Cat N
Processo n. 1					x
Processo n. 2		x			
Processo n. 3	x		x		
...					
Processo n. N			x		

Approccio per funzione OR



L'OR Management è orientato agli eventi. Il rischio è definito dall'incrocio tra Event Type e processo in cui questo si colloca.

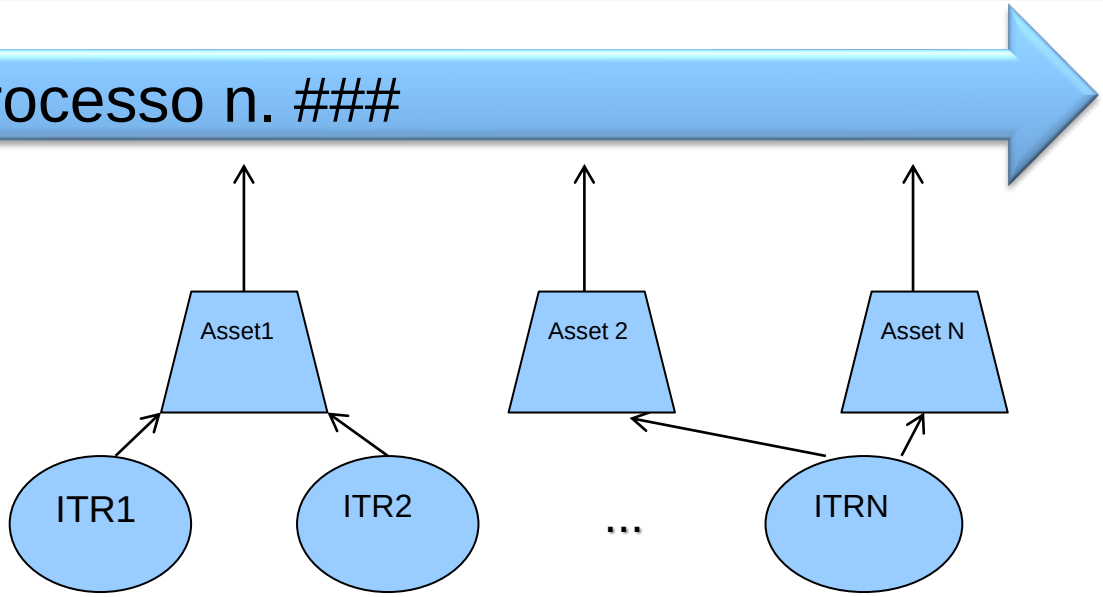
Focalizzazione su eventi

IT Risk Mapping

L’analisi del rischio IT è focalizzata sulle vulnerabilità degli asset informatici e le possibili minacce correlate per formare uno scenario di rischio potenziale;

	Threat cat 1	Threat Cat 2	Threat Cat 3	...	Threat Cat N
Asset n. 1					X
Asset n. 2		X			
Asset n. 3	X		X		
...					
Asset n. N			X		

