Ordine Ingegneri Pavia
Introduzione alla ISO/IEC 27001

Cesare Gallotti

Pavia, 7 ottobre 2015

Cesare Gallotti

Agenda

- Introduzione
  - il contesto della sicurezza delle informazioni;
  - la famiglia degli standard ISO/IEC 27000.
- La gestione del rischio relativo alla sicurezza delle informazioni;
- I controlli di sicurezza delle informazioni;
- Il ciclo PDCA;
- La certificazione ISO/IEC 27001.

Obiettivi dell'incontro

Sarano fornite risposte alle seguenti domande:

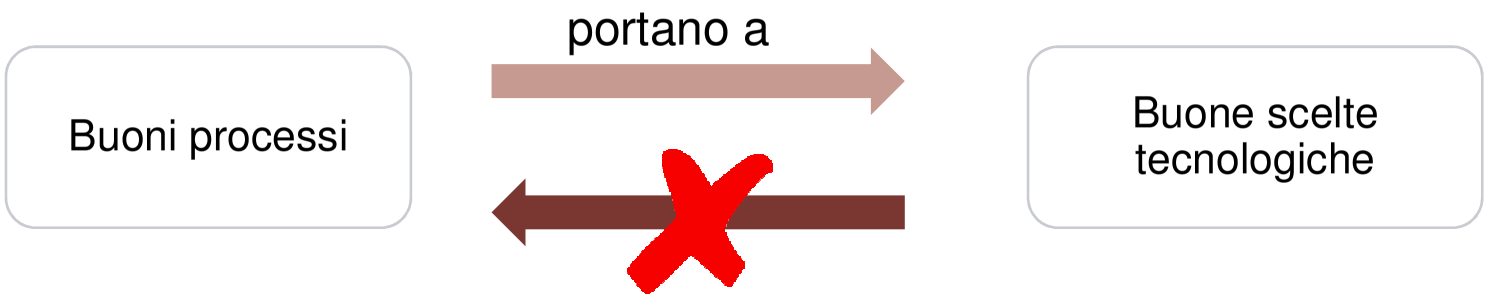
- Cos'è la sicurezza delle informazioni?
- Cos'è un sistema di gestione per la sicurezza delle informazioni?
- Quali sono le attività dei processi di valutazione e trattamento del rischio?
- Quali sono i controlli di sicurezza delle informazioni?
- Quali sono gli standard e le norme relative alla sicurezza delle informazioni?

Cesare Gallotti

- Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.
- Ha condotto numerosi progetti di consulenza per la pubblica amministrazione e per il settore privato. Opera, sia in Italia che all'estero, come Lead Auditor ISO/IEC 27001 e ISO 9001. Ha progettato ed erogato corsi di Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.
- Tra gli attestati di studio e i titoli professionali, si segnalano: le certificazioni CEPAS Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001:2008, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e ISO 22301 e il perfezionamento postlaurea in "Computer Forensics e investigazioni digitali".
- E' capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.
- Riferimenti:
  - Web: www.cesaregallotti.it
  - Blog: blog.cesaregallotti.it
  - Twitter: @cesaregallotti

