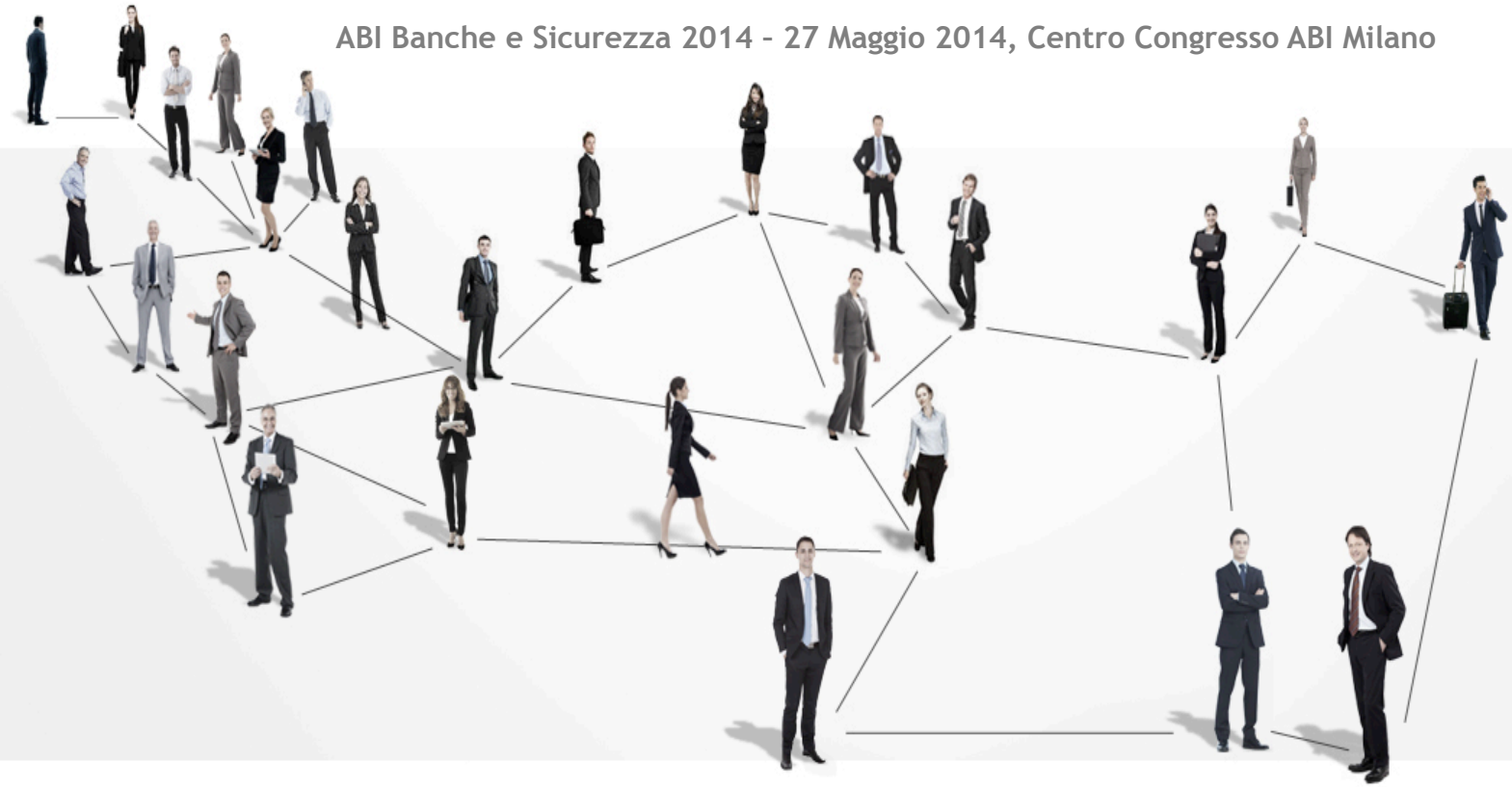
Un *framework* di riferimento per la gestione della sicurezza e del rischio informatico nelle banche

Ing. Andrea Agosti
Responsabile Servizio Security (BU Sicurezza, Rischi e Compliance ICT)

ABI Banche e Sicurezza 2014 – 27 Maggio 2014, Centro Congresso ABI Milano

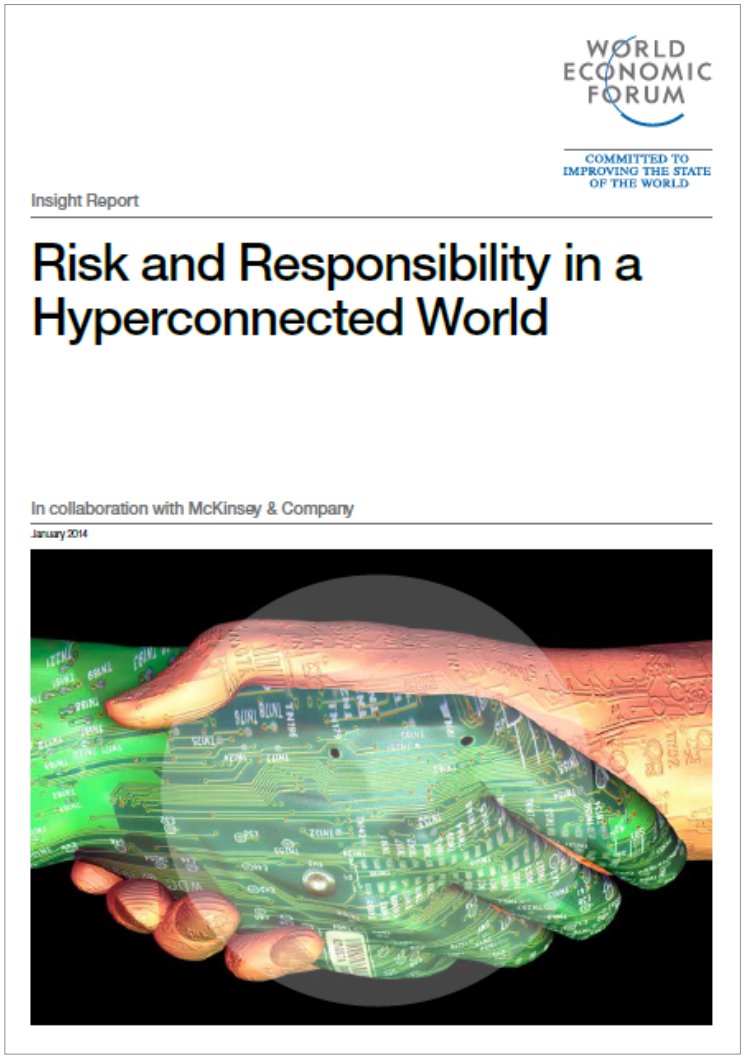


Agenda dell'intervento

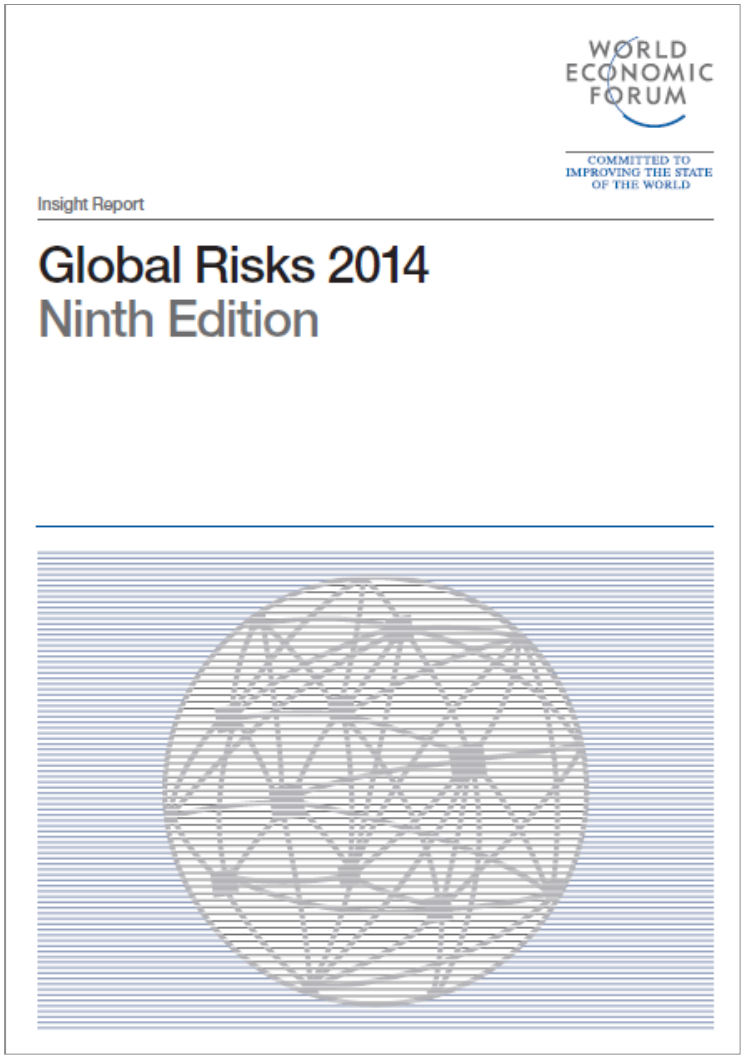
- ***Premessa: il concetto di rischio informatico alla luce delle Nuove Disposizioni di Vigilanza***
- Il modello di riferimento proposto da Oasi per la gestione del rischio informatico
- Conclusioni e raccomandazioni di Oasi per gli Istituti di Credito
- L'azienda Oasi – Outsourcing Applicativo e Servizi Innovativi S.p.A.

