# Il processo di analisi dei rischi (parte V)

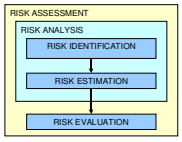
**Marco Domenico Aime**
**< m.aime @ polito.it >**

***Politecnico di Torino***
***Dip. di Automatica e Informatica***

1

## 3. Classificazione dei rischi (risk evaluation)

- **i livelli di rischio sono confrontati contro i criteri di valutazione dei rischi definiti in fase di definizione del contesto**
- **in pratica si vuole determinare:**
  - se un rischio individuato richiede ulteriore trattamento
  - le priorità nel trattamento dei rischi individuati




2

## Considerazioni utili alla classificazione

- **le dimensioni di sicurezza:**
  - se una dimensione non è importante per l'organizzazione (es. segretezza), i rischi con impatto limitato ad essa sono poco rilevanti
- **l'importanza assoluta del processo/attività supportata da un asset o insieme di asset:**
  - si deve dare priorità ai rischi che impattano i processi con importanza più elvata
- **requisiti legali e normativi:**
  - anche in assenza di rischi rilevanti potremmo dover soddisfare requisiti esterni

3

## Considerazioni utili alla classificazione

- **insiemi di best practice:**
  - un utile criterio è il confronto dello stato di rischio con un insieme di best practice
    - si determina sotto quali aspetti lo stato del sistema si discosta dalla best practice e in quale misura
  - in genere definite in termini di controlli suggeriti per tipologia di sistema
    - es. ISO 27002, NIST SP 800-53

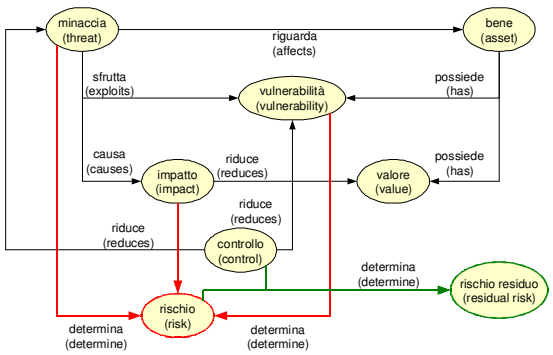
4

## Controlli aggiuntivi e rischio residuo

- **se alla fase di 'trattamento dei rischi' si associa la decisione vera e propria di come trattare i rischi individuati e la pianificazione delle attività necessarie...**
- **... allora la fase di valutazione può includere il suggerimento di ulteriori controlli per mitigare i livelli di rischio**
  - 'rischio residuo' = stima della variazione del rischio dovuta all'introduzione di contromisure aggiuntive

5

## Rischi residui




6

## Controlli aggiuntivi e rischio residuo

- **in genere si costruiscono molteplici scenari di trattamento dei rischi:**
  - adottando strategie di mitigazione diverse
  - suggerendo insiemi di controlli aggiuntivi diversi
  - calcolando per ognuno il rischio residuo
- **la selezione degli scenari è basata sui criteri di rischio identificati nella fase di definizione del contesto**

7

## Documentazione dei risultati

- **la fase di classificazione dei rischi genera i risultati finali del processo di valutazione (risk assessment)**
- **la loro documentazione (unitamente ai risultati delle fasi precedenti, che ne costituiscono il fondamento e giustificazione) è alla base di:**
  - accettazione e valutazione da parte del committente dei risultati dell'intero processo
  - successivo processo di trattamento dei rischi
  - ulteriori processi di valutazione dei rischi
    - super sistema che include il sistema target
    - iterazione della valutazione nel tempo e/o in risposta a cambiamenti nel sistema o contesto

8

## Documentazione dei risultati

- **parte del rapporto finale è indirizzato al management:**
  - a differenza di un'ispezione o audit, che ricercano manchevolezze, non ha forma accusatoria ma sistematica e analitica
  - aiuta a decidere su come cambiare politiche, procedure, budget, personale operativo e gestionale
- **è fondamentale documentare esplicitamente le assunzioni e le scelte fatte in tutte le fasi che hanno determinato i risultati**
  - (tracciabilità dei risultati)

9

## Processo strutturato

- **in termini di processo strutturato si tratta di:**
  1. classificare i rischi
  2. classificare i controlli esistenti
  3. selezionare scenari di trattamento (opzionale)

10

## Processo strutturato

- **classificare i rischi:**
  - tradurre le stime di rischio dalla rappresentazione in termini di dimensioni di sicurezza ad una basata su dimensioni a livello organizzativo:
    - es. norme, vincoli contrattuali, aspetti etici, danni alla reputazione, costi aggiuntivi di ricerca/sviluppo/gestione, processi/attività, ...
  - aggregare i rischi in classi in base a:
    - tipo di impatto e/o livello di rischio
  - assegnare una priorità di trattamento a ogni classe di rischio