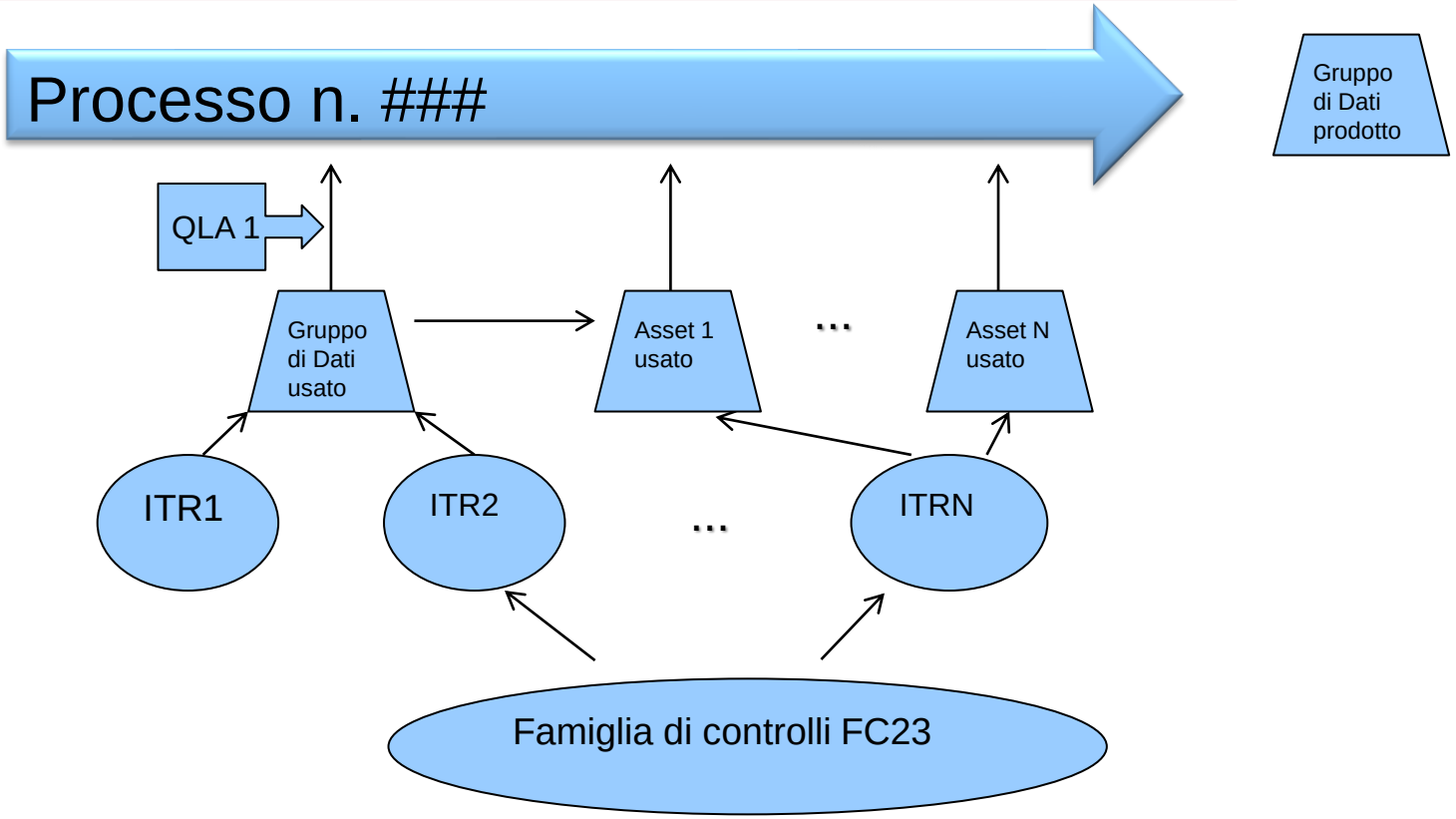
IT Risk Mapping



L'IT Risk Management è orientato quindi all'Asset IT. Il raccordo con i processi avviene identificando preventivamente gli Asset associati a ciascun processo.

Focalizzazione sugli Asset

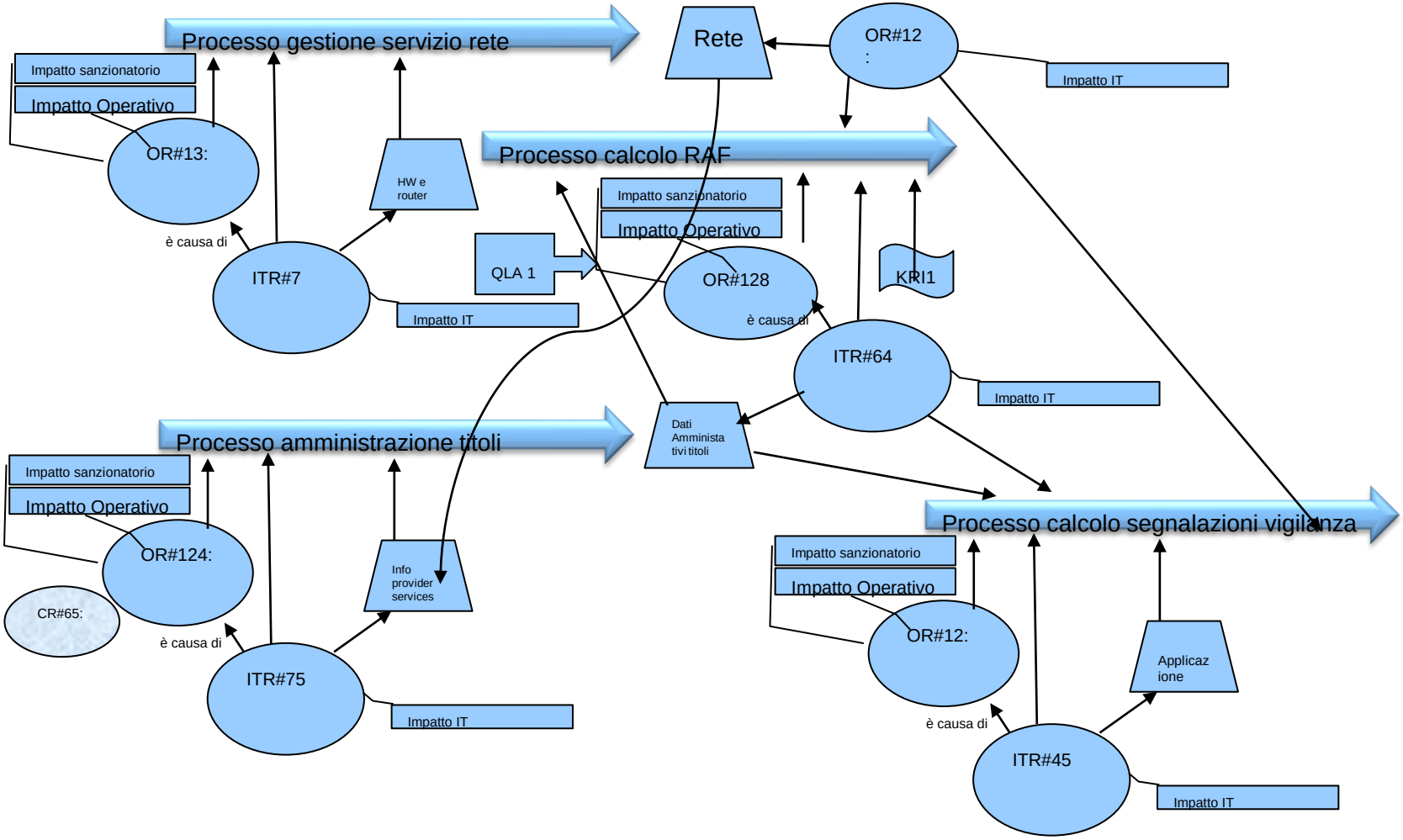
Analisi



Il legame con il processo avviene con un QLA (Quality Level Agreement) che rappresenta la base per l'elemento di scenario analysis del processo

.