I cosiddetti "*Cyber Risks*" sono diventati un tema all'attenzione anche presso Organizzazioni Internazionali quali il World Economic Forum

Risk and Resp. in a Hyperconnected World



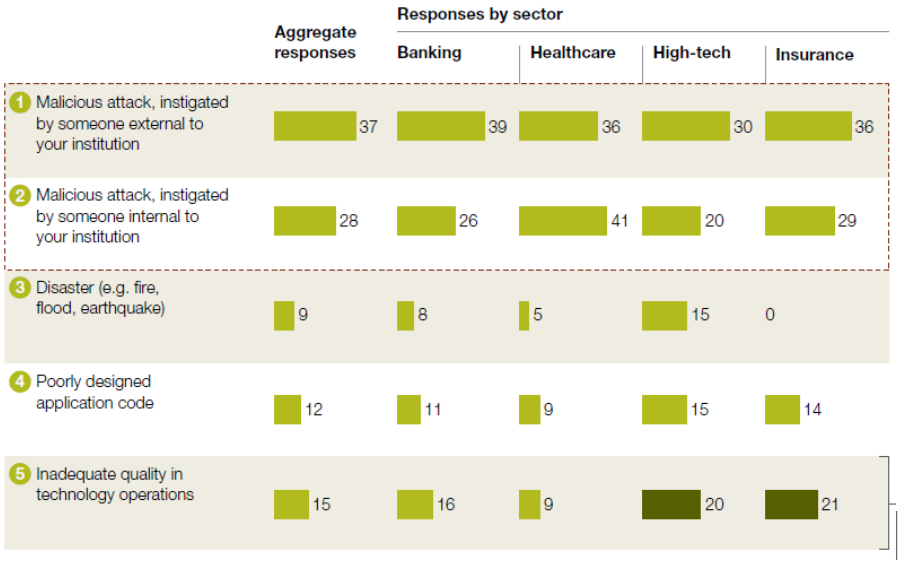
Global Risk 2014 Report



I Cyber Risks sono ritenuti a livello globale i rischi tecnologici più significativi, con un picco di attenzione proprio presso l'industria bancaria

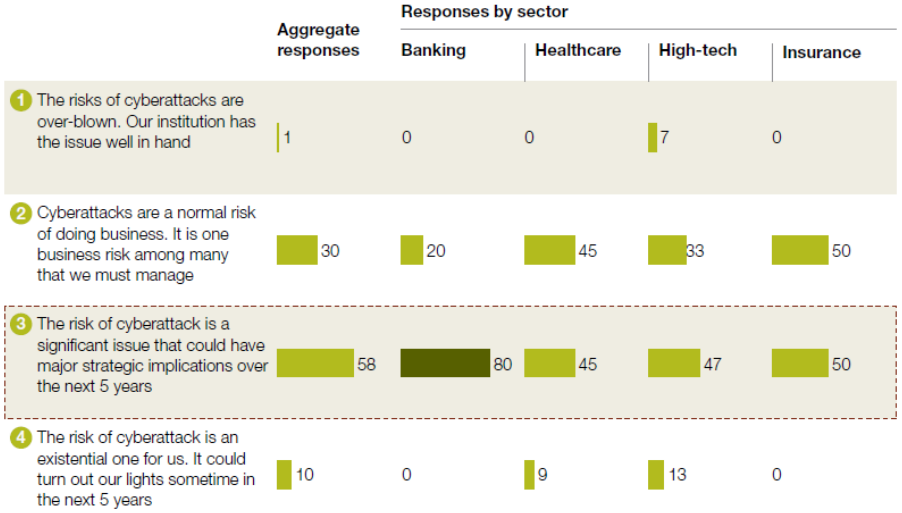
Technology risks most likely to have a strategic and negative impact on business

% of respondents



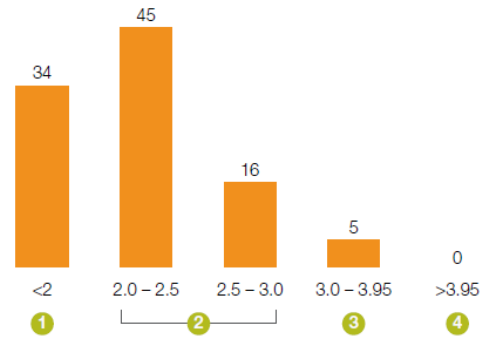
Level of concern about malicious attacks to condentiality, integrity & availability of data and information systems

% of respondents



Distribuzione % del *Cyber Risk Management Maturity* scores

% of firms

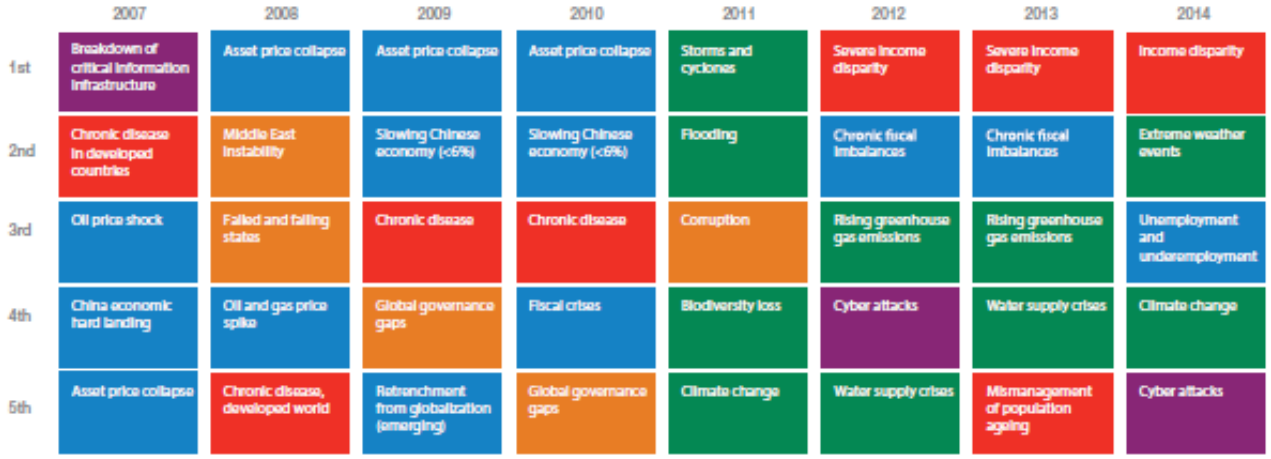


- Only 21% of respondents were rated "mature" or better on 4 or more of the 8 practice areas
  - Only 5% rated "mature" or better overall
  - No organizations at top overall rating of "robust"
- Only one respondent was "mature" or better in every practice area
- 34% of respondents were "nascent" or "developing" in at least 4 of 8 areas

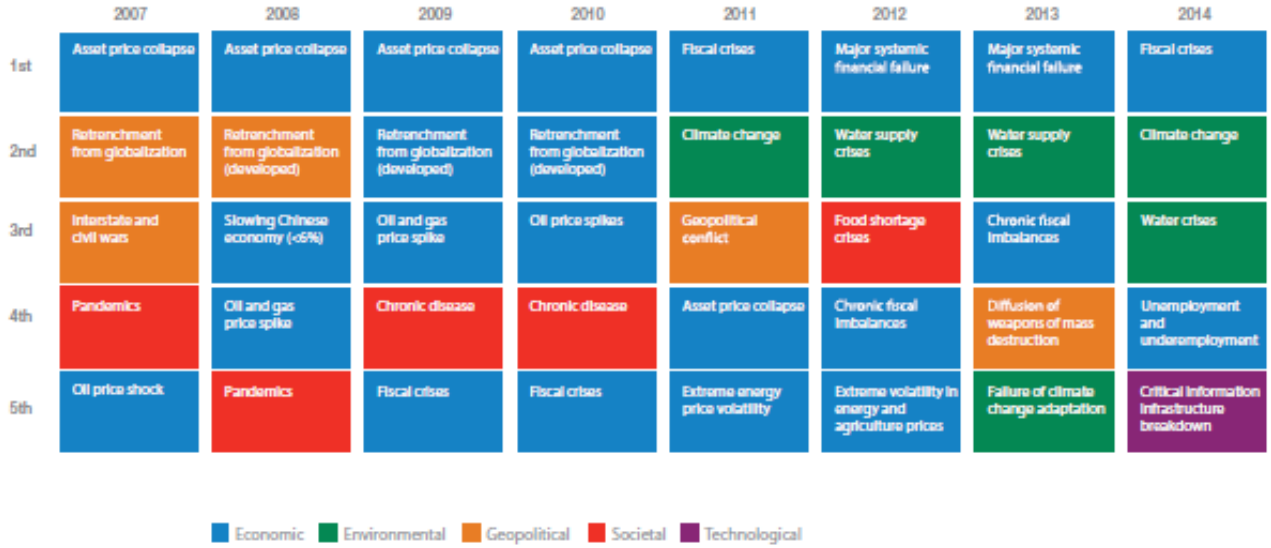
1. **Nascent**
   - Best effort based evaluation and mitigation of cyber risks
   - No defined single point of accountability nor a clearly defined escalation path to top management
2. **Developing**
   - Mostly qualitative framework for evaluating and mitigating cyber risks
   - Overall consistent governance model and known single point of accountability in each BU with a defined reporting line to top management
3. **Mature**
   - Quantitative approach for evaluating and qualitative approach for mitigating cyber risks
   - Defined cybersecurity governance model with a single point of accountability within a BU that owns the risks and decision-making
4. **Robust**
   - Robust quantitative approach for evaluating and mitigating cyber risks
   - Clearly identified individuals accountable for cybersecurity of each asset

I Cyber Risks sono ritenuti a livello globale i rischi a maggiore probabilità di accadimento e con i maggiori potenziali impatti negativi

