Gli scenari in ambito IT: stato dell'arte di uno strumento

G.Bertocchi, F.Della Mea, A.Piamonte

26 MAGGIO 2023

Perchè un focus sugli scenari

- I metodi di valutazione del rischio ICT richiedono una fase di identificazione dei rischi stessi
- Le norme ed i framework si stanno sempre più orientando all'approccio "basato su scenari"
- Alcuni modelli di valutazione definiscono le caratteristiche (attributi) che devono essere descritti negli scenari di rischio
- A seconda del modello di valutazione del rischio scelto, alcune caratteristiche devono essere quantificate, non solo descritte

Temi di discussione

- I metodi di valutazione del rischio ICT richiedono una fase di identificazione dei rischi stessi
- Le norme ed i framework si stanno sempre più orientando all'approccio "basato su scenari"
- Alcuni modelli di valutazione definiscono le caratteristiche (attributi) che devono essere descritte negli scenari di rischio
- Le caratteristiche devono essere quantificate, non solo descritte

Agenda

- Introduzione: scenari e valutazione del rischio
- Le nuove ISO27002 e 27005
- Gli scenari di rischio ISACA e l'utilizzo nel modello quantitativo FAIR
- Altri spunti: MITRE, DORA

Agenda

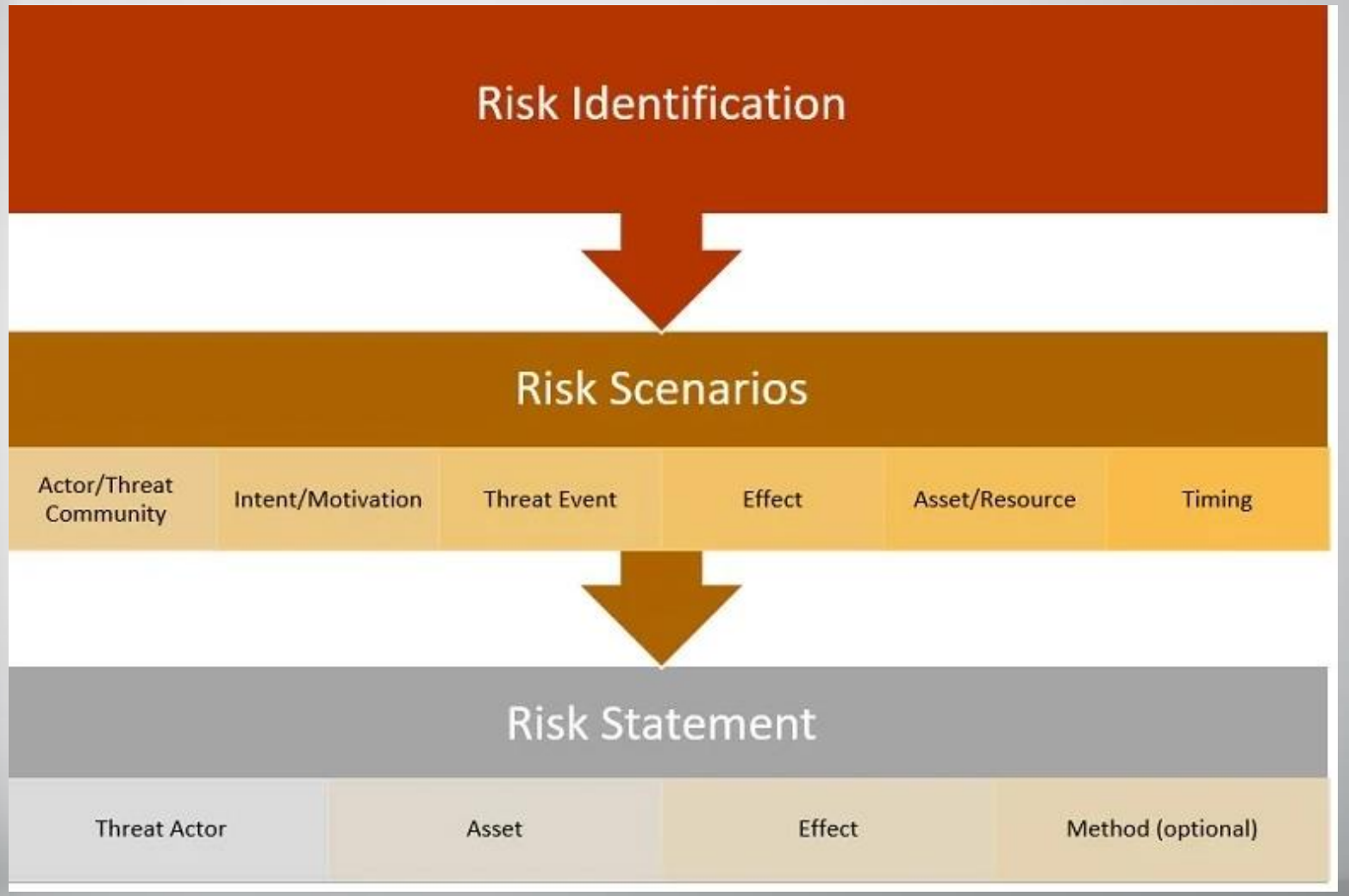
- Introduzione: scenari e valutazione del rischio
- ISO27002 e 27005
- Gli scenari di rischio ISACA e l'utilizzo nel modello quantitativo FAIR
- Altri spunti: MITRE, DORA
- Considerazioni conclusive

Per iniziare: una definizione

- *Risk management is both art and science. There is no better example of risk as an art form than risk scenario building and statement writing. Scenario building is the process of identifying the critical factors that contribute to an adverse event and crafting a narrative that succinctly describes the circumstances and consequences if it were to happen.*

- How to Write Strong Risk Scenarios and Statements
- **Author:** Tony Martin-Vegue, CISM, CISSP, Open FAIR 29 September 2021
- How to Write Strong Risk Scenarios and Statements *https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-31/how-to-write-strong-risk-scenarios-and-statements 2/8*

Cerchiamo di migliorare la definizione
(fonte ISACA)



I possibili componenti di un risk statement (fonte ISACA)

- **Attore della minaccia:** Descrive l'individuo o il gruppo che può agire contro un bene. Un attore della minaccia può essere un individuo interno all'organizzazione, oppure esterno, come un'organizzazione di criminali informatici. L'intento può essere : azioni dolose, non intenzionali o accidentali, anche gli eventi di forza maggiore sono considerati attori di minacce.
- **Asset:** un asset è qualsiasi cosa di valore per l'organizzazione, tangibile o intangibile. Ad esempio, persone, denaro, attrezzature fisiche, proprietà intellettuale, dati e reputazione.
- **Effetto:** In genere, nel rischio tecnologico, un evento avverso può compromettere la riservatezza, l'integrità, la disponibilità o la privacy di un asset. L'effetto potrebbe estendersi anche al rischio d'impresa, al rischio operativo e ad altre aree.
- **Metodo:** Se lo scenario di rischio lo richiede, è possibile definire anche un metodo. Ad esempio, se l'analisi del rischio riguarda specificamente l'hacking attraverso l'iniezione SQL, quest'ultima può essere inclusa come metodo.

Esempi di risk statement

- *Un dipendente condivide dati riservati relativi alla produzione con la concorrenza, con conseguente perdita di vantaggio competitivo.*
- *Dei criminali informatici infettano gli endpoint con ransomware che cripta i file e blocca le postazioni di lavoro, con conseguente interruzione delle operazioni.*
- *Dei criminali informatici copiano dei dati riservati dei clienti e minacciano di renderli pubblici a meno che non venga pagato un riscatto, con conseguenti costi di risposta, danni alla reputazione e potenziali cause legali.*
- ***CONTENGONO TUTTI L'INDICAZIONE DI UN LOSS EVENT***

ISO 27001

- Iso 27001:2022- *(Information security, cybersecurity and privacy protection — Information security management systems — Requirements*) non cita la parola scenario e dedica poche (ma significative) righe al rischio

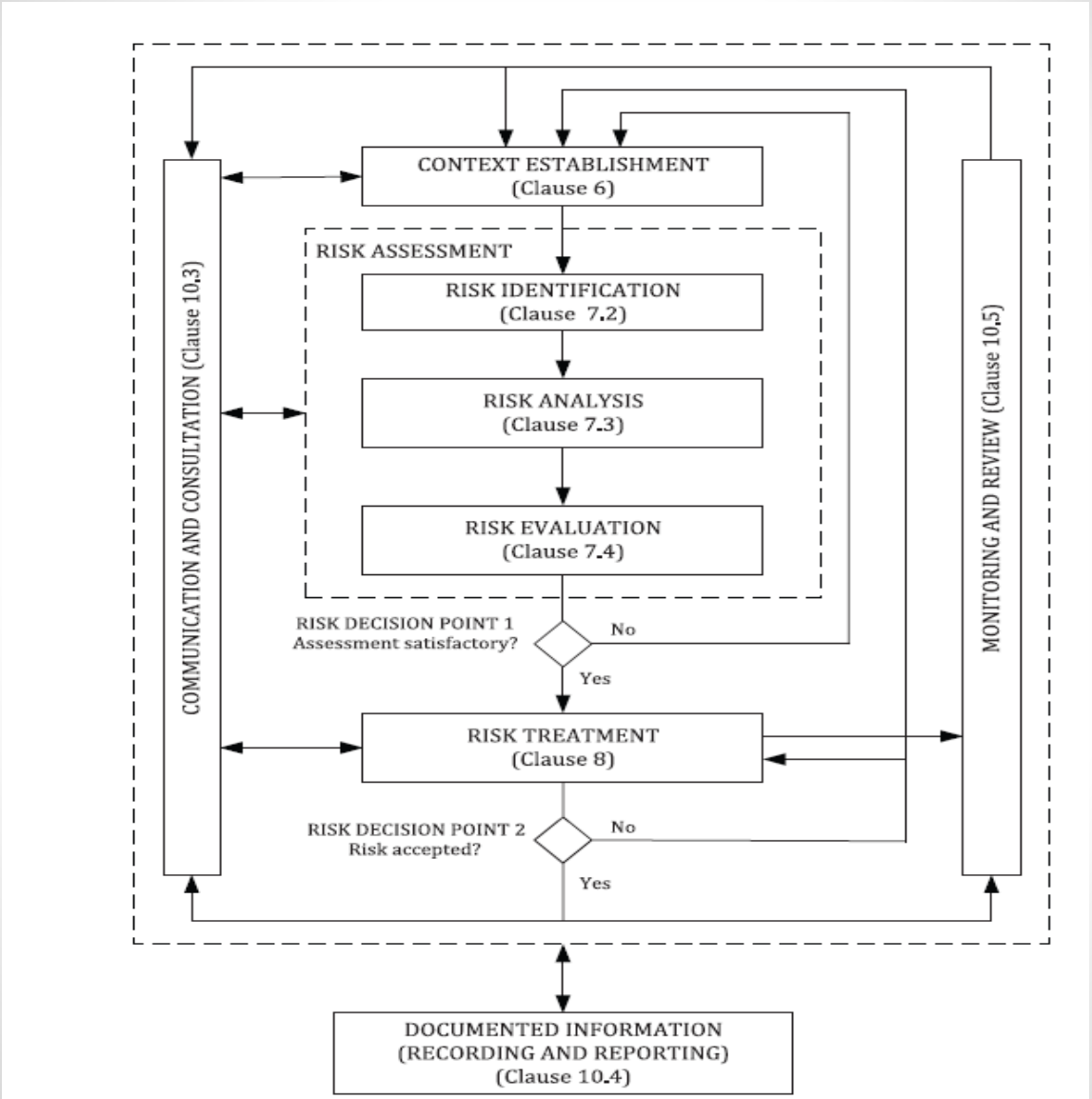
- **6 Planning** *(una delle 2 pianificazioni espressamente previste)*
- **6.1 Actions to address risks and opportunities**
  - **6.1.1 General**
  - **6.1.2 Information security risk assessment**
  - **6.1.3 Information security risk treatment**
- *6.2 Information security objectives and planning to achieve them*

