

Gestione dei rischi informatici (Risk Management)

Prof. Francesco Bergadano

**Dipartimento di Informatica
Università di Torino**

Sommario

- Il rischio informatico:
 - Perimetro
 - Probabilità dell'evento
 - Impatto
- Standard e certificazione ISO 27001, per la gestione della sicurezza delle informazioni
- Metodologia OWASP, per la gestione di rischi legati ad applicazioni Web-oriented

Il rischio informatico

Il rischio informatico consiste nel possibile verificarsi (con una certa probabilità) di eventi rilevanti per un insieme di sistemi ICT (perimetro), che possono avere un impatto negativo (impact) sul business o sui beni di una organizzazione.

Il rischio informatico

Natura dell'impatto e probabilità del verificarsi dell'evento determinano la gravità del rischio:

Gravità del rischio = Probabilità(evento)*Peso(impact)

Perimetro

Definisce l'oggetto rispetto al quale si svolgono l'analisi e la gestione del rischio, ad esempio:

- Un'intera organizzazione
- Un dipartimento o business unit
- Un ben definito insieme di reti e calcolatori
- Un insieme di applicazioni informatiche, anche se fisicamente esterne all'organizzazione (es. in cloud)

Metodologie e standard

- ISO 27001 (orientato ad una organizzazione o ad un suo sottoinsieme)
- OWASP (orientato ad una singola Web application)

ISO 27001

- Norma internazionale ISO 27001:2005, che prevede il rilascio di una certificazione da parte di un ente accreditato.
- Indirizza la gestione del rischio informatico nel contesto generale della gestione dei rischi aziendali.
- Si fonda sul concetto di «sistema di gestione», come per altre norme, es. qualità (ISO 9001), ambiente (ISO 14001), sicurezza alimentare (ISO 22000).

ISO 27001

Fornisce i requisiti per attuare e mantenere un

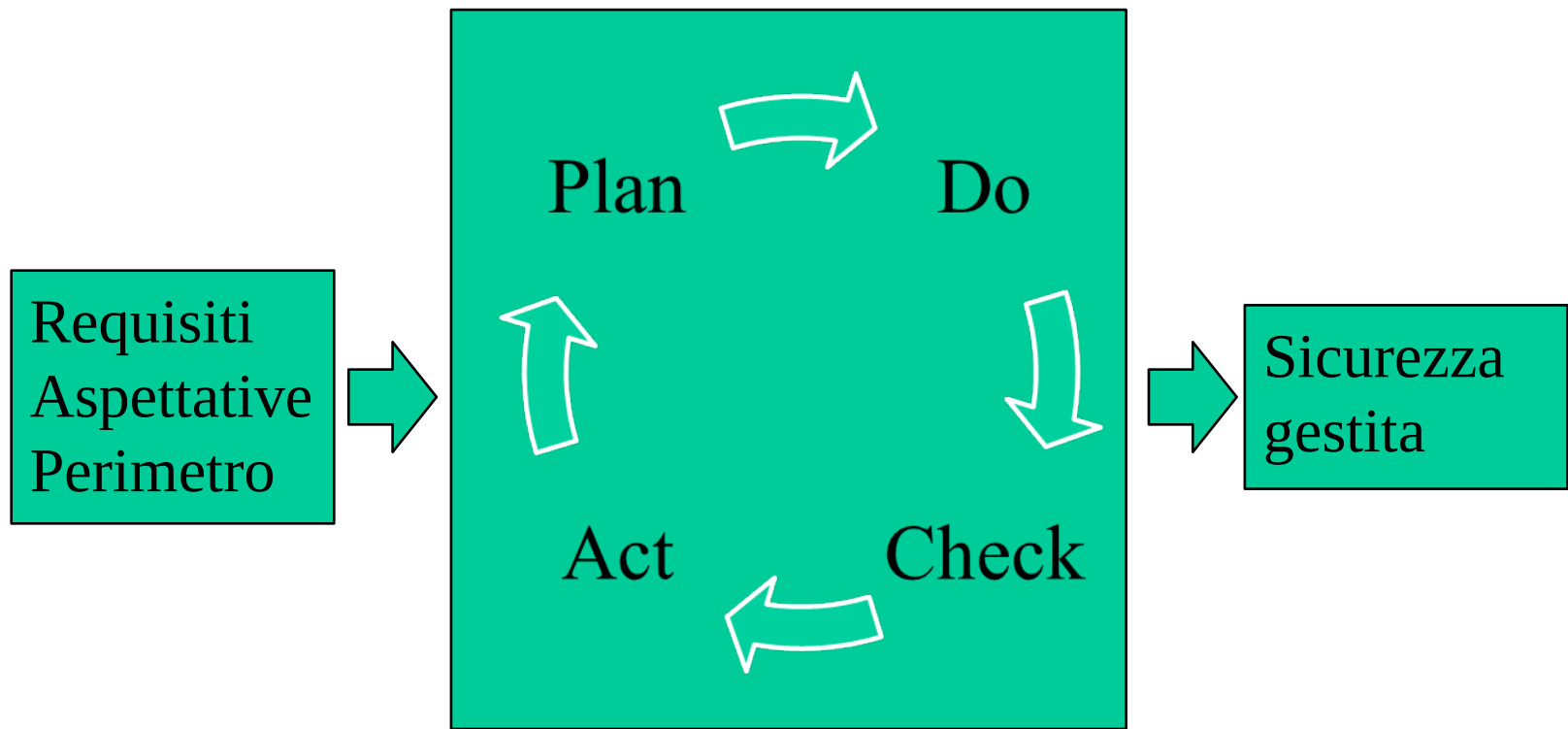
Sistema di Gestione della Sicurezza delle Informazioni
(Information Security Management System – ISMS)

secondo un approccio per processi.