Top 5 Global Risks in Terms of Likelihood



Top 5 Global Risks in Terms of Impacts

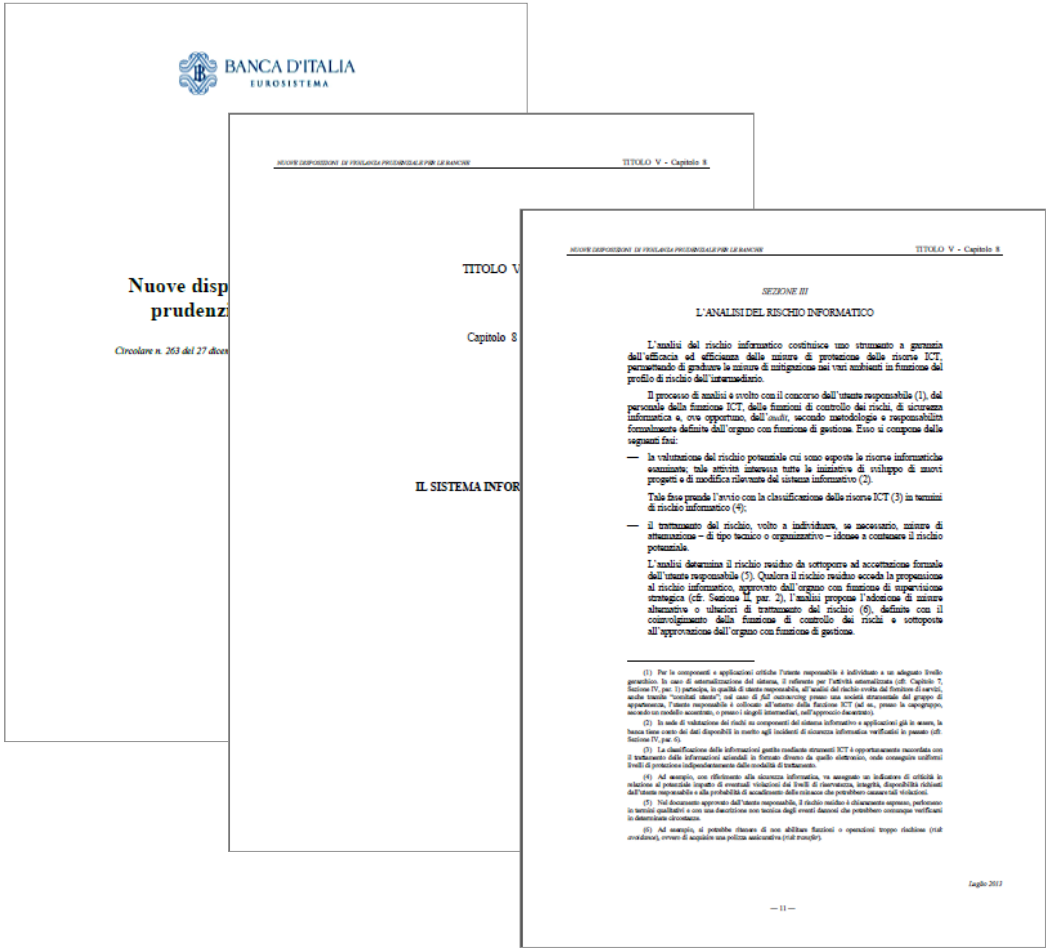


[…] In addition to the socio-economic and nevironmental risks, ***cyber attacks*** *and the* ***breakdown*** *of* ***critical information infrastructure*** *are* ***prominent risks****. This arguably reflects the* ***increasing digitization*** *of* ***economies*** *and* ***societies****, where rising dependence on information and data, as well as the systems to analyse and use them, has made* ***attacks more likely*** *and* ***their effects more impactful****.*

Le Nuove Disposizioni di Vigilanza Prudenziale introducono novità importanti in materia di analisi e gestione del rischio informatico

Nuove Disposizioni di Vigilanza Prudenziale

Titolo V – Capitolo 8 – Sezione II (L'analisi del rischio informatico)


BANCA D'ITALIA
EUROSISTEMA

Nuove disp
prudenz

Circolare n. 263 del 27 dice

TITOLO V - Capitolo 8

TITOLO V

Capitolo 8

IL SISTEMA INFOR

TITOLO V - Capitolo 8

SEZIONE III

L'ANALISI DEL RISCHIO INFORMATICO

L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario.

Il processo di analisi è svolto con il concorso dell'utente responsabile (1), del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, dell'*audit*, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione. Esso si compone delle seguenti fasi:

— la valutazione del rischio potenziale cui sono esposte le risorse informatiche esaminate; tale attività interessa tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (2).

Tale fase prende l'avvio con la classificazione delle risorse ICT (3) in termini di rischio informatico (4);

— il trattamento del rischio, volto a individuare, se necessario, misure di attenuazione – di tipo tecnico o organizzativo – idonee a contenere il rischio potenziale.

L'analisi determina il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile (5). Qualora il rischio residuo ecceda la propensione al rischio informatico, approvato dall'organo con funzione di supervisione strategica (cfr. Sezione II, par. 2), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (6), definite con il coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.

(1) Per le componenti e applicazioni critiche l'utente responsabile è individuato a un adeguato livello gerarchico. In caso di esternalizzazione del sistema, il referente per l'attività esternalizzata (cfr. Capitolo 7, Sezione IV, par. 1) partecipa, in qualità di utente responsabile, all'analisi del rischio svolta dal fornitore di servizi; anche laddove "consulenti esterni", nel caso di *full outsourcing* presso una società strumentale del gruppo di appartenenza, l'utente responsabile è collocato all'interno della funzione ICT (ad es., presso la capogruppo, secondo un modello accentrato, o presso i singoli intermediari, nell'approccio decentrato).

(2) In sede di valutazione dei rischi su componenti del sistema informativo e applicazioni già in essere, la banca tiene conto dei dati disponibili in merito agli incidenti di sicurezza informatica verificatisi in passato (cfr. Sezione IV, par. 6).

(3) La classificazione delle informazioni gestite mediante strumenti ICT è opportunamente raccordata con il trattamento delle informazioni aziendali in formato diverso da quello elettronico, onde conseguire uniformi livelli di protezione indipendentemente dalle modalità di trattamento.

(4) Ad esempio, con riferimento alla sicurezza informatica, va assegnato un indicatore di criticità in relazione al potenziale impatto di eventuali violazioni dei livelli di riservatezza, integrità, disponibilità richiesti dall'utente responsabile e alla probabilità di accadimento delle minacce che potrebbero causarne tali violazioni.

(5) Nel documento approvato dall'utente responsabile, il rischio residuo è chiaramente espresso, preferendo in termini qualitativi e con una descrizione non tecnica degli eventi dannosi che potrebbero comunque verificarsi in determinate circostanze.

(6) Ad esempio, si potrebbe rinunciare di non abilitare funzioni o operazioni troppo rischiose (*risk avoidance*), ovvero di acquisire una polizza assicurativa (*risk transfer*).

Luglio 2013

— 11 —

Principali novità

- La **Vigilanza** si occupa direttamente anche di **rischio informatico**, in quanto la sana* e prudente** gestione si basa anche su una **corretta** pianificazione, gestione operativa e controllo della **variabile informatica**

- Il rischio informatico **non** è una **nuova categoria** di rischio, ma un **driver specifico** dei **rischi** di primo (operativo) e secondo (strategico e reputazionale) pilastro di Basilea II, determinato dall'**utilizzo** delle **tecnologie ICT**

- La gestione del rischio informatico è:
  - effettuata con il **concorso** di più **funzioni aziendali**
  - **integrata** con la **gestione** dei **rischi aziendali** e il **Risk Appetite Framework**
  - di **responsabilità** degli **Organi** di **Gestione e Supervisione**

(*) Sana, cioè che l'attività d'impresa degli intermediari finanziari sia svolta nel pieno rispetto delle regole
(**) Prudente, cioè che per fare profitti gli intermediari finanziari non mettano a rischio la propria esistenza e il denaro loro affidato

Quadro di sintesi delle principali previsioni in tema di rischio informatico

Ambito	Principali previsioni normative
1 Compiti degli Organi Aziendali	▪ Compiti dell'Organo con Funzione di Supervisione Strategica ▪ Compiti dell'Organo con Funzione di Gestione
2 Metodologia e processi	▪ Fase 1 – Valutazione del rischio potenziale delle risorse informatiche ▪ Fase 2 – Trattamento del rischio potenziale delle risorse informatiche ▪ Fase 3 – Confronto rischio residuo con propensione al rischio informatico ▪ Fase 4 – Predisposizione informativa sui risultati del processo complessivo
3 Attori, ruoli e responsabilità	▪ Funzione Utente responsabile ▪ Funzione di Sicurezza informatica ▪ Funzione di Risk Management ▪ Funzione ICT ▪ Funzione di Revisione Interna
4 Modalità di esecuzione	▪ Perimetro di applicazione ▪ Frequenza di ripetizione
5 Documenti aziendali	▪ Documento di indirizzo strategico del sistema informativo ▪ Metodologia di analisi del rischio informativo ▪ Rapporto sintetico sulla situazione del rischio informatico

Quadro di sintesi delle principali definizioni in tema di rischio informatico

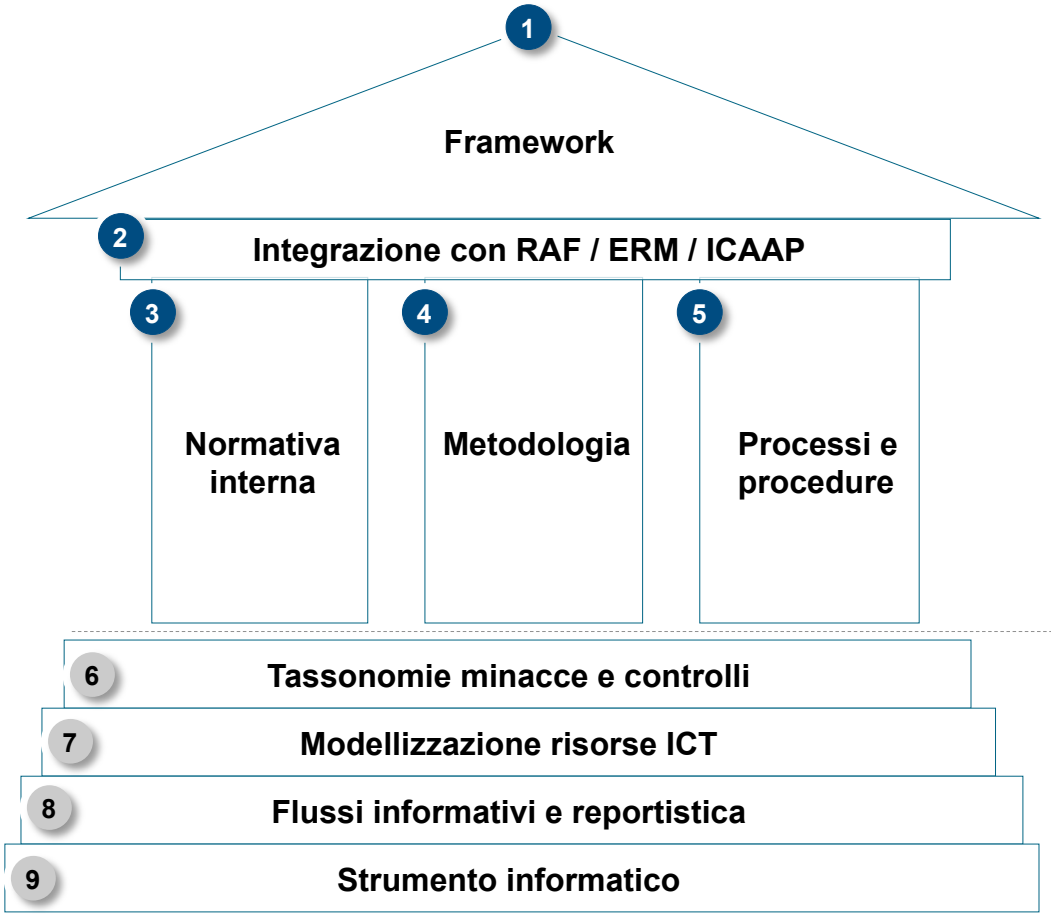
	Ambito	Definizione
1	**Rischio informatico**	Il **rischio** di incorrere in **perdite economiche**, di **reputazione** e di **quote di mercato** in relazione all'**utilizzo** di tecnologie ICT (Information and Communication Technology). Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i **rischi operativi**, **reputazionali** e **strategici**
2	**Rischio informatico residuo**	Il **rischio informatico** a cui l'intermediario **è esposto** una volta applicate le **misure** di **attenuazione** individuate nel processo di analisi dei rischi
3	**Obiettivo analisi del rischio informatico**	L'analisi del rischio informatico costituisce uno **strumento** a **garanzia** dell'**efficacia** ed **efficienza** delle **misure** di **protezione** delle **risorse ICT**, permettendo di **graduare** le misure di mitigazione nei vari ambienti in funzione del **profilo** di **rischio** dell'intermediario. […] La gestione della sicurezza informatica comprende i processi e le misure, la cui intensità dipende dalle **risultanze** del **processo** di **analisi dei rischi** , volte a garantire a ciascuna risorsa informatica una adeguata **protezione**
4	**Risorsa informatica**	Un **bene** dell'**azienda** afferente all'**ICT** che concorre alla **ricezione**, **archiviazione**, **elaborazione**, **trasmissione** e **fruizione** dell'informazione gestita dall'intermediario
5	**Utente responsabile**	– La **figura aziendale** identificata per **ciascun sistema** o **applicazione** e che ne assume formalmente la **responsabilità**, in rappresentanza degli **utenti** e nei rapporti con le funzioni preposte allo **sviluppo** e alla **gestione tecnica**. – Per le componenti e applicazioni critiche l'utente responsabile è individuato a un adeguato livello gerarchico. – Nel caso di *full outsourcing* presso una **società strumentale** del gruppo di appartenenza, l'utente responsabile è collocato **all'esterno** della funzione ICT (ad es., presso capogruppo, secondo un modello accentrato, o presso i singoli intermediari, nell'approccio decentrato)