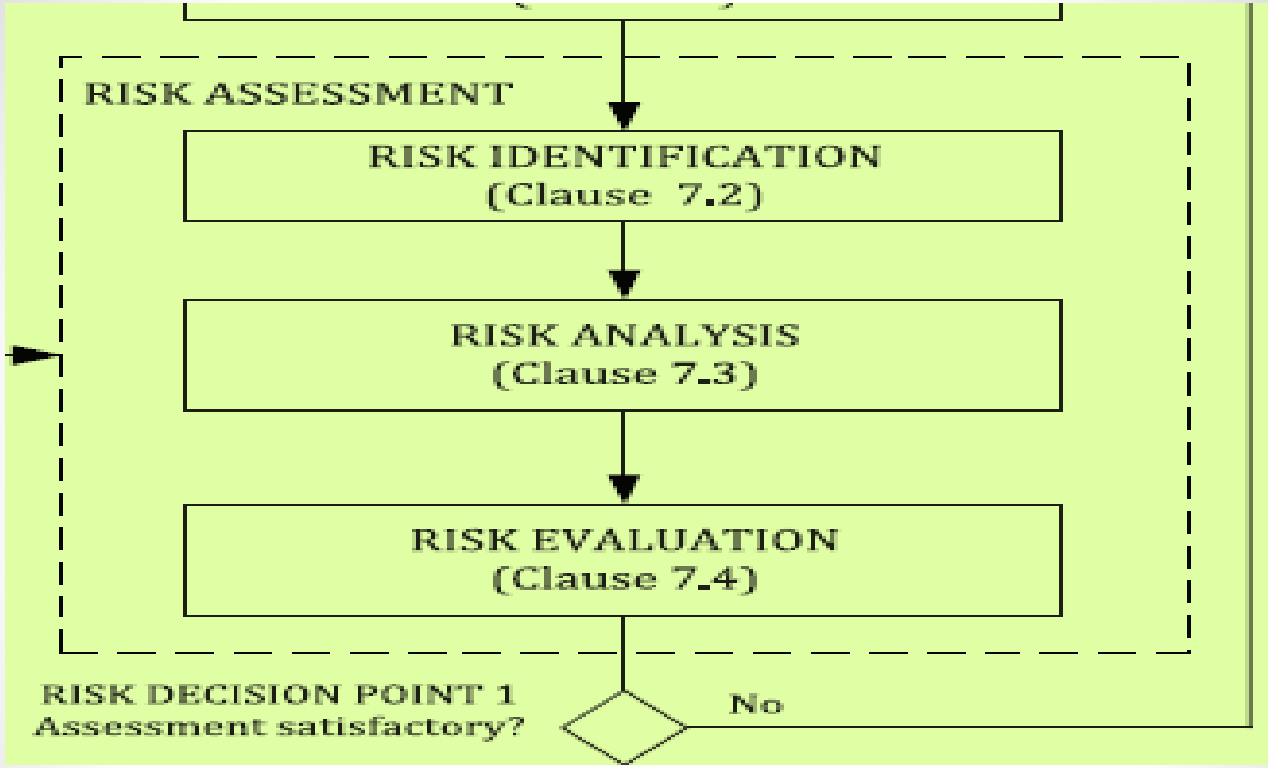
- **8 Operation** *(2 delle 3 attività operative espressamente previste)*
- *8.1 Operational planning and control*
- **8.2 Information security risk assessment**
- **8.3 Information security risk treatment**

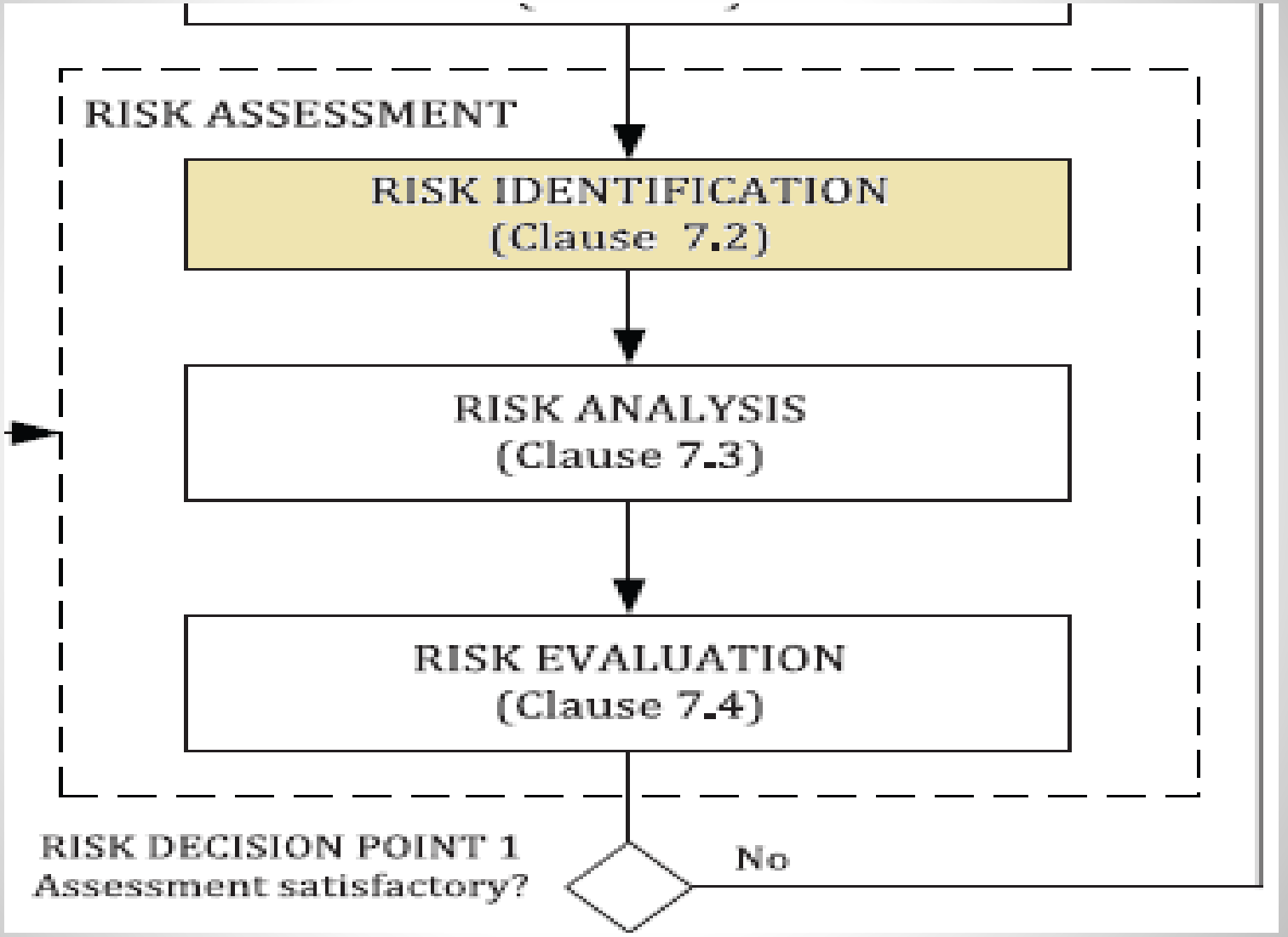
ISO 27005

- ISO 27005:2022 (*Information security, cybersecurity and privacy protection — Guidance on managing information security risks)* introduce il concetto di risk scenario e ne fa uno degli elementi fondanti della metodologia.
- LE DEFINIZIONI
- **3.1.4**
- **risk scenario**
- sequence or combination of *events* (3.1.11) leading from the initial cause to the unwanted *consequence* (3.1.14)
- **3.1.11**
- **event**
- occurrence or change of a particular set of circumstances
- Note 1 to entry: An event can have one or more occurrences, and can have several causes and several *consequences* (3.1.14).
- Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.
- **3.1.14**
- **consequence**
- outcome of an *event* (3.1.11) affecting objectives
- Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.
- Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.
- Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

ISO 27005 Information security risk management process




RISK ASSESSMENT
RISK IDENTIFICATION
(Clause 7.2)
RISK ANALYSIS
(Clause 7.3)
RISK EVALUATION
(Clause 7.4)
RISK DECISION POINT 1
Assessment satisfactory?
No


RISK ASSESSMENT
RISK IDENTIFICATION
(Clause 7.2)
RISK ANALYSIS
(Clause 7.3)
RISK EVALUATION
(Clause 7.4)
RISK DECISION POINT 1
Assessment satisfactory?
No

ISO 27005 Approcci per l'identificazione dei rischi

- ISO/IEC 27001 does not mandate a particular approach to be used to fulfil the requirements in ISO/IEC 27001:2022, 6.1.2. **(***Information security risk assessment)*
- Nevertheless, there are two main approaches for assessment: an event-based approach and an asset-based approach.
- ISO/IEC 27001:2022, 6.1.2 c), requires the organization to define and apply an information security risk assessment process that identifies the information security risks.
- There are two approaches commonly used to perform risk identification.
- a) Event-based approach: identify strategic scenarios through a consideration of risk sources, and how they use or impact interested parties to reach those risk's desired objective.
- b) Asset-based approach: identify operational scenarios, which are detailed in terms of assets, threats and vulnerabilities.

ISO 27005 Approcci per identificare i rischi e costruire gli scenari (1)

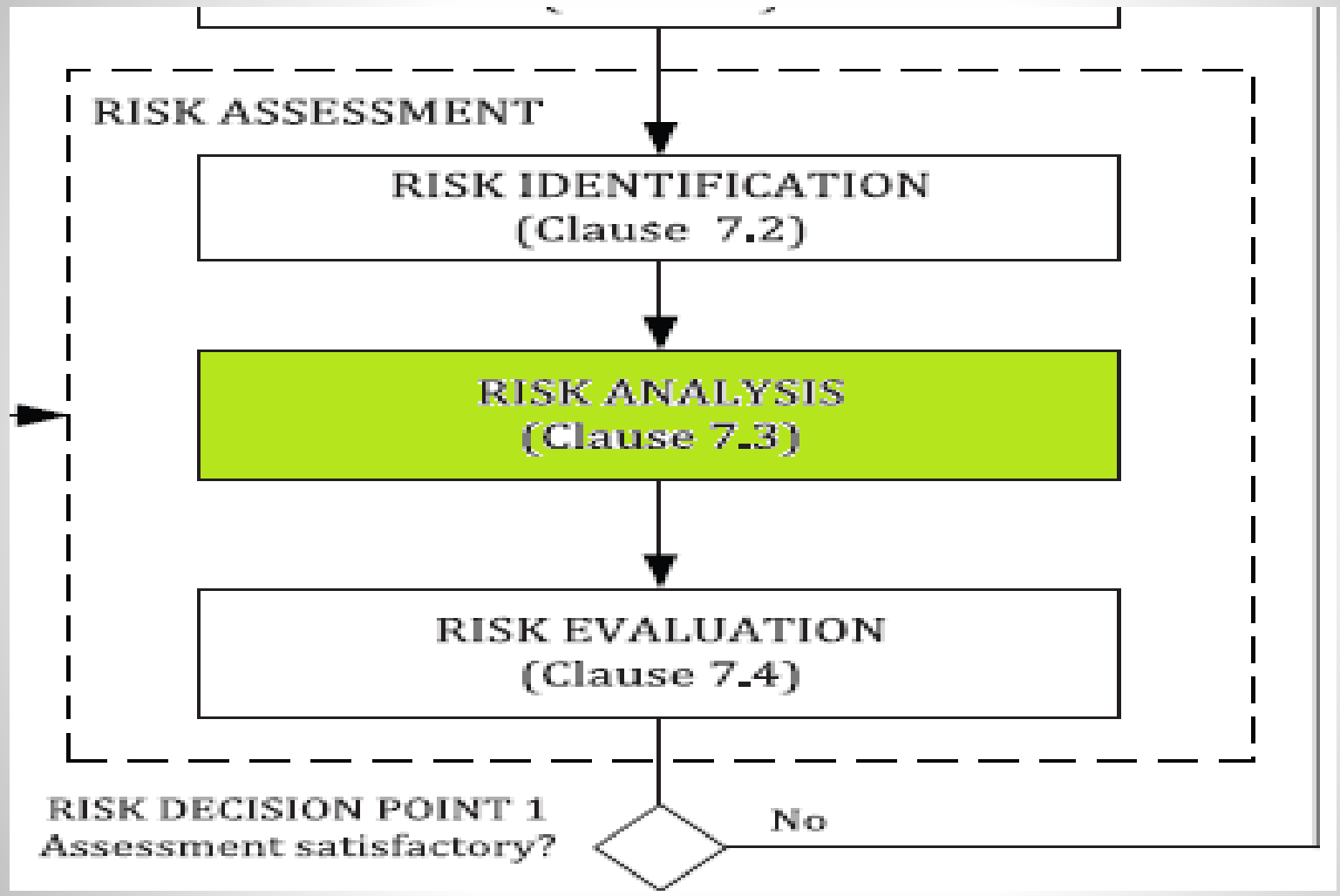
- In un approccio event-based, i rischi possono essere identificati e stimati attraverso una valutazione degli eventi e delle conseguenze. Gli eventi e le conseguenze possono spesso essere determinati dall'analisi delle preoccupazioni del top management, dei proprietari del rischio e dei requisiti identificati nella determinazione del contesto dell'organizzazione (ISO/IEC 27001:2022, clausola 4). I colloqui con il top management e con i responsabili di un processo aziendale possono aiutare a identificare non solo gli eventi e le conseguenze rilevanti, ma anche i proprietari del rischio.
- Un approccio event-based può stabilire scenari di alto livello o strategici senza dover dedicare molto tempo all'identificazione degli asset a livello dettagliato. Ciò consente all'organizzazione di concentrare gli sforzi per il trattamento dei rischi critici. La valutazione degli eventi con questo approccio può avvalersi di dati storici qualora i rischi rimangano immutati per lunghi periodi. Nel caso di rischi per i quali i dati storici non siano disponibili o affidabili, le indicazioni basati sulla conoscenza e l'esperienza degli esperti o l'indagine delle fonti di rischio possono aiutare la valutazione.

