Banca Popolare di Sondrio

www.popso.it

L'A[1].B[2].C[3]. per il governo dell'IT in tempi di crisi

① **A**llineamento al business

② **B**udget di spesa

③ **C**ompliance e sicurezza

Milo Gusmeroli

Information & Communication Technology

- ✓ Strategico
- ✓ Differenziante
- ✓ Innovativo

....allora spendere meglio.

- ✓ Servizio
- ✓ Supporto
- ✓ Commodity

....allora spendere per riqualificare il ruolo.

Le azioni conseguenti <u>immediate</u> generalizzate:

- Rinegoziazione con i fornitori;
- Selezione dei fornitori-partnership;
- Outsourcing o insourcing.

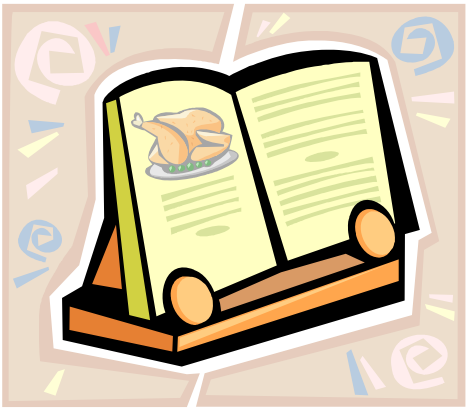
costi  **ricavi** 

Le azioni conseguenti <u>ragionate</u> e tendenziali:

- Investimenti legati al business;
- Misurazione dei risultati attesi o ottenuti;
- Investimenti in ambiti differenziati/caratterizzanti;
- Non perdere di vista l'innovazione e i comportamenti dei clienti attuali e potenziali.

costi  **ricavi** 

Come e con quali implicazioni?



Non esiste una ricetta valida per tutti perché ognuno ha il proprio "metabolismo" e le proprie "intolleranze".

Come e con quali implicazioni?

Però è certo che un IT "statico" e "complesso" appesantisce il business e lo rende poco reattivo al mercato e ai cambiamenti.

Ma per superare la crisi agilità e flessibilità sono indispensabili.

La visione in Banca Popolare di Sondrio

Comprimere il rischio e la complessità

Comprimere i costi e le inefficienze

Allinearsi al business

Valorizzare le opportunità della tecnologia

Assottigliare i vincoli all'evoluzione

L’esperienza di Banca Popolare di Sondrio

Governo - Compliance e sicurezza

- ✓ norme internazionali di riferimento, catalogo IT, SLA, standard tecnologici, valutazione risultati, gestione fornitori, sistemi di certificazione di qualità e sicurezza

Selezione progetti – Allineamento al business e al budget

- ✓ ragionare per processi (trasversali) per progettare e implementare procedure univoche (non verticali)
- ✓ coinvolgere unità di business nei progetti e declinare i risultati attesi
- ✓ Garantire la necessaria attenzione ai temi della sicurezza

L’esperienza di Banca Popolare di Sondrio

Ruoli

- ✓ rivedere e valorizzare ruoli non settoriali (architetti, PMO, demand manager)
- ✓ rendere gli “innovatori” conoscitori delle effettive esigenze aziendali
- ✓ condividere il portafoglio progetti, le priorità e i risultati attesi

Tecnologia per la tecnologia

- ✓ definire regole, standard e impatti organizzativi

FARE: …….