Agenda dell'intervento

- Premessa: il concetto di rischio informatico alla luce delle Nuove Disposizioni di Vigilanza
- ***Il modello di riferimento proposto da Oasi per la gestione del rischio informatico***
- Conclusioni e raccomandazioni di Oasi per gli Istituti di Credito
- L'azienda Oasi – Outsourcing Applicativo e Servizi Innovativi S.p.A.

Il modello di riferimento proposto da Oasi per introdurre la gestione del rischio informatico, in accordo alle Nuove Disposizioni di Vigilanza

Modello di riferimento



Elementi costituenti del modello

GOVERNO

1. Framework di riferimento a livello di Gruppo Bancario per il rischio informatico
2. Allineamento / integrazione del rischio informatico con il RAF e ERM
3. Normativa interna per la regolamentazione della gestione del rischio informatico
4. Metodologia per l'analisi e la gestione del rischio informatico
5. Processi / procedure per l'esecuzione delle attività necessarie alla gestione del rischio informatico

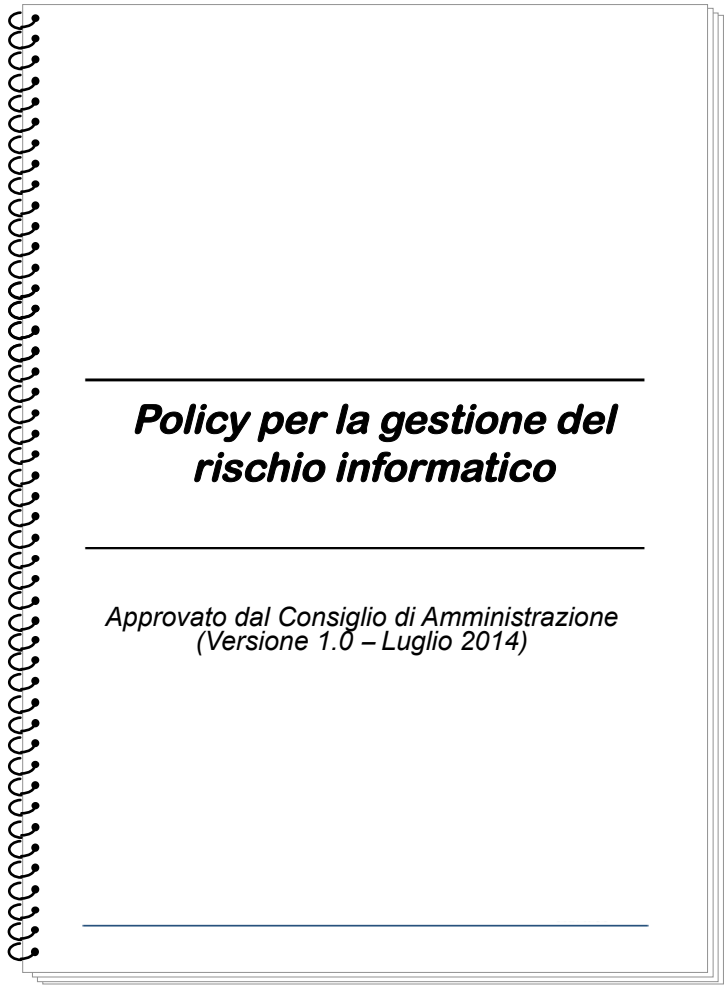
ESECUZIONE

6. Tassonomie driver / eventi di rischio informatico e relativi controlli / misure
7. Modellizzazione risorse informatiche e architetture del sistema informativo
8. Flussi informativi e reportistica verso gli Organi aziendali
9. Strumentazione operativa per lo svolgimento delle attività di analisi e gestione del rischio informatico

La normativa interna in tema di rischio informatico: la "*IT Risk Policy*" nel contesto del framework dei rischi aziendali

ESEMPLIFICATIVO

Policy per la gestione del rischio IT



Indice degli argomenti

Sezione I - **PREMESSA**
- Scopo del documento
- Struttura del documento
- Processo di redazione, approvazione e review

Sezione II - **CARATTERI GENERALI**
- Definizione di rischio informatico
- Caratteristiche del rischio informatico
- Fonti del rischio informatico
- …

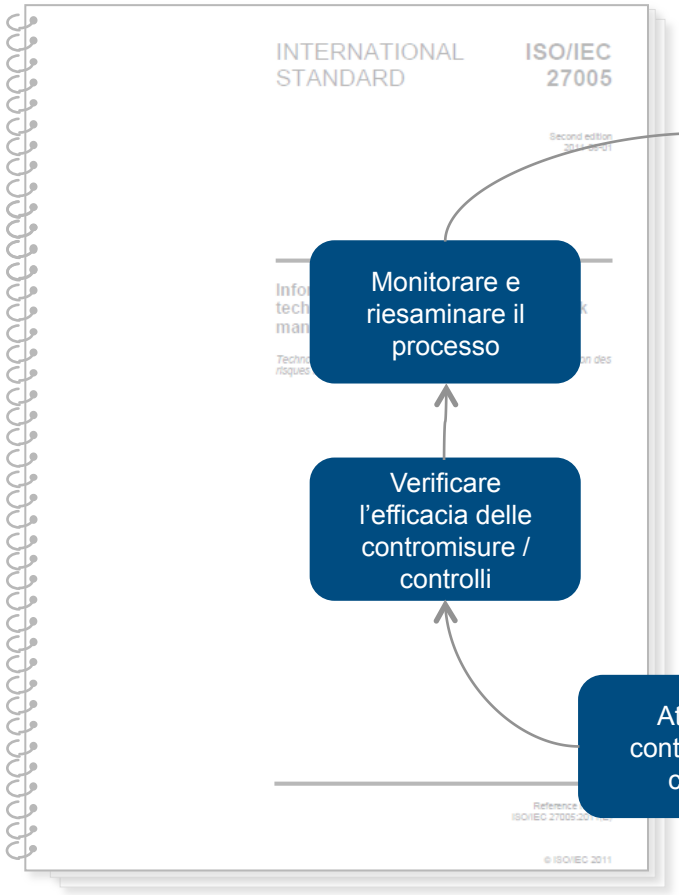
Sezione III - **ASSETTO ORGANIZZATIVO**
- Organi e funzioni aziendali coinvolte
- Ruoli e responsabilità
- Macro attività operative
- …

Sezione IV - **METODOLOGIA**
- Censimento degli asset
- Calcolo degli impatti
- …

Sezione V - **PROCESSO DI GESTIONE**
- Definizione del profilo di rischio
- Sistema delle soglie di sorveglianza
- Fase di identificazione dei rischi informatici
- Fase di misurazione / valutazione dei rischi informatici
- Fase di trattamento dei rischi informatici
- Fase di monitoraggio dei rischi informatici
- …

La metodologia di riferimento per l'analisi e la gestione del rischio informatico (ISO-IEC 27005, *Information Security Risk Management*)

Il modello di riferimento elaborato secondo best practice relative a standard per la gestione del rischio si sviluppa attraverso un ciclo iterativo che mira all'identificazione dei rischi, l'analisi, il trattamento ed il monitoraggio dei rischi residui



Definire Framework di riferimento

Identificare e mappare i rischi

Identificare i proprietari dei rischi

Valutare i rischi

Fissare dei livelli accettabili di rischio (RAF)

Identificare delle risposte adeguate al rischio (Action Plan)