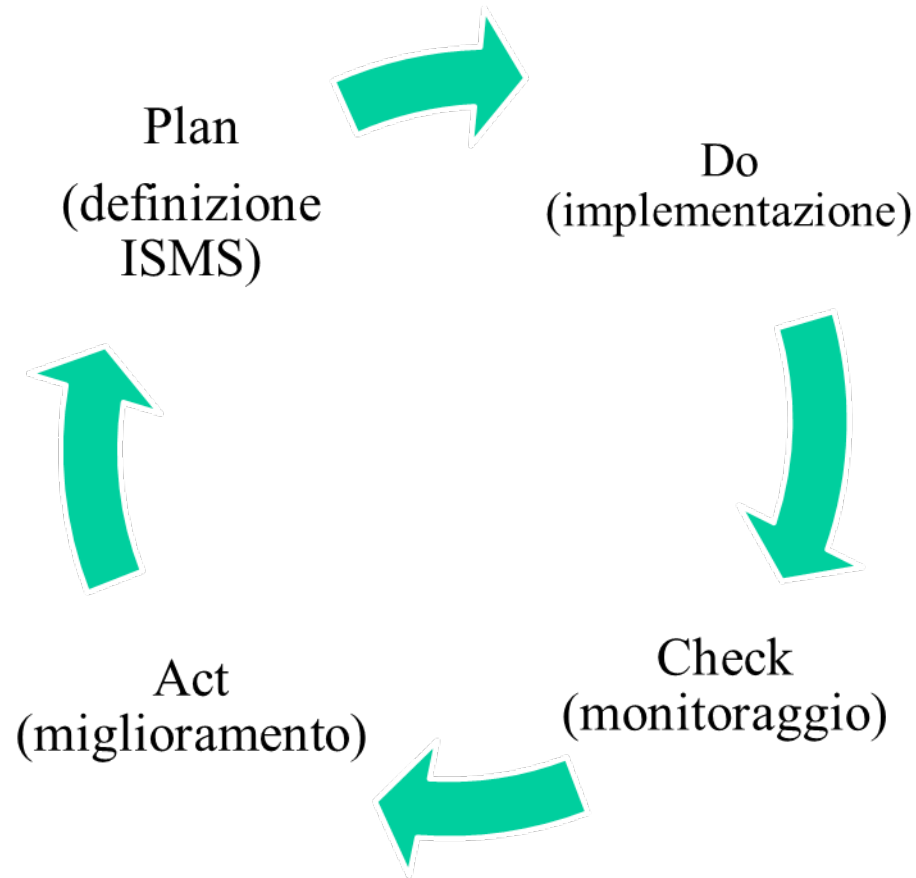
ISMS secondo la ISO 27001

- E' un sistema di gestione della sicurezza mirato a implementare controlli di sicurezza adeguati all'organizzazione e al perimetro individuato
- Ha in input i requisiti di sicurezza e produce in output i risultati attesi attraverso processi e azioni necessarie (approccio per processi)
- Il sistema ISMS viene continuamente migliorato attraverso un modello PDCA (Plan-Do-Check-Act)

Ciclo di Deming – modello PDCA (plan-do-check-act)



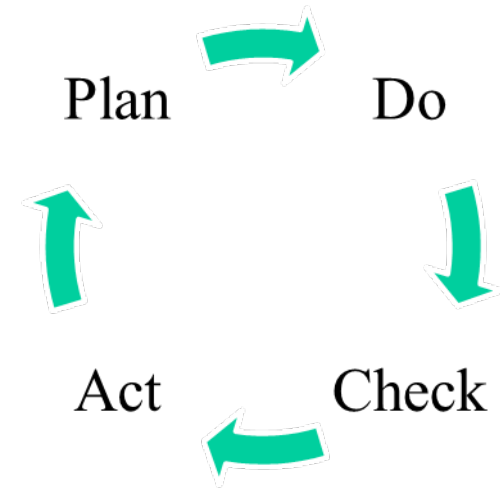
Ciclo di Deming – modello PDCA (plan-do-check-act)



Termini chiave per un ISMS

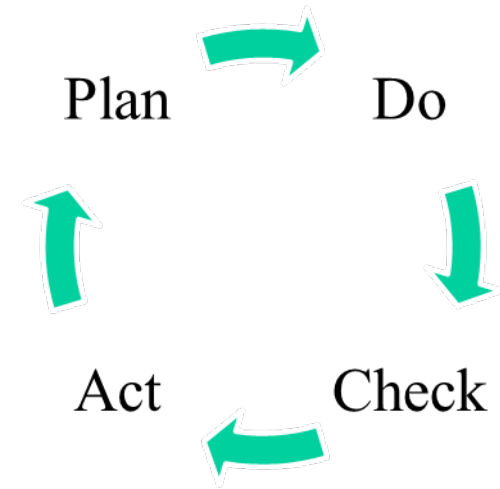
- Asset: qualunque bene o entità che può avere un valore per l'organizzazione (es. beni fisici, persone, applicazioni informatiche).
- Sicurezza delle informazioni: la protezione delle caratteristiche di confidenzialità, integrità.
- Controlli: mezzi per gestire e limitare il rischio (organizzativi o tecnici).
- Minacce (threats): evento possibile, con un impatto

Plan



1. Definire il perimetro
2. Scrivere una «Politica dell'ISMS»
3. Analizzare e valutare il rischio
4. Trattare il rischio
5. Ottenere approvazione ed autorizzazione
6. Redigere lo «Statement of Applicability»

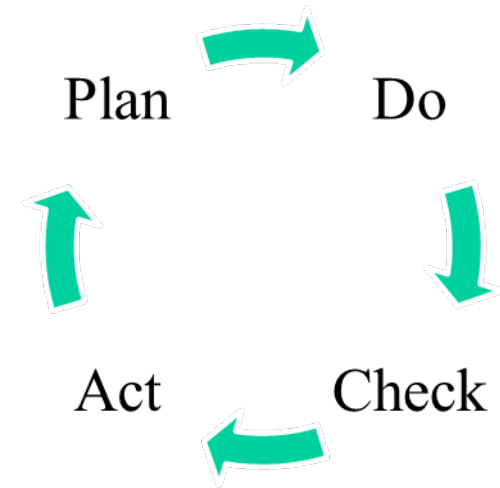
Plan



1. Definire il perimetro:

- Perimetro fisico (edifici, risorse)
- Anagrafica degli asset
- Risorse tecnologiche (es. server, reti, servizi esterni)

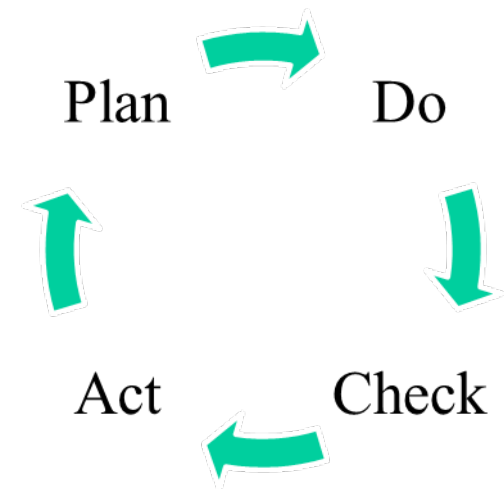
Plan



2. Scrivere una «Politica dell'ISMS»
(parte della security policy), che:

- definisca principi strategici generali
- tenga conto degli obblighi contrattuali e di vincoli specifici dell'organizzazione rispetto al perimetro
- si integri con il sistema di gestione dei rischi (anche non informatici) dell'organizzazione
- definisca i criteri per la valutazione dei rischi

