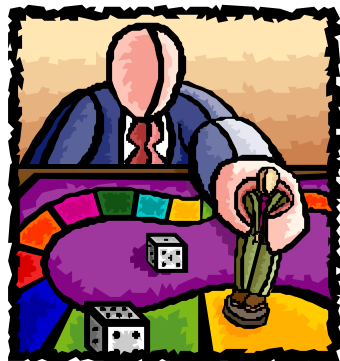




Centrale d'Allarme Interbancaria (CAI) e ISO/IEC 17799: un metodo di verifica

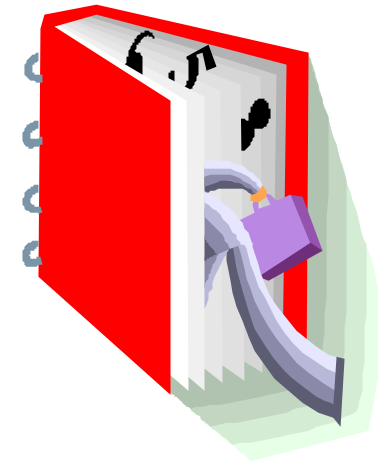
Roma, 25 novembre 2003



Agatino Grillo, CISA, CISSP
EUROS Consulting

Sommario

- CAI - Centrale d'Allarme Interbancaria
- Sicurezza e CAI: il contesto di riferimento
- Approccio Euros  SPOT
- Link e riferimenti



Parte prima

CAI - Centrale d'Allarme Interbancaria



CAI – Centrale d'Allarme Interbancaria - introduzione

4/50

- Il Decreto Legislativo 30 dicembre 1999, n. 507 ha riformato la disciplina sanzionatoria relativa agli assegni bancari e postali emessi senza autorizzazione o senza provvista presso la Banca d'Italia.
- L'obiettivo della riforma è stato la costruzione di un sistema sanzionatorio, *alternativo a quello penale*, la cui efficacia si basa sulla disponibilità delle informazioni e sull'applicazione di misure di carattere interdittivo nei confronti degli autori di comportamenti illeciti.

CAI – Centrale d'Allarme Interbancaria^{5/50} - Introduzione

- È stato creato dunque un archivio informatizzato, denominato Centrale d'Allarme Interbancaria (C.A.I.) che si compone di una sezione centrale presso la Banca d'Italia e di sezioni remote presso le banche, gli uffici postali, gli intermediari vigilati emittenti carte di pagamento e le prefetture;
- l'archivio non contiene solo le informazioni sui soggetti revocati all'emissione di assegni, ma anche un insieme di altre informazioni utili a verificare la corretta utilizzazione degli strumenti di pagamento censiti.

CAI – Centrale d'Allarme Interbancaria – ^{6/50}

Gestione dell'archivio

- Sezione centrale
 - L'Ente responsabile, oltre che al rispetto delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza dell'art. 15 L. 675 è tenuto ad adottare ogni ulteriore misura necessaria per la sicurezza nel trattamento dei dati e per l'affidabilità, l'efficienza e la continuità del servizio.

CAI – Centrale d'Allarme Interbancaria – ^{7/50}

Gestione dell'archivio

- Sezioni remote
 - Gli Enti segnalanti privati sono tenuti a garantire che le sezioni dell'archivio che risiedono presso di essi presentino un adeguato livello di efficienza e di sicurezza, rispondendo del rispetto delle vigenti disposizioni in materia di trattamento dei dati.
 - Gli Enti segnalanti privati, in base alla propria struttura tecnica e organizzativa, adottano processi di gestione della sicurezza del sistema informativo coerenti con l'esigenza di garantire la funzionalità e l'efficienza dell'archivio, tenendo anche conto di quanto indicato nell'allegato al Regolamento di Banca d'Italia "Sicurezza del sistema informativo" e di ulteriori indicazioni di Banca d'Italia.

CAI – Centrale d'Allarme Interbancaria – ^{8/50}

Controllo accessi

- Modalità di accesso ai dati
 - ogni consultazione effettuata sui dati dell'archivio deve essere registrata (persona fisica, oggetto, data) e gestita in modo da non alterare i dati;
 - il soggetto interessato accede ai dati contenuti nell'archivio tramite gli enti segnalanti privati;
 - è possibile accedere ai dati non nominativi contenuti nell'archivio presso gli enti segnalanti privati

CAI – Centrale d'Allarme Interbancaria – ^{9/50}

Controllo accessi

➤ Controlli

- Ente Responsabile - La Banca d'Italia controlla che la gestione dell'archivio sia improntato ai principi di affidabilità ed efficienza e sia conforme alla normativa di riferimento.
- Enti segnalanti privati - La Banca d'Italia nell'esercizio delle funzioni di vigilanza verifica il rispetto delle disposizioni del regolamento e delle altre normative di riferimento.

CAI – Centrale d'Allarme Interbancaria – requisiti di sicurezza

10/50

- Gli enti privati segnalanti devono adottare processi di gestione della sicurezza del sistema informativo CAI (...) volte a definire adeguatamente e ad aggiornare periodicamente le politiche per la sicurezza del sistema.

CAI – Centrale d'Allarme Interbancaria – requisiti di sicurezza

11/50

- Ogni ente segnalante privato:
 - oltre ad assicurare il rispetto delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza in applicazione alla L. 675/96,
 - deve **definire e governare un processo per la gestione della sicurezza** del sistema informativo dell'archivio CAI.