Attuare le contromisure / controlli

Verificare l'efficacia delle contromisure / controlli

Monitorare e riesaminare il processo

Risk Identification

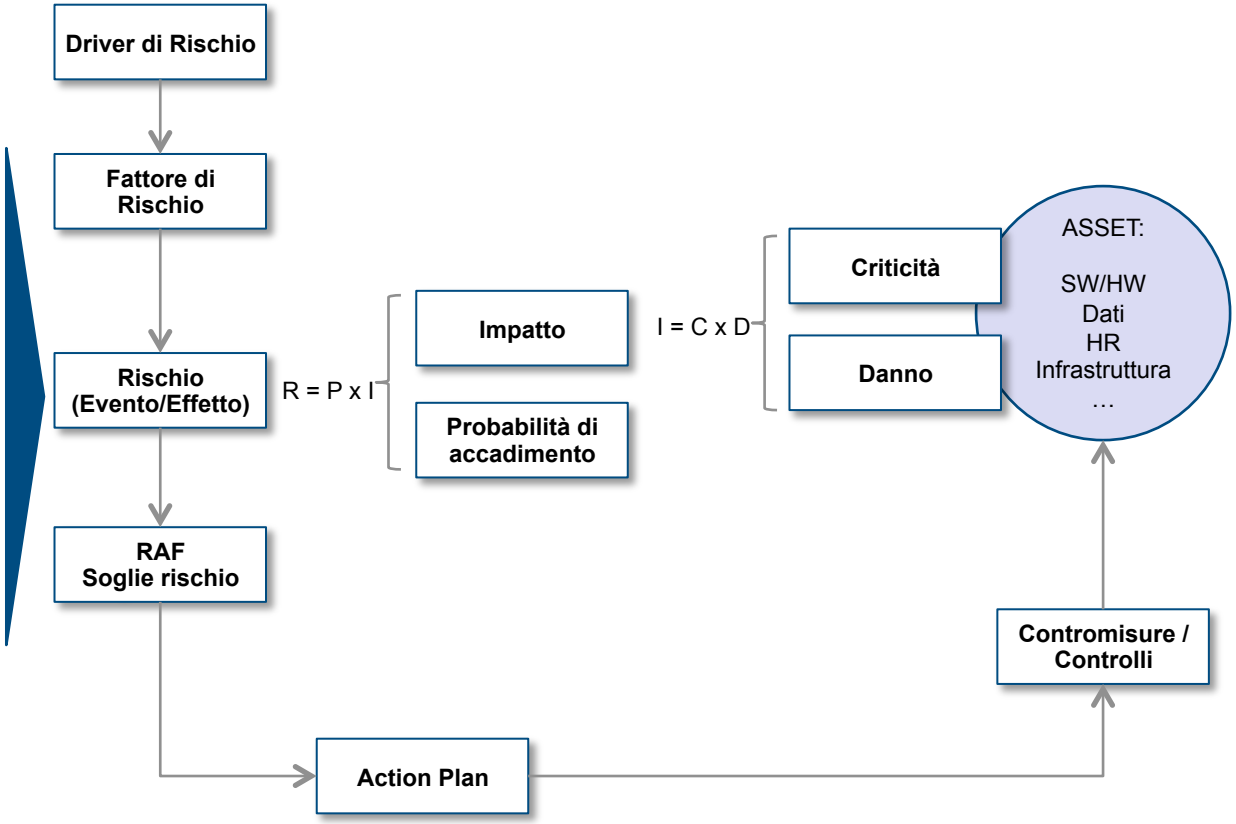
Risk Analysis

Risk Treatment

Risk Monitoring

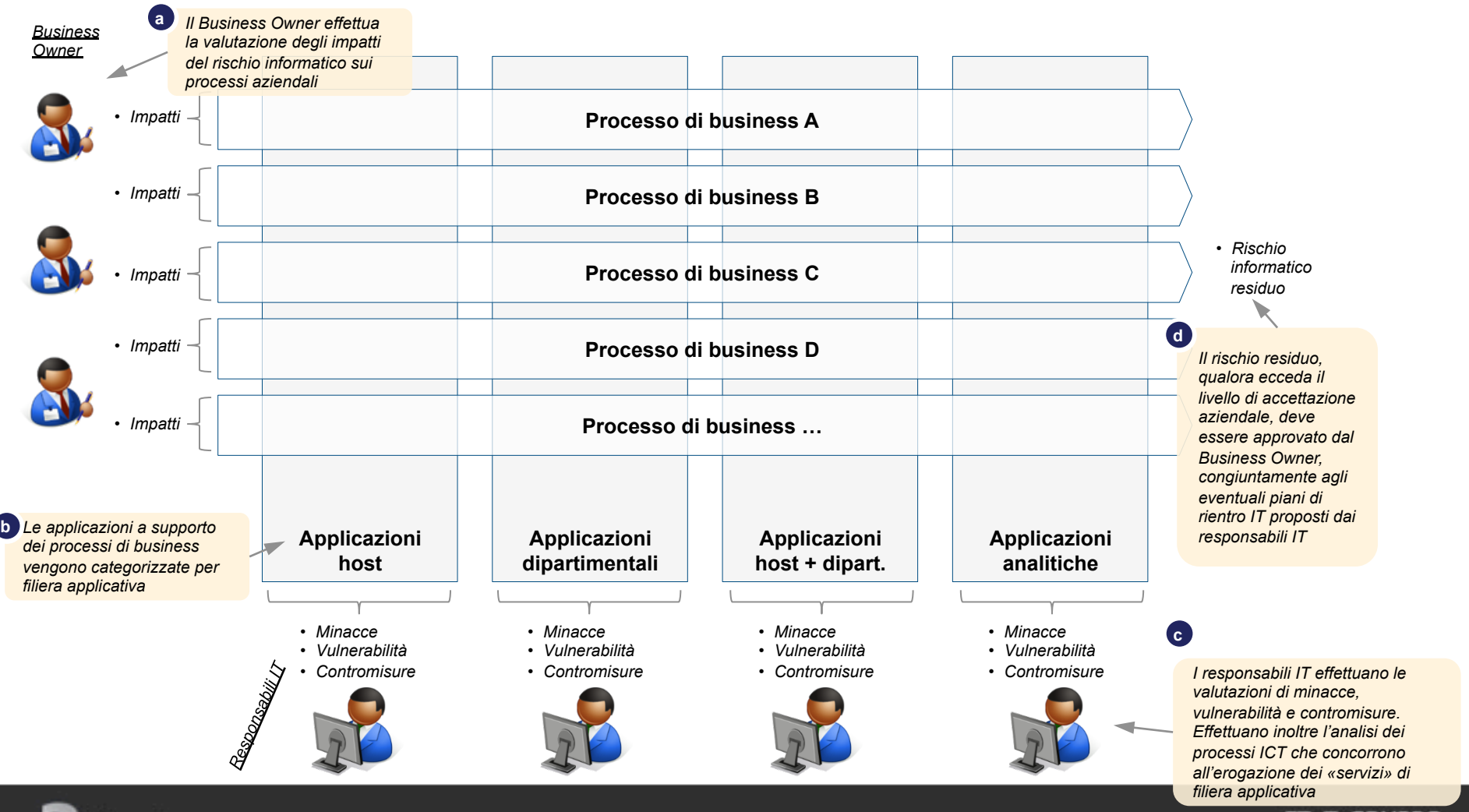
Il modello di misurazione e di calcolo del rischio informatico *potenziale* e del rischio informatico *residuo*

1. Identificazione e classificazione delle risorse, individuazione della relativa vulnerabilità
2. Individuazione delle minacce (interne/esterne) cui possono essere esposte le risorse
3. Individuazione dei danni che possono derivare dalle minacce, considerando la probabilità di accadimento
4. Identificazione delle possibili contromisure
5. Analisi costi/benefici degli investimenti per l'adozione delle contromisure
6. Definizione del piano delle azioni preventive e correttive
7. Documentazione ed accettazione del rischio residuo



L'approccio all'esecuzione dell'analisi del rischio informatico: la vista per processi di business integrata con le architetture del sistema informativo

*La metodologia definita ha l'obiettivo di **definire il livello di rischio informatico** relativo ai processi aziendali, valutarne eventuali modifiche a seguito di **progetti / change evolutive** in ambito IT e fornire risultati **integrabili** con il modello complessivo di Risk Management (rif. Risk Appetite Framework)*

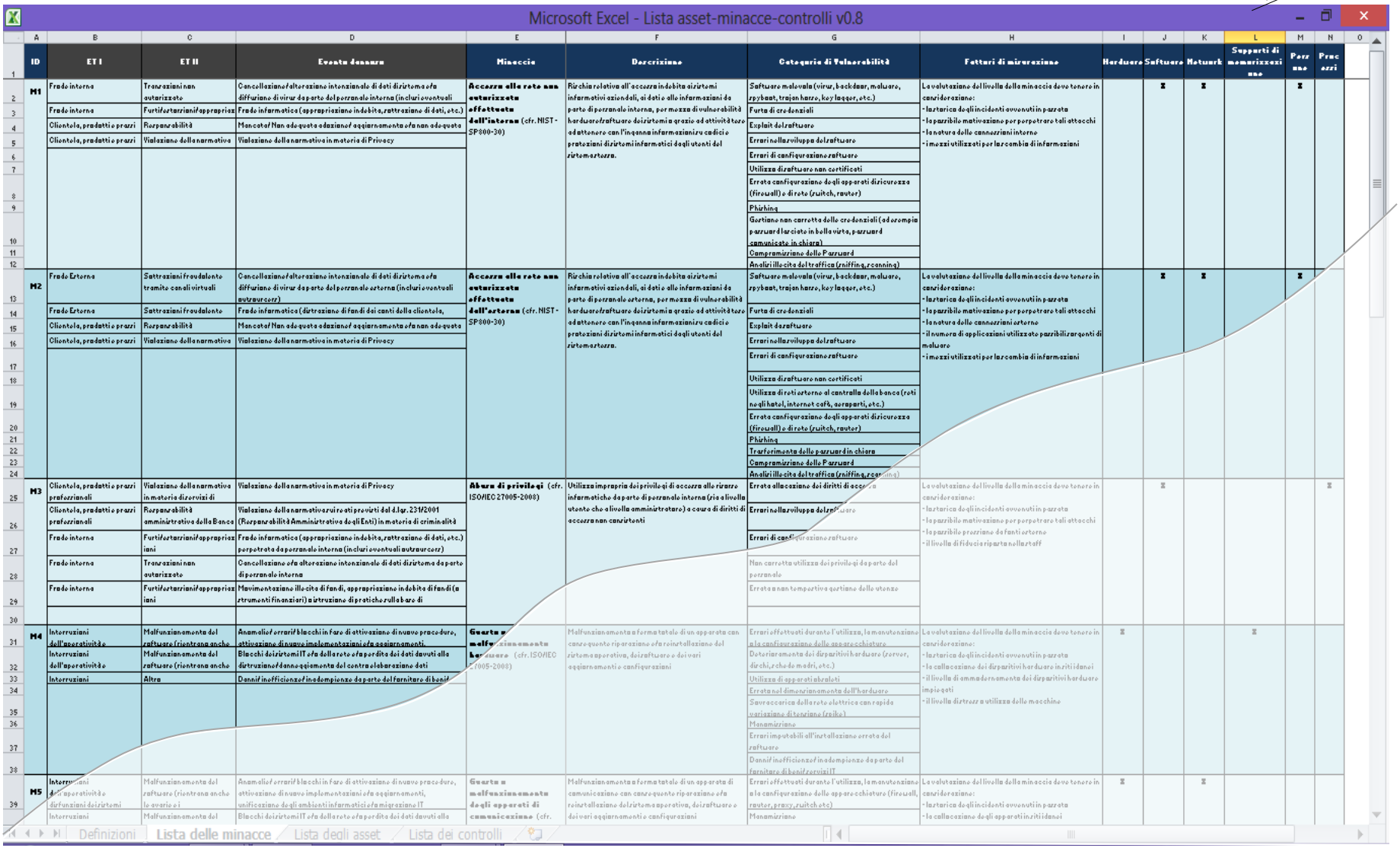


Le dimensioni di analisi del rischio informatico: protezione delle informazioni, conformità delle procedure e continuità dell'erogazione dei servizi