Il governo dell' IT: Obiettivi e Azioni

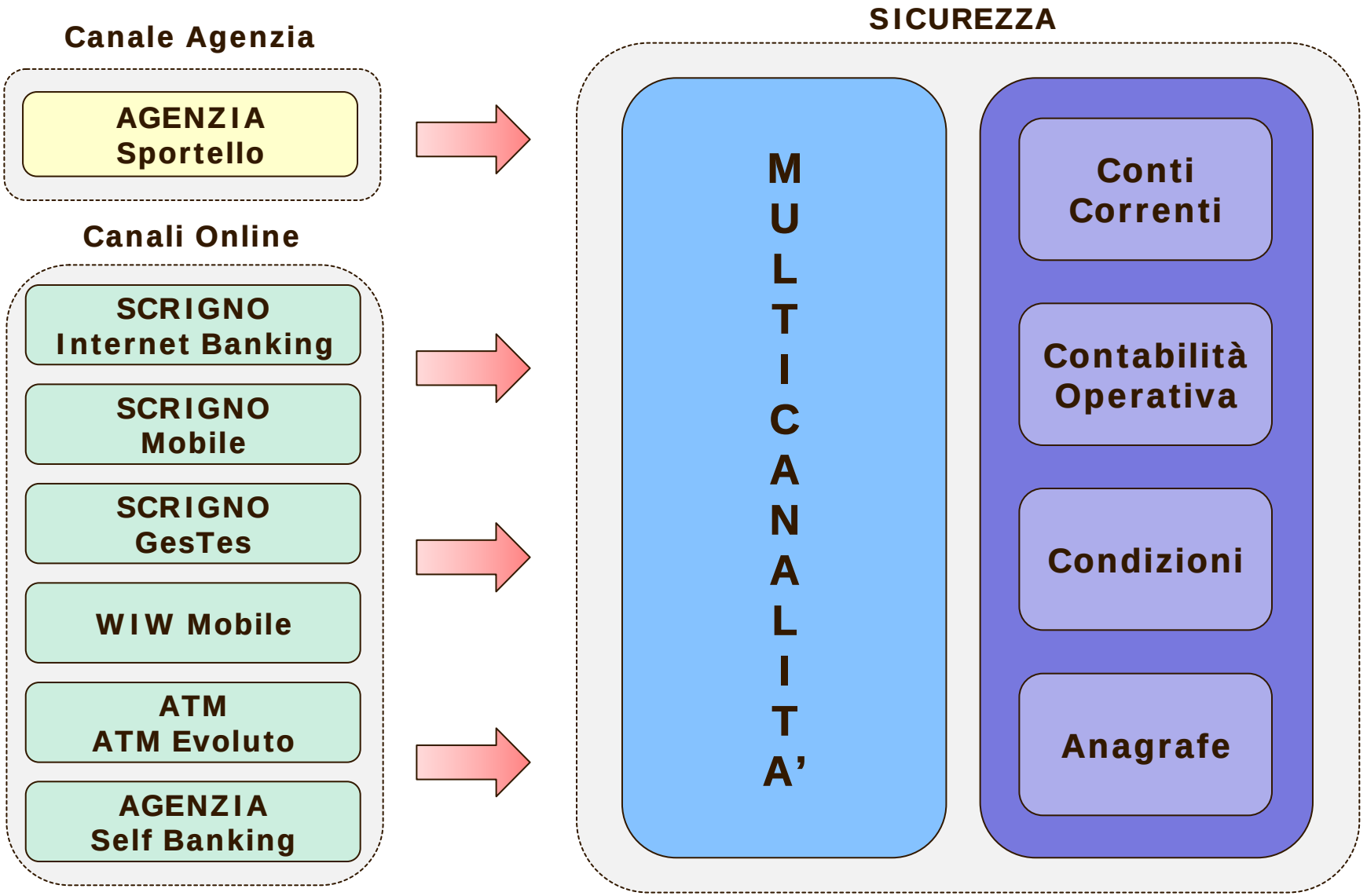
Obiettivi	Azioni
1. Contenere / Ridurre i costi mantenendo i livelli di servizio	**a) Allocare correttamente le risorse sui servizi attraverso l'analisi di indicatori economici** **b) Migliorare i processi interni di erogazione dei servizi** **c) Gestire al meglio l'acquisizione / gestione delle risorse**
2. Ampliare / innovare i servizi offerti in allineamento con il business	**a) Selezionare le evoluzioni in modo allineato con il piano industriale della banca** **b) Gestire correttamente la scelta degli investimenti** **c) Velocizzare la realizzazione e la modifica dei servizi erogati a fronte delle richieste utente**
3. Gestire complessità, rischi e obsolescenza tecnologica	**a) Impedire che vincoli tecnologici e / o la gestione dei rischi tecnologici porti all'obsolescenza** **b) Impedire che l'obsolescenza divenga un freno all'evoluzione**