ISO 27005 Approcci per identificare i rischi e costruire gli scenari (2)

- Con un approccio asset-based, i rischi possono essere identificati e valutati attraverso un'analisi degli asset, delle minacce e delle vulnerabilità. Un asset è qualsiasi cosa che abbia un valore per l'organizzazione e che quindi richieda protezione. Gli asset devono essere identificati tenendo conto che un sistema informativo è costituito da attività, processi e informazioni da proteggere. Gli asset possono essere identificati come asset primari e di supporto in base alla loro tipologia e priorità, evidenziando le loro dipendenze, nonché le loro interazioni con le fonti di rischio e l'organizzazione. Una minaccia sfrutta una vulnerabilità di un asset per compromettere la riservatezza, l'integrità e/o la disponibilità delle relative informazioni. Per le fasi successive della valutazione del rischio, è necessario stilare un elenco di asset associati alle informazioni e alle strutture di elaborazione delle informazioni.
- L'approccio asset-based può identificare le minacce e le vulnerabilità specifiche degli asset e consente all'organizzazione di determinare un trattamento del rischio specifico a livello dettagliato.

ISO 27005 Approcci per identificare i rischi e costruire gli scenari (3)

- I due approcci differiscono solo per quanto riguarda il livello a cui viene avviata l'identificazione. Entrambi gli approcci possono descrivere lo stesso scenario di rischio, ad esempio a livello di dettaglio di un asset informativo e al livello dell'intera organizzazione.
- L'identificazione delle fonti di rischio con approccio event-based richiede tipicamente di passare dal livello generale dello scenario al livello di dettaglio.
- Mentre una valutazione asset-based dovrà risalire dall'asset allo scenario, al fine di fornire visibilità sul modo in cui le conseguenze si accumulano.
- L'identificazione del rischio deve considerare i rischi indipendentemente dal fatto che la loro fonte sia sotto il controllo dell'organizzazione. Quando si valutano scenari di rischio complessi, è opportuno condurre una valutazione iterativa del rischio. Il primo ciclo dovrebbe concentrarsi sulle osservazioni di alto livello e i cicli successivi dovrebbero affrontare ulteriori livelli di dettaglio fino a quando non si possono identificare le cause profonde dei rischi.


RISK ASSESSMENT
RISK IDENTIFICATION
(Clause 7.2)
RISK ANALYSIS
(Clause 7.3)
RISK EVALUATION
(Clause 7.4)
RISK DECISION POINT 1
Assessment satisfactory?
No

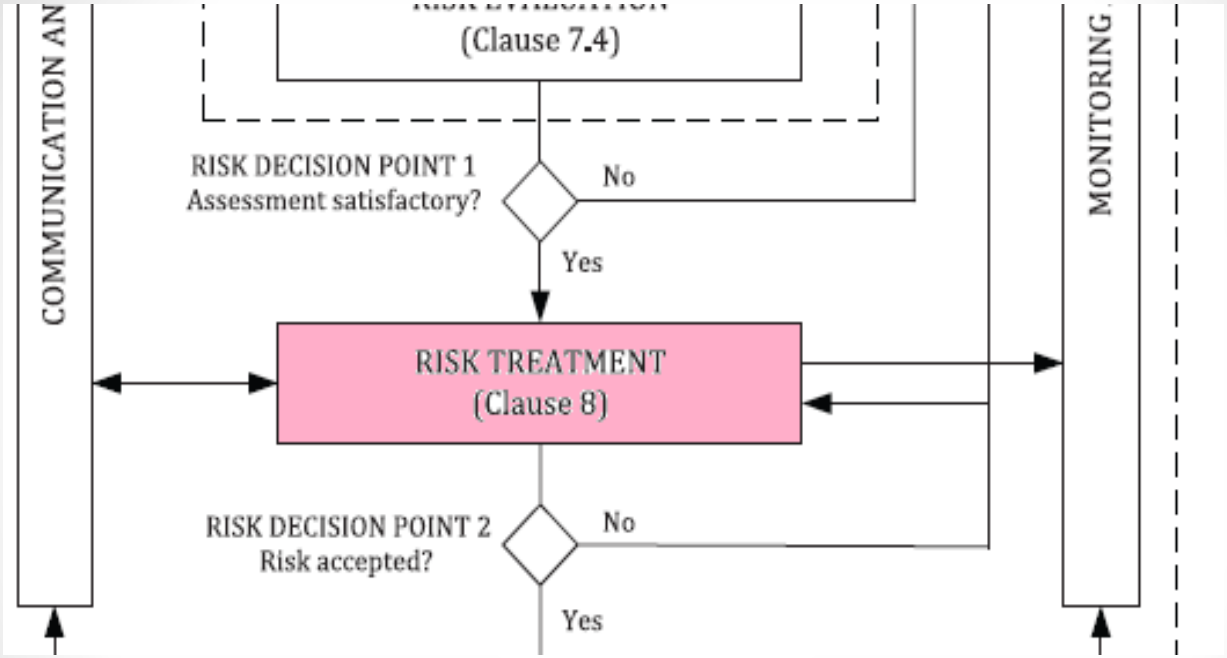
ISO 27005 Uso degli scenari (1)

- **7.3.2 Assessing potential consequences**
- NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 d) 1).
- Input: A list of identified relevant event or risk scenarios, including identification of risk sources, and business processes, business objectives and consequence criteria. Furthermore, lists of all existing controls, their effectiveness, implementation and usage status.
- Action: The consequences resulting from the failure to adequately preserve confidentiality, integrity or availability of information should be identified and assessed.
- ……
- Output: A list of potential consequences related to risk scenarios with their consequences related to assets or events, depending on the approach applied.
- **7.3.3 Assessing likelihood**
- NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 d) 2).
- Input: A list of identified relevant event or risk scenarios, including identification of risk sources, and business processes, business objectives and likelihood criteria. Additionally, lists of all existing controls, their effectiveness, implementation and usage status.
- Action: The likelihood of occurrence of possible or actual scenarios should be assessed and expressed using established likelihood criteria.
- ……
- Output: A list of events or risk scenarios complemented by likelihoods that these occur.

ISO 27005 Uso degli scenari (2)

- **7.3.4 Determining the levels of risk**
- NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 d) 3).
- Input: A list of risk scenarios with their consequences related to assets or events and their likelihood *(quantitative or qualitative).*
- Action: The level of risk should be determined as a combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios.
- ……
- Output: A list of risks with level values assigned.
- Implementation guidance:
- The level of risk can be determined in many possible ways. It is commonly determined as a combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios. Alternative calculations can include an asset value as well as likelihood and consequence. In addition, *the calculation is not necessarily linear, e.g. it can be likelihood squared combined with consequence.* In any case the level of risk should be determined using the criteria established as described in 6.4.3.4.

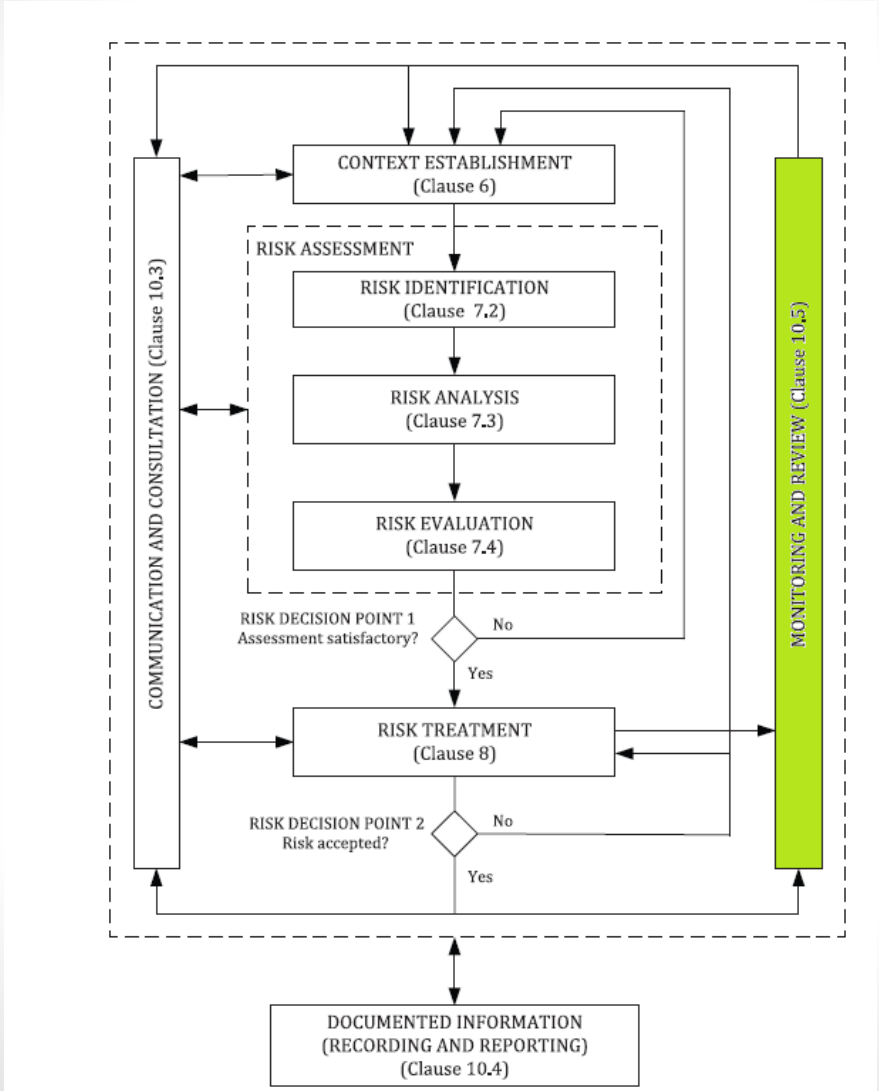
ISO 27005


COMMUNICATION AN
(Clause 7.4)
RISK DECISION POINT 1
Assessment satisfactory?
No
Yes
RISK TREATMENT
(Clause 8)
RISK DECISION POINT 2
Risk accepted?
No
Yes
MONITORING

ISO 27005 Uso degli scenari (3)

- **8 Information security risk treatment process**
- **8.1 General**
- **……..**
- **8.2 Selecting appropriate information security risk treatment options**
- NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 a).
- Input: A list of prioritized risks with event or risk scenarios that lead to those risks.
- Action: Risk treatment options should be chosen.
- Trigger: Selecting appropriate information security risk treatment options becomes necessary if no risk treatment plan is existing or the plan is incomplete.
- Output: A list of prioritized risks with the selected risk treatment options.

ISO 27005


CONTEXT ESTABLISHMENT
(Clause 6)
RISK ASSESSMENT
RISK IDENTIFICATION
(Clause 7.2)
RISK ANALYSIS
(Clause 7.3)
RISK EVALUATION
(Clause 7.4)
RISK DECISION POINT 1
Assessment satisfactory?
No
Yes
RISK TREATMENT
(Clause 8)
RISK DECISION POINT 2
Risk accepted?
No
Yes
COMMUNICATION AND CONSULTATION (Clause 10.3)
MONITORING AND REVIEW (Clause 10.5)
DOCUMENTED INFORMATION
(RECORDING AND REPORTING)
(Clause 10.4)

ISO 27005 Uso degli scenari nel Monitoring

- **10.5 Monitoring and review**
- **10.5.1 General**
- NOTE This subclause relates to ISO/IEC 27001:2022, 9.1.
- The organization's monitoring process (see ISO/IEC 27001:2022, 9.1) should encompass all aspects of the risk assessment and risk treatment processes for the purposes of:
  - a) ensuring that the risk treatments are effective, efficient and economical in both design and operation;
  - b) obtaining information to improve future risk assessments;
  - c) analysing and learning lessons from incidents (including near misses), changes, trends, successes and failures;
  - d) detecting changes in the internal and external context, including changes to risk criteria and the risks themselves, which can require revision of risk treatments and priorities;
  - e) identifying emerging risks.
- Retained risk scenarios, coming from the risk management activities, can be transposed into monitoring scenarios *in order to ensure an effective monitoring process*. Further details about monitoring scenarios are given in A.2.7.