Dimensione	Driver
Informazioni	– **Riservatezza:** divulgazione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti – **Integrità:** modifica del contenuto dei dati accidentale oppure effettuato da una terza parte, essendo compreso nell'alterazione anche il caso limite della generazione ex novo di dati ed informazioni. – **Disponibilità:** impossibilità di un sistema a svolgere una funzione richiesta in determinate condizioni ad un dato istante o durante un dato intervallo di tempo
Applicazioni	– **Conformità:** violazione di normative esterne a seguito di interruzione / conduzione errata delle operazioni informatiche a supporto dei processi di business – **Accountability:** impossibilità di identificare un singolo utente o di determinarne le azioni o il comportamento nelle operazioni informatiche a supporto dei processi di business – **Verificabilità:** impossibilità di condurre indagini rispetto al comportamento del singolo utente nell'erogazione delle operazioni informatiche a supporto dei processi di business
Servizio informatico	– **Tempestività:** impossibilità di rendere disponibili dati / elaborazioni nei tempi necessari all'utente finale per problematiche legate ai servizi informatici – **Prestazioni:** impossibilità di erogare in modo efficace ed efficiente i processi di business per problematiche legate ai servizi informatici

Le dimensioni di analisi del rischio informatico: il "catalogo" delle minacce

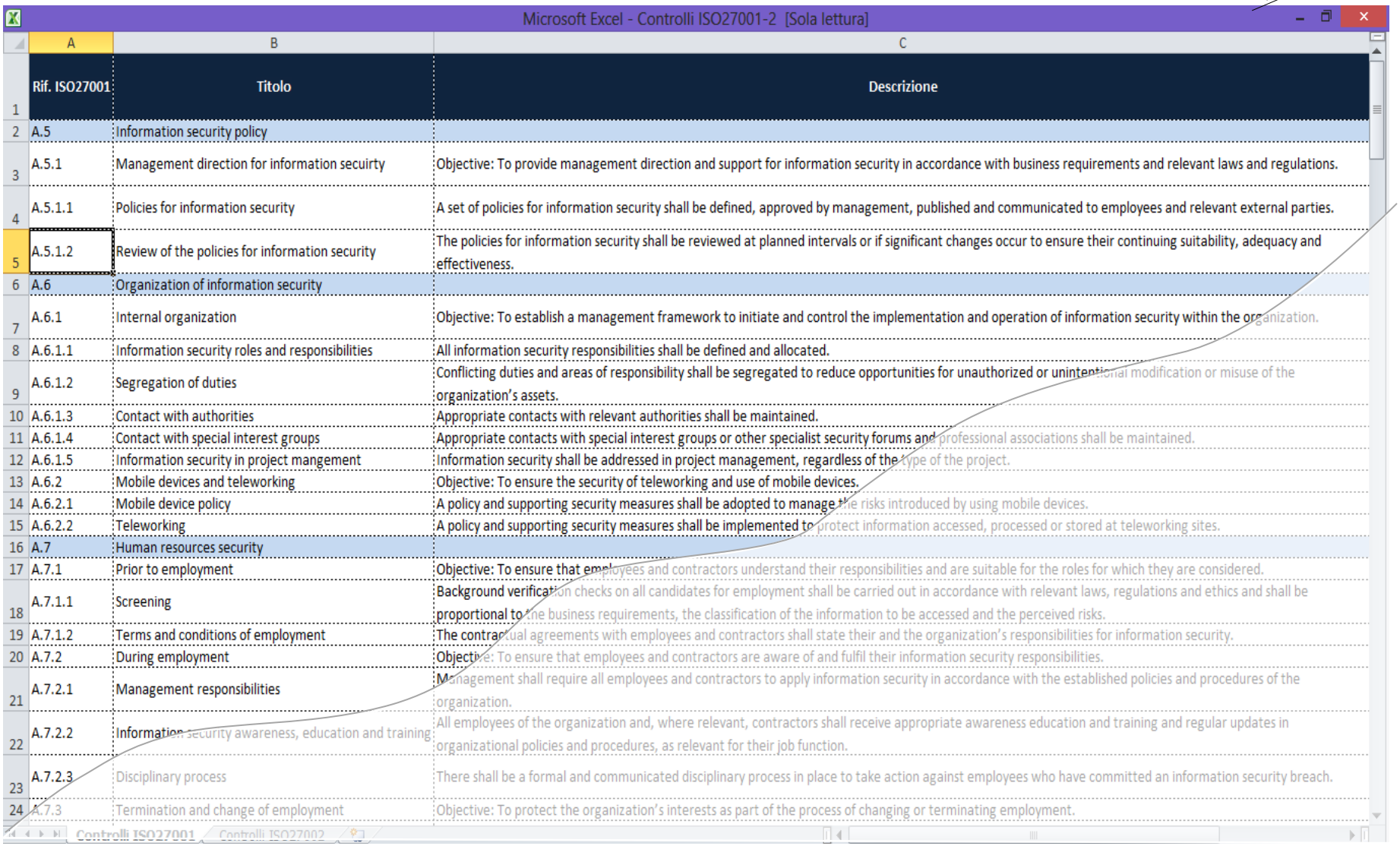
ESEMPLIFICATIVO



ID	ET I	ET II	Evento dannoso	Minaccia	Descrizione	Categoria di Vulnerabilità	Fattori di misurazione	Hardware	Software	Network	Supporti di memorizzazione	Persone	Processi
M1	Frode interna	Transazioni non autorizzate	Cancellazione/alterazione intenzionale di dati di/sistema e/o diffusione di virus da parte del personale interno (inclusi eventuali	**Accesso alle reti non autorizzato effettuato dall'interno** (cfr. NIST-SP800-30)	Rischio relativo all'accesso indebito ai sistemi informativi aziendali, ai dati e alle informazioni da parte di personale interno, per mezzo di vulnerabilità hardware/software dei sistemi in grazie ad attività tese ad ottenere con l'inganno informazioni su codici e protezioni dei sistemi informatici dagli utenti del sistema stesso.	Software malevolo (virus, backdoor, malware, spybowt, trojan horse, keylogger, etc.)	La valutazione del livello della minaccia deve tenere in considerazione: - la storica degli incidenti avvenuti in passato - la possibile motivazione per perpetrare tali attacchi - la natura delle connessioni interne - i mezzi utilizzati per lo scambio di informazioni		X	X		X	
	Frode interna	Furti/ostruzionismo appropriazioni	Frode informatica (appropriazione indebita, sottrazione di dati, etc.)			Furto di credenziali							
	Clientela, prodotti e prezzi	Responsabilità	Mancata/Non adeguata adozione/aggiornamento e/o non adeguata			Exploit dei software							
	Clientela, prodotti e prezzi	Violazione della normativa	Violazione della normativa in materia di Privacy			Errori nello sviluppo dei software							
						Errori di configurazione software							
						Utilizzo di software non certificati							
						Errata configurazione degli apparati di sicurezza (firewall) e di rete (switch, router)							
						Phishing							
						Gestione non corretta delle credenziali (ad esempio password lasciate in bella vista, password comunicate in chiaro)							
						Compromissione delle Password							
						Analisi illecita del traffico (sniffing, scanning)							
M2	Frode Esterna	Sottrazioni fraudolente tramite canali virtuali	Cancellazione/alterazione intenzionale di dati di/sistema e/o diffusione di virus da parte del personale esterno (inclusi eventuali autori esterni)	**Accesso alle reti non autorizzato effettuato dall'esterno** (cfr. NIST-SP800-30)	Rischio relativo all'accesso indebito ai sistemi informativi aziendali, ai dati e alle informazioni da parte di personale esterno, per mezzo di vulnerabilità hardware/software dei sistemi in grazie ad attività tese ad ottenere con l'inganno informazioni su codici e protezioni dei sistemi informatici dagli utenti del sistema stesso.	Software malevolo (virus, backdoor, malware, spybowt, trojan horse, keylogger, etc.)	La valutazione del livello della minaccia deve tenere in considerazione: - la storica degli incidenti avvenuti in passato - la possibile motivazione per perpetrare tali attacchi - la natura delle connessioni esterne - il numero di applicazioni utilizzate possibili vettori di malware - i mezzi utilizzati per lo scambio di informazioni		X	X		X	
	Frode Esterna	Sottrazioni fraudolente	Frode informatica (distrazione di fondi dai conti della clientela,			Furto di credenziali							
	Clientela, prodotti e prezzi	Responsabilità	Mancata/Non adeguata adozione/aggiornamento e/o non adeguata			Exploit dei software							
	Clientela, prodotti e prezzi	Violazione della normativa	Violazione della normativa in materia di Privacy			Errori nello sviluppo del software							
						Errori di configurazione software							
						Utilizzo di software non certificati							
						Utilizzo di reti esterne al controllo della banca (reti negli hotel, internet cafè, aeroporti, etc.)							
						Errata configurazione degli apparati di sicurezza (firewall) e di rete (switch, router)							
						Phishing							
						Trafugamento delle password in chiaro							
						Compromissione delle Password							
						Analisi illecita del traffico (sniffing, scanning)							
M3	Clientela, prodotti e prezzi professionali	Violazione della normativa in materia di servizi di	Violazione della normativa in materia di Privacy	**Abuso di privilegi** (cfr. ISO/IEC 27005-2008)	Utilizzo improprio dei privilegi di accesso allo sistema informatico da parte di personale interno (sia a livello utente che a livello amministratore) a causa di diritti di accesso non congruenti	Errata allocazione dei diritti di accesso	La valutazione del livello della minaccia deve tenere in considerazione: - la storica degli incidenti avvenuti in passato - la possibile motivazione per perpetrare tali attacchi - la possibile provenienza da fonti esterne - il livello di fiducia riposta nello staff		X				X
	Clientela, prodotti e prezzi professionali	Responsabilità amministrativa della Banca	Violazione della normativa sui reati previsti dal d.lgs. 231/2001 (Responsabilità Amministrativa degli Enti) in materia di criminalità			Errori nello sviluppo del software							
	Frode interna	Furti/ostruzionismo appropriazioni	Frode informatica (appropriazione indebita, sottrazione di dati, etc.) perpetrata da personale interno (inclusi eventuali autori esterni)			Errori di configurazione software							
	Frode interna	Transazioni non autorizzate	Cancellazione e/o alterazione intenzionale di dati di/sistema da parte di personale interno			Non corretta utilizzo dei privilegi da parte del personale							
	Frode interna	Furti/ostruzionismo appropriazioni	Movimentazione illecita di fondi, appropriazione indebita di fondi (strumenti finanziari) a/sottrazione di pratiche sulla base di			Errata o non tempestiva gestione delle utenze							
M4	Interruzioni dell'operatività e	Malfunzionamento del software (rientrano anche	Anomalie/errori/blocchi in fase di attivazione di nuove procedure, attivazione di nuove implementazioni e/o aggiornamenti,	**Guasto e malfunzionamento hardware** (cfr. ISO/IEC 27005-2008)	Malfunzionamento o formattazione di un apparato con conseguente riparazione e/o reinstallazione del sistema operativo, del software o dei vari aggiornamenti e configurazioni	Errori effettuati durante l'utilizzo, la manutenzione o la configurazione delle apparecchiature	La valutazione del livello della minaccia deve tenere in considerazione: - la storica degli incidenti avvenuti in passato - la collocazione dei dispositivi hardware in siti idonei - il livello di ammodernamento dei dispositivi hardware impiegati - il livello di stress a utilizzo delle macchine	X			X		
	Interruzioni dell'operatività e	Malfunzionamento del software (rientrano anche	Blocchi di/sistemi IT e/o della rete e/o perdita dei dati dovuti alla			Deterioramento dei dispositivi hardware (server, dischi, echo di madri, etc.)							
	Interruzioni	Altro	Danni/inefficienze/indempienze da parte del fornitore di beni/servizi IT			Utilizzo di apparati obsoleti							
						Errata/non dimensionamento dell'hardware							
						Sovraccarico della rete elettrica con rapida variazione di tensione (spike)							
						Manomissione							
						Errori imputabili all'installazione errata del software							
						Danni/inefficienze/indempienze da parte del fornitore di beni/servizi IT							
M5	Interruzioni dell'operatività e/o disfunzioni dei/sistemi	Malfunzionamento del software (rientrano anche lo svario e i	Anomalie/errori/blocchi in fase di attivazione di nuove procedure, attivazione di nuove implementazioni e/o aggiornamenti, unificazione degli ambienti informatici e/o migrazione IT	**Guasto e malfunzionamento degli apparati di comunicazione** (cfr.	Malfunzionamento o formattazione di un apparato di comunicazione con conseguente riparazione e/o reinstallazione del sistema operativo, del software o dei vari aggiornamenti e configurazioni	Errori effettuati durante l'utilizzo, la manutenzione o la configurazione delle apparecchiature (firewall, router, proxy, switch etc)	La valutazione del livello della minaccia deve tenere in considerazione: - la storica degli incidenti avvenuti in passato - la collocazione degli apparati in siti idonei	X		X			
	Interruzioni	Malfunzionamento del	Blocchi di/sistemi IT e/o della rete e/o perdita dei dati dovuti alla			Manomissione							