Il modello di **Performance Management** di una Direzione IT deve mettere in condizione di **verificare** attraverso **indicatori di sintesi** il **grado di attuazione delle azioni** e il **raggiungimento degli obiettivi**

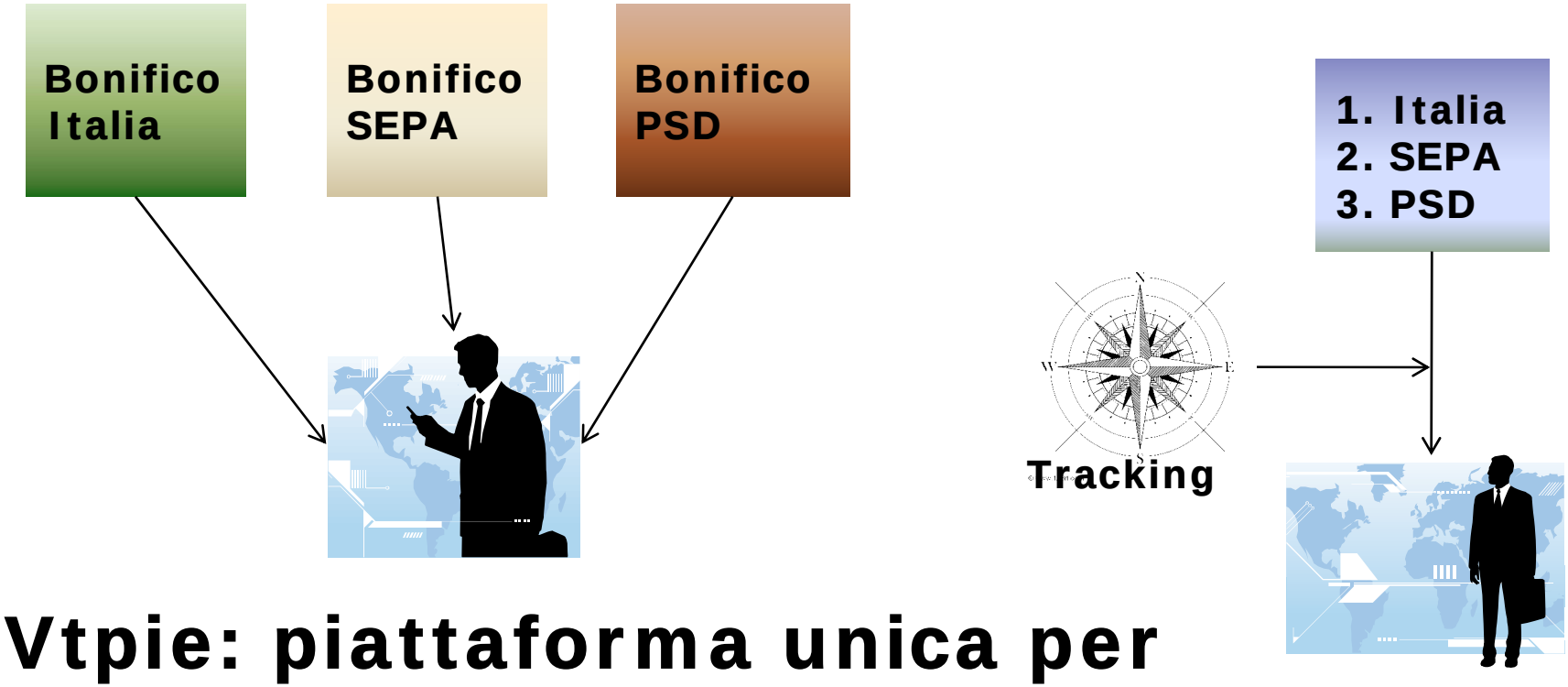
Nel concreto…

Due esempi di progetti integrati
- **Allineati al business, con Budget precisi e attese di ritorno, nonché conformi alle normative**