CAI – Centrale d'Allarme Interbancaria – governo della sicurezza

12/50

- L'ente segnalante deve intraprendere le seguenti azioni:

1. Definire le **politiche per la sicurezza** del sistema informativa della CAI;

2. Definire i **confini del sistema informativo** della CAI in termini di struttura organizzativa, collocazione fisica, risorse e tecnologie;

3. **Analizzare** adeguatamente i **rischi** in modo da identificare le minacce alle risorse, le vulnerabilità e gli impatti sull'ente segnalante privato e quindi determinare il livello di rischio globale;

4. **Selezionare** dall'elenco previsto (realizzato utilizzando le specifiche ISO/IEC 17799: 2000 come riferimento) i **controlli** ritenuti appropriati. Tali controlli non sono esaustivi e ulteriori controlli possono essere individuati.

5. **Redigere un documento** che spieghi le ragioni che hanno portato alla scelta di ogni singolo controllo selezionato, in termini di risorse da proteggere a fronte di minacce e vulnerabilità. In questo documento devono essere indicate le ragioni che hanno indotto all'eventuale esclusione di alcuni controlli.

CAI – Centrale d'Allarme Interbancaria - Processi

13/50

- Revisioni e modifiche
 - I passi descritti devono essere riesaminati periodicamente oppure in occasione di eventi significativi.
 - La validità delle procedure adottate deve essere verificata per valutarne la coerenza con le politiche aziendali di sicurezza e l'adeguatezza tecnica.
- Procedure
 - Le procedure devono essere documentate in modo che risultino chiaramente le responsabilità e i principali ruoli delle funzioni e dei soggetti coinvolti.
 -
- Auditing
 - Il sistema informativo della CAI deve essere assoggettato a procedure di auditing.

CAI – Centrale d'Allarme Interbancaria –

Gestione della documentazione

14/50

- I documenti sopra definiti devono essere:
 - prontamente disponibili;
 - periodicamente rivisti, coerentemente con le politiche di sicurezza e immediatamente sostituiti in caso di obsolescenza;
 - gestiti con una procedura di controllo delle versioni.
 - L'ente segnalante privato è tenuto a conservare le evidenze relative all'applicazione dei controlli che dimostrino la conformità con i requisiti di sicurezza della CAI (per esempio: tracce di audit, autorizzazioni all'accesso logico e/o fisico, ecc.)
 - Tali evidenze possono essere in formato cartaceo e/o elettronico, memorizzate e gestite in modo che siano prontamente disponibili, adeguatamente protette, leggibili, identificabili e tracciabili rispetto alle attività a cui si riferiscono.

CAI – Centrale d'Allarme Interbancaria - 15/50

L'Elenco dei controlli suggeriti

- L'elenco proposto rappresenta un insieme minimo tratto dalle specifiche ISO/IEC 17799: 2000.
- Essi non garantiscono la sicurezza della CAI, che dipende fortemente dall'ambiente tecnico e organizzativo in cui la procedura è inserita, bensì forniscono solo un insieme minimo di linee guida.

CAI – Centrale d'Allarme Interbancaria - 16/50

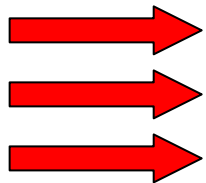
L'Elenco dei controlli suggeriti

- In particolare l'ente deve attivare opportuni presidi finalizzati ad assicurare:
 - un'efficace e sicura gestione operativa dei flussi informativi tra strutture centrali e periferiche dell'ente stesso;
 - una chiara definizione e separazione di ruoli e responsabilità tra gestori delle risorse informative e utilizzatori delle stesse
- Con riferimento alle sezioni remote dell'archivio, ogni ente segnalante privato è tenuto a verificare che ogni flusso informativo ricevuto dall'ente responsabile sia perfettamente congruente con le segnalazioni inviate dallo stesso ente segnalante.
- In caso di incongruenza dei dati l'ente segnalante è tenuto ad attivarsi tempestivamente presso l'ente responsabile

CAI – Centrale d'Allarme Interbancaria^{17/50}

L'Elenco dei controlli suggeriti

- Security policy (cap. 3)
- Organizational security (cap. 4)
- Asset classification and control (cap. 5)
- Personnel security (cap. 6)
- Physical and environmental security (cap. 7)
- **Communications and operations management (cap. 8)**
- **Access control (cap. 9)**
- **Systems development and maintenance (cap. 10)**
- Business Continuity Management (cap. 11)
- Compliance (cap. 12)



CAI – Centrale d'Allarme Interbancaria - 18/50

L'Elenco dei controlli suggeriti

- 8.1. Procedure operative e responsabilità
- 8.5 Gestione della rete
- 8.6 Gestione e sicurezza dei supporti di memorizzazione

- 9.1 Requisiti aziendali per l'accesso al sistema
- 9.2. Gestione dell'accesso degli utenti;
- 9.3 Responsabilità dell'utente;
- 9.5 Controllo degli accessi al sistema operativo;
- 9.6 Controllo dell'accesso alle applicazioni;
- 9.7. Monitoraggio dell'accesso e dell'uso del sistema;

- 10.2 Sicurezza delle applicazioni;
- 10.5 Sicurezza dei processi di sviluppo e supporto;

Parte seconda

Sicurezza e CAI: il contesto di riferimento



Il contesto – le banche, orientamenti della Vigilanza

- I sistemi informativi devono garantire elevati livelli di sicurezza;
- devono essere individuati e documentati adeguati presidi volti a garantire la sicurezza fisica e logica dell'hardware e del software, comprendenti:
 - procedure di back up dei dati e di *disaster recovery*;
 - individuazione dei soggetti autorizzati ad accedere ai sistemi e relative abilitazioni;
 - possibilità di risalire agli autori degli inserimenti o delle modifiche dei dati.