ISO 27005 Uso degli scenari nel Monitoring

- **10.5.2 Monitoring and reviewing factors influencing risks**
- NOTE This subclause relates to ISO/IEC 27001:2022, 9.1.
- Input: All risk information obtained from the risk management activities.
- Action: Risks and their factors (i.e. value of assets, consequences, threats, vulnerabilities, likelihood of occurrence) should be monitored and reviewed to identify any changes in the context of the organization at an early stage, and to maintain an overview of the complete risk picture.
- ……
- Output: Continual alignment of the management of risks with the organization's business objectives, and with risk acceptance criteria.
- Implementation guidance:
- ……
- Risks are not static. Event scenarios, asset values, threats, vulnerabilities, likelihoods and consequences can change abruptly without any indication. Constant monitoring should be carried out to detect these changes.
- ……

ISO 27005 Componenti della valutazione dei rischi

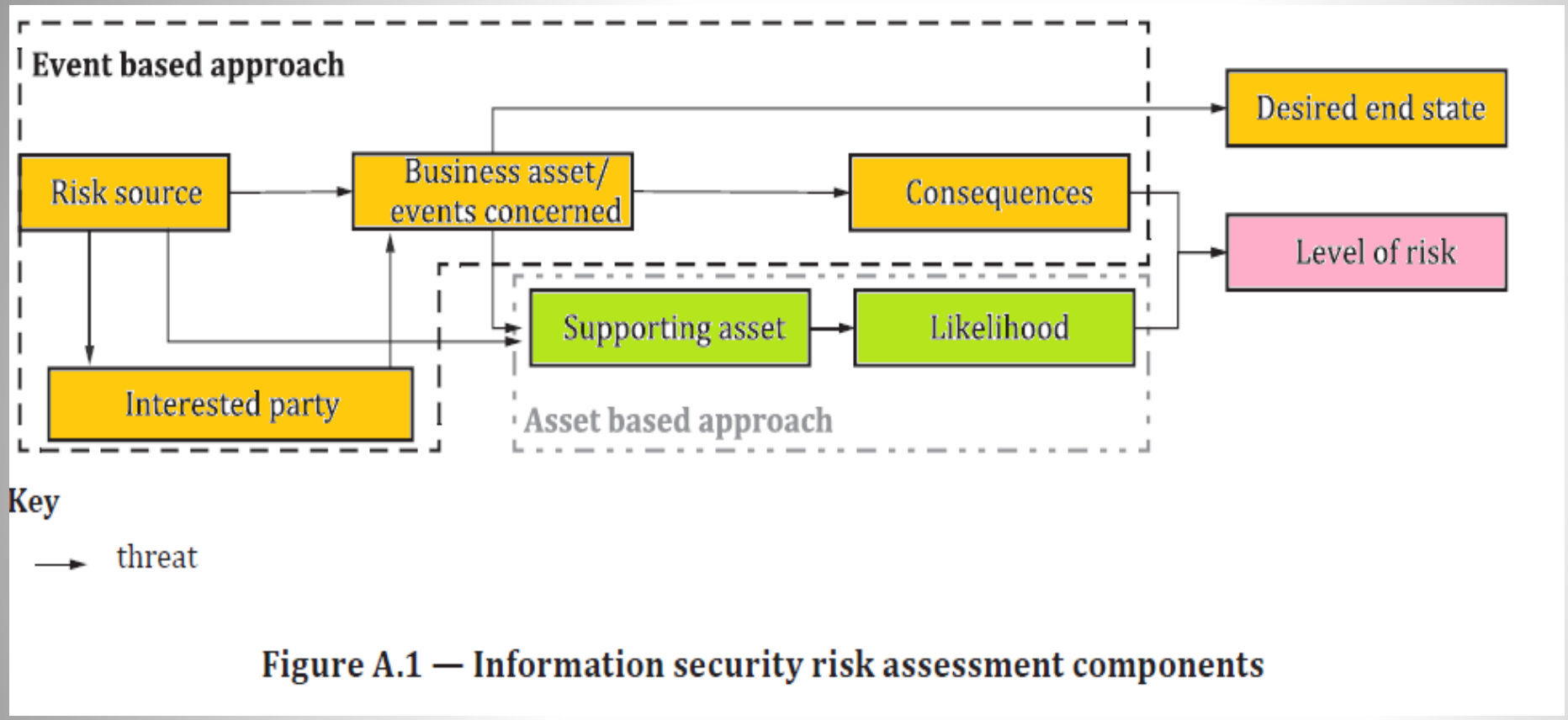


Figure A.1 — Information security risk assessment components

ISO 27005 (Appendice A) Event-based approach and ecosystem

- **A.2.4.1 Ecosystem**
- In un approccio event-based , gli scenari dovrebbero essere costruiti analizzando i diversi percorsi, rilevanti per le interazioni tra l'organizzazione e le parti interessate, che formano un ecosistema che le fonti di rischio possono utilizzare per raggiungere gli asset aziendali e il loro DES (Desired End State).
- Un numero crescente di metodi di attacco utilizza i collegamenti più vulnerabili di tale ecosistema per raggiungere i propri obiettivi.
- Le parti interessate nell'ambito dell'ISMS che devono essere prese in considerazione quando si analizzano gli scenari di rischio possono essere di due tipi:
- - parti esterne, tra cui: clienti; partner, co-appaltatori; fornitori di servizi (subappaltatori, fornitori)…….
- - parti interne, tra cui: servizi di supporto proposti dalla gestione IT; entità commerciali che utilizzano dati commerciali; filiali (in particolare, situate in altri Paesi)……..
- L'obiettivo dell'identificazione delle parti interessate è ottenere una visione chiara dell'ecosistema, al fine di individuare i soggetti più vulnerabili. L'individuazione dell'ecosistema dovrebbe essere affrontata come studio preliminare del rischio. La Figura A.3 mostra l'identificazione delle parti interessate dell'ecosistema.

DES (desired end state) e target objectives

Table A.8 — Example classification of motivations to express the DES

Conquer	Long-term capture of resources or economic markets, gaining political power or imposing values
Acquire	Predatory approach, resolutely offensive, driven by capturing resources or benefits
Prevent	Offensive approach to limit the actions of a third party
Maintain	Efforts to maintain an ideological, political, economic or social situation
Defend	Adopting a strictly defensive fallback stance, or an explicitly threatening attitude (e.g. intimidation) in order to prevent the aggressive behaviour of a clearly designated opponent or prevent their action by slowing them down, etc.
Survive	Protecting an entity at all costs, which can lead to extremely aggressive actions

Table A.9 — Examples of target objectives

Target objective	Description
Spying	Intelligence operation (state-related, economic). In many cases, the attacker aims for a long-term installation in the information system and with total discretion. Weaponry, space, aeronautics, the pharmaceutical sector, energy and certain activities of the State (economics, finance, and foreign affairs) are privileged targets.
Strategic pre-positioning	Pre-positioning generally aimed at an attack over the long term, without the end purpose being clearly established (e.g. compromising telecom operator networks, infiltration of mass information internet sites in order to launch an operation of political or economic influence with a strong echo). Sudden and massive compromising of computers in order to form a botnet can be affiliated with this category.
Influence	Operation aimed at diffusing false information or at altering it, mobilizing opinion leaders on the social networks, destroying reputations, disclosing confidential information, degrading the image of an organization or of a State. The end purpose is generally to destabilize or modify perceptions.
Obstacle to func-	Sabotage operation aimed for example at making an Internet site unavailable, causing information

ISO 27005 (Appendice A) Ecosystem

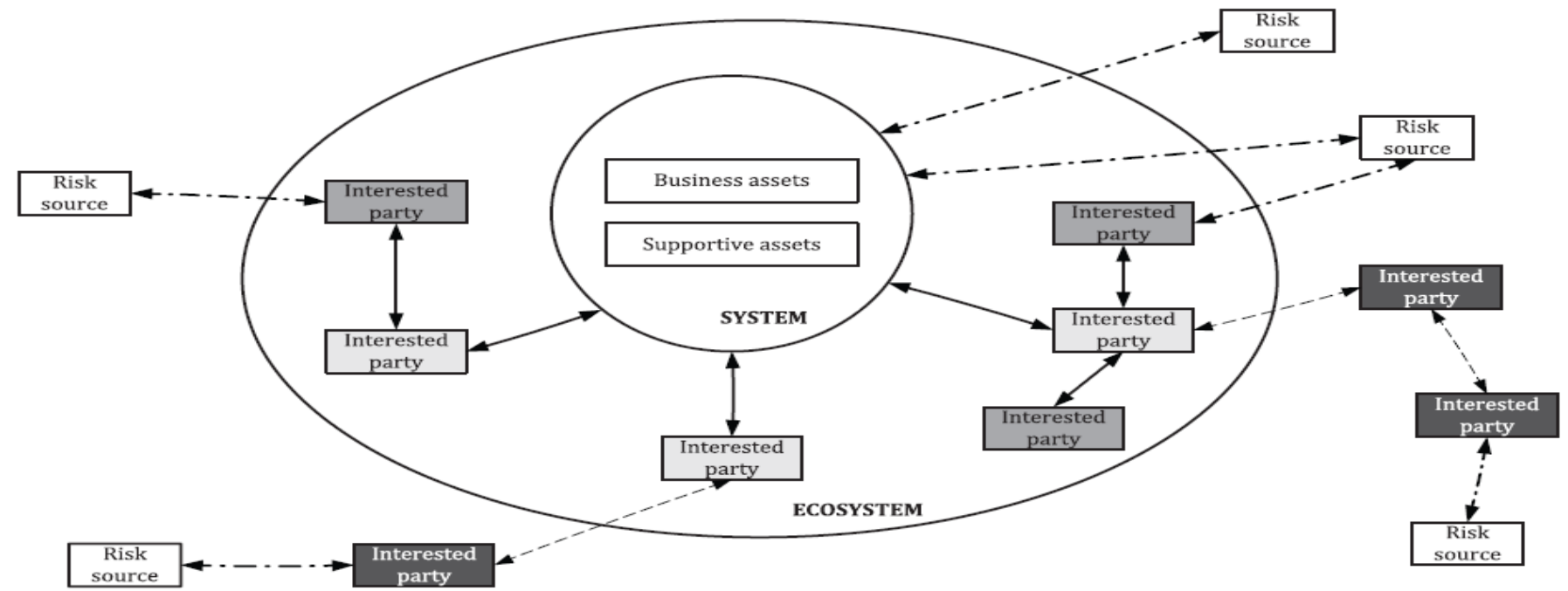


Figure A.3 — Identification of the interested parties of the ecosystem

ISO 27005 (Appendice A) Strategic scenarios

- **A.2.4.2 Strategic scenarios**
- Sulla base delle informazioni sulle fonti di rischio e sugli eventi interessati, è possibile immaginare scenari realistici di alto livello (scenari strategici), indicando in che modo una fonte di rischio può procedere per raggiungere il suo DES (Desired End State). Questi scenari vengono identificati per deduzione, partendo dalle fonti di rischio e dai loro DES: per ognuno di essi, si possono porre le seguenti domande, dal punto di vista della fonte di rischio:
- - Quali sono gli asset aziendali dell'organizzazione a cui le fonti di rischio devono mirare per raggiungere il loro DES?
- - Per rendere possibile o facilitare il loro attacco, è probabile che attacchino le parti critiche interessate dell'ecosistema che hanno accesso privilegiato agli asset aziendali?
- Una volta identificati gli elementi più esposti, è possibile disegnare lo scenario strategico, descrivendo la sequenza degli eventi generati dalla fonte di rischio per raggiungere il suo DES. La violazione degli asset aziendali corrisponde agli eventi finali, mentre gli eventi riguardanti l'ecosistema sono eventi intermedi. Lo scenario strategico riflette una valutazione delle conseguenze direttamente ereditate dagli eventi in questione.
- Questi scenari possono essere rappresentati sotto forma di grafici di attacco o direttamente sulla vista dell'ecosistema della mappatura del sistema informativo, sovrapponendo i percorsi di attacco.
- Gli scenari strategici richiedono un'ulteriore considerazione della probabilità degli eventi. L'approccio basato sugli asset e gli scenari operativi associati possono essere utilizzati per definire la probabilità degli eventi. Gli esempi di minacce presentati di seguito possono essere utilizzati per ottenere le valutazioni necessarie.