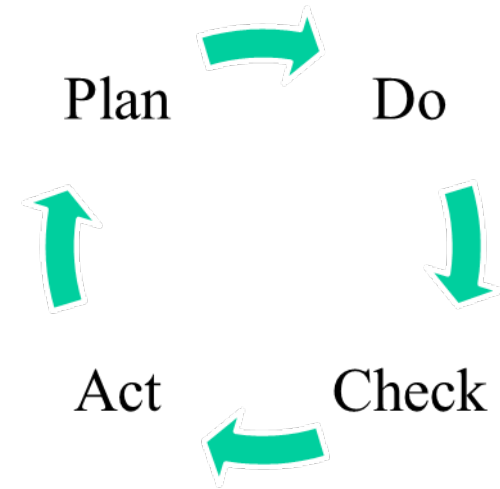
Plan



3a. Analizzare e valutare il rischio, identificando:

- asset e loro responsabili
- minacce (threats)
- contromisure esistenti (controls)
- vulnerabilità sfruttabili dalla minacce (vulnerabilities)
- tipologie di conseguenze degli incidenti

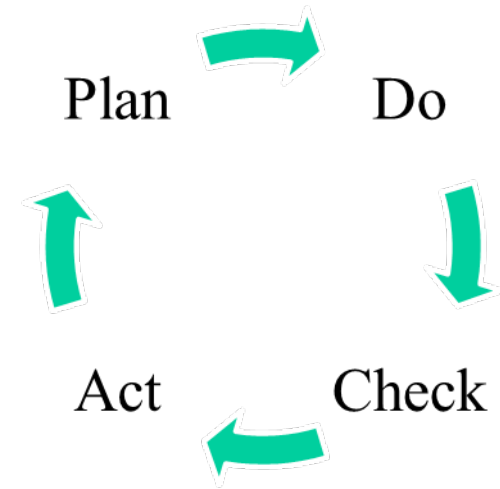
Plan



3b. Valutare il rischio, stimando:

- impatti e conseguenze per l'organizzazione, nel caso che le minacce possano causare un corrispondente incidente
- la probabilità P che un certo incidente si verifichi
- i livelli di rischio per ogni minaccia (ad esempio con una formula come $\text{rischio} = f(P, \text{impatto})$)

Plan



4. Trattare il rischio:

- applicare ulteriori controlli (vedi slide successiva)
- inserire il rischio in una lista di rischi ‘accettati’
- trasferire i rischi (es. con una assicurazione)

A valle di questa fase, occorre valutare il rischio residuo, seguendo lo schema del precedente punto 3b.

Controlli ISO 27001 (“appendice A”, vedi anche file separato)

A.5 Security policy

A.6 Organization of information security

A.7 Asset management

A.8 Human resources security

A.9 Physical and environmental security

A.10 Communications and operations management

A.11 Access control

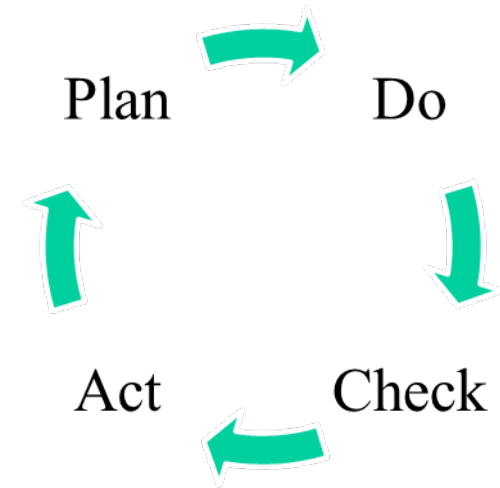
A.12 Information systems acquisition, development and maintenance

A.13 Information security incident management

A.14 Business continuity management

A.15 Compliance

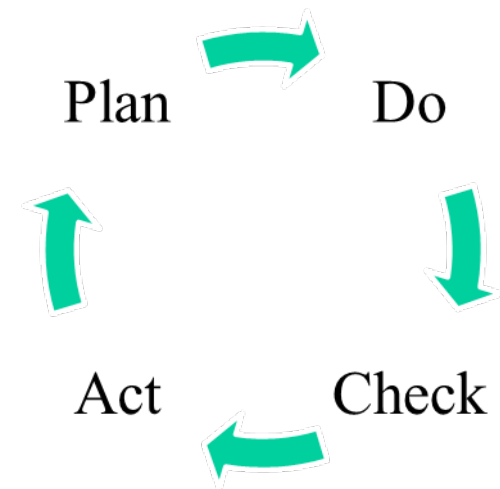
Plan



5. Ottenere approvazione dalla direzione:

- per l'accettazione del rischio residuo
- per l'implementazione dei controlli selezionati

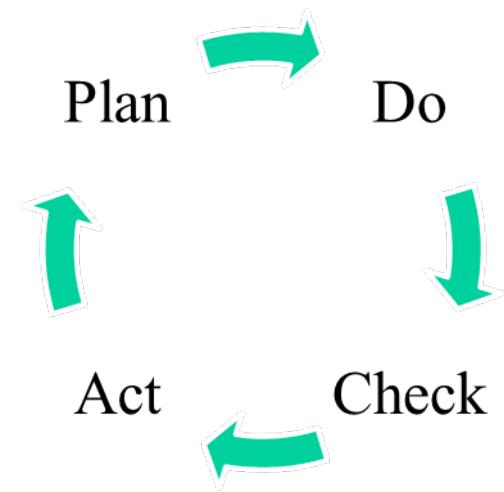
Plan



6. Redigere lo «Statement of Applicability», con:

- Controlli esistenti
- Controlli aggiuntivi, selezionati in base al piano di riduzione dei rischi
- Selezione dei controlli che verranno effettivamente attuati e delle tempistiche di attuazione, motivando tali scelte sulla base della politica dell'ISMS.

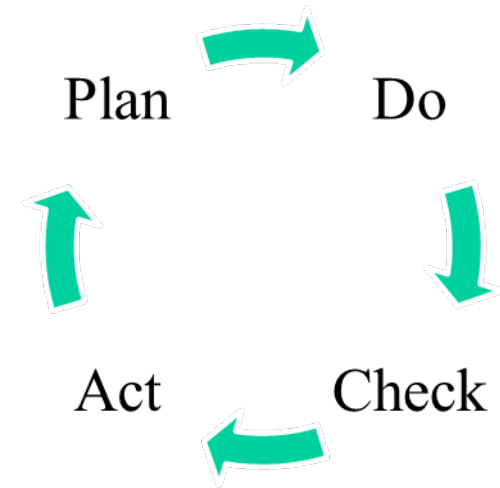
Plan



finora abbiamo «pianificato» ...