Risk Network Analysis



Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Analisi Top Down

- **Idea chiave è valutare la probabilità di accadimanto di una minaccia in funzione della vulnerabilità della famiglia di controlli:**
  - Valutazione di come viene implementata ogni singola famiglia di controlli di un determinato standard (ISO27001, NIST, …) complessivamente per tutta l'azienda non per singolo asset.
  - Calcolare un valore di Esposizione residua al Rischio per ogni famiglia.
  - Incrociare (mappare) ogni singola famiglia di controllo con ogni singola minaccia dando anche una valutazione in termini di applicabilità (coerenza) della famiglia rispetto alla minaccia.
  - Prendere l'esposizione residua della famiglia di controllo massima per ogni minaccia. Tale valore viene valutato come la probabilità si accadimento della minaccia.

Analisi Top-down

- La probabilità di accadimento della minaccia in generale viene poi valutata singolarmente rispetto ad ogni singolo asset
- Viene poi valutato l'impatto dello scenario di rischio sull'asset
- Il rischio finale è il prodotto della probabilità di accadimento della minaccia per l'impatto di un determinato scenario di rischio

Analisi Bottom up

- Al contrario si parte dalla valutazione della probabilità della singola minaccia relativamente ad un asset
- Viene valutato l'impatto
- Si calcola un rischio lordo
- Si valuta l'applicazione dei controlli sul singolo asset
- Si valuta il rischio residuo

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Cyber Attack

- **Ha senso parlare di probabilità di accadimento di un cyber attack?**
- **Se esiste una vulnerabilità dove credete che si concentrerà il nemico?**
- **Per un incidente informatico o un evento operativo è logico parlare di probabilità di accadimento, per un attacco deliberato da una mente criminale è più logico mettersi nei panni dell'attaccante e individuare dove attaccheremmo noi**
- **L'idea è quella di lasciar perdere le analisi di probabilità e concentrarsi su analisi delle vulnerabilità delle difese.**

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Tattiche militari o da protezione civile

❑ Definizione di stati di allerta

- Bianca: non ci sono segnali di pericolo imminente
- Verde: ci sono segnali di pericolo di attacco ma non vi è alcun evidenza di essere sotto attacco.
- Giallo: Ci sono segnali specifici di pericolo di attacco, vi sono segnali di essere sotto attacco ma le difese sembrano reggere.
- Arancione: Ci sono segnali specifici e certi di essere sotto attacco. E' probabile che il nemico sia già riuscito ad entrare dentro le «mura esterne» e stia tentando di violare dati o processi.
- Rosso: Siamo sotto attacco evidente e sono a rischio la continuità operativa di alcuni processi, l'integrità di qualche dato, la riservatezza di dati o la disponibilità di dati o server non critici.
- Viola: E' stata violata l'integrità o la riservatezza o la disponibilità di servizi critici o di dati.

Individuazione degli elementi critici e vitali

- **Individuazione di**
  - Asset critici
  - Processi critici
  - Persone critiche
- **Definizione dei livelli minimi di servizio e della qualità minima accettabile in regime di emergenza**
- **Creazione di barriere fisiche e informatiche che definiscano uno o più livelli di «mura interne». Portare gli elementi critici all'interno delle «mura interne» appropriate.**
- **Definizione dei livelli di privilegio e delle modalità di ingresso all'interno delle «mura interne»**

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Procedure di emergenza, escalation e flessibilità nell'adozione delle difese

- **Individuare e stabilire in anticipo cosa fare nel momento in cui si è in un determinato livello di allerta:**
- **Esempio:**
- **Allerta Bianca) Ripristinare i controlli normali. Abbassare la guardia a livelli di costo prestabilito. Liberare da reperibilità. Possibilità di Smart Working. Etc…**

Piani di emergenza

- **Allerta Verde) comunicare l'allerta Verde. Adottare i controlli di livello verse. Alzare la guardia su raccolta indicatori, log.**
- **Allerta gialla) Comunicare l'allerta gialla. Adottare la robustezza dei controlli al giallo. Revocare ferie e permessi sistemisti. Prepararsi all'isolamento della zona protetta asset critici. Controllare che la zona protetta non sia compromessa. Togliere possibilità di smart working ai sistemisti.**

Piani di emergenza

- **Allerta Arancione) Comunicare l'allerta arancione. Adottare i controlli arancioni. Isolare gli asset, i processi e le persone critiche nella zona protetta. Attivare e potenziare intelligence su sistemi interni per bonificare area normale interna alle mura.**
- **Allerta Rossa) Comunicare l'allerta Rossa. Adottare controlli rossi. Divieto di accesso a tutte le persone non autorizzate nella zona restricted. Attivazione di piani di detecting costosi ma più efficaci. Sospensione delle attività non core.**
- **Allerta Viola) Comunicare l'allerta Viola. Attivazione Disaster recovery.**