La multicanalità nella visione BPS



SEPA - PSD



Vtpie: piattaforma unica per i bonifici dipartimentale accedibile in multicanalità

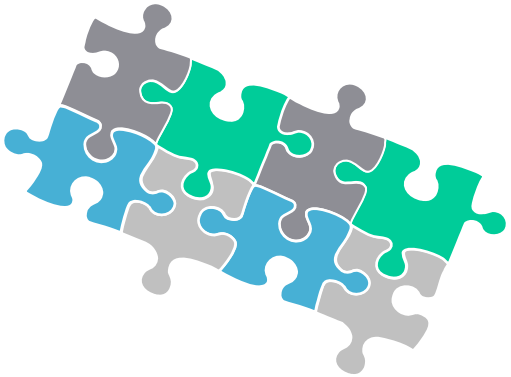
Altro ancora…

- ✓ **Cruscotti monitoraggio rischi, incidenti, funzionalità**
- ✓ **ITIL**
- ✓ **SOA con prudenza**
- ✓ **Virtualizzazione**
- ✓ **Ambienti di test e di sviluppo (duplicati e innovativi)**
- ✓ **Gestione delle informazioni**
- ✓ **Server farm cogestione**

Compliance e Sicurezza

Visione e attuazione

Quali azioni per contenere i rischi informatici?



- Incrementare ed automatizzare i livelli di controllo
- Governare la crescente complessità delle informazioni raccolte attraverso diversi sistemi di presidio della sicurezza e adottare meccanismi di correlazione tra eventi
- Mantenere un confronto costante con le informazioni di sistema
- Ridurre i tempi necessari per intercettare azioni anomale per poter intervenire con la tempestività necessaria
- Supportare chi fa la gestione della Sicurezza

In linea con le vigenti normative sulla sicurezza informatica, con le indicazioni di ABI ed in accordo con lo standard di sicurezza ISO 27001 adottato dall'azienda

Sicurezza multicanale: la ISO27001 come risposta strutturata

Il valore di una scelta strategica:
l'adozione di standard come una opportunità di miglioramento.

- 2004: Prime attività di gap analisys
- Fine 2005: Certificazione BS7799 del servizio SCRIGNO*Internet Banking*
- Fine 2006: Adeguamento alla ISO27001
- Inizio 2007: Estensione dell'ambito di certificazione a tutti i servizi del portale SCRIGNO*bps*
- Inizio 2008: Estensione dell'ambito alla gestione della Server Farm
- **2009/2010: Estensione dell'ambito al nuovo sportello**