Fonte: Istruzioni di Vigilanza per gli Intermediari Finanziari iscritti nell'«Elenco Speciale»

Circolare n. 216 del 5 agosto 1996 - 6° aggiornamento del 15 ottobre 2002

Il contesto – le banche, orientamenti della Vigilanza

- L'alta direzione (al cui vertice è posto di norma il Direttore generale) deve:
 - garantire un'efficace gestione dell'operatività aziendale e dei rischi cui l'intermediario si espone;
 - individuare e valutare i fattori di **rischio**;
 - verificare la funzionalità, l'efficacia e l'efficienza del sistema dei controlli interni;
 - definire i compiti delle strutture dedicate alle funzioni di controllo;
 - definire i flussi informativi necessari a garantire al CdA piena conoscenza dei fatti aziendali;

Fonte: Istruzioni di Vigilanza per gli Intermediari Finanziari iscritti nell'«Elenco Speciale»

Circolare n. 216 del 5 agosto 1996 - 6° aggiornamento del 15 ottobre 2002

Il contesto – le banche, orientamenti della Vigilanza

- In linea con gli indirizzi emersi in ambito internazionale a seguito degli eventi dell'11 settembre 2001, la Banca d'Italia, ha avviato un complesso di iniziative volte a verificare:
 - il livello di preparazione del sistema finanziario italiano a fronteggiare eventi catastrofici,
 - a sanare le situazioni ritenute non adeguate,
 - a elevare il grado di sicurezza operativa dei principali intermediari finanziari, delle infrastrutture dei mercati e del sistema dei pagamenti.

Fonte: Banca D'Italia, "Assemblea Generale Ordinaria Dei Partecipanti", maggio 2003

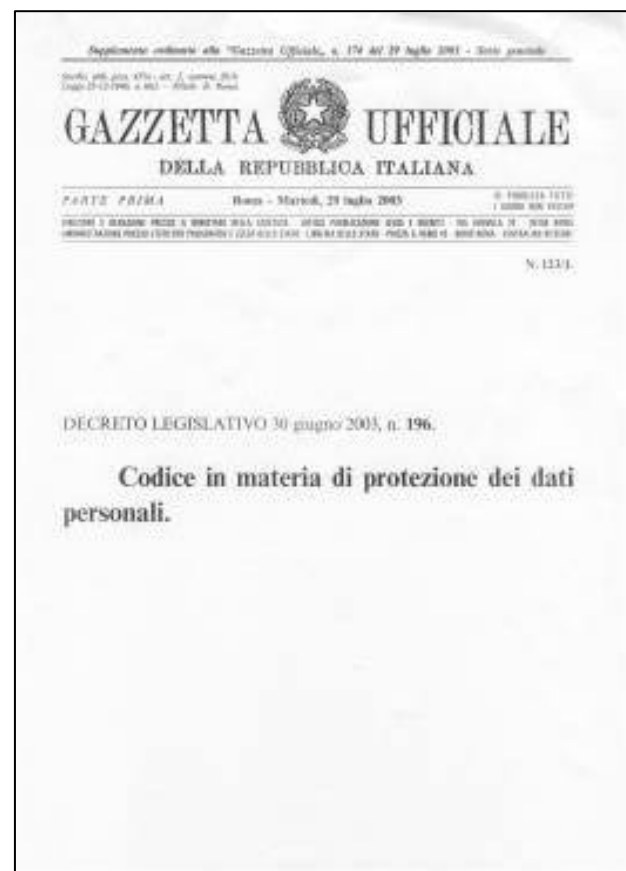
Il contesto - difesa delle infrastrutture critiche

- L'instabilità internazionale determinata dagli eventi dell'11 settembre 2001 ha prodotto una fortissima "domanda di sicurezza";
- uno dei risultati è stato di spostare il focus anche sulla difesa delle infrastrutture critiche (trasporti, comunicazioni, *finance*) ed anche di far lavorare insieme, su questo tema, le istituzioni pubbliche e governative con le organizzazioni private.



Codice in materia di dati personali – vigore

- Codice protezione dati personali
 - Il Decreto Legislativo 30 giugno 2003 n° 196 riunisce in unico ambito la Legge 675/1996 e gli altri Decreti successivi, e completa l'armonizzazione con le Direttive UE e i codici deontologici che si sono succeduti in questi anni;
 - Il codice entra in vigore il 1° gennaio 2004.



Codice in materia di dati personali – novità

- Il “Codice” introduce novità rilevanti in termini di misure di sicurezza da adottare:
 - in primis si parla di “sicurezza dei dati e dei sistemi” ponendo in tal modo l’attenzione non solo sulla protezione delle informazioni ma sul concetto più ampio di sistema informatico attraverso il quale viene effettuato il trattamento;
 - sono state, inoltre, inserite nuove misure di sicurezza quali quelle relative alle copie di sicurezza dei dati (*back-up*) e alla continuità del servizio (*business continuity*);
 - sono state aggiunte, infine, nuove norme adatte a tutelare la sicurezza dei dati dalle nuove criticità che nascono dalla interconnessione dei sistemi quali la protezione contro l’accesso abusivo e l’aggiornamento periodici dei programmi (*patch*).