27005 (Appendice A) Asset-based approach

- **A.2.2 Assets**
- Quando si applica l'approccio asset-based all'identificazione del rischio, è necessario identificare gli asset.
- Nel processo di valutazione del rischio, nell'ambito dello sviluppo degli scenari di rischio, l'identificazione di eventi, conseguenze, minacce e vulnerabilità deve essere collegata agli asset.
- Nel processo di trattamento del rischio, ogni controllo è applicabile a un sottoinsieme di asset.
- Gli asset possono essere suddivisi in due categorie:
- - asset primari/di business - informazioni o processi di valore per un'organizzazione;
- - asset di supporto - componenti del sistema informativo su cui si basano uno o più asset aziendali.
- *Gli asset di business e quelli di supporto sono correlati, pertanto le fonti di rischio identificate per gli asset di supporto possono avere un impatto sugli asset di business.*
- *Per questo motivo, è importante identificare le relazioni tra gli asset e comprendere il loro valore per l'organizzazione*

ISO 27005 (Appendice A) Asset dependency

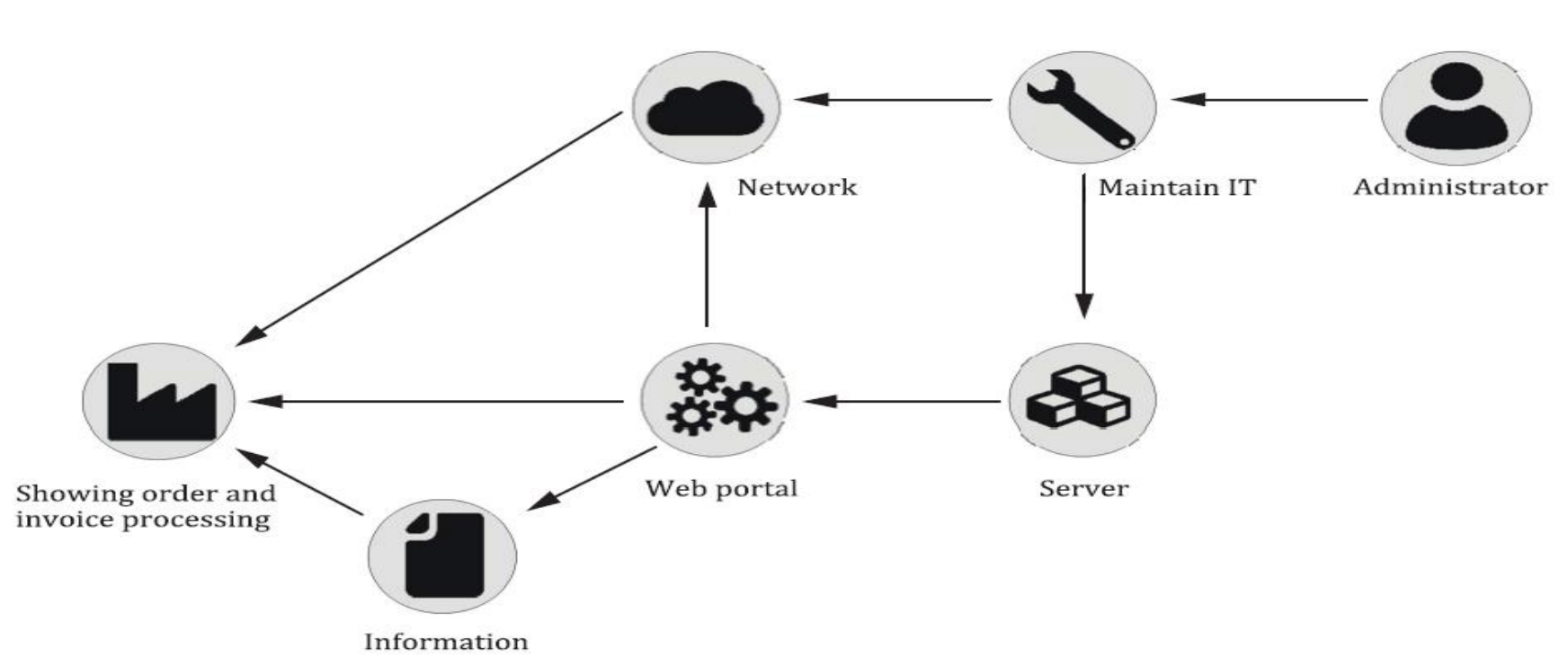


Figure A.2 — Example of an asset dependency graph

La Figura A.2 indica gli asset dipendenti per l'asset aziendale "elaborazione ordini e fatture" e può essere letto come segue:
- "Amministratore" (tipo: risorsa umana), che, se non adeguatamente formato, propaga un rischio per l'asset.
- "Maintain IT" (tipo: servizio), che propaga il rischio all'asset.
- "Server" (tipo: hardware) o all'asset "Rete" (tipo: connettività di rete). Il server, se smette di funzionare o la rete non è configurata correttamente, causa il rischio per l'asset.
- "Portale web" (tipo: applicazione), se smette di funzionare o non è disponibile.

Senza il "portale web", il processo aziendale "presentazione dell'ordine e dell'elaborazione della fattura" non offre ai clienti il processo previsto.

ISO 27005 (Appendice A) Using risk scenarios for risk assessment

Gli scenari di rischio possono essere costruiti utilizzando sia un approccio event-based, sia un approccio asset-based o entrambi.

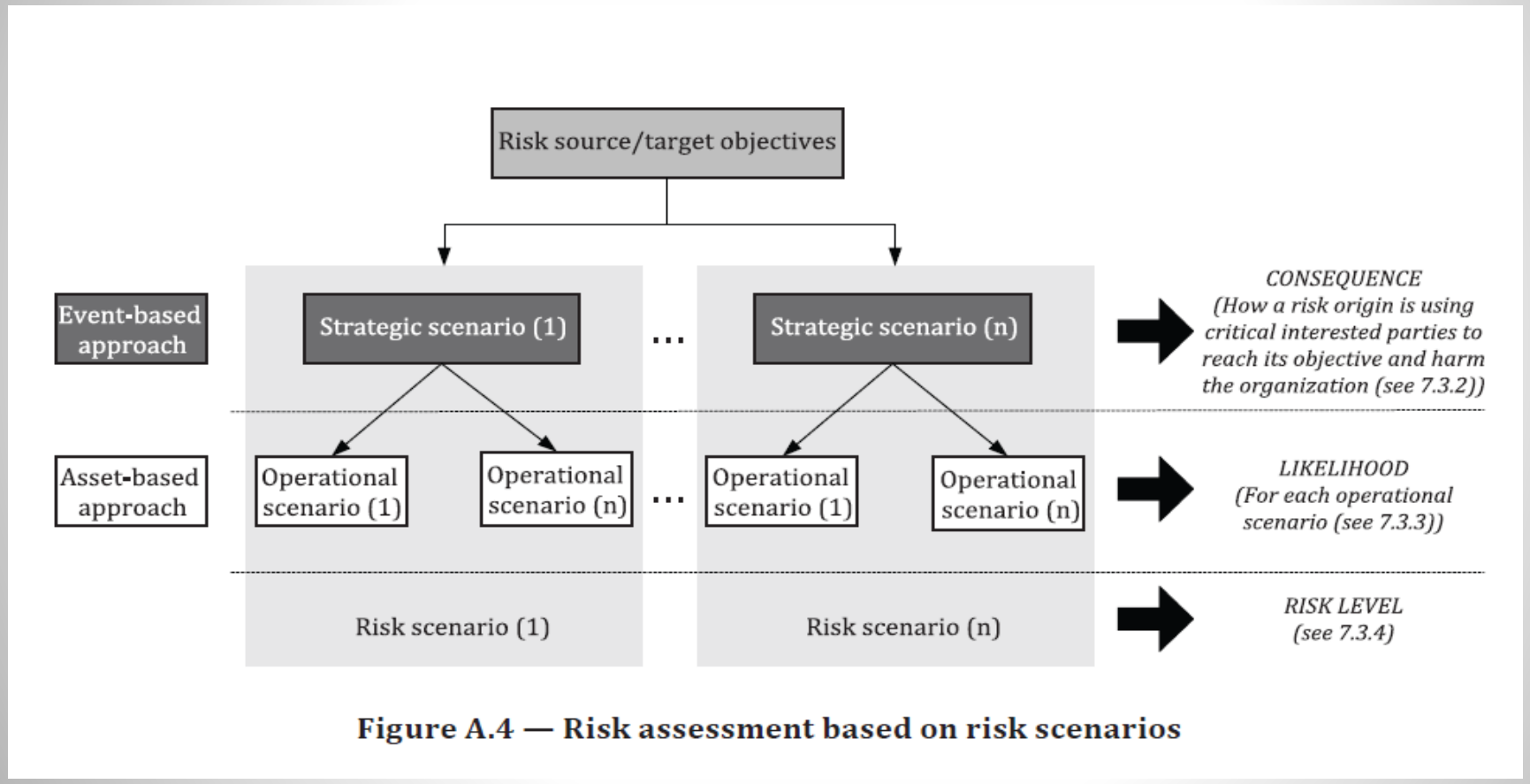


Figure A.4 — Risk assessment based on risk scenarios

ISO 27005 (Appendice A) Examples of risk scenarios in both approaches

Risk source	Target objective DES (Desired End State)	Strategic risk scenario **(Event-based approach)**	Operational risk scenario **(Asset-based approach)**
Authoritarian state	Acquiring a strategic attack vector	Subverting critical infrastructure	Deploying hidden and persistent malware in the supply chain
Organized crime	Development of illegal activities	Exploitation of port infrastructure	Infiltration of the dockers' union
			Taking control of a computerized flow management system
		Tax carousel fraud	Creating shell companies to carry out fake exchanges on the carbon tax market
		Extortion	Distributing ransomware
Aggressive business	Obtaining a market monopoly	Influencing the regulator	Corrupting a decision-maker
		Removing competitors	Defamation campaign on social networks

ISO 27005 (Appendice A) Monitoring risk-related events

- **A.2.7 Monitoring risk-related events**
- Il monitoraggio degli eventi correlati al rischio consiste nell'identificazione dei fattori che possono influenzare uno scenario di rischio per la sicurezza delle informazioni.
- In questo contesto, i fattori sono identificati come un insieme di elementi che consentono di rilevare un comportamento inatteso nei confronti di un determinato asset e che possono essere integrati nelle capacità e negli strumenti di monitoraggio dell'organizzazione per determinare l'innesco di uno scenario di rischio per la sicurezza delle informazioni.
- Il monitoraggio degli eventi correlati al rischio può essere definito utilizzando diversi indicatori provenienti da scenari operativi o strategici. Possono essere di diversa natura (tecnica, organizzativa, comportamentale, risultati di audit, ecc.) Gli eventi vengono monitorati in base a priorità definite, come l'entità delle conseguenze e la probabilità dell'evento.