Indice e scaletta del corso

- **Terza parte: IT Risk e Cyber Risk**
  - Introduzione all'IT Risk management
  - Cenni su ISO 27001
  - Cambio di prospettiva dal Processo all'Asset
  - Analisi Top Down vs Bottom Up
  - Probabilità di accadimento o certezza?
  - Gestione degli stati di allerta e individuazione strutture critiche
  - Procedure di emergenza, escalation e flessibilità nell'adozione delle difese
  - Intelligence

Intelligence

- Come in guerra si vincono le battaglie spesso se si hanno informazioni aggiornate e vere sugli attaccanti così nei cyber attack.
- Necessità di intelligence
- Test sulla vulnerabilità delle nostre difese.
- Simulazioni di attacco e penetration test.
- Condivisione delle informazioni in tempo reale tra aziende e entità diverse.

Indice e scaletta del corso

- **Terza parte: Aspetti pratici e criticità di un progetto di operational risk management**
  - Aspetti organizzativi del Risk Management
  - Criticità di progetto

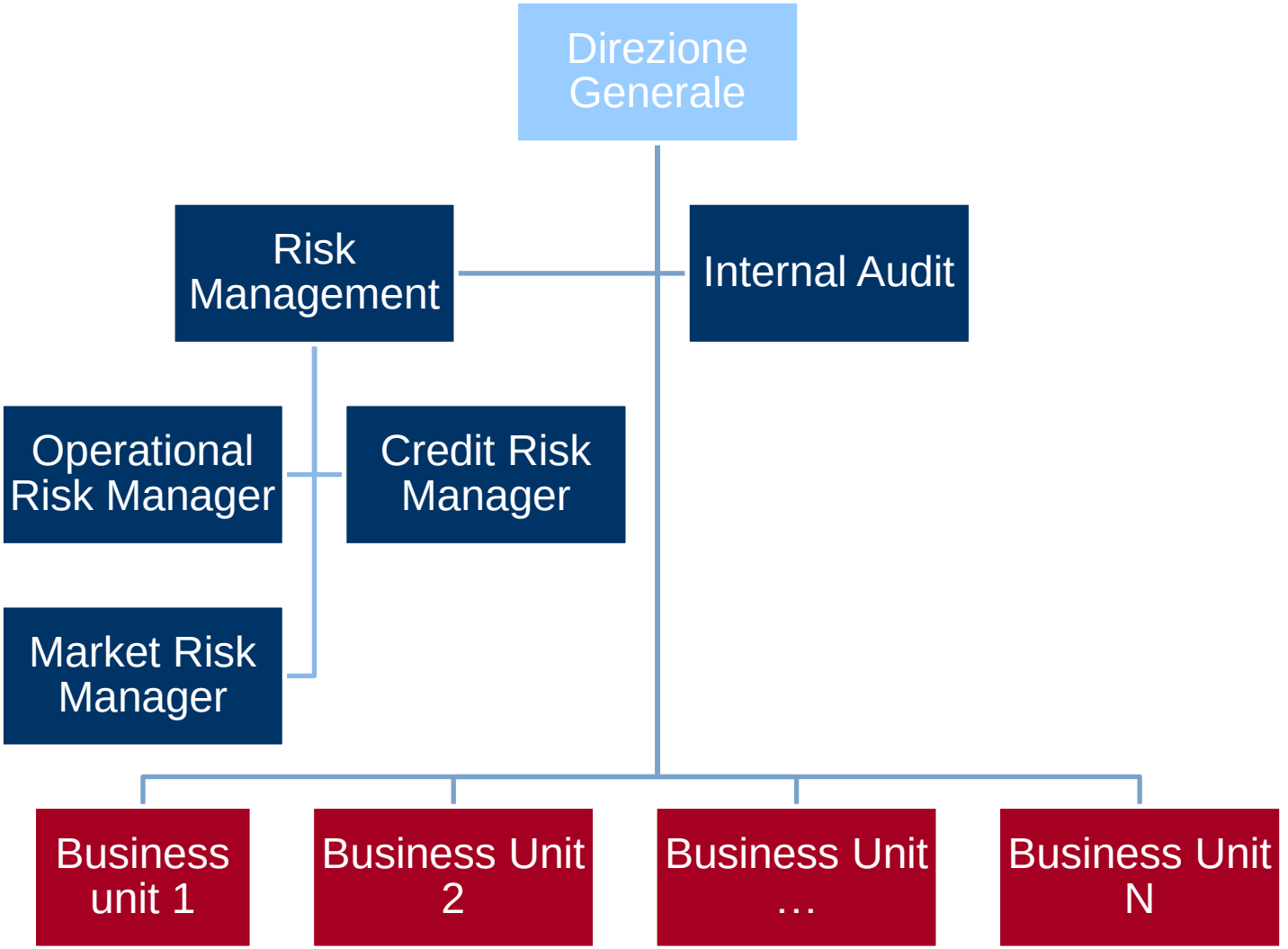
Aspetti organizzativi per un sistema di RM