Codice in materia di dati personali – rischi informatici

- La progettazione, realizzazione e gestione delle misure di sicurezza richiede l'adozione di un piano globale di sicurezza che deve scaturire, a sua volta, da una valutazione attenta ed obiettiva dei **rischi informatici**;
- *il titolare che tratta dati personali in modo lecito e sicuro deve organizzare la loro protezione non solo con le misure di sicurezza minime e più ampie, ma anche governando tutti gli altri processi che, sinergicamente, accompagnano il ciclo di vita dei dati.*

Codice in materia di dati personali –

Art. 31: Obblighi di sicurezza

- I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, **i rischi** di:
 - distruzione o perdita, anche accidentale, dei dati stessi;
 - di accesso non autorizzato;
 - di trattamento non consentito;
 - di trattamento non conforme alle finalità della raccolta.

Codice in materia di dati personali – misure minime

- il controllo dell'accesso ai dati è garantito da:
 - autenticazione informatica;
 - credenziali di autenticazione;
 - sistema di autorizzazione.

- Altre nuove misure:
 - l'adozione di procedure per la generazione e la custodia di copie di sicurezza dei dati;
 - il ripristino della disponibilità dei dati e dei sistemi;
 - la protezione dei dati sensibili o giudiziari contro l'accesso abusivo;
 - gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

Codice in materia di dati personali – trattamento che presenta rischi specifici

➤ Art.17:

- I dati diversi da quelli sensibili e giudiziari possono presentare particolari **rischi specifici** per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato;
- i rischi sono correlati alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare;
- (tali dati) possono essere trattati nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti dal Garante in applicazione dei principi sanciti dal Codice e nell'ambito di una verifica preliminare all'inizio del trattamento.

Parte terza

Approccio Euros



Soluzione Euros per CAI –

Euros Consulting

31/50



- Euros Consulting è nata nel 1998 dalla fusione di Cefor e Istinform, primarie società di formazione e consulenza, con l'obiettivo di offrire, in primis al mercato delle Banche, un servizio integrato e una solida partnership per lo sviluppo
- Il capitale azionario è suddiviso fra:
 - associazioni di categoria (abi, assbank, asspopol bank, federcasse)
 - circa 90 aziende bancarie



Soluzione Euros per CAI –

Euros Consulting

32/50

EUROS Consulting

SPOT

**Business Unit
SICUREZZA E CONTROLLI**

ICT auditing

E-security

Controlli per attività
di Internal auditing

Controlli per attività
antiriciclaggio e *GIANOS*®©

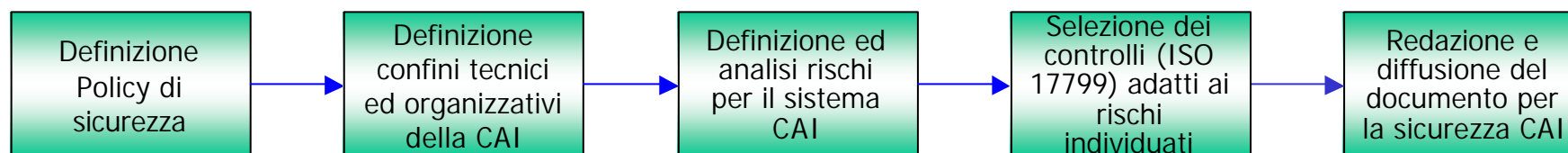
SecurityNet® e
Club sul Computer Crime®



Soluzione Euros per CAI –

Gli obblighi

33/50



Soluzione Euros per CAI – il metodo

- Prima fase: assessment delle misure di sicurezza CAI
 - Illustrazione metodo e definizione dei confini dell'intervento
 - Analisi del modello di sicurezza esistente
 - Supporto all'analisi del rischio (IT Rapid Risk Assessment - *metodologia Euros Consulting*)
 - Rilevazione dei processi di sicurezza e selezione dei controlli
 - collegamento con "impianto" di tutela dei dati personali
 - Individuazione degli adeguamenti
 - Verifica degli impatti
 - Aggiornamento dei regolamenti aziendali
 - Stesura dei documenti necessari agli adempimenti normativi per la sicurezza della CAI

Soluzione Euros per CAI – il metodo

35/50

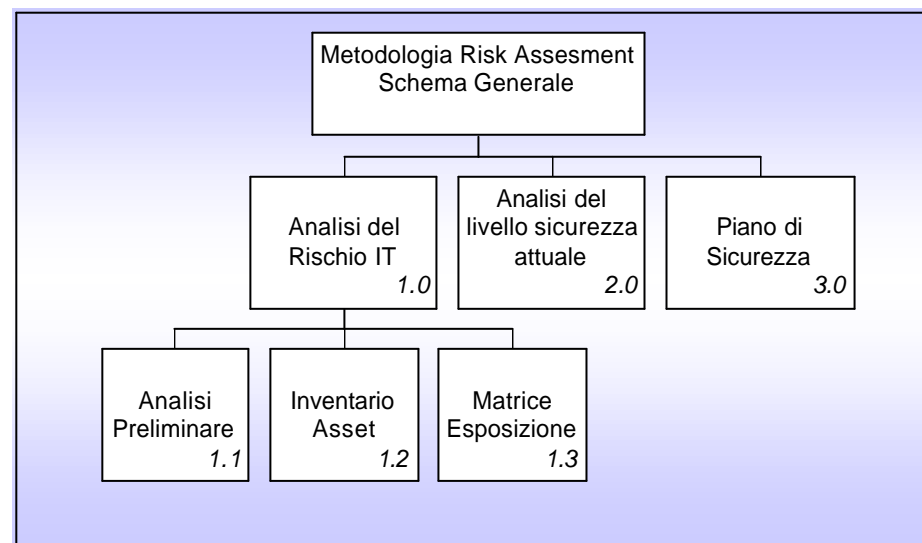
- Seconda fase: sistema di documentazione per la sicurezza CAI
 - Completamento degli adeguamenti individuati (normative)
 - Sviluppo sistema di documentazione della sicurezza CAI