ISO 27005 (Appendice A) Esempio della relazione tra scenari e monitoraggio

Table A.13 — Example of risk scenario and monitoring risk-related events relationship

Risk components	Examples		Events to monitor
Strategic scenario (event based)	Sensitive documents are destroyed by an administrator		
Events concerned	Loss of critical documents		
Severity of consequence	Descriptive measure: high		
Operational scenarios (asset based)	Usage of administrator rights to destroy the sensitive documents by directly accessing the database	- >	Detection of a direct access to the database outside of the normal working hours
	Root access in order to modify the system date/time		
	Malware infection of the administrator workstation with a propagation on the database	- >	Detection of operations impacting a large volume of data (Destruction)
Likelihood	Descriptive measure: medium		
Risk source	Administrator		
Target objective	Compromising of the sensitive document availability		
DES	Compromising of the system		
Security controls	Backup strategy implementation		
	Anti-malware solution		
	NTP implementation		
	OS Hardening		
	Access rights restriction on operational data		

- Dopo questa *non semplice* introduzione proviamo a vedere se abbiamo degli strumenti che ci consentano di costruire e applicare in modo «semplice» degli scenari di rischio

Agenda

- Introduzione: scenari e valutazione del rischio
- ISO27002 e 27005
- Gli scenari di rischio ISACA e l'utilizzo nel modello quantitativo FAIR
- Altri spunti: MITRE, DORA
- Considerazioni conclusive

ISACA Risk Scenarios

+

Cybersecurity Risk Quantification

ISACA Risk Scenarios 19 Cathegories

1 - IT investment decision making, portfolio definition and maintenance
Inability to make the correct IT investments in competitive IT product and service portfolio

2- Program and projects life cycle management
Inability to execute programs and projects within time, budget and as per requirements

3 - IT cost and oversight
Inability to provide IT services within agreed and reasonable resource limitations

4 - IT expertise, skills and behavior
Inability to recruit and maintain adequate IT staffing levels to support business needs

5 - Enterprise/IT architecture
Inability to select, develop, acquire and implement IT systems that integrate with enterprise architecture

6 - IT operations
Inability to provide reliable IT services because of operational IT mishaps

7 - User access rights management
Inability to protect systems from deliberate or inadvertent system compromise, misuse or loss

8 - Software adoption and use
Inability of business processes to benefit from newly developed products and services

9 - IT hardware
Inability to continually support and maintain technology systems (including aging and legacy systems) that are supporting business processes

10 - Internal and external security threats (hacker, malware, etc.)
Malicious access to and compromise or misuse of technology systems impacting the confidentiality, integrity or availability of technology systems and business information

11 - Third-party/supplier incidents
Inability to meet service-level requirements because of failure of third-party suppliers

12 - Noncompliance
Inability to comply with policies, standards, laws and regulations related to technology

13 - Geopolitical issues
Inability to protect against geopolitical issues, e.g., actions in/from foreign countries

14 -Industrial action
Inability to provide IT services because of industrial action of employees or service providers.

15 - Acts of nature
Natural or man-made disasters affecting critical resources

16 - Emerging technologies and innovation
Inability to exploit new technologies into innovative processes and products

17 - Environmental
Inability to deliver IT services in an environmentally friendly manner or in line with environmental regulations

18 - Data and information management
Inability to achieve and preserve adequate data and information quality and protection

19 - Disastrous events
Events that might threaten employee safety or the destruction/theft of physical assets

88 Scenari

Cathegory	Ref	Risk
1 - IT investment decision making, portfolio definition and maintenance Inability to make the correct IT investments in competitive IT product and service portfolio	1A	Misaligned Programs
	1B	Misaligned Investment
	1C	Incorrect Software
	1D	Wrong Infrastructure
	1E	Investment Duplications and Overlaps
	1F	New Investment Programs
2 - Program and projects life cycle management Inability to execute programs and projects within time, budget and as per requirements	2A	Failing Projects-REVISED-LRY
	2C	Insufficient Technology-REVISED-LRY
	2D	Late Delivery of IT Projects
	2F	Immature Software
3 - IT cost and oversight: Inability to provide IT services within agreed and reasonable resource limitations	3A	User-Created and Ad-Hoc Solutions
	3B	IT Services Change Management
	3C	Costly and Ineffective I&T-Related Purchases
	3D	Inadequate Requirements Resulting in Ineffective SLAs
	3E	Lack of Funding for I&T-Related Investment
4 - IT expertise, skills and behavior: Inability to recruit and maintain adequate IT staffing levels to support business needs	4A	Insufficient Internal Skills or Knowledge
	4C	Inability to Recruit or Retain IT Staff
	4D	Recruiting Lack of Due Diligence
	4E	Insufficient I&T Training
	4F	Overreliance on Key Staff
	4G	Lack of Feedback on Job Performance

Per ogni scenario: documento Word con 5 tabelle

- A - Risk Scenario Description
- B - Risk Scenario Components
- C - Risk Scenario Scope and Extent
- D - Controls to Mitigate the Risk Scenario
- E - Key Risk Indicators

Rischio 7I Scheda A Scenario Description

IT Risk Scenario: Authorized Users Conduct Unauthorized Actions			
A. Risk Scenario Description			
Risk Scenario Title	Authorized users intentionally or accidentally conduct unauthorized actions.		
Risk Type	2—Service quality; 3—Data and system protection; 4—Legal and regulatory compliance		
Risk Scenario Category	User access rights management: Inability to protect systems from malicious or inadvertent system compromise, misuse or loss		
Risk Scenario Reference	7I		
Risk Statement	A privileged user accesses sensitive organizational information in excess of their job duties, exposing the enterprise to a privacy violation or data disclosure incident.		
Risk Owner	Business Process Owner CIO/CTO/CDO/CISO	Risk Oversight	I&T Governance Board Chief Risk Officer (CRO)

Rischio 7I
Scheda B
Risk Scenario Components

B Risk Scenario Components			
Actor/Threat Community	Untrained/accidental insiders Malicious insiders		
Intent/Motivation	Authorized users with access to information resources intentionally or unintentionally affect the confidentiality, integrity or availability of systems, causing a security incident.		
Threat Event	A security incident is caused by the actions of an insider		
Assets/Resources	▪ Customer sensitive information ▪ Vendor sensitive information ▪ Employee sensitive information		
Consequence	The consequence of this risk scenario ranges from damaged reputation, due to the leakage of sensitive information, to the loss of relationships with customers and possible fines, penalties or regulatory action depending on type of enterprise.		
	Impact Dimensions (potential forms of loss)	✓ **Productivity**	Leaks of sensitive, personal information about staff, contractors or vendors may affect the productivity of the entire enterprise.
		✓ **Cost of Response**	Time/efforts to identify root causes and recover from an incident
		✓ **Replacement Cost**	N/A
		✓ **Competitive Advantage**	If the events are severe enough and public facing, the enterprise can lose customers and a competitive advantage.
		✓ **Reputation**	If the events(s) are severe enough and public facing, an enterprise's reputation is adversely impacted due to negative publicity or continued customer service degradation.
		✓ **Fines and Judgements**	If the events are severe enough and public facing, exposure to fines and regulatory actions is possible.
Timing	• The duration of the incident can be very short or prolonged, depending on job scope and overlap of duties. • Early detection and corrective action are key to limit the scope and nature of this risk scenario.		

Rischio 7I Scheda C Risk Scenario Scope and Extent

C Risk Scenario Scope and Extent		
Extent of the Scenario	**Worst Case**	A significant amount of sensitive and confidential information is exposed and there is no plan to adequately respond to this type of crisis by the enterprise. Many of the customers stop doing business with the enterprise due the impact on the enterprise reputation based on poor business decisions resulting from inaccurate and incomplete information. In addition, the fines and penalties imposed are very considerable.
	Typical or Most Likely Case	There is an adequate plan to respond to these types of incidents. It is shown that the leakage of information is not due to a lack of preventive measures on the part of the enterprise, so the fines and penalties are minimal. A small amount of sensitive and confidential information is exposed because the leakage of sensitive information is detected timely. Only a smaller number of customers cancel their business relationships with the enterprise in response to the enterprise's proper crisis response plan.
	Best Case	There is an adequate plan to respond to these types of incidents. It is shown that the leakage of information is not due to a lack of preventive measures on the part of the enterprise, so there are no fines and penalties. Just the sensitive and confidential information of one customer is exposed because of the detection of the leakage of sensitive information. No customers cancel their business relationships with the enterprise in response to the enterprise's proper crisis response plan.
Assumptions	○ The enterprise has a privacy incident response plan. ○ The enterprise has an adequate level of awareness about data privacy issues. ○ The recertification of privileged accesses is carried out sporadically by the enterprise.	

Rischio 7I Scheda D Control Description (COBIT 19 Management Practices)

D. Controls to Mitigate the Risk Scenario						
	Control Description	Control Type	Effect on Impact	Effect on Frequency	Essential Control	Reference
1	**Communicate management objectives, direction and decisions made.** Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the enterprise.	Preventive	Yes	Yes	Yes	**COBIT APO01.02**
2	**Establish roles and responsibilities.** Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability.	Preventive	Yes	Yes	Yes	**COBIT APO01.05**
3	**Define information (data) and system ownership**. Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners classify information and systems and protect them in line with their classification.	Preventive	Yes	Yes	Yes	**COBIT APO01.07**
4	**Maintain the skills and competencies of personnel.** Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	Preventive	Yes	Yes	Yes	**COBIT APO07.03**
5	**Define and communicate the enterprise's data management strategy and roles and responsibilities.** Define how to manage and improve the enterprise's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	Preventive	Yes	Yes	Yes	**COBIT APO14.01**

Rischio 7I Scheda E Indicator

E. Key Risk Indicators			
	Indicator	KRI Description	Lead/Lag
1	Program and quality management	Frequency of communication on management objectives and direction for I&T	Lead
2	Data and information management	Number of I&T-related roles assigned to individuals	Lead
3	Program and quality management	Percentage of data assets with clearly defined owners	Lead
4	Program and quality management	Percentage of information systems with clearly defined owners	Lead
5	Program and quality management	Percentage of information items classified according to the agreed classification levels	Lead
6	Data and information management	Number of data management breaches in comparison to the defined strategy	Lag
7	Data and information management	Percentage of roles and responsibilities identified to support the governance of data management and the interaction between governance and the data management function	Lead
8	Staff skills and competencies	Identified key skills and competencies missing in the resource matrix	Lead
9	Staff skills and competencies	Number of identified gaps between required and available skills	Lead
10	Staff skills and competencies	Number of training programs provided	Lead

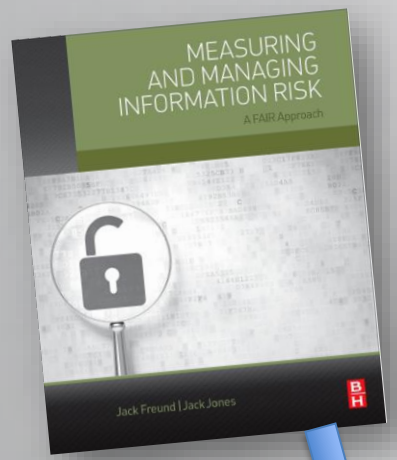
Rivediamo le schede che ci interessano maggiormente

- B - Risk Scenario Components
- D - Controls to Mitigate the Risk Scenario

Rischio 7I
Scheda B
Risk Scenario Components

B Risk Scenario Components				
Actor/Threat Community	Untrained/accidental insiders Malicious insiders			**Attaccante, capacità**
Intent/Motivation	Authorized users with access to information resources intentionally or unintentionally affect the confidentiality, integrity or availability of systems, causing a security incident.			**Motivazione**
Threat Event	A security incident is caused by the actions of an insider			**Frequenza minacce**
Assets/Resources	▪ Customer sensitive information ▪ Vendor sensitive information ▪ Employee sensitive information			**Oggetto del rischio**
Consequence	The consequence of this risk scenario ranges from damaged reputation, due to the leakage of sensitive information, to the loss of relationships with customers and possible fines, penalties or regulatory action depending on type of enterprise.			
	Impact Dimensions (potential forms of loss)	✓ **Productivity**	Leaks of sensitive, personal information about staff, contractors or vendors may affect the productivity of the entire enterprise.	**Stima degli impatti**
		✓ **Cost of Response**	Time/efforts to identify root causes and recover from an incident	
		✓ **Replacement Cost**	N/A	
		✓ **Competitive Advantage**	If the events are severe enough and public facing, the enterprise can lose customers and a competitive advantage.	
		✓ **Reputation**	If the events(s) are severe enough and public facing, an enterprise's reputation is adversely impacted due to negative publicity or continued customer service degradation.	
		✓ **Fines and Judgements**	If the events are severe enough and public facing, exposure to fines and regulatory actions is possible.	
Timing	• The duration of the incident can be very short or prolonged, depending on job scope and overlap of duties. • Early detection and corrective action are key to limit the scope and nature of this risk scenario.			