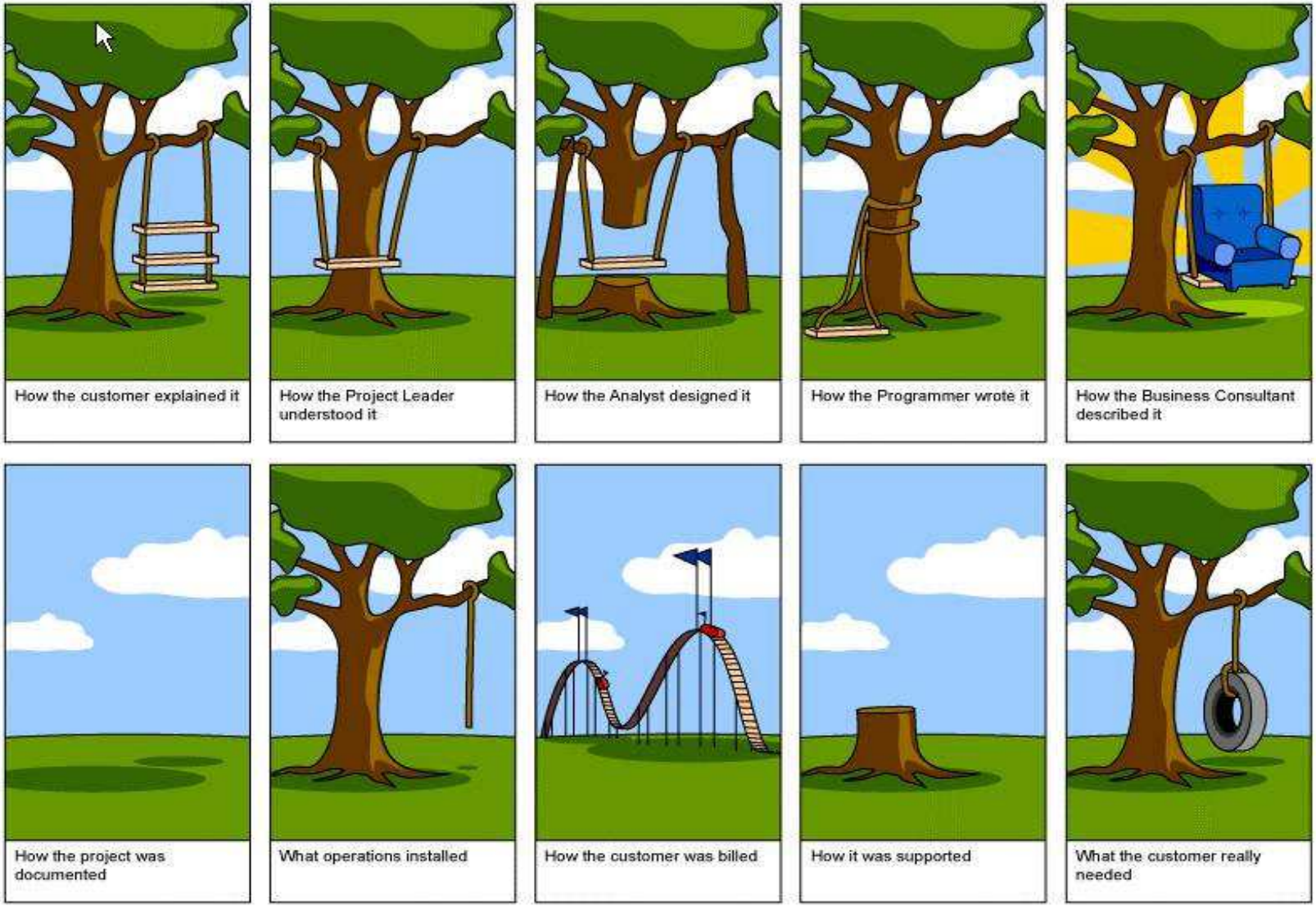
Sistema di gestione per la sicurezza delle informazioni

La sicurezza si basa sulla buona gestione



Processi per: scegliere, attuare, mantenere.