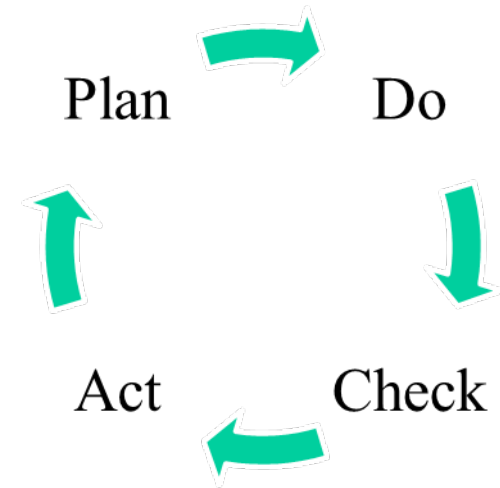
... ma non abbiamo ancora «fatto» nulla

Do



- Definire un piano di impementazione
- Realizzare i controlli selezionati
- Misurare l'efficacia dei controlli realizzati
- Attuare un piano di formazione
- Gestire l'operatività dei controlli e la loro manutenzione ed evoluzione ordinaria

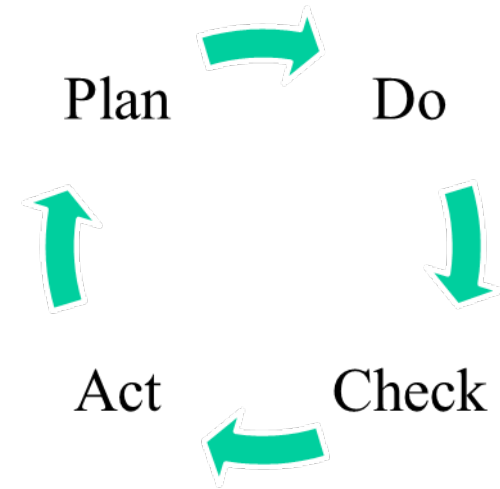
Check



(a) Monitoraggio per rilevare problemi

- Rilevare errori nei sistemi informatici e in particolare in quelli modificati dai controlli implementati
- Identificare gli incidenti di sicurezza
- Verificare se le azioni intraprese per risolvere un incidente sono state efficaci

Check

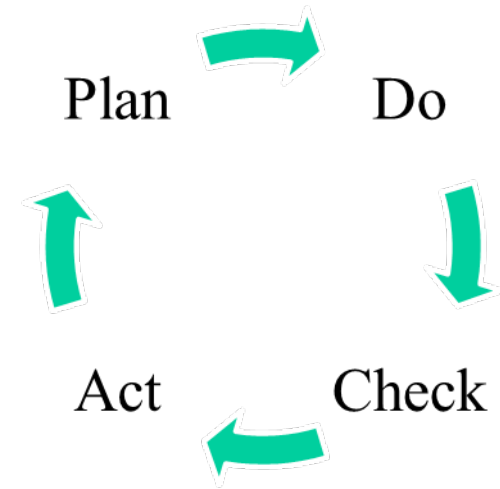


(b) Riesame proattivo

- Audit di sicurezza (es. Pentest, Assessment, interviste)
- Misurazione dell'efficacia dei controlli
- Verifica dell'attuazione requisiti di sicurezza contenuti nelle politiche

(c) Riesame della valutazione dei rischi residui

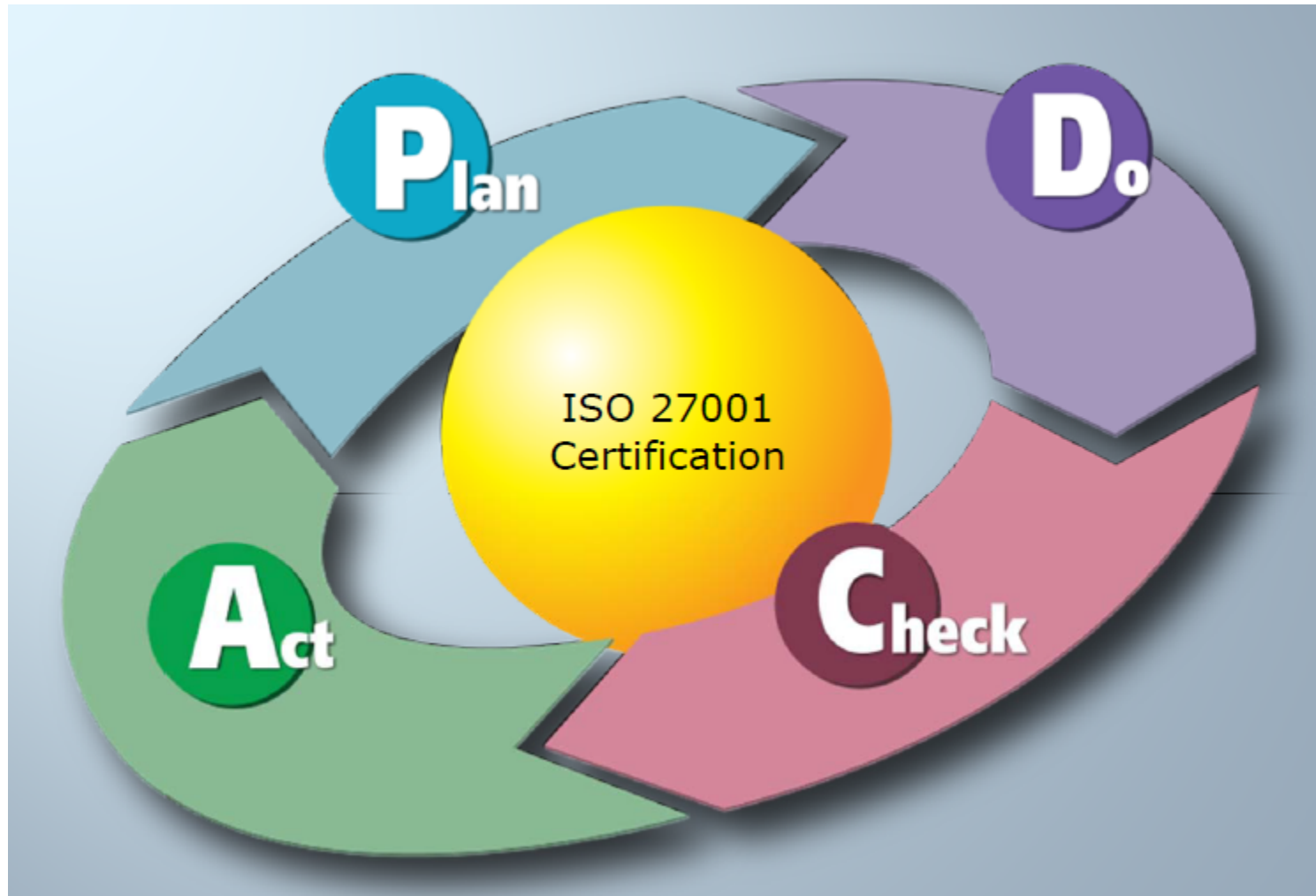
Act



Migliorare l'ISMS:

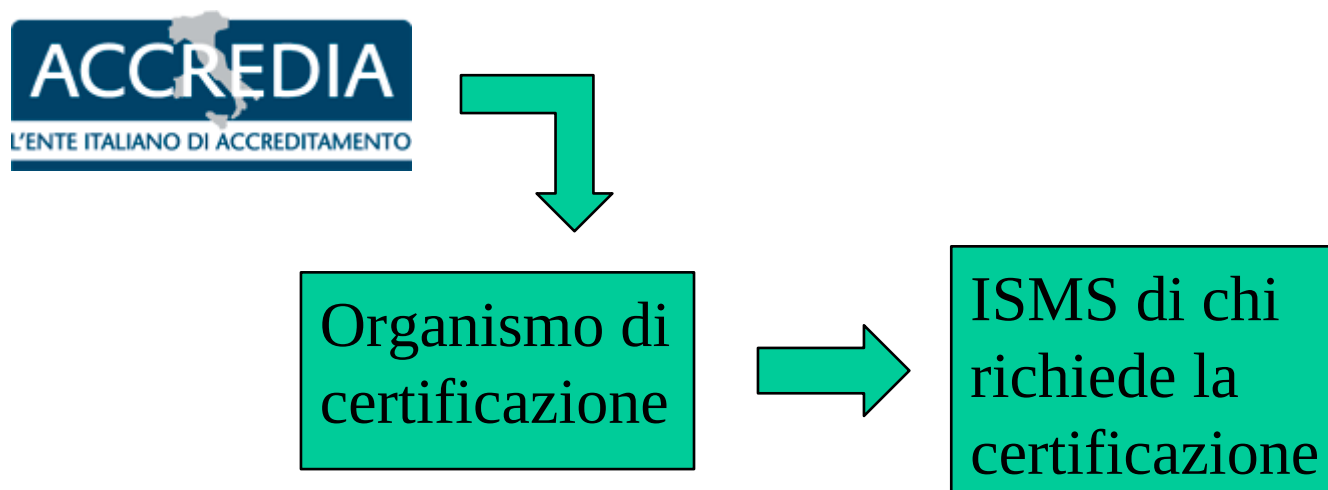
- Identificare i miglioramenti necessari, sulla base delle risultanze della fase di check
- Attuare i miglioramenti sopra definiti
- Verificare che i miglioramenti siano efficaci

Ciclo di Deming e certificazione ISO 27001

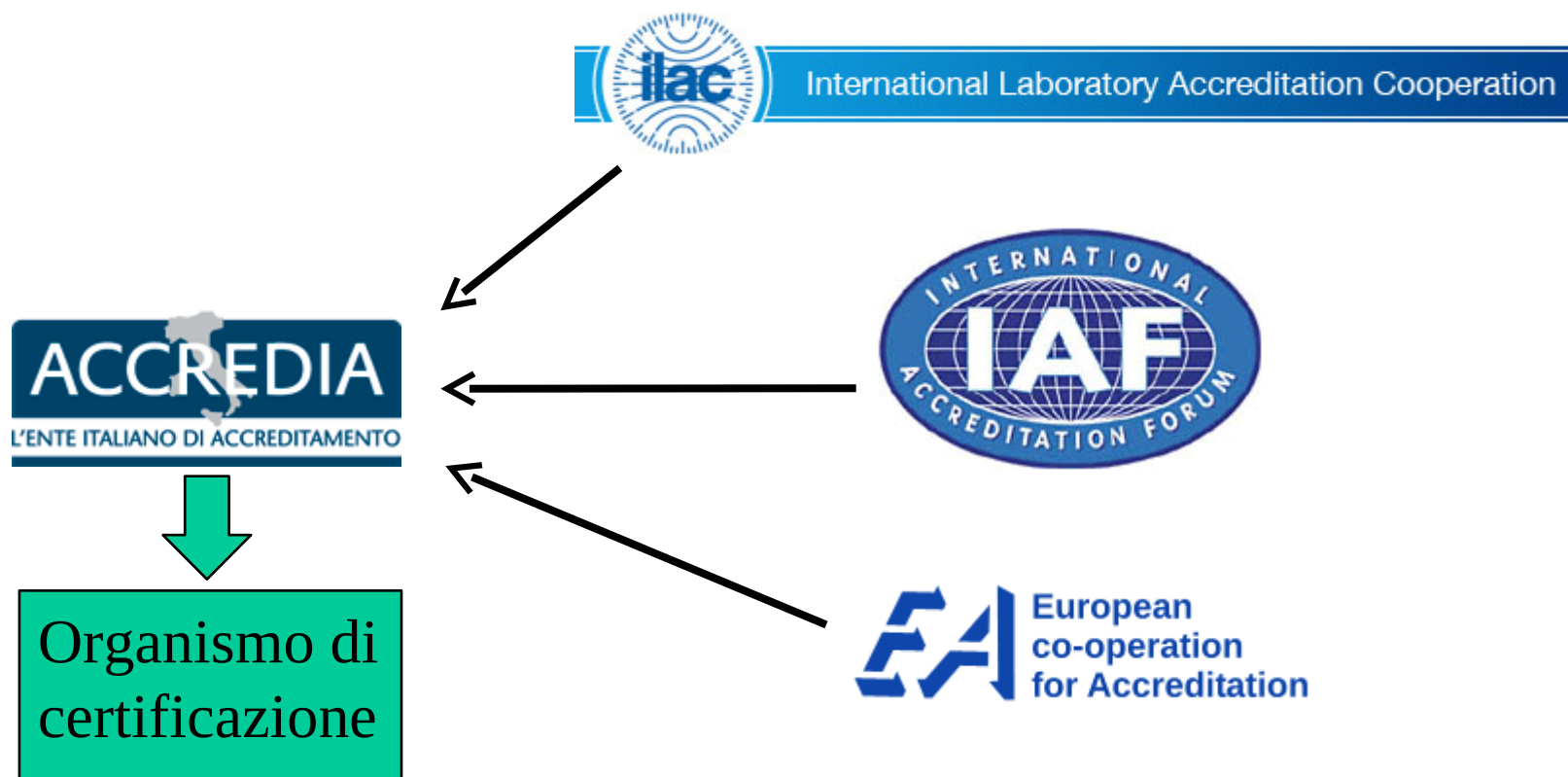


Certificazione ISO 27001

Certificazione da parte di un ente accreditato - in Italia, da Accredia (ex Sinal e Sincert):