Le dimensioni di analisi del rischio informatico: il "catalogo" dei controlli

ESEMPLIFICATIVO



Microsoft Excel - Controlli ISO27001-2 [Sola lettura]

	A	B	C
1	Rif. ISO27001	Titolo	Descrizione
2	A.5	Information security policy	
3	A.5.1	Management direction for information secuirty	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
4	A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
5	A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
6	A.6	Organization of information security	
7	A.6.1	Internal organization	Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.
8	A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.
9	A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
10	A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.
11	A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
12	A.6.1.5	Information security in project mangement	Information security shall be addressed in project management, regardless of the type of the project.
13	A.6.2	Mobile devices and teleworking	Objective: To ensure the security of teleworking and use of mobile devices.
14	A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
15	A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.
16	A.7	Human resources security	
17	A.7.1	Prior to employment	Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
18	A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
19	A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.
20	A.7.2	During employment	Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
21	A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
22	A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
23	A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
24	A.7.3	Termination and change of employment	Objective: To protect the organization's interests as part of the process of changing or terminating employment.

Controlli ISO27001 | Controlli ISO27002

La Scorecard del rischio informatico: rischio potenziale, rischio residuo, livello di adeguatezza dei controlli e stati dei *Key Risk Indicator*

ESEMPLIFICATIVO

Di seguito si riporta la rappresentazione di una scheda riassuntiva di valutazione dei processi / attività oggetto di analisi dell'esposizione ai rischi.

Scheda di analisi complessiva dei rischi

P.1 - Processo «Gestione servizi Rete Interbancaria»	Risk analysis: Rischio inerente	Risk analysis: Rischio residuo	Livello adeguatezza dei controlli
A.1.1-Ricezione flussi dati da RNI			1
R.1.1 – Alterazione dati informatici			

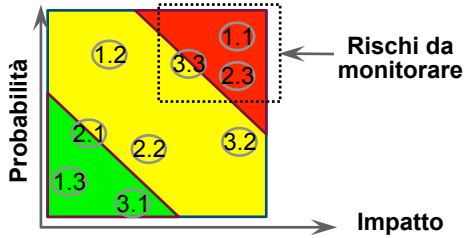
Key Risk Indicators	Tipo KRI	Valore soglia	Valore osservato	Trend
	Predittivo	20%	15%	- 8%
	Misura	10	15	+10%

Valutazione danno:
- Economico
- Reputazionale
- Legale

Livello valutazione rischio
Debole / assente
Significativo
Forte
Elevato

Livello adeguatezza controlli
4. Completo
3. Soddisfacente
2. Mediocre
1. Non Adeguato

Ottenute le diverse valutazioni, si procede con il posizionamento nella matrice di rischio in funzione di frequenza e perdita



Dati ricavabili

- Informazioni che verranno rilevate dal Risk Manager attraverso opportune interview dai responsabili delle strutture organizzative interessate al rilevamento del rischio

Dati presenti e rilevabili

- Informazioni presenti all'interno dei sistemi informativi aziendali che possono essere estratte e raccolte in modo automatico nelle diverse strutture organizzative

Obiettivo è fornire una valutazione dei rischi ponderata e aderente alla realtà della banca, attraverso il coinvolgimento delle funzioni interessate per la valutazione del rischio sotto il profilo economico, reputazionale e legale

Le modalità di gestione del rischio informatico tra prevenzione / protezione, trasferimento, accettazione e piani di emergenza

Le decisioni che riguardano la gestione e il controllo del rischio dovranno essere valutate sugli asset principali, quali Organizzazione, Processo e Sistemi IT, identificando le opportune azioni correttive. Possiamo indicare le seguenti modalità di gestione del rischio:

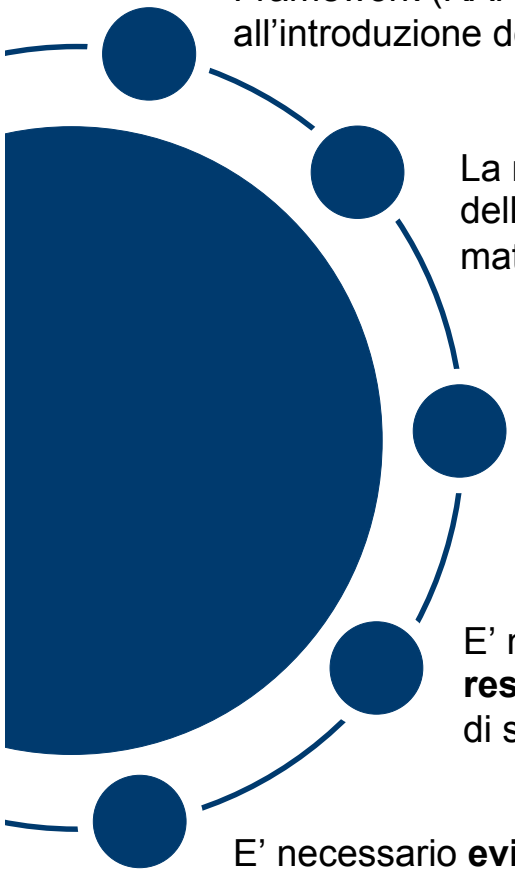
Modalità di gestione del rischio	Tipologia	Descrizione
Prevenzione	EX ANTE	Riduzione della probabilità di accadimento di eventi sfavorevoli attraverso l'adozione di opportune misure di valore aziendale
Protezione	EX ANTE	Riduzione delle perdite derivanti dalla manifestazione di eventi sfavorevoli, contenendo quindi l'effetto negativo attraverso l'adozione di opportune misure di valore aziendale
Copertura assicurativa	EX ANTE	Assunzione di una posizione rischiosa opposta a quella da gestire, attraverso la stipulazione di un contratto finanziario con soggetti specifici (società assicuratrici) e/o adottando le tecniche specifiche di risk hedging attraverso i derivati, esternalizzando così il rischio stesso senza influenzarlo (trasferimento del rischio)
Ritenzione e accettazione	EX ANTE	Assunzione di un rischio, poiché giudicato accettabile o trascurabile rispetto ad un valore di soglia, attraverso politiche di accantonamento calcolate in base al rapporto tra downside risk e il patrimonio
Business Continuity Management (BCM) **Crisis Management (CM)**	EX POST	Definizione delle misure di gestione per il ripristino delle attività aziendali critiche individuate attraverso la Business Impact Analysis (BIA), con misure ex ante (prevenzione, protezione e copertura assicurativa) e ex post (monitoraggio, contenimento e riduzione)

L'obiettivo è di scegliere (fase di decisione) la migliore alternativa per modificare l'esposizione al rischio della Banca relativamente agli ambiti analizzati. Le modalità di gestione del rischio "classiche" dovranno essere contestualizzate e attualizzate in base agli asset identificati per l'analisi del rischio

Agenda dell'intervento

- Premessa: il concetto di rischio informatico alla luce delle Nuove Disposizioni di Vigilanza
- Il modello di riferimento proposto da Oasi per la gestione del rischio informatico
- ***Conclusioni e raccomandazioni di Oasi per gli Istituti di Credito***
- L'azienda Oasi – Outsourcing Applicativo e Servizi Innovativi S.p.A.