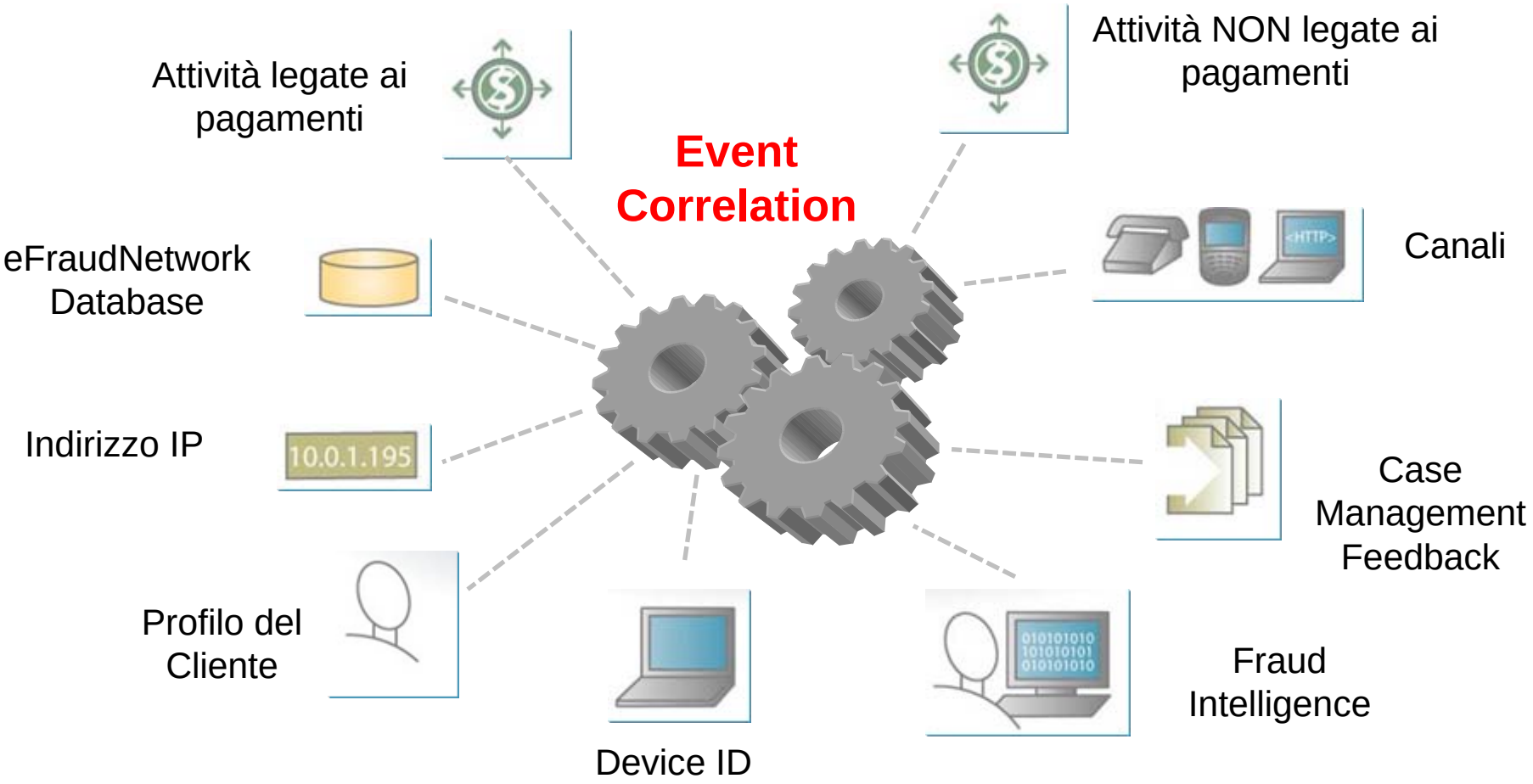
Sicurezza multicanale in sintesi

I rischi operativi, di frode interna o esterna di dati o di valori, di immagine o reputazione, rivenienti dalle vulnerabilità connesse all'ambito informatico sono in costante aumento ed evoluzione.

Il relativo presidio non può essere validamente affrontato con controlli di tipo "tradizionale".

Servono soluzioni informatiche, nuove competenze e rivisti modelli di relazione e collaborazione.

Sicurezza multicanale: *event correlation* come strumento di presidio



Impatti organizzativi e sul sistema dei controlli interni:

1. **Identificazione dei rischi informatici emergenti connessi ad azioni fraudolente interne ed esterne**
2. **Aggiornamento nel continuo della mappa dei rischi della specie, stante l'evoluzione della tecnologia e del crimeware**

Stretta collaborazione tra Internal Auditor e

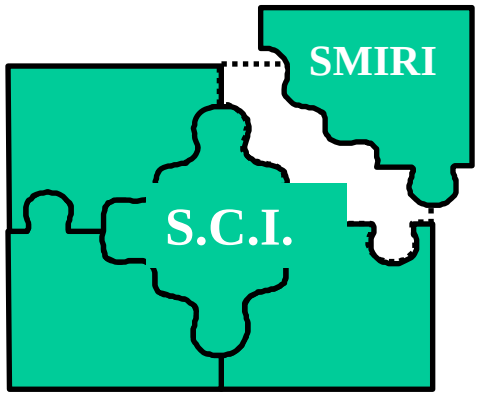
Organizzazione IT – Sicurezza IT – Risk Management

S.M.I.R.I.