Scheda B
Risk Scenario Components



- Attaccante, capacità
- Motivazione
- Frequenza minacce
- Oggetto del rischio
- Stima degli impatti

TCom	TEF Min	TEF ML	TEF Max	TCap Min	TCap ML	TCap Max
Nation states	0.20 (once in 20 years)	0.06 (once in 15 years)	0.10 (once in 10 years)	95	98	99
Cyber criminals	0.5 (once in 2 years)	2 (twice a year)	12 (once a month)	60	85	98
Privileged insider	0.04 (once in 25 years)	0.06 (once in 15 years)	0.10 (once a decade)	98	99	99
Non-privileged insiders	0.06 (once in 15 years)	0.10 (once in 10 years)	1 (once a year)	40	50	95
Malware	0.5 (once every 2 years)	2 (twice a year)	6 (once every 2 months)	40	60	95

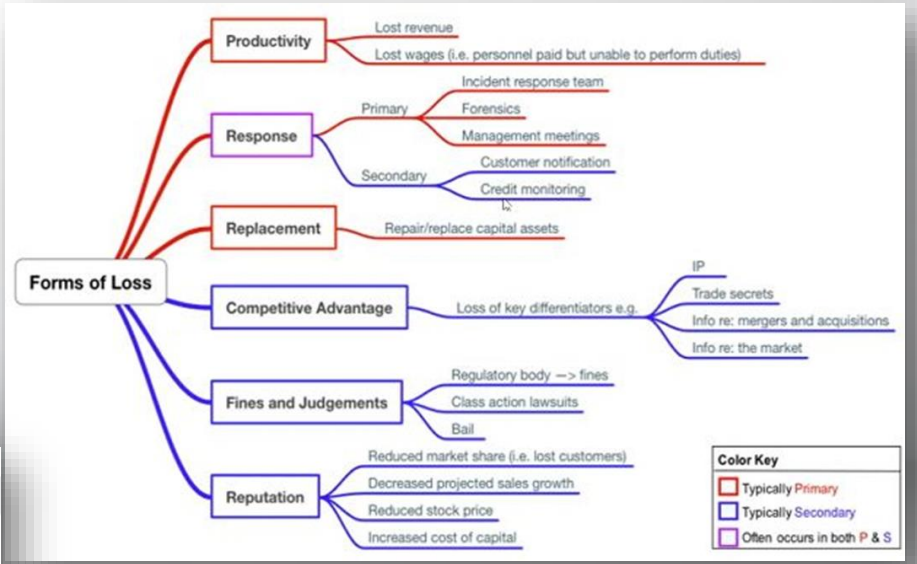
Table 4.6 Nation State FAIR Risk Factors

TCom	TEF Min	TEF ML	TEF Max	TCap Min	TCap ML	TCap Max
Nation states	0.20 (once in 20 years)	0.06 (once in 15 years)	0.10 (once in 10 years)	95	98	99

TCap, threat capability; TCom, threat community; TEF, threat event frequency; Max, maximum; Min, minimum; ML, most likely.

Table 8.12 Secondary Loss Estimates Involving Reputation Damage

Loss Type	Minimum	Most Likely	Maximum	Confidence
Sec response	$2500	$11,500	$7,000,000	Moderate
Sec fines & judgments	$0	$0	$2,000,000	Moderate
Sec reputation	$0	$150	$3,750,000	Moderate



Scheda D
Control Description (COBIT 19 Management Practices).

D. Controls to Mitigate the Risk Scenario						
Control Description		Control Type	Effect on Impact	Effect on Frequency	Essential Control	Reference
1	**Communicate management objectives, direction and decisions made.** Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the enterprise.	Preventive	Yes	Yes	Yes	**COBIT APO01.02**
2	**Establish roles and responsibilities.** Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability.	Preventive	Yes	Yes	Yes	COBIT **APO01.05**
3	**Define information (data) and system ownership.** Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners classify information and systems and protect them in line with their classification.	Preventive	Yes	Yes	Yes	**COBIT APO01.07**
4	**Maintain the skills and competencies of personnel.** Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	Preventive	Yes	Yes	Yes	**COBIT APO07.03**
5	**Define and communicate the enterprise's data management strategy and roles and responsibilities.** Define how to manage and improve the enterprise's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	Preventive	Yes	Yes	Yes	**COBIT APO14.01**

Controlli ?

Ad ogni scenario di rischio corrisponde uno scenario di controlli che fanno riferimento al COBIT.

È possibile passare da COBIT ad altri frameworks usando le mappature disponibili (*)

1. COBIT to CSF (NIST)
2. CSF to ISO 27002(2013) (NIST)
3. ISO 27002 to ISO 27002 (2022) (ISO)

**) Ovviamente se rimaniamo nell'ambito della Cybersecurity*

Listed below are the practices associated with each of the governance and management objectives in COBIT® 2019.
The practices are sorted in the order in which they appear in *COBIT® 2019 Framework: Governance and Management Objectives.*

Objectives: 40
Practices: 231

MAP

Area	Domain	Objective	Objective	Objective	Objective	Practice ID	Practice Name	Practice Description	Mapping ISO 27002	CSF
						APO01.02	Communicate management objectives, direction and decisions made.	Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the organization.	5.1 - Policies for information security 5.2 - Information security roles and responsibilities 5.4 - Management responsibilities 5.19 - Information security in supplier relationships 5.24 - Information security incident management planning and preparation 6.3 - Information security awareness, education and training	ID.AM-6 - Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established ID.GV-1 - Organizational cybersecurity policy is established and communicated ID.GV-2 - Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners PR.AT-4 - Senior executives understand their roles and responsibilities RS.CO-1 - Personnel know their roles and order of operations when a response is needed
						APO01.05	Establish roles and responsibilities.	Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability.	5.2 - Information security roles and responsibilities 5.4 - Management responsibilities 5.19 - Information security in supplier relationships 5.24 - Information security incident management planning and preparation 6.3 - Information security awareness, education and training	ID.AM-6 - Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established ID.GV-2 - Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners DE.DP-1 - Roles and responsibilities for detection are well defined to ensure accountability RS.CO-1 - Personnel know their roles and order of operations when a response is needed
						APO01.07	Define information (data) and system ownership.	Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners classify information and systems and protect them in line with their classification.	5.3 - Segregation of duties 5.10 - Acceptable use of information and other associated assets 5.13 - Labelling of information 5.14 - Information transfer 5.15 - Access control 6.1 - Screening 6.2 - Terms and conditions of employment 6.5 - Responsibilities after termination or change of employment 6.6 - Confidentiality or non-disclosure agreements 7.5 - Protecting against physical and environmental threats 7.6 - Working in secure areas 7.8 - Equipment siting and protection 8.2 - Privileged access rights 8.3 - Information access restriction 8.4 - Access to source code 8.7 - Protection against malware 8.18 - Use of privileged utility programs 8.19 - Installation of software on operational systems 8.20 - Networks security 8.22 - Segregation of networks 8.24 - Use of cryptography 8.26 - Application security requirements 8.32 - Change management	PR.DS-1 - Data-at-rest is protected PR.DS-2 - Data-in-transit is protected PR.DS-5 - Protections against data leaks are implemented PR.DS-6 - Integrity checking mechanisms are used to verify software, firmware, and information integrity

Nel caso dello scenario 7I : Authorized users intentionally or accidentally conduct unauthorized actions.

Eliminando quelli ripetuti, i controlli ISO27002-2022 rimanenti sono : **29**

5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.11	Return of assets
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.19	Information security in supplier relationships
5.24	Information security incident management planning and preparation
6.1	Screening
6.2	Terms and conditions of employment
6.3	Information security awareness, education and training
6.4	Disciplinary process
6.5	Responsibilities after termination or change of employment
6.6	Confidentiality or non-disclosure agreements
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.8	Equipment siting and protection
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.7	Protection against malware
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.22	Segregation of networks
8.24	Use of cryptography
8.26	Application security requirements
8.32	Change management

Come valutare la loro efficacia complessiva (CRQ) nella gestione del rischio ?

Per rispondere dobbiamo chiederci : come operano i controlli ?

Due considerazioni importanti . . .

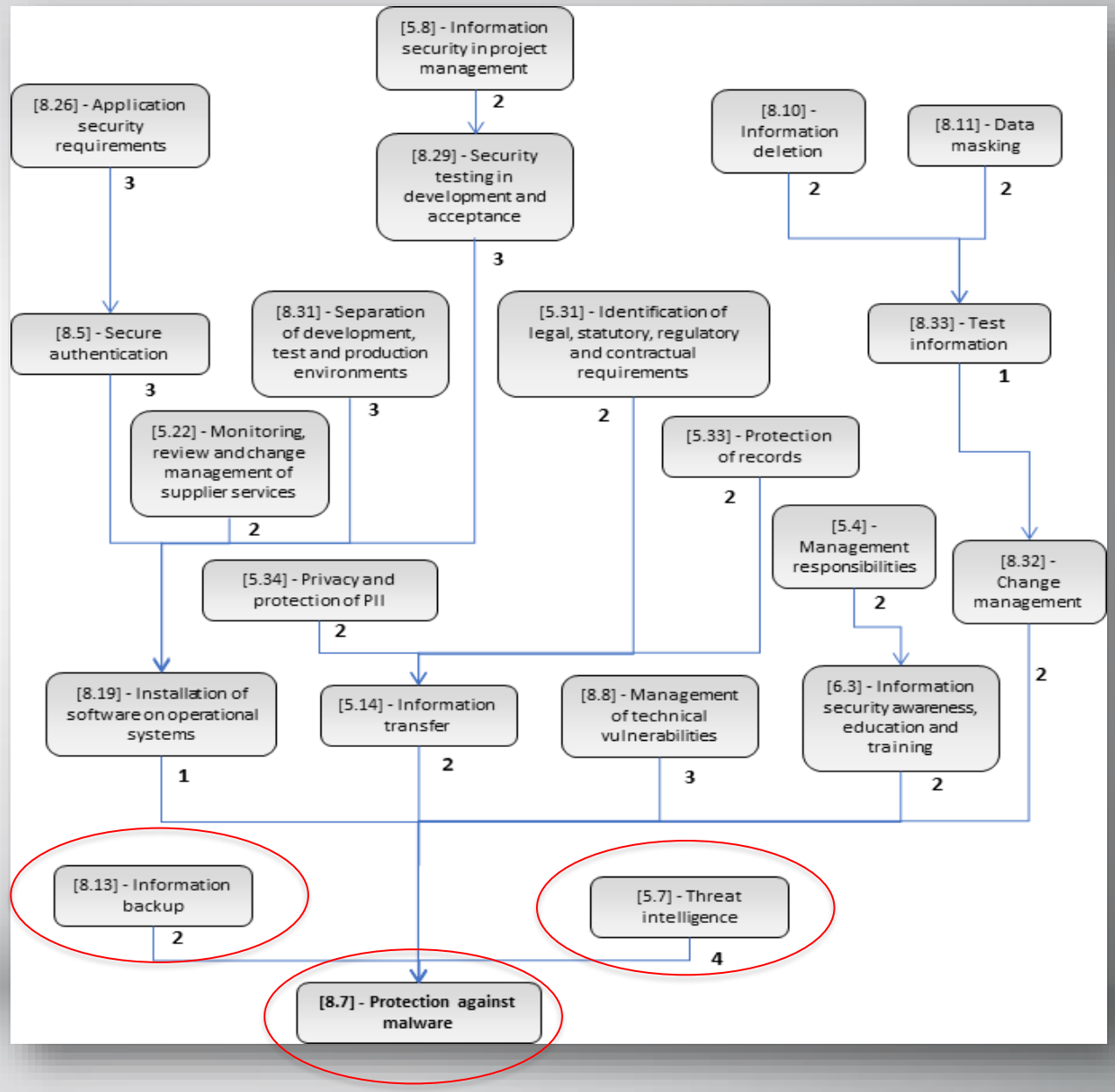
5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.11	Return of assets
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.19	Information security in supplier relationships
5.24	Information security incident management planning and preparation
6.1	Screening
6.2	Terms and conditions of employment
6.3	Information security awareness, education and training
6.4	Disciplinary process
6.5	Responsibilities after termination or change of employment
6.6	Confidentiality or non-disclosure agreements
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.8	Equipment siting and protection
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.7	Protection against malware
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.22	Segregation of networks
8.24	Use of cryptography
8.26	Application security requirements
8.32	Change management

- Controlli che operano direttamente sul rischio (LEC : Loss Event Control, 53/93)