- **Un sistema di Risk Management deve avere i seguenti requisiti**
  - Completezza: deve controllare la più ampia tipologia di rischi possibile
  - Indipendenza: Il Risk Manager deve essere indipendente dalle funzioni di business e dalle funzioni preposte al controllo
  - Condivisione e coerenza dei dati e delle metodologie
  - Tempestività e continuità: le segnalazioni devono avvenire tempestivamente
  - Trasparenza e diffusione dei modelli utilizzati per l'analisi
  - Responsabilità e delega da parte del CDA;

Aspetti organizzativi Risk Management

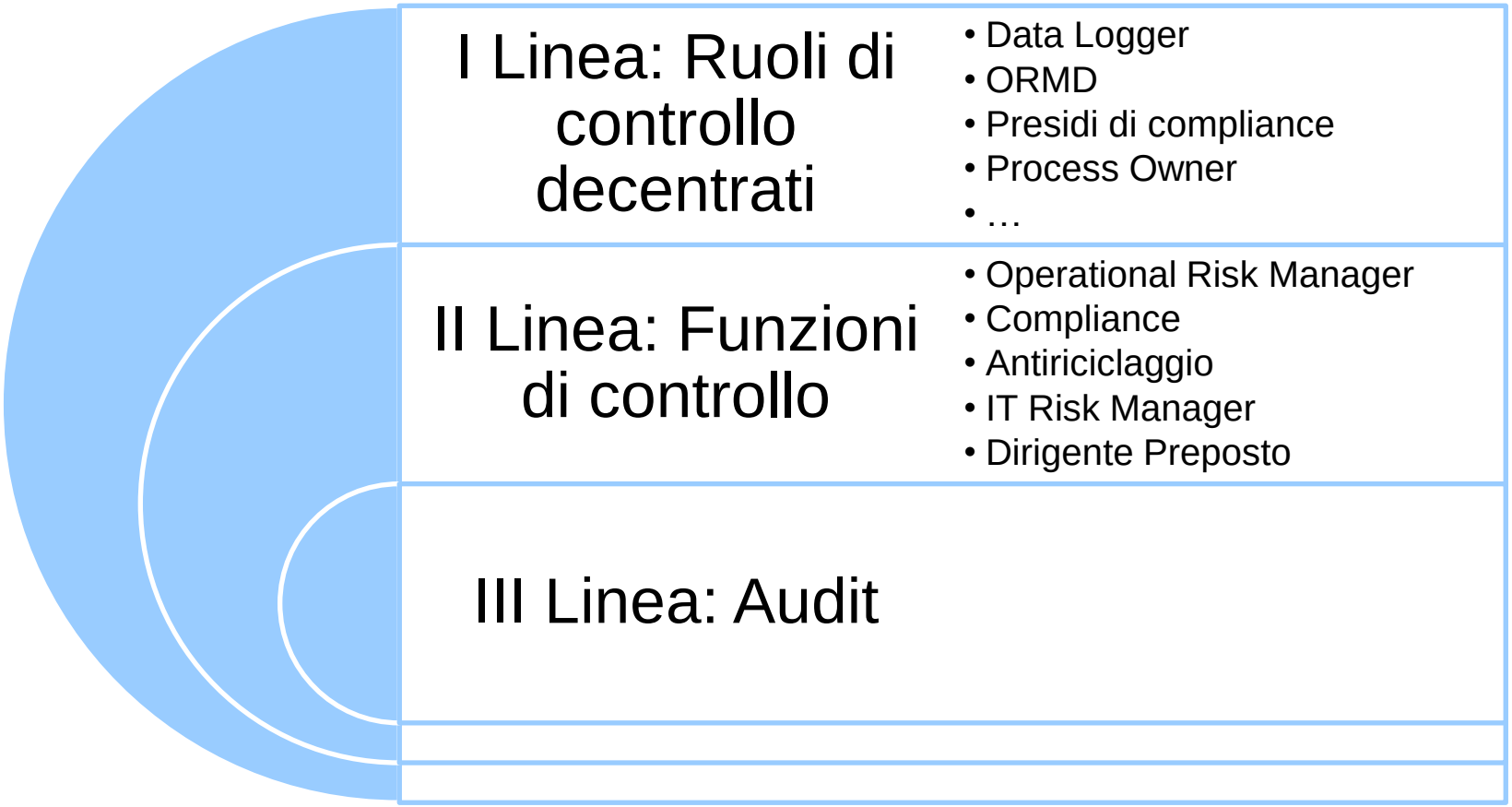
- **Alcune linee guida**
  - Forte coinvolgimento dell'Alta Direzione (approva revisiona e definisce i principi guida della metodologia
  - Continua verifica da parte dell'Internal Auditing dell'efficacia del processo
  - Condivisione con il collegio sindacale
  - Responsabilità di tutto il management per l'implementazione e lo sviluppo di politiche, processi
  - Regolare reporting alla direzione
  - Politiche e procedure per controllare e mitigare il rischio; revisione periodica delle strategie di monitoraggio e mitigazione
  - Business contingency plan per assicurare l'operatività in caso di eventi estremi

Esempio di Organizzazione



Sistemi di controllo e Risk Governance

Le tre linee di difesa della banca



Esigenze per Operational Risk Manager

Disporre di una **LDC centralizzata** a cui possono contribuire differenti uffici anche decentrati attraverso un **workflow**

Svolgere periodiche **valutazioni** del rischio operative applicando **metodologie standardizzate**

Deve svolgere analisi di **Stress Test** e di scenario

Far crescere la **cultura del rischio** in azienda e coinvolgere le strutture decentrate nella gestione ordinaria.