Processi per scegliere



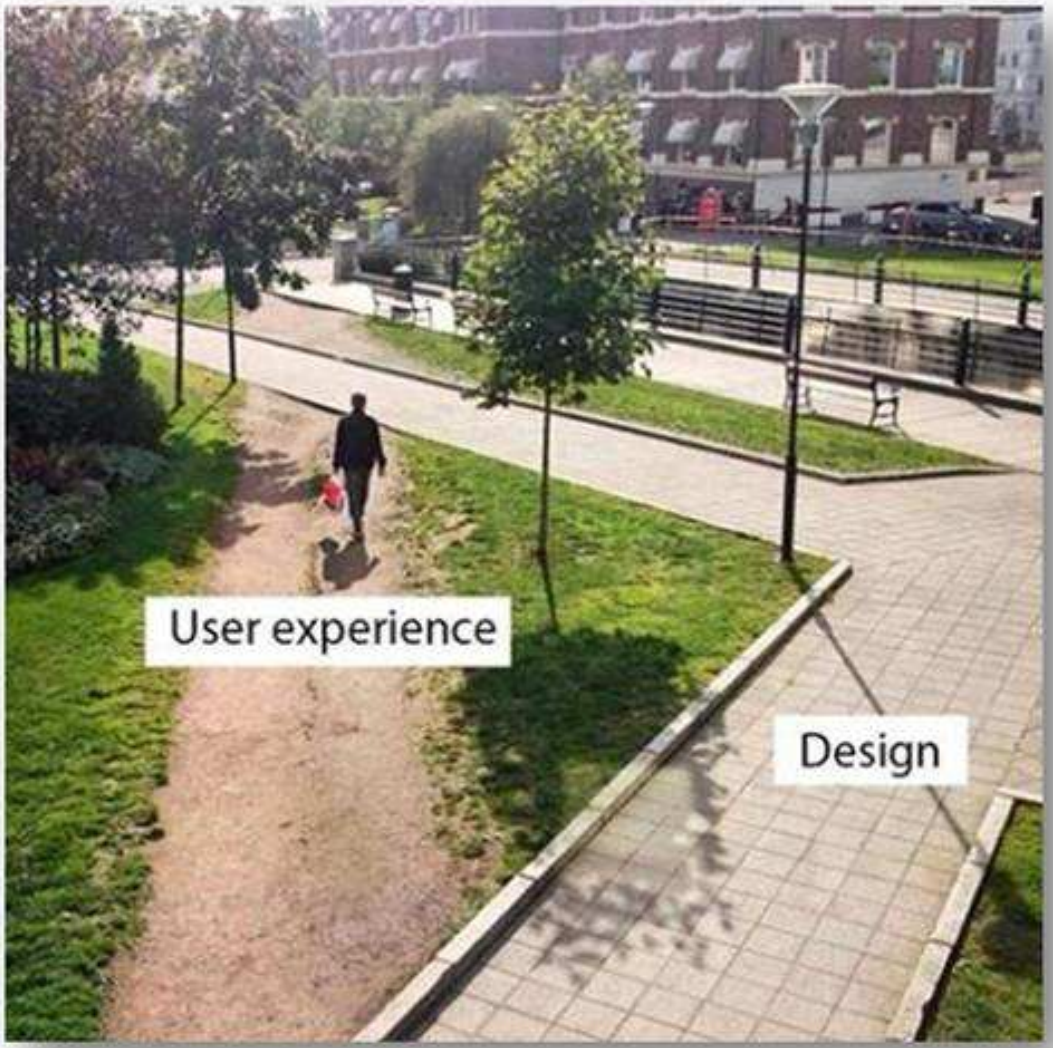
Processi per attuare

Prodotti comprati e mai usati

Ritardi (es. 1386-1965)

Processi per mantenere (1/2)

Processi per mantenere (2/2)



Obiettivi di un sistema di gestione per la sicurezza delle informazioni

- Ridurre gli incidenti;
- Ridurre gli impatti degli incidenti;
- Imparare dall'esperienza (propria e altrui) e migliorare.

Due leggi di sicurezza delle informazioni

Principio di Schneier:

la sicurezza è una catena: è forte come il suo anello più debole.

Corollario di Mitnick:

l'anello più debole sono le persone

Sistema di gestione per la sicurezza delle informazioni

Parte del sistema di gestione complessivo per

- stabilire,
- attuare,
- supervisionare,
- riesaminare,
- mantenere,
- migliorare

la sicurezza delle informazioni.

*Insieme di elementi **interrelati e interagenti** per **stabilire** obiettivi di sicurezza delle informazioni e **raggiungerli**.*

Norme di riferimento

- ISO/IEC 27000: 2014
- ISO/IEC 27001: 2013 e UNI CEI ISO/IEC 27001: 2014
- ISO/IEC 27002: 2013 e UNI CEI ISO/IEC 27002: 2014
- ISO 31000:2009 e UNI ISO 31000:2010

Informazioni

- Informazione: conoscenza o dati che hanno significato e valore.
- Le informazioni possono esistere in molte forme. Possono essere stampate o scritte su carta, gestite con strumenti informatici, trasmesse via posta o con mezzi elettronici, presentate in film o fotografie o dette in conversazioni.
- Qual è la differenza tra dati e informazioni?
  - T. S. Eliot, The rock, 1934
  - Where is the wisdom we have lost in knowledge?
    Where is the knowledge we have lost in information?

Sicurezza delle informazioni

- Il mantenimento della loro (ISO/IEC 27000)
  - riservatezza (le informazioni non sono rese disponibili o note a individui, entità o processi non autorizzati);
  - integrità (accuratezza e completezza);
  - disponibilità (accessibilità e usabilità su richiesta di un'entità autorizzata, secondo i tempi previsti).
- Altre proprietà da preservare (normalmente incluse nella "integrità"):
  - efficacia (utilità per l'utilizzatore);
  - affidabilità (verità e credibilità; anche sinonimo di accuratezza);
  - autenticità (essere chi o cosa è dichiarato);
  - conformità (coerente con le normative e i regolamenti applicabili);
  - non ripudiabilità (capacità di provare che un evento o un'azione e le entità che lo hanno originato, se dichiarato è accaduto).

Incidenti

- Incidente di sicurezza delle informazioni: uno o più eventi non voluti o non attesi che hanno una significativa probabilità di compromettere le attività e minacciare la sicurezza delle informazioni.
- Elenchiamo degli incidenti di sicurezza delle informazioni realmente accaduti.
- Associamoli ai 3 parametri di sicurezza che hanno subito degli impatti.