Certificazione ISO 27001 – collegamenti internazionali



Banche Dati

» home » Banche Dati » Organism

Organismi accreditati

Totale risultati 10
pagina numero **1**

Organismo di Certificazione	Sito Web
CERMET Soc. Cons. a r.l.	http://www.cermet.it/
CERTIQUALITY S.r.l.	http://www.certiquality.it/
CSQA Certificazioni S.r.l.	http://www.csqa.it/
DASA RÄGISTER S.p.A.	http://www.dasa-raegister.com
Det Norske Veritas Italia S.r.l.	http://www.dnvba.it/
ICIM S.p.A.	http://www.icim.it/
IMQ S.p.A.	http://www.imq.it/
RINA Services S.p.A.	http://www.rina.org
S.C. ALL CERT SYSTEMS S.r.l.	http://www.allcert.ro
TÜV Italia S.r.l.	http://www.tuv.it/

→ **Organismi di certificazione e ispezione**

→ Organismi esteri riconosciuti per il settore IAF 28

→ Laboratori di prova

→ Laboratori di taratura

→ Organizzazioni/aziende con sistema di gestione certificato

→ Organizzazioni/aziende certificate FSM

Metodologie e standard per la gestione del rischio informatico

- ISO 27001 (orientato ad una organizzazione o ad un suo sottoinsieme) – **approccio per processi**
- OWASP (orientato ad una singola Web application) – **approccio tecnologico, ma collegato a parametri rilevanti per il business**

Che cos'è OWASP?

www.owasp.org



Che cos'è OWASP?

quanto sotto è tratto da www.owasp.org

- Worldwide not-for-profit organization focused on improving the security of software.
- Everyone is free to participate in OWASP and all OWASP materials are available under a free and open software license.
- OWASP does not endorse or recommend commercial products or services

OWASP

- Limitato principalmente alle Web Application, che però rappresentano oggi una parte rilevante della ICT delle grandi organizzazioni
- Famoso per la “top ten” delle vulnerabilità Web
- Propone un metodo pratico ed efficace per l’analisi e la gestione del rischio relativo alla sicurezza delle applicazioni Web

OWASP top ten 2013

A1 Injection

A2 Broken Authentication and Session Management

A3 Cross-Site Scripting (XSS)

A4 Insecure Direct Object References

A5 Security Misconfiguration

A6 Sensitive Data Exposure

A7 Missing Function Level Access Control

A8 Cross-Site Request Forgery (CSRF)

A9 Using Known Vulnerable Components

A10 Unvalidated Redirects and Forwards

OWASP risk analysis and management

Basato sui concetti di **rischio, minaccia, agente della minaccia, vulnerabilità, impatto**:

Gravità del rischio = $f(\text{probabilità}, \text{impatto})$

Probabilità = $g(\text{agente della minaccia}, \text{vulnerabilità})$

Impatto = $h(\text{impatto tecnologico}, \text{impatto di business})$

OWASP risk analysis and management – 5 step

- Identificare il rischio
- Valutare la probabilità (likelihood)
- Valutare l'impatto
- Calcolare la gravità del rischio
- Decidere le contromisure

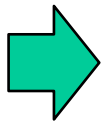
Identificare il rischio

Un singolo rischio è definito da:

- Tipo di minaccia (es. accesso dispositivo non autorizzato ad un conto bancario)
- Agenti della minaccia (es. hacker su Internet)
- Vulnerabilità coinvolta (es. Xsite Request Forgery)
- Impatto di business (es. bonifico non autorizzato e possibile indennizzo al cliente)

Identificazione del rischio

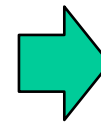
Agente
della
minaccia



Tecnologi
a di
attacco



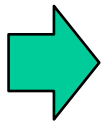
vulnerabilità



Impatto di
Business

Rischio = possibilità che si verifichi un evento, con un impatto di business negativo, attuato da un agente, usando certe tecniche e vulnerabilità.