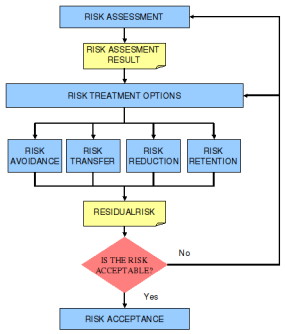
11

## Processo strutturato

- **classificare i controlli esistenti:**
  - confronto dei controlli esistenti con insiemi di:
    - norme, vincoli, o best practice rilevanti
- **selezionare scenari di trattamento (opzionale):**
  - costruire scenari di trattamento alternativi
  - per ogni scenario
    - stimare e classificare i rischi residui
    - classificare il nuovo insieme di controlli

12

## 4. Trattamento dei rischi (risk treatment)




fonte: ISO 27005

14

## Opzioni di trattamento

- **rifiuto (avoidance)**
  - evitare il rischio eliminando causa e/o conseguenze della minaccia/vulnerabilità (es. eliminare funzioni o parti del sistema)
- **trasferimento (transfer)**
  - trasferire il rischio a terze parti (es. assicurazioni, outsourcing)
- **riduzione (reduction)**
  - limitare il rischio implementando controlli aggiuntivi che riducono/eliminano la vulnerabilità e/o l'impatto
- **accettazione (retention)**
  - accettare il rischio potenziale e le sue conseguenze

15

## Valutazione delle opzioni di trattamento

- **la valutazione e scelta delle opzioni di trattamento tiene conto di criteri contrastanti**
  - es. alcune opzioni possono risultare al momento tecnicamente irrealizzabili o richiedere investimenti significativi per il mantenimento
- **produce il piano di trattamento dei rischi (risk treatment plan)**
- **tecniche di analisi:**
  - analisi costi / benefici
  - analisi multi-criterio

18

## Criteri

- **temporali (di acettazione rischi, di implementazione)**
- **finanziari**
- **tecnici**
- **di integrazione (con funzioni e controlli esistenti)**
- **ambientali (spazio disponibile, clima, topografia)**
- **legali (informazioni personali)**
- **legati al personale (personale specializzato)**
- **di usabilità (accettazione da parte del personale)**
- **culturali (accettazione da parte del personale)**
- **etici**

19

## Costi

- **di base, il costo di trattamento deve essere proporzionato ai benefici ottenuti**
- **la stima dei costi deve tener conto di:**
  - costi di acquisizione (hardware, software)
  - costi di implementazione (personale, formazione)
  - costi di mantenimento (servizi di terze parti, politiche e procedure aggiuntive, personale aggiuntivo, performance o funzionalità ridotte a causa della presenza del trattamento)
  - eventuale costi di dismissione in caso di cambiamento nei requisiti

20

## Bilanciamento

- **in genere è necessaria una combinazione di opzioni**
  - es. ridurre la probabilità di una minaccia, ridurre l'impatto associato, poi trasferire o accettare il rischio residuo
- **è utile mantenere un bilanciamento tra le diverse tipologie di controlli**
  - preventivi / investigativi / reattivi
  - tecnici / procedurali / gestionali
  - aiuta a mantenere un livello di sicurezza più efficace, efficente e robusto

21

## Risorse finanziarie

- **alcuni trattamenti possono risultare necessari ma non implementabili nei limiti delle risorse finanziarie disponibili:**
  - devono essere identificati in attesa di ulteriori risorse, o per giustificare la richiesta dirisorse addizionali

22

## Controlli esistenti

- **alcuni controlli esistenti possono risultare insufficienti:**
  - a volte è più costoso rimpiazzare un controllo insufficiente rispetto a lasciarlo al suo posto e aggiungere un altro controllo

23

## Controlli esistenti

- **alcuni controlli esistenti possono risultare eccessivi:**
  - la loro rimozione deve essere considerata molto attentamente
    - confronto tra costi di rimozione e costi di mantenimento
    - dato che i controlli hanno influenze reciproche, vanno valutati gli effetti complessivi della rimozione
    - un controllo può essere utile al di fuori del contesto di analisi

24

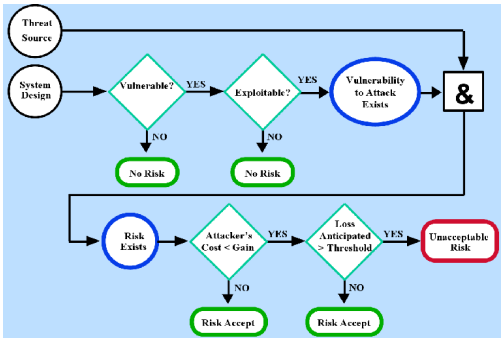
## Pianificazione

- **il piano di trattamento dei rischi deve identificare chiaramente priorità e ordine delle azioni da intraprendere**
- **in genere, la definizione e analisi di scenari di trattamento alternativi facilita enormemente il confornto tra opzioni di trattamento e la costruzione del piano di trattamento dei rischi**