Ciclo PDCA e requisiti di sistema

Leadership

Azioni correttive

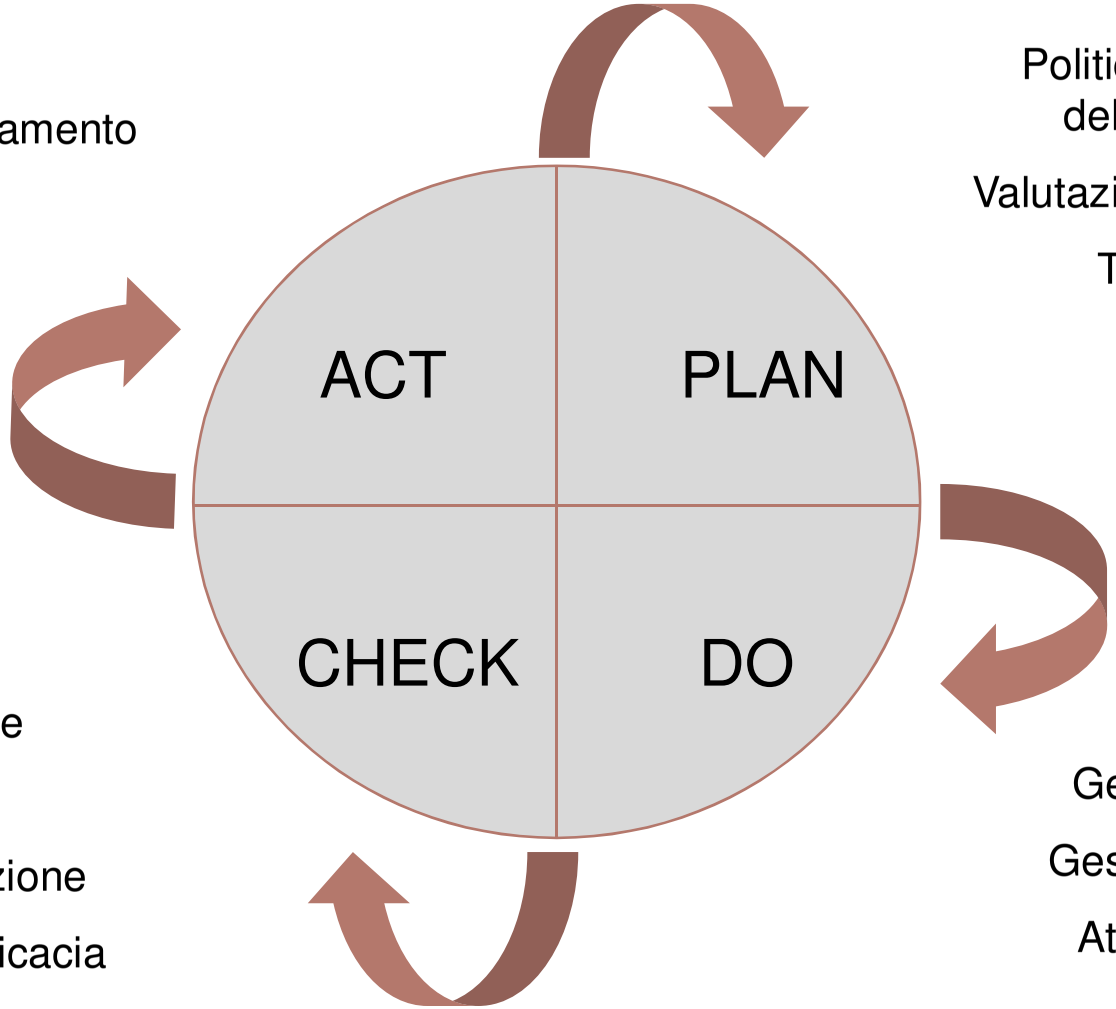
Azioni di miglioramento

Aggiornamenti

Politica di sicurezza delle informazioni

Valutazione del rischio

Trattamento del rischio



Verifiche tecniche

Audit interni

Riesame di direzione

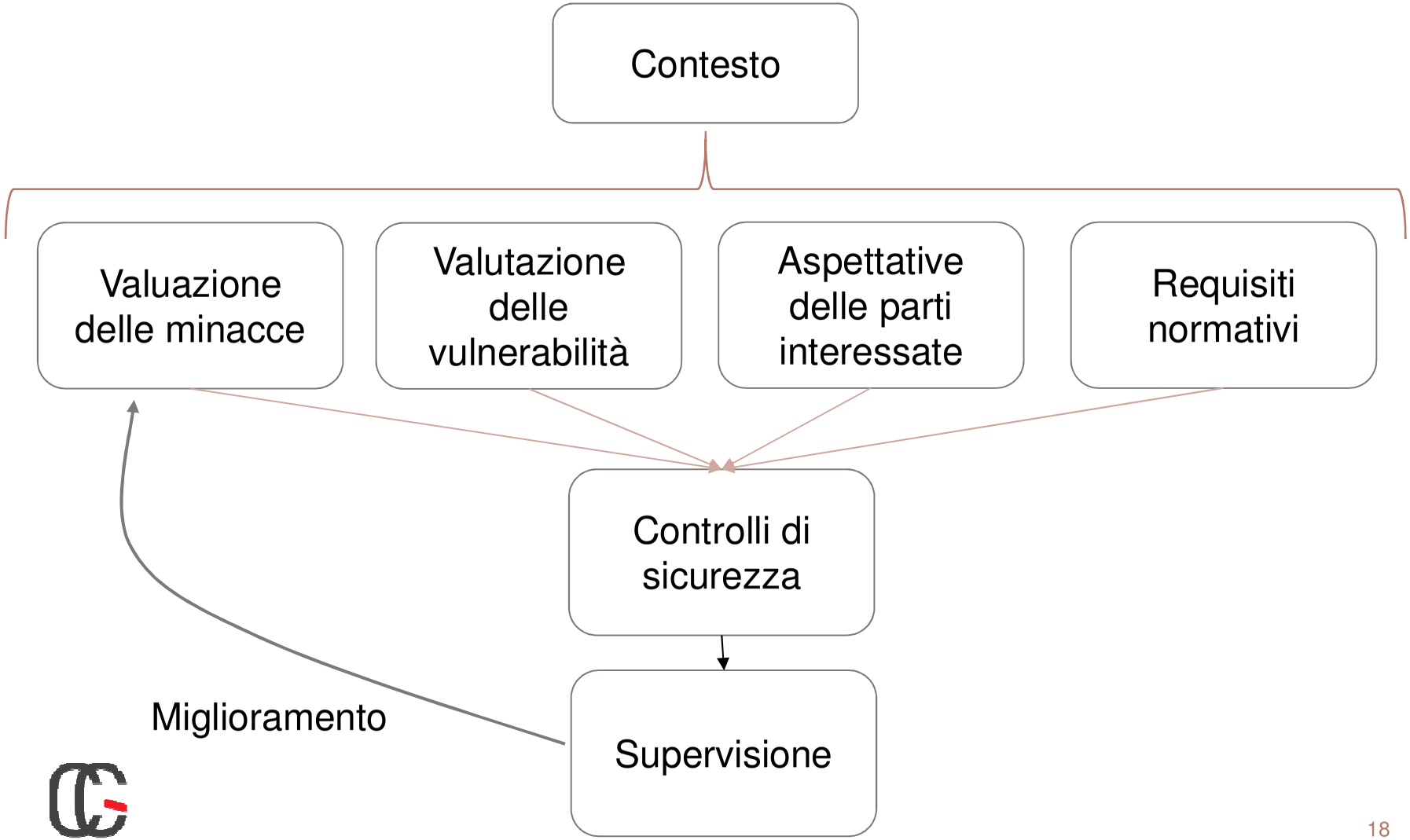
Valutazioni di efficacia

Gestire le risorse

Gestire documenti

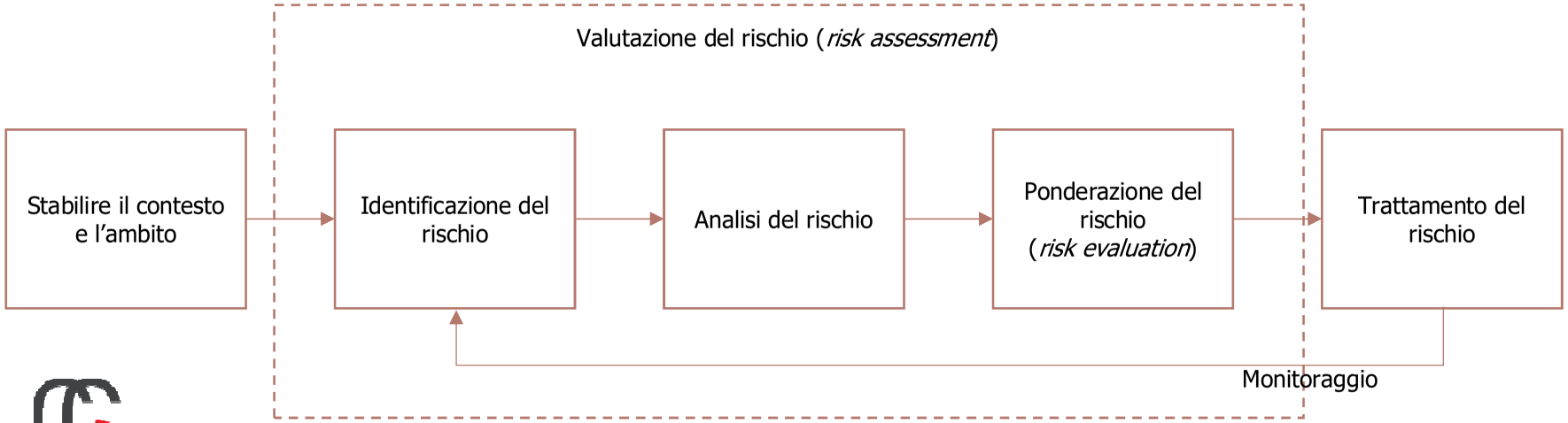
Attuare i controlli

Valutazione del rischio



Analisi, ponderazione, valutazione

- Analisi del rischio: Processo di comprensione della natura dei rischi e di determinazione del loro livello.
- Criteri di rischio: Termini di riferimento a fronte dei quali è valutata la significatività del rischio.
- Ponderazione del rischio: Processo di comparazione dei risultati dell'analisi dei rischi rispetto ai criteri di rischio per determinare se il rischio e/o la sua espressione quantitativa sia accettabile o tollerabile.