Favorire e stimolare la **responsabilizzazione** attraverso l'utilizzo di **Deleghe** autorizzative formali

Gestire le manifestazioni economiche effettuando una adeguata analisi di impatto coinvolgendo le strutture preposte

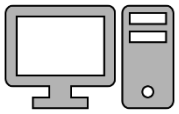
Proporre, pianificare e gestire **attività** di controllo e di mitigazione

Definire e valutare **indicatori** per prevenire situazioni di rischio

Giustificare, argomentare e dimostrare i motivi di una decisione presa nei confronti di autorità interne ed esterne

Avere una **visione complessiva** dei rischi e delle criticità connesse

Esigenze per ICT Risk Manager



Disporre di cataloghi centralizzati relativi a **asset IT, minacce, scenari, controlli, contromisure**

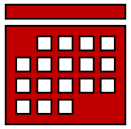
Svolgere periodiche **valutazioni** del rischio ICT applicando **metodologie standardizzate**

Deve saper distiguere tra semplice segnalazioni e incidenti ICT, segnalando i Major Incident e contribuendo alla LDC

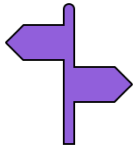
Far crescere la **cultura del rischio** in azienda e coinvolgere le strutture decentrate nella gestione ordinaria.

Gestire un efficace sistema dei controlli adottando standard di settore (ISO, NIST, COBIT, …)

Collegare le analisi del rischio IT con le valutazioni di **impatto di business e continuità operativa**

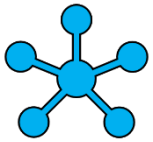


Proporre, pianificare e gestire **attività** di controllo e di mitigazione



Definire e valutare **indicatori** per prevenire situazioni di rischio

Giustificare, argomentare e dimostrare i motivi di una decisione presa nei confronti di autorità interne ed esterne



Avere una **visione complessiva** dei rischi e delle criticità connesse

Esigenze per Compliance Risk Manager

Disporre di una **Legal Inventory** dedicata alla compliance normativa

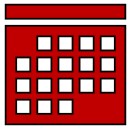
Svolgere periodiche **valutazioni** del rischio di non-conformità applicando **metodologie standardizzate**

A seguito della introduzione del **GDPR** disporre di un **Registro dei trattamenti** e svolgere periodicamente la DPIA - PIA

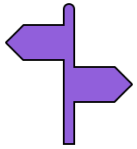
Far crescere la **cultura del rischio** in azienda e coinvolgere le strutture decentrate nella gestione ordinaria.

Gestire un efficace sistema di **presidi di controllo** adottando standard o policy interne

Gestire proattivamente i **Data Breach** e i relativi follow-up entro i termini previsti dalla normativa

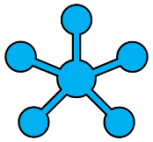


Proporre, pianificare e gestire **visite ispettive e azioni** di controllo e di mitigazione



Definire e valutare **indicatori** per prevenire situazioni di rischio

Giustificare, argomentare e dimostrare i motivi di una decisione presa nei confronti di autorità interne ed esterne

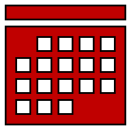


Avere una **visione complessiva** dei rischi e delle criticità connesse

Esigenze per CRO e Risk Manager

Disporre di una **Legal Inventory** dedicata alla Governance bancaria

Gestire i **Rischi Limite** nella definizione della Propensione al Rischio (**RAF**) e i relativi sforamenti (**Breach**)



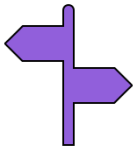
Proporre, pianificare e gestire **attività** di controllo e di mitigazione

Giustificare, argomentare e dimostrare i motivi di una decisione presa nei confronti di autorità interne ed esterne

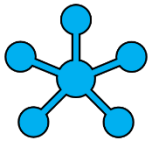
Gestire i **rischi reputazionali** e le azioni volte a mitigarne gli effetti

Deve svolgere **analisi di scenario e** reportistica unificata tra Financial e non-financial Risk (**Tableau du bord**)

Gestire i **rischi Data driven** derivanti da scarsa qualità dei dati (garanzie dei mutui, …)