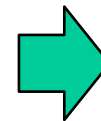
Agente
della
minaccia



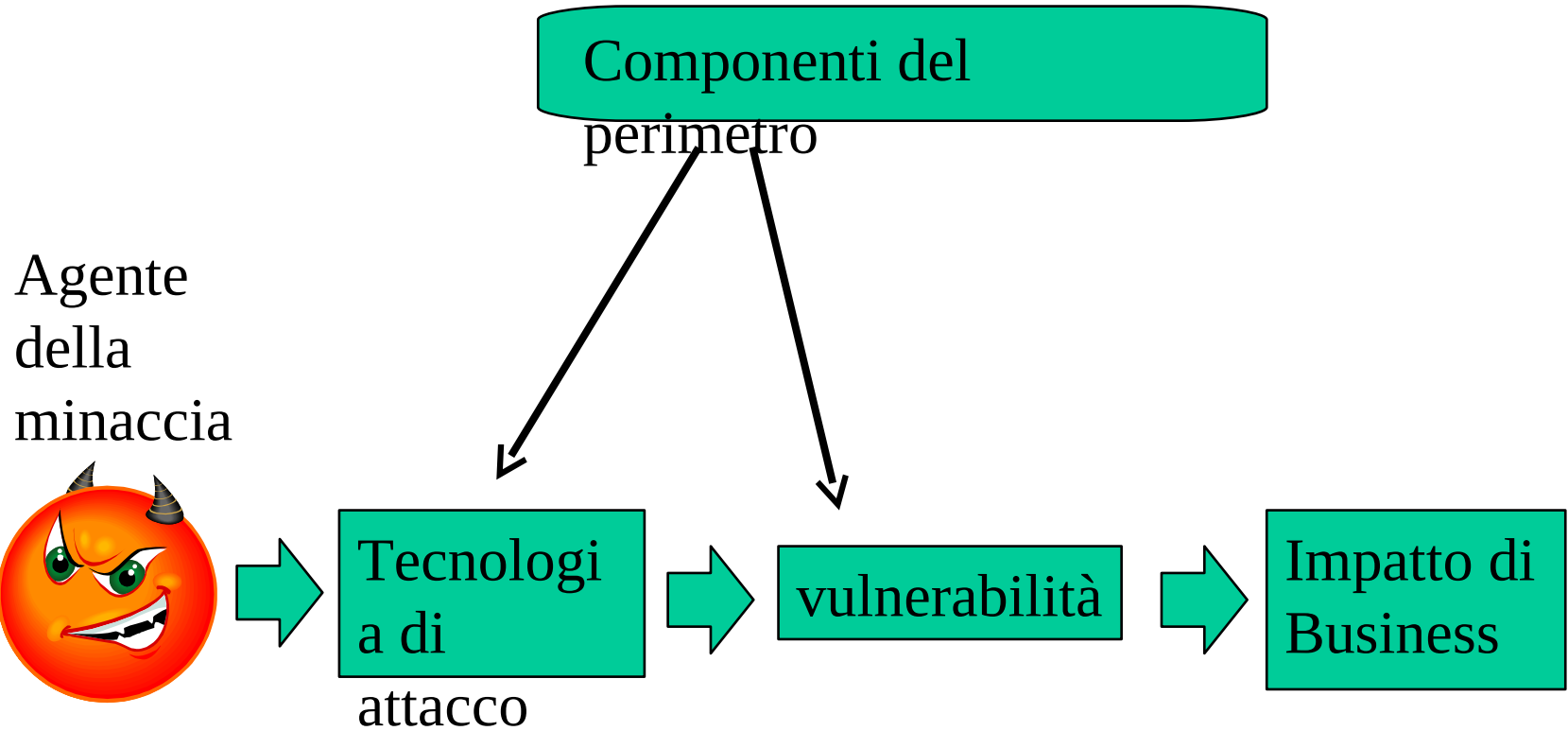
Tecnologi
a di
attacco



vulnerabilità



Impatto di
Business



Valutare la probabilità che l'evento legato al rischio accada

Owasp suggerisce di valutare:

- Agente della minaccia
- Vulnerabilità coinvolta

Andando poi a combinare le due valutazioni:

Probabilità = $g(\text{agente della minaccia}, \text{vulnerabilità})$

Valutare la probabilità che l'evento legato al rischio accada

Owasp suggerisce di valutare

- Agente della minaccia
- Vulnerabilità coinvolta

Andando poi a combinare le

Probabilità = $g(\text{agente della minaccia})$

- Livello di competenza necessario
- Motore (es. economico)
- Opportunità (disponibilità di risorse proprie, accesso a risorse aziendali o di terzi)
- Dimensione (quanti agenti di questo tipo esistono)

Valutare la probabilità che il rischio accada

Es.:

1 = security skills

3 = neworking/programming

4 = advanced computer use

6 = some tech skills

9 = no tech skills

- Livello di competenza necessario

- Motore (es. economico)

- Opportunità (disponibilità di risorse proprie, accesso a risorse aziendali o di terzi)

- Dimensione (quanti agenti di questo tipo esistono)

Andando poi a combinare le

Probabilità = g(agente della

Valutare la probabilità che il rischio accada

Es.:

1 = nessun guadagno

4 = guadagno possibile

9 = guadagno elevato

- Livello di competenza necessario
- Movente (es. economico)
- Opportunità (disponibilità di risorse proprie, accesso a risorse aziendali o di terzi)
- Dimensione (quanti agenti di questo tipo esistono)

Andando poi a combinare le

Probabilità = g(agente della

Valutare la probabilità che il rischio accada

Es. (accesso a risorse):

0 = accesso completo

4 = accesso specifico

7 = qualche accesso

9 = nessun accesso

- Livello di competenza necessario

- Motore (es. economico)

Opportunità
(disponibilità di risorse proprie, accesso a risorse aziendali o di terzi)

- Dimensione (quanti agenti di questo tipo esistono)

Andando poi a combinare le

Probabilità = g(agente della

Valutare la probabilità che il rischio accada

Es.:

2 = sviluppatori

2 = amministratori sistema

4 = utenti intranet

5 = partner

6 = utenti autenticati

9 = utenti Internet

- Livello di competenza necessario
- Motore (es. economico)
- Opportunità (disponibilità di risorse proprie, accesso a risorse aziendali o di terzi)
- Dimensione (quanti agenti di questo tipo esistono)

Andando poi a combinare le

Probabilità = g(agente della

Valutare la probabilità che l'evento legato al rischio accada

Owasp suggerisce di valutare

- Agente della minaccia
- Vulnerabilità coinvolta

Andando poi a combinare le

Probabilità = $g(\text{agente della minaccia})$

- Quanto è facile scoprirla
- Quanto è facile sfruttarla
- Conoscenza della vulnerabilità da parte degli agenti
- Facilità di rilevamento (detection) dall'attacco

Valutare la probabilità che lo al rischio accada

Es.:

1 = impossibile in pratica

3 = difficile

7 = facile

9 = automatica con tool

Quanto è facile
scoprirla

Quanto è facile
sfruttarla

- Conoscenza della vulnerabilità da parte degli agenti
- Facilità di rilevamento (detection) dall'attacco

Andando poi a combinare le

Probabilità = $g(\text{agente della})$

Valutare la probabilità che l'attacco al rischio accada

Es.:

1 = sconosciuta

4 = nascosta

6 = ovvia

9 = pubblica

- Quanto è facile scoprirla
- Quanto è facile sfruttarla
- Conoscenza della vulnerabilità da parte degli agenti
- Facilità di rilevamento (detection) dall'attacco

Andando poi a combinare le

Probabilità = $g(\text{agente della})$

Valutare la probabilità che un attacco al rischio accada

Es.:

1 = programmato
nell'applicazione

3 = in log e analizzato

8 = in log

9 = no log

- Quanto è facile scoprirla
- Quanto è facile sfruttarla
- Conoscenza della vulnerabilità da parte degli agenti
- Facilità di rilevamento (detection) dall'attacco

Andando poi a combinare le

Probabilità = $g(\text{agente della})$

Valutare la probabilità che l'evento legato al rischio accada

Probabilità = $g(\text{agente della minaccia}, \text{vulnerabilità})$

Possibile approccio secondo OWASP:

g = media aritmetica dei valori da 0 a 9 ottenuti per ciascuna categoria di valutazione, sia per l'agente che per la vulnerabilità.