Soluzione Euros per CAI –

l'analisi dei rischi

36/50

- Le tipologie di rischio previste sono:
 - Riservatezza
 - Integrità
 - Continuità del servizio (disponibilità)



Soluzione Euros per CAI –

l'analisi dei rischi

- Produzione della Matrice di esposizione al rischio potenziale. Nell'applicazione proposta la matrice riporta:
 - in ciascuna riga, l'indicazione delle classi di beni;
 - in ciascuna colonna l'indicazione delle classi di minacce, così come tratta dal catalogo;
 - negli incroci il valore "X" quando per tale combinazione è possibile il verificarsi dell'evento rischio al sistema informativo CAI e dunque esiste un rischio potenziale

Riservatezza

Inventario minacce										
	Accesso non autorizzato ai dati	Divulgazione non consentita dei dati	Accesso non autorizzato alle applicazioni	Virus, worm, codici ostili	Furto HW o delle infrastrutture	Inosservanza Privacy	Abuso e modifica privilegi	Intercettazione dati	Mascheramento identità	Furto dati ed informazioni
Inventario dei beni										
a) le informazioni:										
database e files di dati	x	x	x	x	x	x	x	x	x	x
documentazione di sistema										
manuali utente										
materiale di formazione										
procedure operative e di supporto										
piani di continuità										

Soluzione Euros per CAI – l'analisi dei rischi

38/50

Integrità

Inventario minacce Inventario dei beni	Modifica non autorizzate ai dati	Utilizzo abusivo applicazioni	Sviluppo, manutenzione errate	Errori negli applicativi	Virus, worm, codici ostili	Danneggiamento alle infrastrutture	Intrusioni	Frodi	Attacco Defacement sito	Incompatibilità del sistema	Inadeguatezza funzionale	Errore umano	Disastro	Introduzione SW dannoso
a) le informazioni:														
database e files di dati	x	x	x	x	x	x	x	x	x	x		x	x	x
documentazione di sistema													x	
manuali utente														
materiale di formazione														
procedure operative e di supporto			x		x	x	x	x	x	x		x	x	
piani di continuità														
soluzioni di emergenza														
archivi di dati	x					x	x	x				x	x	
b) il software:														
applicativo			x	x	x	x	x	x	x	x		x	x	x
di sistema			x		x	x	x	x	x			x	x	x
tools di sviluppo														
utilities														
c) gli impianti:														
sistemi di elaborazione (mainframe, monitor, pc, modem)						x	x					x	x	
apparati di comunicazione (routers, centralini telefonici, fax risponditori)						x	x					x	x	
supporti magnetici (nastri e dischi)						x	x					x	x	
altri impianti tecnici (alimentazione elettrica, impianti di condizionamento)						x	x					x	x	
mobili e arredi						x							x	
locali						x							x	
d) i servizi:														
servizi di elaborazione e di comunicazione					x		x		x	x	x	x	x	x
servizi generali (es. riscaldamento, illuminazione, energia elettrica, condizionamento)														