- Valutazione del rischio: Processo complessivo di analisi del rischio e di ponderazione del rischio.



Definizioni

- Minaccia: la possibile causa di un incidente che può portare danni ad un sistema o ad un'organizzazione.
- Vulnerabilità: una debolezza di un bene o di un gruppo di beni che può essere sfruttata da una o più minacce per concretizzarsi.
- Livello di rischio: Espressione quantitativa di un rischio o combinazione di rischi, espresso in termini di combinazione di conseguenze e della loro verosimiglianza.
- Formula

$$R \propto P \bullet D$$

Trattamento del rischio

- Evitare il rischio decidendo di non avviare o continuare con l'attività che dà origine al rischio.
- Assunzione o l'aumento del rischio al fine di perseguire un'opportunità.
- Rimozione della fonte di rischio (della minaccia).
- Cambiamento della verosimiglianza della minaccia.
- Cambiamento delle conseguenze.
- Condivisione del rischio con altro soggetto o soggetti (compresi i contratti e il finanziamento dei rischi).
- Ritenzione del rischio per scelta consapevole.

Caratteristiche della valutazione del rischio

- Ripetibilità.
- Confrontabilità.
- Mantenibilità.
- Coerenza.
- Completezza.
- Flessibilità.

Alcune domande

- Quale livello di dettaglio?
- Valutare le informazioni, i processi o gli “asset”?
- Chi e come coinvolgere?
- I vulnerability assessment rappresentano un’analisi del rischio?
- Analisi qualitative o quantitative?

Controlli di sicurezza
Politiche

- Politiche e regole di sicurezza delle informazioni.

Controlli di sicurezza
Organizzazione interna

- Responsabilità e poteri per i processi;
- Responsabilità e poteri per le funzioni;
- Segregazione dei compiti.

Controlli di sicurezza
Gestione delle persone

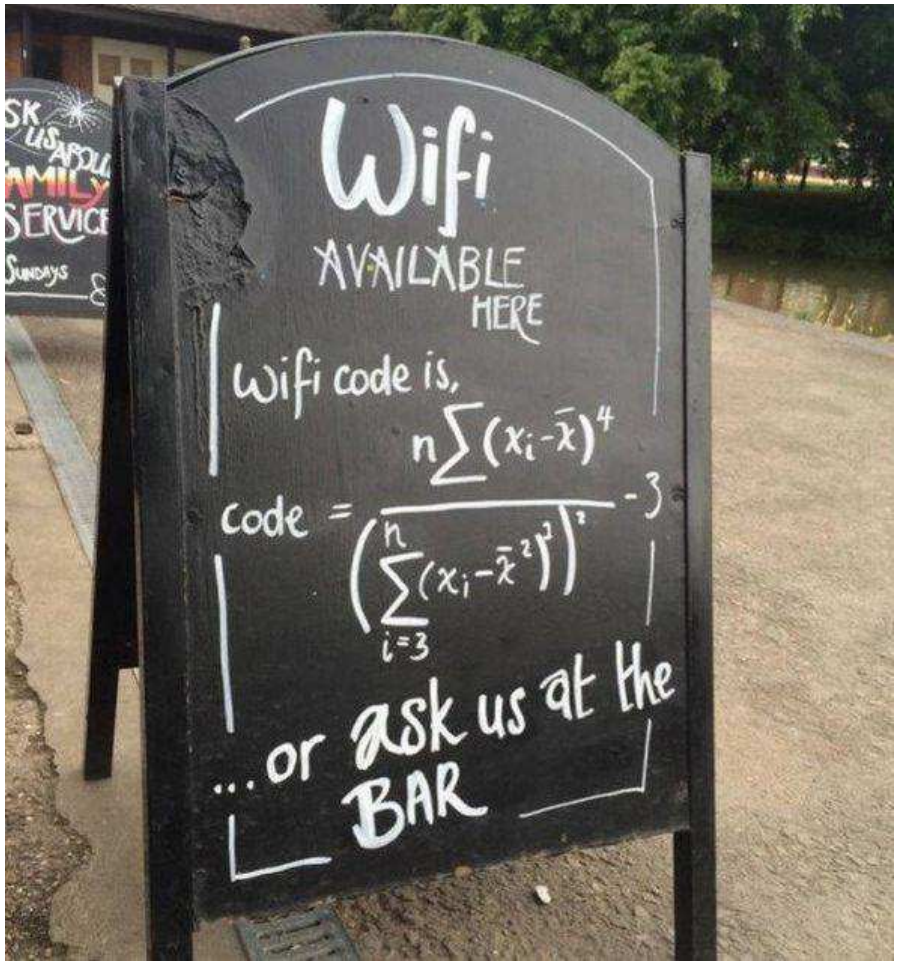
- prima;
- durante
  - formazione;
- dopo l'impiego.