Definire e valutare **indicatori** per prevenire situazioni di rischio



Avere una **visione complessiva** dei rischi e un **Registro Unico** dei rischi

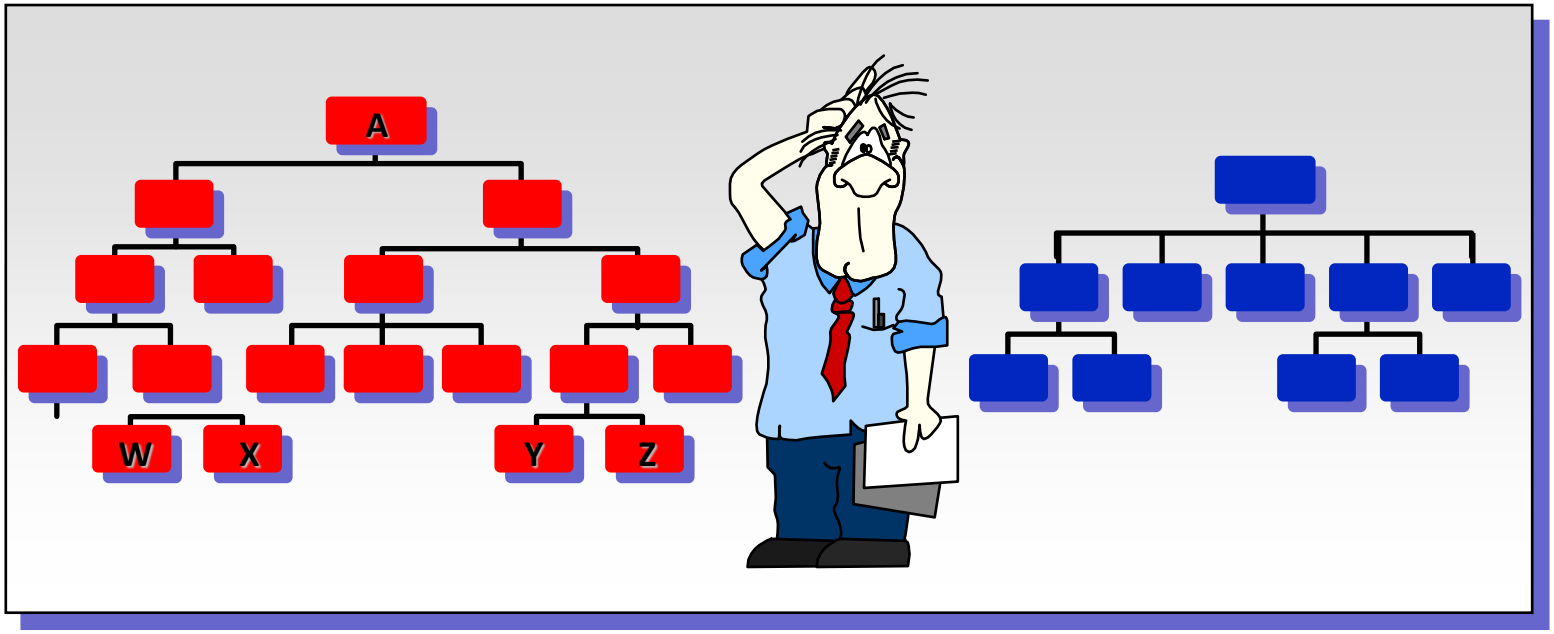
Valutare **i rischi Terze Parti** contribuendo alla definizione dei rischi IT

Indice e scaletta del corso

- **Terza parte: Aspetti pratici criticità ed esempi di un progetto di operational risk management in una banca italiana**
  - Aspetti organizzativi del Risk Management
  - Criticità di progetto

I processi devono essere scomposti in un modo comprensibile

- **I processi devono essere scomposti in un numero di livelli che sia:**
  - Funzionale agli obiettivi del progetto
  - Comprensibile



I fattori critici nell’applicazione dlela metodologia

- **Il principale fattore di rischio di fallimento di un progetto è la cosiddetta "Resistenza al cambiamento", ovvero la naturale propensione umana a trovare difficile qualunque cambiamento del proprio modo di operare**
  - L'insieme delle attività dedicate alla gestione del cambiamento organizzativo prendono quindi il nome di "Gestione del cambiamento" o "*Change management*"

- **Per minimizzare questo rischio e implementare un progetto di successo è opportuno procedere a:**
  - Assicurarsi l'impegno della Direzione ed in particolare la loro capacità e propensione a prendere decisioni in tempi rapidi (in modo da minimizzare l'impatto di problemi che dovessero sorgere e mantenere un clima positivo)
  - Assicurarsi di avere uno staff di persone sufficientemente ampio
  - Identificare ed analizzare i cosiddetti "fattori abilitatori e le barriere" al cambiamento
  - Definire, pianificare, implementare e monitorare un piano di gestione dei cambiamenti che esalti gli abilitatori e riduca le barriere al cambiamento
  - Determinare e comunicare le responsabilità organizzative di ciascun cambiamento