Valutare l'impatto dell'evento legato al rischio

Owasp suggerisce di valutare:

- Impatto tecnologico
- Impatto di business

Andando poi a combinare le due valutazioni:

$\text{Impatto} = h(\text{impatto tecnologico}, \text{impatto di business})$

Valutare l'impatto dell'evento legato al rischio

Owasp suggerisce di valutare

- Impatto tecnologico
- Impatto di business

Andando poi a combinare le

Impatto = h(impatto tecnologico

- Perdita di confidenzialità
- Perdita di integrità dei dati
- Mancata disponibilità del servizio
- Mancata tracciabilità rispetto ai responsabili (loss of accountability)

Valutare l'impatto legato al rischio

Es.:

2 = pochi dati non rilevanti

6 = pochi dati rilevanti

6 = molti dati non rilevanti

7 = molti dati rilevanti

9 = tutti i dati

- Perdita di confidenzialità
- Perdita di integrità dei dati
- Mancata disponibilità del servizio
- Mancata tracciabilità rispetto ai responsabili (loss of accountability)

Andando poi a combinare le

Impatto = $h(\text{impatto tecnologico} \times \text{rischio})$

Valutare l'impatto

delegato al rischio

Es.:

2 = pochi dati poco modificati

3 = pochi dati molto cambiati

5 = molti dati poco cambiati

7 = molti dati molto cambiati

9 = tutti i dati modificabili

- Perdita di confidenzialità
- Perdita di integrità dei dati
- Mancata disponibilità del servizio
- Mancata tracciabilità rispetto ai responsabili (loss of accountability)

Andando poi a combinare le

Impatto = h(impatto tecnologico)

ss)

Valutare l'impatto

delegato al rischio

Es.:

1 = pochi servizi secondari
5 = pochi servizi primari
5 = molti servizi secondari
7 = molti servizi primari
9 = tutti i servizi

- Perdita di confidenzialità
- Perdita di integrità dei dati
- Mancata disponibilità del servizio
- Mancata tracciabilità rispetto ai responsabili (loss of accountability)

Andando poi a combinare le

Impatto = h(impatto tecnologico)

ss)

Valutare l'impatto

delegato al rischio

Es.:

1 = tracciabilità completa

7 = possibile tracciabilità

9 = anonimato totale

- Perdita di confidenzialità
- Perdita di integrità dei dati
- Mancata disponibilità del servizio
- Mancata tracciabilità rispetto ai responsabili (loss of accountability)

Andando poi a combinare le

Impatto = $h(\text{impatto tecnologico})$

ss)

Valutare l'impatto dell'evento legato al rischio

Owasp suggerisce di valutare

- Impatto tecnologico
- Impatto di business

Andando poi a combinare le

Impatto = $h(\text{impatto tecnologico})$

- Entità del danno finanziario
- Danno di immagine
- Mancata rispondenza a leggi e regolamenti (compliance)
- Violazione della privacy (in termini del numero di persone coinvolte)

Valutare l'impatto

delegato al rischio

Es.:

1 = meno del costo di
eliminare la vulnerabilità
3 = non significativo rispetto
all'utile annuo
7 = significativo rispetto
all'utile annuo
9 = bancarotta

- Entità del danno finanziario
- Danno di immagine
- Mancata rispondenza a leggi e regolamenti (compliance)
- Violazione della privacy (in termini del numero di persone coinvolte)

Andando poi a combinare le

Impatto = $h(\text{impatto tecnologico})$

ss)

Valutare l'impatto

Es.:

1 = minimo

4 = perdita di clienti importanti

5 = perdita del «goodwill»

9 = brand damage

Legato al rischio

- Entità del danno finanziario
- Danno di immagine
- Mancata rispondenza a leggi e regolamenti (compliance)
- Violazione della privacy (in termini del numero di persone coinvolte)

Andando poi a combinare le

Impatto = $h(\text{impatto tecnologico} \times \text{rischio})$

Valutare l'impatto

rigato al rischio

Es.:

2 = violazione minore

5 = violazione evidente

7 = violazione di profilo elevato

- Entità del danno finanziario
- Danno di immagine
- Mancata rispondenza a leggi e regolamenti (compliance)
- Violazione della privacy (in termini del numero di persone coinvolte)

Andando poi a combinare le

Impatto = $h(\text{impatto tecnologico} \times \text{entità del danno})$

Valutare l'impatto

rigato al rischio

Es.:

3 = una persona

5 = centinaia di persone

7 = migliaia di persone

9 = milioni di persone

- Entità del danno finanziario
- Danno di immagine
- Mancata rispondenza a leggi e regolamenti (compliance)

Violazione della privacy (in termini del numero di persone coinvolte)

Andando poi a combinare le

Impatto = $h(\text{impatto tecnologico})$

ss)

Valutare l'impatto dell'evento legato al rischio

Impatto = $h(\text{impatto tecnologico}, \text{impatto di business})$

Possibile approccio secondo OWASP:

h = media aritmetica dei valori da 0 a 9 ottenuti per ciascuna categoria di valutazione, sia per l'impatto tecnologico che per quello di business.

Valutare il livello di rischio

Livello di rischio = $f(\text{probabilità}, \text{impatto})$

Possibile approccio secondo OWASP:

0,1,2 = “low” – 3,4,5 = “average” – 6,7,8,9 = “high”

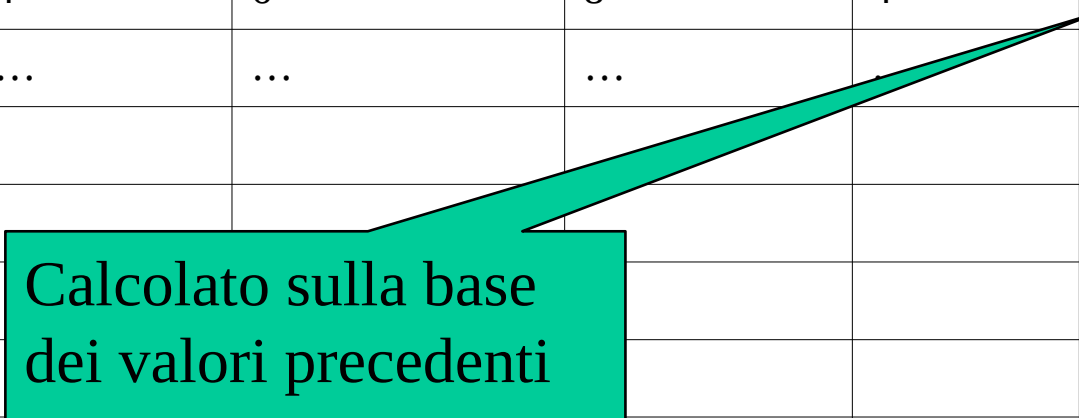
Valutare il livello di rischio

Livello di rischio = $f(\text{probabilità}, \text{impatto})$ con f come da questa tabella

		Probabilità		
		Low	Average	High
Impatto	High	Average	High	Critical
	Average	Low	Average	High
	Low	No risk	Low	Average

OWASP Risk Analysis

Risk ID number	Diffusione threat agent	Importanza della vulnerabilità	Impatto tecnologico	Impatto di Business	Livello di rischio
1					
2					
3					
...
i	4	6	8	4	high
...



Calcolato sulla base dei valori precedenti

Metodologia OWASP: decidere le contromisure

- *stimare l'extra effort di sviluppo per eliminare le vulnerabilità individuate*
- *decidere quali interventi programmare*
- *decidere se effettuare ulteriori test*
- *decidere se dismettere o aggiornare l'applicazione*

Gestione e analisi del rischio informatico