25

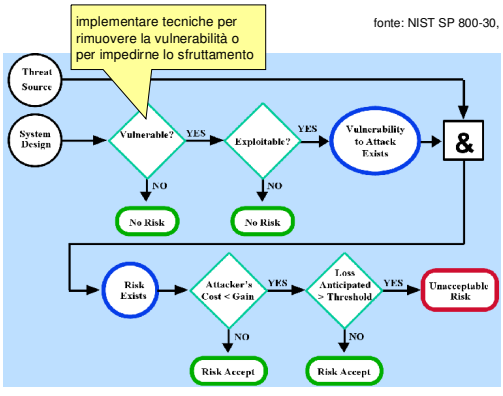
## Opzioni di riduzione

fonte: NIST SP 800-30, pp. 28

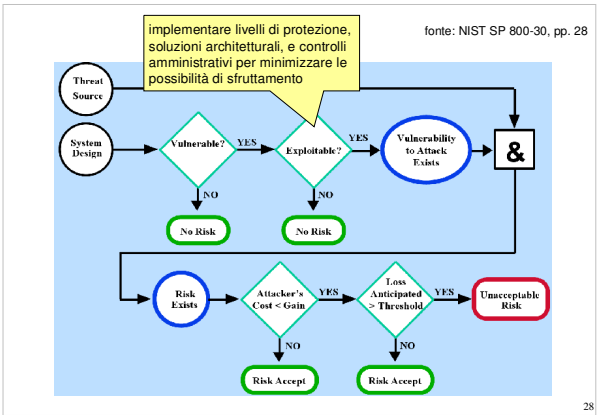


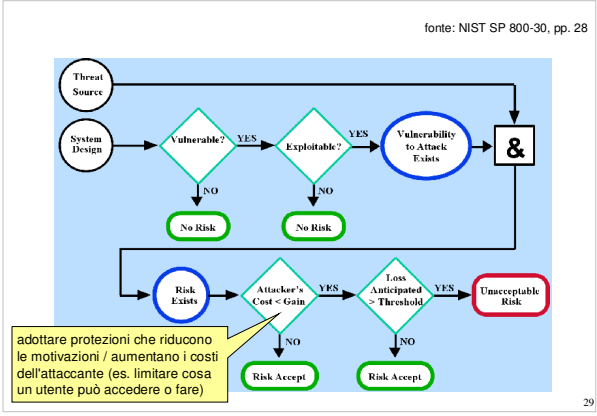

26

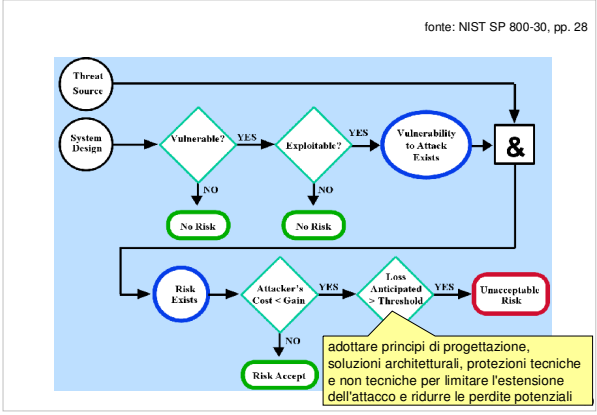
fonte: NIST SP 800-30, pp. 28




27


fonte: NIST SP 800-30, pp. 28
implementare livelli di protezione, soluzioni architetturali, e controlli amministrativi per minimizzare le possibilità di sfruttamento
Threat Source
System Design
Vulnerable?
YES
Exploitable?
YES
Vulnerability to Attack Exists
&
NO
NO
No Risk
No Risk
Risk Exists
Attacker's Cost < Gain
YES
Loss Anticipated > Threshold
YES
Unacceptable Risk
NO
NO
Risk Accept
Risk Accept
28


fonte: NIST SP 800-30, pp. 28
Threat Source
System Design
Vulnerable?
YES
Exploitable?
YES
Vulnerability to Attack Exists
&
NO
NO
No Risk
No Risk
Risk Exists
Attacker's Cost < Gain
YES
Loss Anticipated > Threshold
YES
Unacceptable Risk
NO
NO
Risk Accept
Risk Accept
adottare protezioni che riducono le motivazioni / aumentano i costi dell'attaccante (es. limitare cosa un utente può accedere o fare)
29


fonte: NIST SP 800-30, pp. 28
Threat Source
System Design
Vulnerable?
YES
Exploitable?
YES
Vulnerability to Attack Exists
&
NO
NO
No Risk
No Risk
Risk Exists
Attacker's Cost < Gain
YES
Loss Anticipated > Threshold
YES
Unacceptable Risk
NO
Risk Accept
adottare principi di progettazione, soluzioni architetturali, protezioni tecniche e non tecniche per limitare l'estensione dell'attacco e ridurre le perdite potenziali