Controlli di sicurezza
Gestione degli asset

- Classificazione e gestione delle informazioni (formato elettronico e fisico);
- Inventario e proprietà degli asset;
- Gestione dispositivi (inclusa dismissione).

Controlli di sicurezza
Controllo degli accessi

- Fisici e informatici (rete e sistemi);
- regole per ogni sistema o archivio;
- assegnazione, riesame e disabilitazione accessi;
- amministratori di sistema.
- Crittografia (non solo per il controllo accessi).



Controlli di sicurezza
Sicurezza fisica

- Perimetro di sicurezza;
- manutenzione impianti.

Controlli di sicurezza
Attività operative

- istruzioni;
- gestione cambiamenti;
- gestione capacità;
- separazione ambienti;
- controllo malware;
- backup e ripristino;
- logging;
- controllo ambiente di produzione;
- vulnerability assessment;
- patching.

Controlli di sicurezza
Comunicazioni

- Controllo della rete informatica;
- controllo delle comunicazioni;
- regole per sistemi di comunicazione.

Controlli di sicurezza
Acquisizione e sviluppo

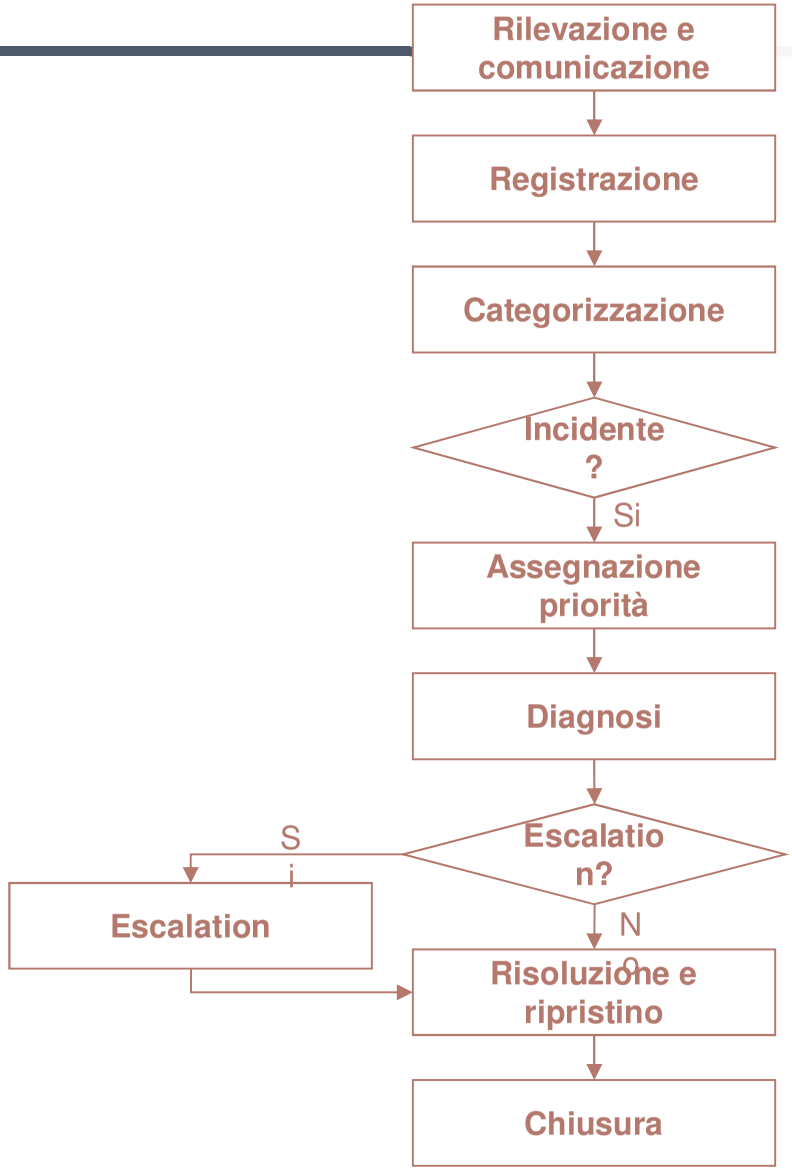
- Regole e processo di sviluppo sicuro (requisiti e test);
- controllo dell'ambiente di sviluppo e test.