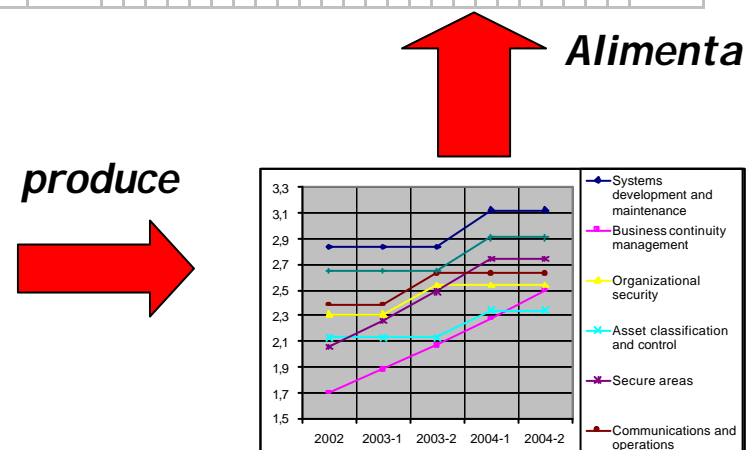
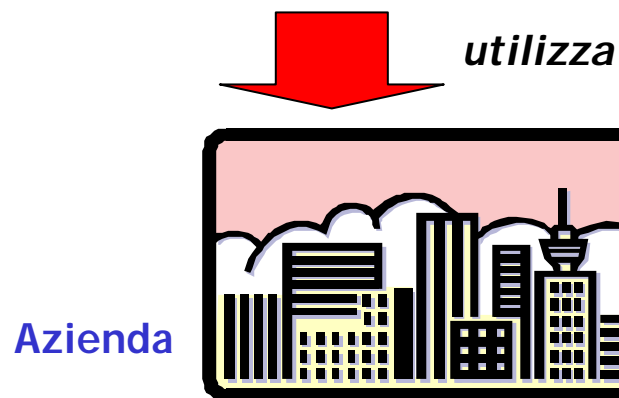
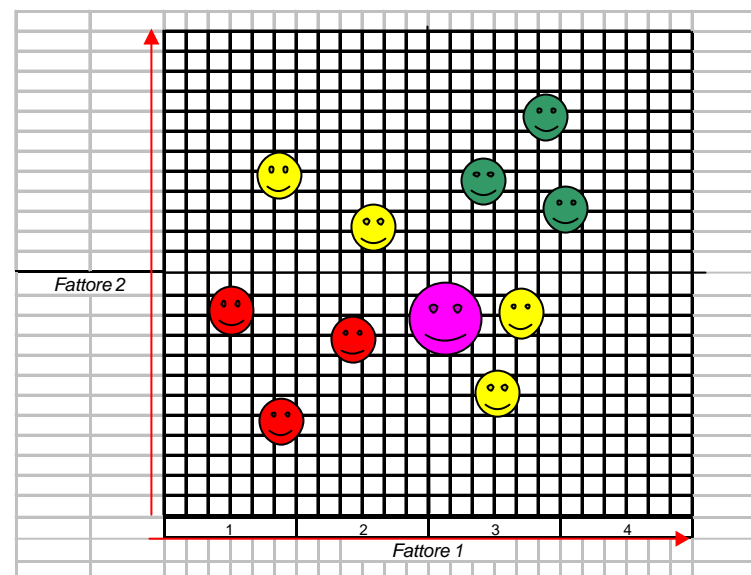
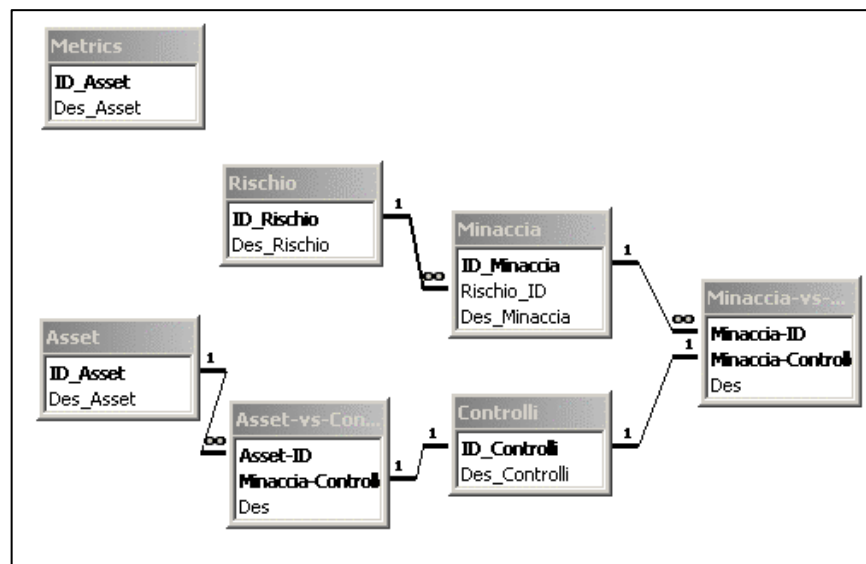
Soluzione Euros per CAI –

L'elenco dei controlli selezionati

39/50

RIF. ISO	SPECIFICA	SELEZIONE	OBIETTIVO E REQUISITI	SITUAZIONE RILEVATA
8.1	<i>Procedure operative e responsabilità</i>	SI	<i>Assicurare la corretta e sicura gestione dei sistemi di trattamento delle informazioni.</i>	<Descrizione dell'operatività rilevata> <Riferimento alla normativa interna esistente>
8.1.1	<i>Procedure operative documentate</i>	SI	<i>Documentare e tenere aggiornate le procedure operative identificate dalla politica di sicurezza, con istruzioni di dettaglio per l'esecuzione dei lavori che includano:</i>	<Descrizione dell'operatività rilevata> <Riferimento alla normativa interna esistente>
		SI	a) elaborazione e trattamento delle informazioni	<Descrizione dell'operatività rilevata> <Riferimento alla normativa interna esistente>
		SI	b) requisiti di schedulazione, interdipendenza con altri sottosistemi, inizio e termine di lavorazione	<Descrizione dell'operatività rilevata> <Riferimento alla normativa interna esistente>
9.2	<i>Gestione dell'accesso degli utenti</i>	SI	<i>Prevenire accessi non autorizzati alle informazioni</i>	<Descrizione dell'operatività rilevata> <Riferimento alla normativa interna esistente>
		NO	d) consegna all'utente di un'attestazione scritta dei suoi diritti di accesso	<Descrizione dell'operatività rilevata – a supporto della motivazione dell'esclusione del controllo> <Riferimento alla normativa interna esistente>

IT Rapid Risk Analysis - modello



IT Rapid Risk Assessment – Obiettivi

- Fornire uno strumento semplice ed assistito;
- individuare template pre-pesati per la definizione degli scenari;
- utilizzare un catalogo delle minacce standard e aggiornabile;
- proporre una metrica di misurazione dell'esposizione al rischio;
- permettere l'analisi e misurazione del rischio real-time.