Conclusioni e raccomandazioni di Oasi per gli Istituti di Credito in materia di analisi, controllo e gestione dei rischi informatici



La metodologia **deve essere «semplice»** per facilitare l'integrazione con il Risk Appetite Framework (RAF), la conduzione dell'analisi in modalità «massiva», parallelamente all'introduzione delle valutazioni su nuovi progetti / change evolutive

La metodologia **deve essere «scalabile»** in termini di livello di dettaglio dell'analisi. Quando i processi di valutazione saranno sufficientemente maturi, sarà più facile introdurre modalità di valutazione più specifiche

La metodologia deve essere **aperta e customizzabile** per potersi adeguare alle esigenze di valutazione di ciascuna banca con le relative specificità e necessità di analisi

E' necessario un **coinvolgimento dei responsabili di business e dei responsabili IT**, condividendo con loro l'approccio e fornendo strumenti di supporto facilmente utilizzabili

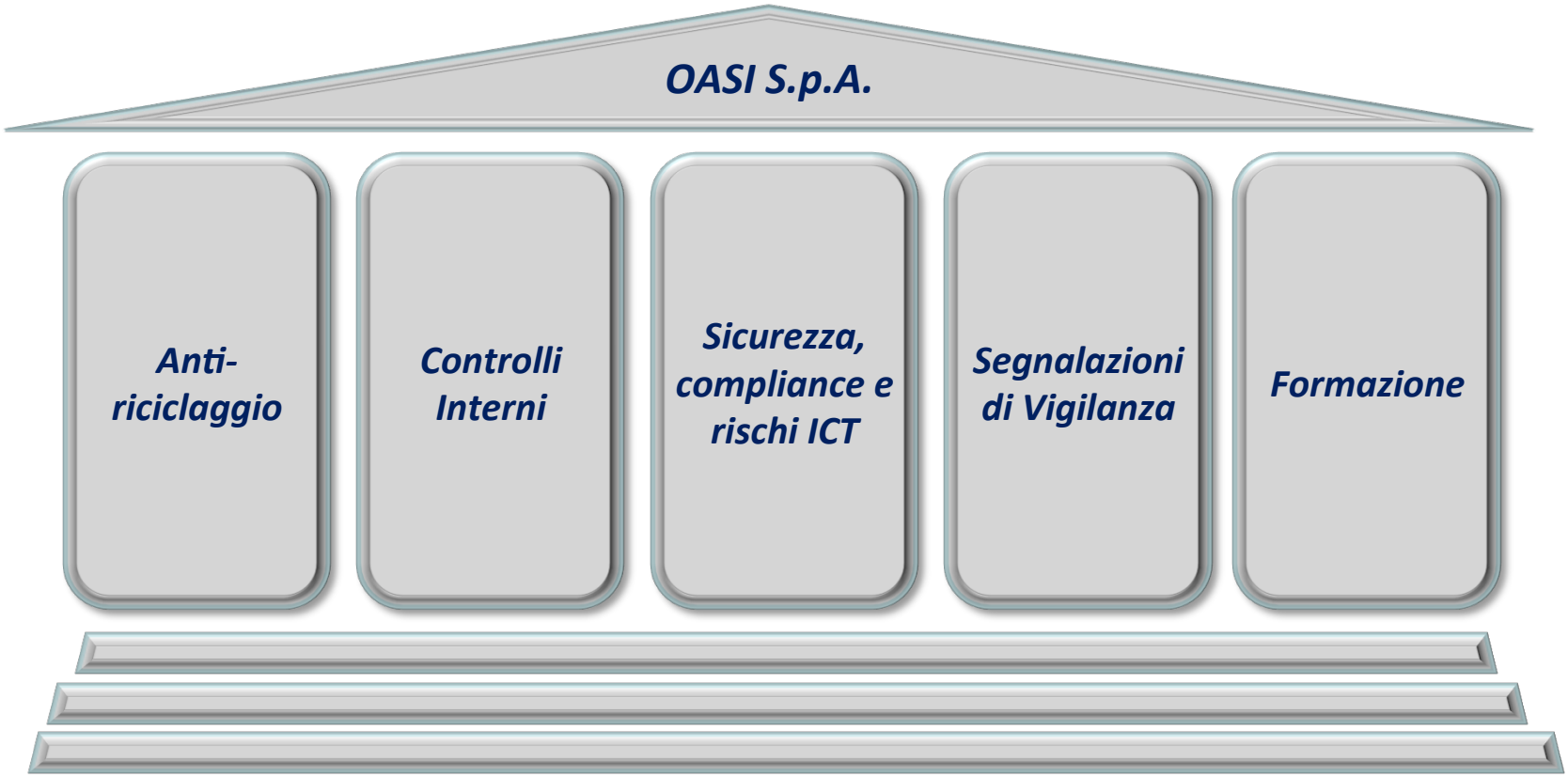
E' necessario **evitare di «ingessare» i processi operativi IT**. Il processo richiede infatti passi formali di approvazione, con rischio di rallentare i processi di autorizzazione (ad esempio per attivazione di nuovi progetti, passaggi in produzione, …)

Agenda dell'intervento

- Premessa: il concetto di rischio informatico alla luce delle Nuove Disposizioni di Vigilanza
- Il modello di riferimento proposto da Oasi per la gestione del rischio informatico
- Conclusioni e raccomandazioni di Oasi per gli Istituti di Credito
- ***L'azienda Oasi – Outsourcing Applicativo e Servizi Innovativi S.p.A.***

OASI è la società del Gruppo ICBPI specializzata nello sviluppo / integrazione di soluzioni informatiche e nei servizi di consulenza, outsourcing e formazione

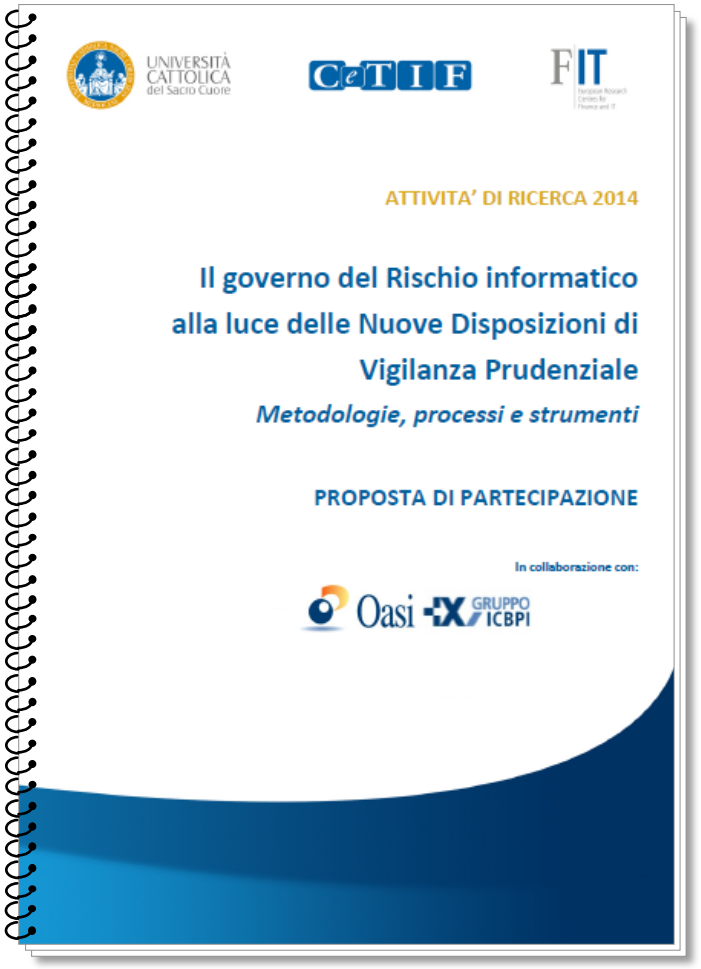
OASI – Outsourcing Applicativo e Servizi Innovativi S.p.A. è la società del gruppo ICBPI leader nelle soluzioni, nella consulenza, nei servizi innovativi e nell'outsourcing in tema di antiriciclaggio, controlli interni, sicurezza, rischi e compliance ICT, Segnalazioni di Vigilanza e Formazione



Oasi S.p.A. ha predisposto un'offerta completa di servizi e soluzioni innovative in materia di sicurezza, compliance e rischi ICT

Ambito	Consulenza	Soluzioni	Servizi / outsourcing
Sicurezza Informatica	- Policy e procedure - Gestione rischio informatico - IT auditing - Conformità Privacy - Certificazioni ISO 27001 - Revisione contrattualistica - Conformità Circ. 263/2006 - Sistemi di reportistica	- Gestione dei log di sicurezza - Classificazione delle informazioni - Data Loss Prevention - Protezione degli endpoint - Gestione del rischio informatico - Advanced Threat Prevention	- Monitoraggio della sicurezza IT - Computer forensics - Vulnerability / penetration test - Revisione del codice sorgente
Antifrode Remote Banking	- Policy e procedure - Gestione rischio frode - Verifiche di conformità - Conformità Circ. 263/2006	- Strong Authentication - Transaction monitoring	- Anti phishing / malware - Active Fraud Prevention - Firma Digitale a valenza legale - Monitoraggio canale CBI
Continuità Operativa	- Analisi degli impatti - Piani di Continuità Operativa - Piani di Disaster Recovery - Verifiche conformità - Certificazioni ISO 22301 - Revisione contrattualistica - Conformità Circ. 263/2006	← - SW per la gestione del piano di BC - SW per la gestione delle crisi →	
Sicurezza Fisica	- Policy e procedure - Gestione rischio rapina - Contrattualistica - Sistemi di reportistica	- SW Gestione apprestamenti - SW Gestione dei mezzi forti - SW Gestione degli allarmi	- Formazione del personale - Assessment di filiali - Assessment sedi direzionali

Oasi è sostenitore di una attività di ricerca condotta dall'Università Cattolica del Sacro Cuore sul tema del governo del rischio informatico



Obiettivi dell'attività di ricerca

- La ricerca si propone di definire un **approccio metodologico** che consenta di presidiare efficacemente il **governo** del **rischio informatico**, in linea con i **principi** definiti dalle **Disposizioni** di **Vigilanza**, orientato alla identificazione dei rischi e delle interdipendenze tra questi, le unità di business, i processi operativi aziendali e i relativi flussi di reporting

- L'attività di ricerca è finalizzata alla **produzione** dei seguenti **output**:
  - ***metodologie*** *e* ***strumenti*** *per la rilevazione, analisi, valutazione, gestione e reporting del rischio informatico*
  - ***modello organizzativo*** *di riferimento per il* ***governo*** *del* ***rischio informatico****, che definisce l'interrelazione con i processi di risk management e gli aspetti collaborativi tra le funzioni preposte al governo dei rischi e dei controlli*
  - ***brief assessment*** *con le banche aderenti che abbia l'obiettivo di supportare l'****applicazione*** *delle* ***metodologie*** *e dei processi identificati da l tavolo di lavoro*

Grazie per l'attenzione

Ing. Andrea Agosti
Responsabile Servizio Security

OASI – Outsourcing Applicativo e Servizi Innovativi S.p.A.
Azienda del Gruppo Bancario Istituto Centrale delle Banche Popolari Italiane
Corso Europa, 18 - 20122 Milano - Tel. +39 02 77051
Cell.:**+39 335 7365157** Ufficio: **02 7705326** Mail: **a.agosti@oasi-servizi.it**