Controlli di sicurezza
Gestione fornitori

- Regole;
- contratti (verifiche preliminari, stipula, controllo);
- controllo della catena di fornitura.

Controlli di sicurezza
Gestione incidenti

- comunicazione,
- diagnosi;
- trattamento;
- raccolta prove.



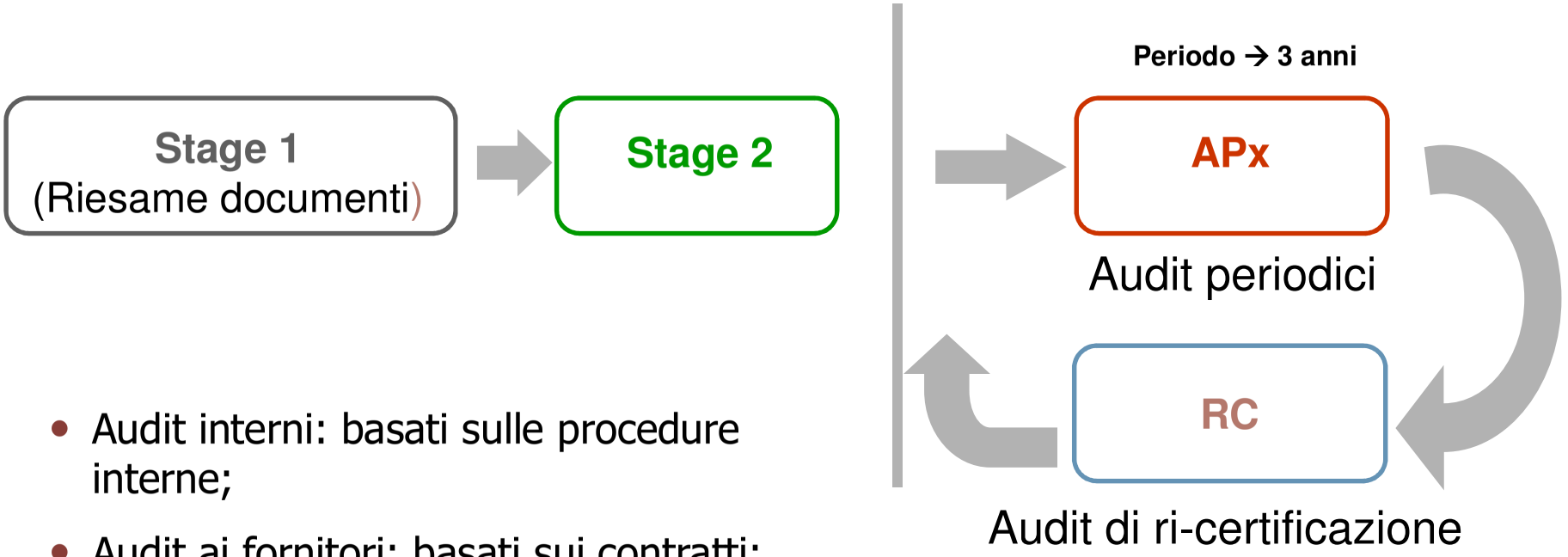
Controlli di sicurezza
Continuità operativa

- analisi;
- attuazione;
- test.

Controlli di sicurezza
Conformità

- Normativa;
- procedure interne.

Processo di audit di certificazione



- Audit interni: basati sulle procedure interne;
- Audit ai fornitori: basati sui contratti;
- Audit di certificazione: basati su standard.

Le norme della serie ISO/IEC 27000

- ISO/IEC 27000:2014 - Termini e definizioni.
- ISO/IEC 27003:2010 – Guida all'interpretazione (nuova nel 2016).
- ISO/IEC 27004:2009 – Monitoraggi e misurazioni (nuova nel 2016?).
- ISO/IEC 27005:2011 – Gestione del rischio (nuova nel 2017?).
- ISO/IEC 27006:2001 – Per gli OdC (nuova a fine 2015).
- ISO/IEC 27009 – Certificazioni specifiche (nel ???).

Altre norme di interesse

- ISO/IEC 27031:2011: relazioni tra ITC e BCP
- ISO/IEC 27035:2011: "Information security incident management"
- ISO/IEC 27037 sulla digital forensics
- ISO 22301:2012: business continuity
- ISO/IEC 24762:2008: linee guida sul Disaster Recovery
- ISO/PAS 22399:2007: sulla preparazione rispetto a incidenti
- ISO 31000:2009: "Risk management — Principles and guidelines"