## Rischio residuo

cfr MAGERIT v2, tecniche (eng version), pp 11

- **calcolo del rischio residuo in MAGERIT:**

| | qualitativa | quantitativa |
|---|---|---|
| **efficienza dei controlli (safeguard efficiency)** | numeri reali: e in [0,1], divisi in:<br>ei = efficienza contro l'impatto, e<br>ef = efficienza control la frequenza | numeri reali: e in [0,1]<br>(1 – ei ) × (1 – ef ) = 1 – e |
| **degradazioni residue (residual degradation)** | dr = d × (1 - ei) | |
| **impatti residui (residual impact)** | residual_impact = v_round(x × dr) | residual_impact = impact x (1 – ei) |
| | l'impatto residuo accumulato è calcolato usando l'impatto accumulato<br>l'impatto residuo riflesso è calcolato usando l'impatto riflesso | |
| **frequenze residue (residual frequency)** | residual_frequency = fk,<br>con k = round( j × (1 – ef) ) | residual_frequency = frequency x (1–ef) |
| **rischi residui (residual risk)** | residual_risk =<br>ℜ(residual_impact, residual_frequency) | residual_risk = residual_impact x residual_frequency |
| | il rischio residuo accumulato è calcolato usando l'impatto residuo accumulato<br>il rischio residuo riflesso è calcolato usando l'impatto residuo riflesso | |

31

## Analisi costi / benefici

- **richiede:**
  1. identificare le conseguenze della non implementazione dell'opzione di trattamento (rischio)
  2. identificare le conseguenze dell'implementazione (rischio residuo)
  3. stimare il costo dell'implementazione

32

## Esempio

| | |
|---|---|
| Cost for enabling system audit feature—No cost, built-in feature | $ 0 |
| Additional staff to perform audit review and archive, per year | $ XX,XXX |
| Training (e.g., system audit configuration, report generation) | $ X,XXX |
| Add-on audit reporting software | $ X,XXX |
| Audit data maintenance (e.g., storage, archiving), per year | $ X,XXX |
| Total Estimated Costs | $ XX,XXX |

fonte: NIST SP 80030, pp C-1

33

## Piano di trattamento

- **procedura generale per lo sviluppo di un piano di trattamento dei rischi:**
  1. prioritizzare gli obiettivi di trattamento (in base ai risultati del processo di valutazione dei rischi)
  2. valutare le opzioni di trattamento e i rischi residui (tipicamente in base ai risultati della valutazione)
  3. effettuare un'analisi costi benefici
  4. selezionare le opzioni di trattamento
  5. identificare le responsabilità
  6. identificare le risorse necessarie
  7. definire un piano temporale di attuazione

35

## Esempio

| (1) Risk (Vulnerability/ Threat Pair) | (2) Risk Level | (3) Recommended Controls | (4) Action Priority | (5) Selected Planned Controls | (6) Required Resources | (7) Responsible Team/Persons | (8) Start Date/ End Date | (9) Maintenance Requirement/ Comments |
|---|---|---|---|---|---|---|---|---|
| Unauthorized users can telnet to XYZ server and browse sensitive company files with the *guest* ID. | High | • Disallow inbound telnet<br>• Disallow 'world' access to sensitive company files<br>• Disable the *guest* ID or assign difficult-to-guess password to the *guest* ID | High | • Disallow inbound telnet<br>• Disallow 'world' access to sensitive company files<br>• Disabled the *guest* ID | 10 hours to reconfigure and test the system | John Doe, XYZ server system administrator; Jim Smith, company firewall administrator | 9-1-2001 to 9-2-2001 | • Perform periodic system security review and testing to ensure adequate security is provided for the XYZ server |

(1) The risks (vulnerability/threat pairs) are output from the risk assessment process
(2) The associated risk level of each identified risk (vulnerability/threat pair) is the output from the risk assessment process
(3) Recommended controls are output from the risk assessment process
(4) Action priority is determined based on the risk levels and available resources (e.g., funds, people, technology)
(5) Planned controls selected from the recommended controls for implementation
(6) Resources required for implementing the selected planned controls
(7) List of team(s) and persons who will be responsible for implementing the new or enhanced controls
(8) Start date and projected end date for implementing the new or enhanced controls
(9) Maintenance requirement for the new or enhanced controls after implementation.

fonte: NIST SP 80030, pp C-1

36