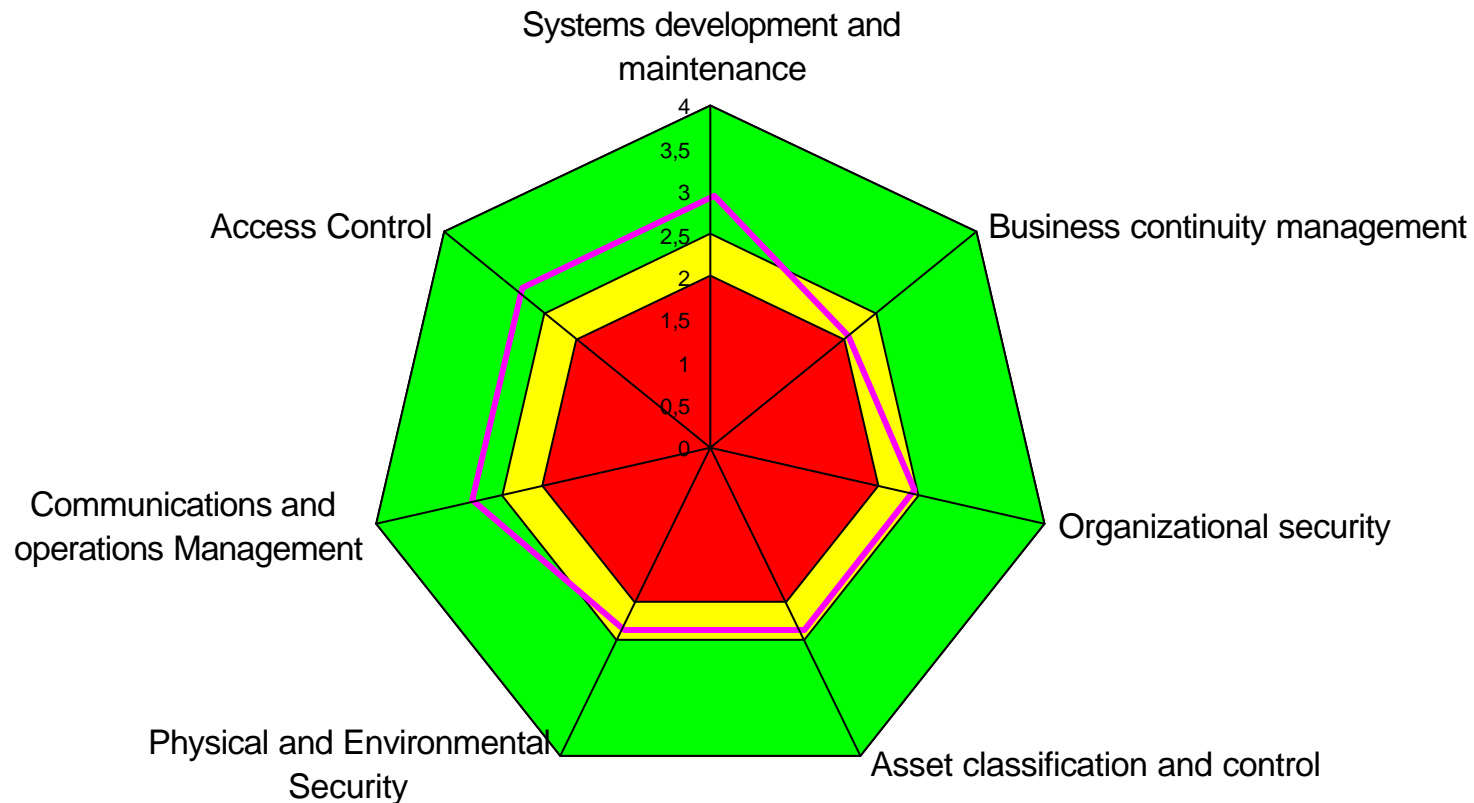
IT Rapid Risk Assessment – Obiettivi

- Calcolo del rischio:
 - Semplificato ed assistito;
 - Non richiede conoscenze specialistiche;
 - Facile da condividere.
- Modello temporale:
 - Attività “periodiche”;
 - Coordinate rispetto alle “normali” attività di gestione.
- Durata e risultati:
 - Le attività sono ridotte nel tempo;
 - La “fotografia” ottenuta è periodicamente “aggiornata”, tenendo conto dell’evoluzione dei processi e delle tecnologie in azienda.

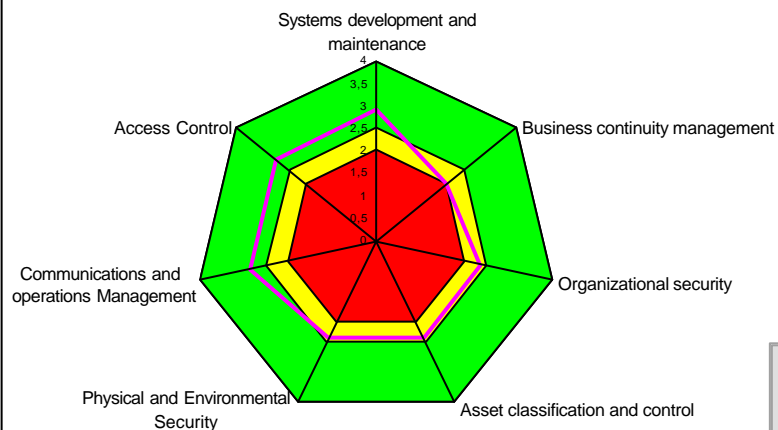
IT Rapid Risk Assessment – Strumento

- Risk Gap Analysis (As-Is To-Be):
 - Permette di confrontare la propria esposizione al rischio (As-Is) rispetto ad un modello di riferimento (To-Be);
- Tracking:
 - Permette di evidenziare l'evoluzione nel tempo della esposizione al rischio indicando e quantificando i miglioramenti;
- Simulazione:
 - Permette l'analisi What-If;
- Benchmarking:
 - Confronto della propria situazione rispetto ad aziende simili (centri consortili, clienti Euros...)