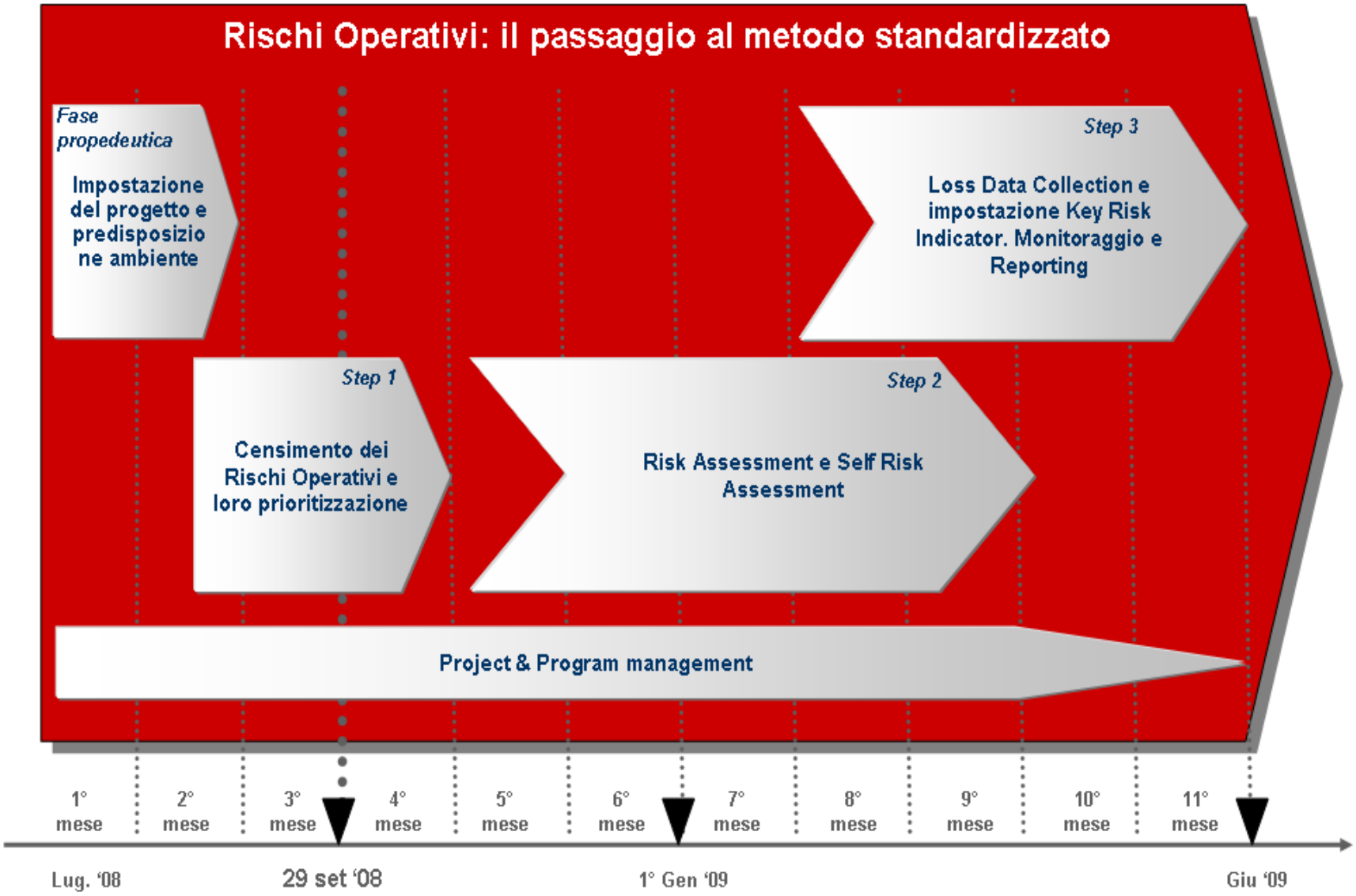
I fattori critici per l'applicazione della metodologia

- **Un altro fattore di resistenza è la resistenza psicologica e reale che si trova nei manager a dichiarare i possibili fallimenti**
  - In genere il manager tenderà a nascondere o coprire i fallimenti soprattutto se sono imputabili alla sua area di influenza.
- **Spesso poi ci si trova a che fare con organizzazioni che non hanno una mappatura completa dei processi**
  - Queste organizzazioni necessitano quindi di una fase preliminare di assessment organizzativo
- **Alcune aziende trovano difficile ancora lavorare per obiettivi.**
  - Anche in questo caso si troverà resistenza all'utilizzo di questa metodologia perché tenderà ad esplicitare gli obiettivi dove fino ad oggi c'era poca volontà di chiarezza

Indice e scaletta del corso

- **Quarta parte: esempio di un progetto di operational risk management in una banca italiana**
  - Esame delle fasi di un progetto reale in banca
  - Analisi di un prodotto di gestione del Rischio Operativo

Fasi e articolazione temporale del progetto



Il Risk Assessment: Esempio modalità di realizzazione

Comunicazione via mail con convocazione e invio allegati

- Proposta e condivisione pianificazione incontri
- Invio in anteprima delle schede rischi predisposte nel corso della fase di individuazione dei rischi delle Risk Unit per una presa visione preventiva

Incontri di Risk Assessment

- Gli incontri prevedono la presenza dei Risk Owner e uno o più esponenti del gdl. Nel corso degli incontri si provvederà a raccogliere tutte le informazioni previste dalla metodologia di assessment dei rischi operativi
- La durata massima di ciascun incontro è stimata in 3 ore (salvo eccezioni)

Analisi dei dati, redazione documentazione di sintesi e invio ai Risk Owner

- A seguito dell'analisi dei dati da parte del gdl, viene predisposta la documentazione di sintesi comunicata via mail ai Risk Owner

Validazione esito Risk Assessment

- Coerentemente con le scadenze concordate, i singoli Risk Owner provvederanno a valutare nel merito la documentazione inviata dal gdl e a procedere alla validazione

Esempio di strumento
informatico di supporto alla
funzione di
Compliance bancaria