Sistema di Monitoraggio ad Indicatori di Rischio Integrati

- Una soluzione innovativa di monitoraggio e controllo flessibile e a misura dell'utente; un elemento fondamentale nell'ambito del mosaico del sistema dei controlli interni

- S.M.I.R.I. consente la gestione efficiente ed efficace di eventi anomali o di situazioni di errore di determinate aree operative aziendali attraverso la definizione e la generazione di indicatori di rischio specifici e la possibilità di realizzare report volti a rappresentare le risultanze, in ottica di controllo a distanza, secondo le diverse "viste" aziendali



S.M.I.R.I.

- L'individuazione di andamenti anomali presuppone l'esame e l'aggregazione del patrimonio informativo aziendale in ottica ispettiva, al fine di evidenziare possibili scostamenti dal budget, da performance o devianze rispetto a benchmark

- L'individuazione di violazioni delle procedure e della regolamentazione richiede l'estrazione immediata di eventuali possibili irregolarità o alert, da indagare

- La valutazione della funzionalità del complessivo sistema dei controlli interni può essere utilmente valutata riferendola ai processi di lavoro, avuta presente la situazione aziendale e l'evoluzione degli stessi, anche a seguito della revisione dei controlli di linea, di interventi organizzativi e di modifiche procedurali, ed è condotta:
  - nel continuo - procedura elettronica, cui seguono interventi telefonici o richiami scritti;
  - in via periodica - estrazione ed elaborazione di dati aggregati per periodo
  - per eccezioni - individuazione di anomalie o segnali di alert anche attraverso verifiche in loco - meglio se guidate

Identitel

Consente di autenticare le operazioni dispositive di conto corrente richieste via Internet (bonifici, giroconti, ricariche cellulari, F24) mediante l'uso del telefonino. Il funzionamento è estremamente semplice: una volta richiesta l'operazione di conto corrente online il cliente visualizzerà sul proprio computer un pin e un numero verde - generato dinamicamente - da chiamare dal proprio telefonino precedentemente abilitato al servizio. Solo dopo aver rilevato la chiamata del cliente dal numero abilitato e dopo aver inserito il pin il sistema permetterà l'effettivo completamento dell'operazione richiesta.

Vantaggi per i clienti:

•comodità nell'utilizzo in quanto non sono necessari strumenti aggiuntivi e ingombranti forniti dalla banca

•facilità di accesso allo strumento di sicurezza, considerato che praticamente tutti gli utenti dispongono di un telefonino

•nessun costo telefonico per il cliente poiché la chiamata di autenticazione viene effettuata verso un numero verde

•nessuna password dispositiva da ricordare/da digitare

•elevato livello di sicurezza poiché l'autenticazione finale avviene tramite un canale di comunicazione (la rete di telefonia mobile) distinto da Internet

PHIL, il pesce “anti-phishing”

PHIL, il pesce “anti-phishing”

Si tratta di un accattivante gioco on line che consente di apprendere, divertendosi, come riconoscere a prima vista gli indirizzi Internet da cui diffidare per proteggersi dal fenomeno conosciuto come phishing.

Il gioco educativo anti-phishing va oltre la spiegazione astratta del concetto di phishing.

Combina l'innalzamento della consapevolezza a un'esperienza in prima persona al fine di creare potenti occasioni formative che si traducono in una maggior protezione.

Al cambiamento siamo tutti favorevoli

purchè…

a dover cambiare siano gli altri.