IT Rapid Risk Assessment – Gap analysis



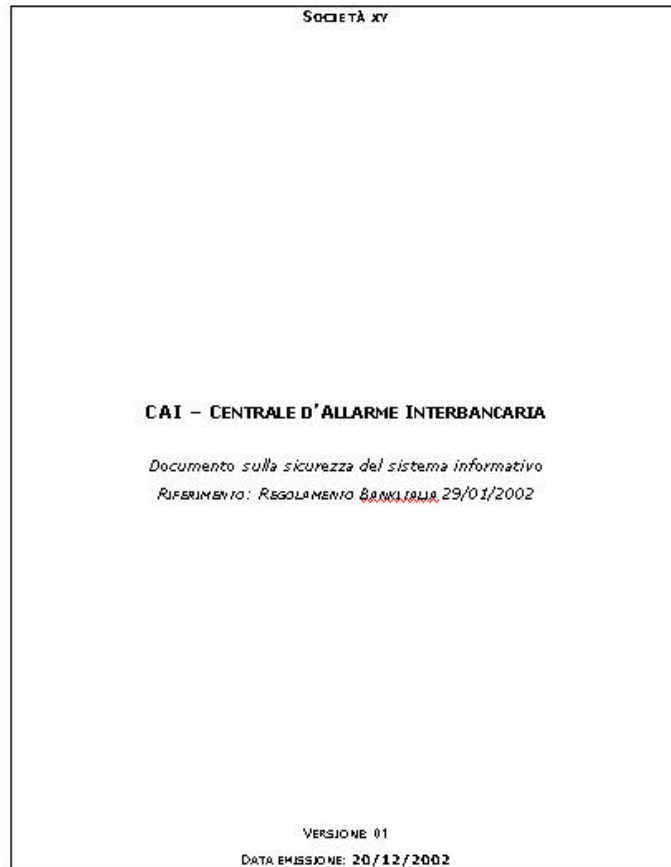
IT Rapid Risk Assessment – Gap analysis



Livello	Significato	Colore di riferimento	
<2	Situazione di rischio		<i>rosso</i>
≥ 2 e < 2,5	Situazione di attenzione		<i>giallo</i>
$\geq 2,5$	Situazione buona		<i>verde</i>

CAI – Centrale Allarme Interbancaria – ^{46/50}

Documenti finali



SOMMARIO

1	PREMESSA.....	4
2	POLITICHE PER LA SICUREZZA.....	5
3	CONFINI DEL SISTEMA INFORMATIVO.....	7
4	ANALISI DEI RISCHI.....	9
4.1	ANALISI DEL RISCHIO.....	9
4.2	RISCHI ANALIZZATI.....	9
4.3	MISURAZIONE DEL RISCHIO.....	10
4.4	L'APPROCCIO SEGUITO.....	10
5	CONTROLLI DI SICUREZZA.....	11
6	REVISIONI E VERIFICHE.....	12

CAI – Centrale Allarme Interbancaria – ^{47/50}

Documenti finali

SOMMARIO

1	PREMESSA.....	4
2	POLITICHE PER LA SICUREZZA.....	5
3	CONFINI DEL SISTEMA INFORMATIVO.....	7
4	ANALISI DEI RISCHI.....	9
4.1	ANALISI DEL RISCHIO.....	9
4.2	RISCHI ANALIZZATI.....	9
4.3	MISURAZIONE DEL RISCHIO.....	10
4.4	L'APPROCCIO SEGUITO.....	10
5	CONTROLLI DI SICUREZZA.....	
6	REVISIONI E VERIFICHE.....	

- Policy di Sicurezza;
- Confini del sistema informativo;
- Analisi dei rischi;
- Controlli di sicurezza
- Revisioni e Verifiche

CAI - norme

- Riforma della disciplina sanzionatoria degli assegni bancari e postali emessi senza provvista o senza autorizzazione (legge 25.6.1999, n. 205; decreto legislativo 30.12.1999, n. 507)
- Istituzione della Centrale d'Allarme Interbancaria "archivio informatizzato istituito presso la Banca d'Italia (legge n. 205 del 25/6/99 e art.36 del D.LGS. n. 507 del 30/12/99)"
- Razionalizzazione dei presidi a tutela della circolazione dell'assegno (libro bianco sull'assegno)

CAI – White Paper

- “Requisiti di sicurezza per la Centrale d’Allarme Interbancaria” in “Quaderni MASIE” disponibile in:
 - www.euros.it/securitynet
 - www.masieonline.org

Fine

Grazie per l'attenzione

a.grillo@euros.it

www.euros.it

www.agatinogrillo.it

www.masieonline.org