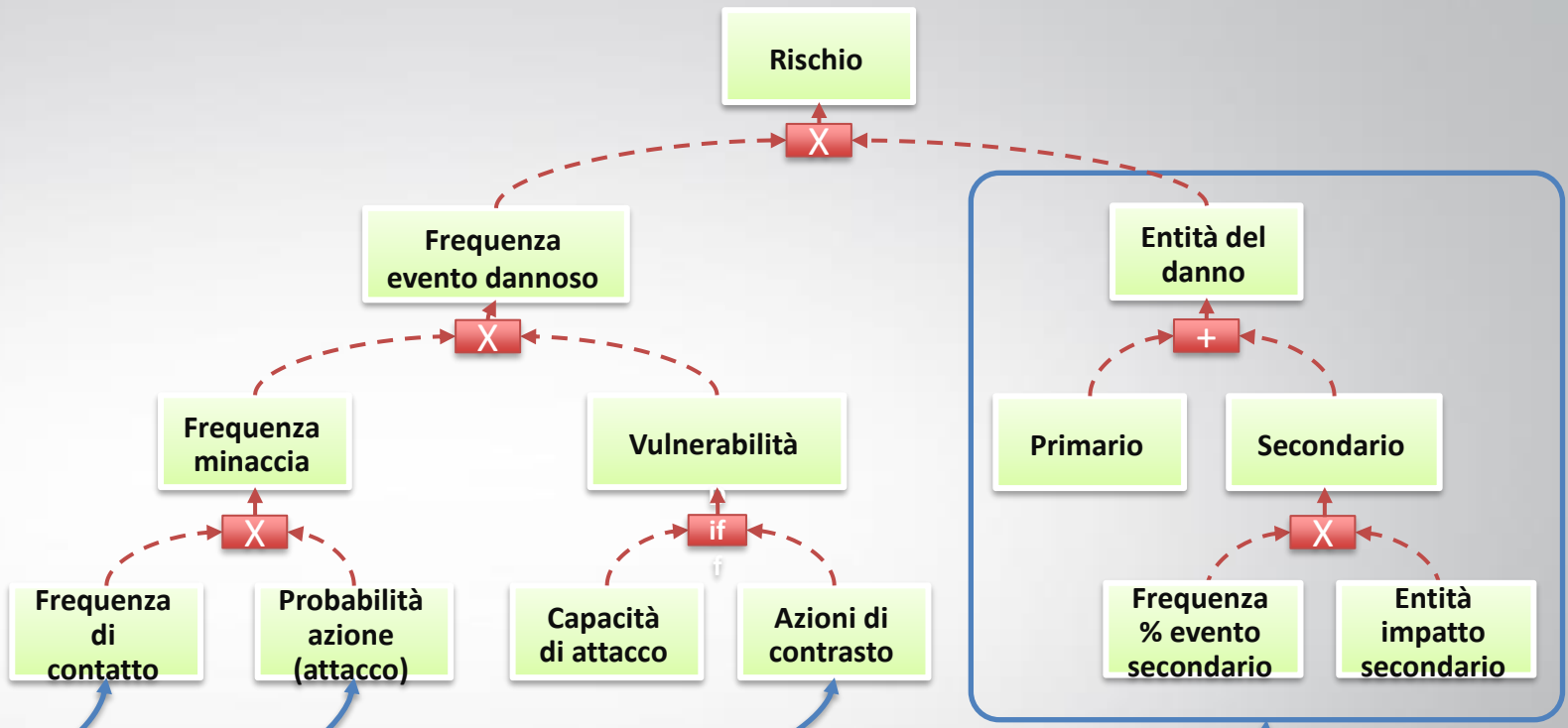
  Ad esempio:
  - Access Control
  - Autentication of information
  - Physical entry Control
  - Cabling security
  - Logging
  - ecc.
- Controlli che operano su gli altri controlli (40/93)

  Ad esempio:
  - Threat intelligence
  - Classification of information
  - Clock synchronization
  - Change management
  - Screening
  - ecc.

Dobbiamo aver presente lo schema e quindi correggere l'efficacia effettiva dei controlli che operano sul rischio:



Dove operano ?
Ogni controllo «diretto» agisce sull'ontologia «rischio» con modalità proprie



The FAIR Controls Analytics Model (FAIR-CAM™)

Riduzione prob. Accadimento		Avoidance
		Deterrence
		Resistance
Riduzione conseguenze	Detection	Visibility
		Monitoring
		Recognition
	Impact reduction	Event termination
		Resilience
		Loss reduction

Risk scenario 7I				CAM-MAP								
ISO/IEC 27002 control identifier	Control name	Combined Capab %	SME adjusted values leave blank uf unchanged	Avoidance	Deterrence	Resistance	Visibility	monitoring	recognition	containement	resiliience	loss reduction
[5.3]	Segregation of duties	30.4%		1		1						
[5.11]	Return of assets	68.6%		1		1						
[5.15]	Access control	59.6%		1		1						
[7.5]	Protecting against physical and environmental threats	20.0%		1		1						1
[7.6]	Working in secure areas	70.3%		1		1						
[7.8]	Equipment siting and protection	55.2%		1		1						
[8.2]	Privileged access rights	39.3%		1	1	1						
[8.3]	Information access restriction	54.1%		1	1	1						
[8.4]	Access to source code	57.4%		1								
[8.7]	Protection against malware	71.1%		1		1	1	1	1	1		
[8.18]	Use of privileged utility programs	56.5%		1								
[8.19]	Installation of software on operational systems	43.8%		1		1						
[8.22]	Segregation of networks	44.4%		1	1	1						

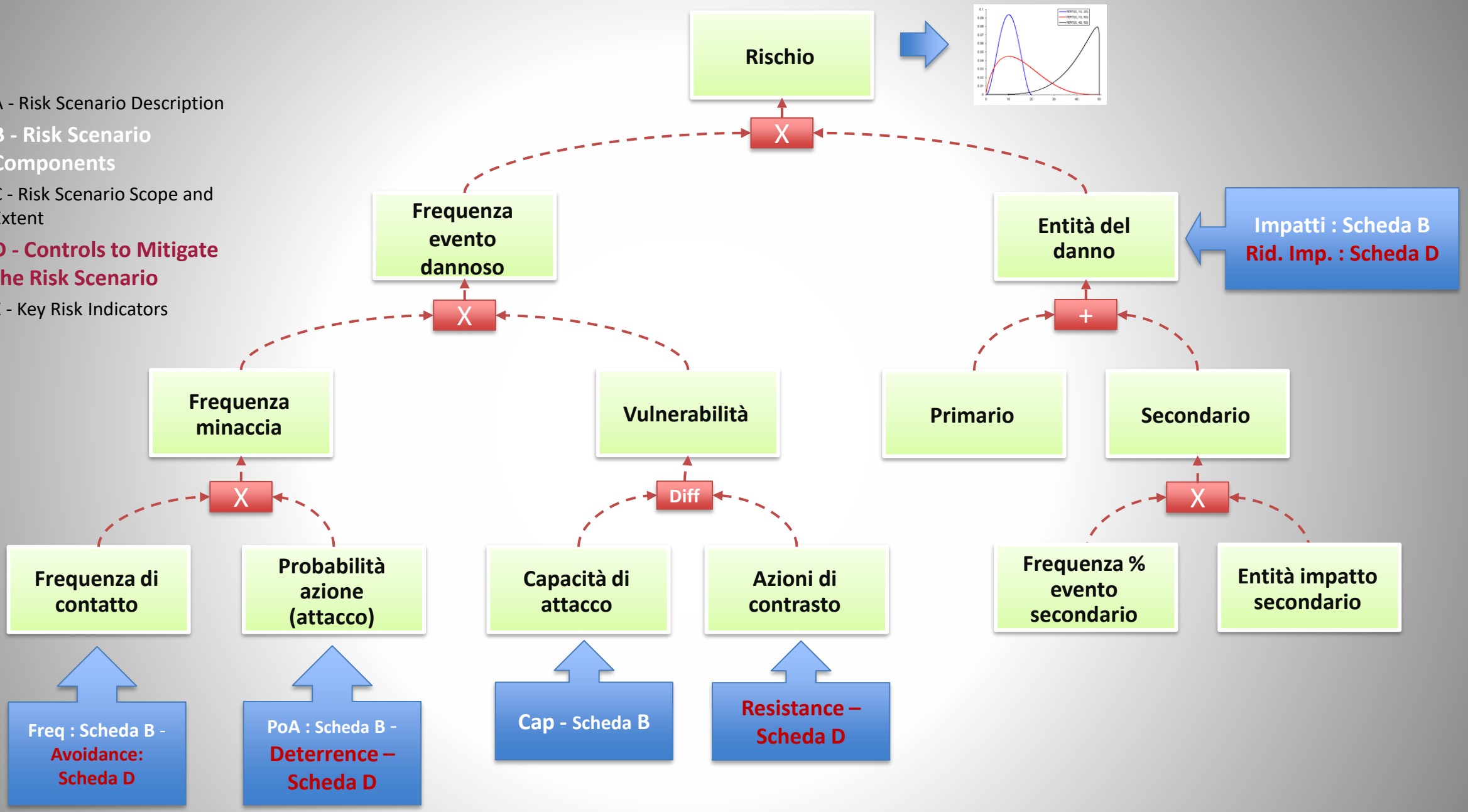
Controlli «diretti»

GDL ISACA ROMA

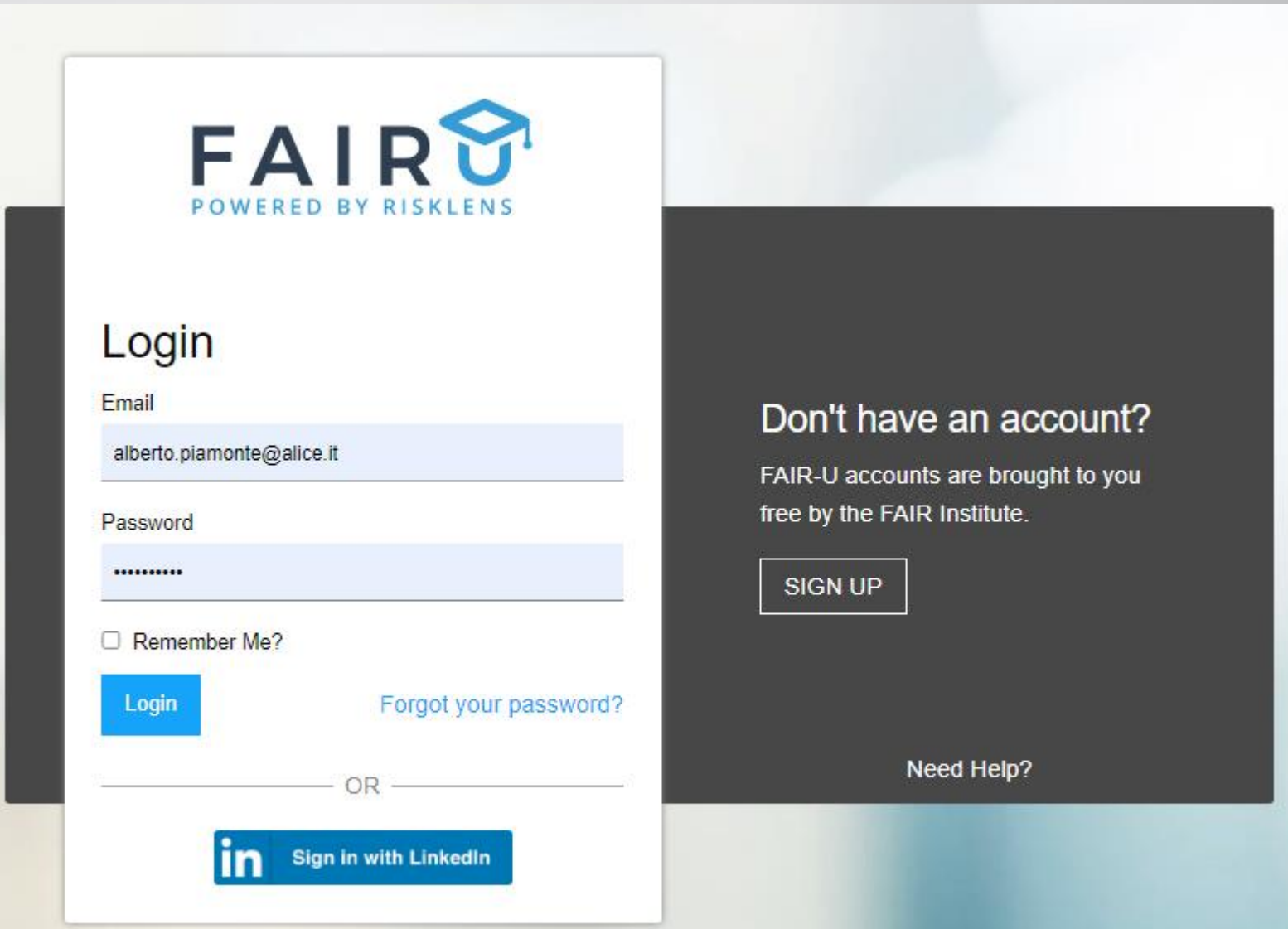
Risk Scenario : 7I :

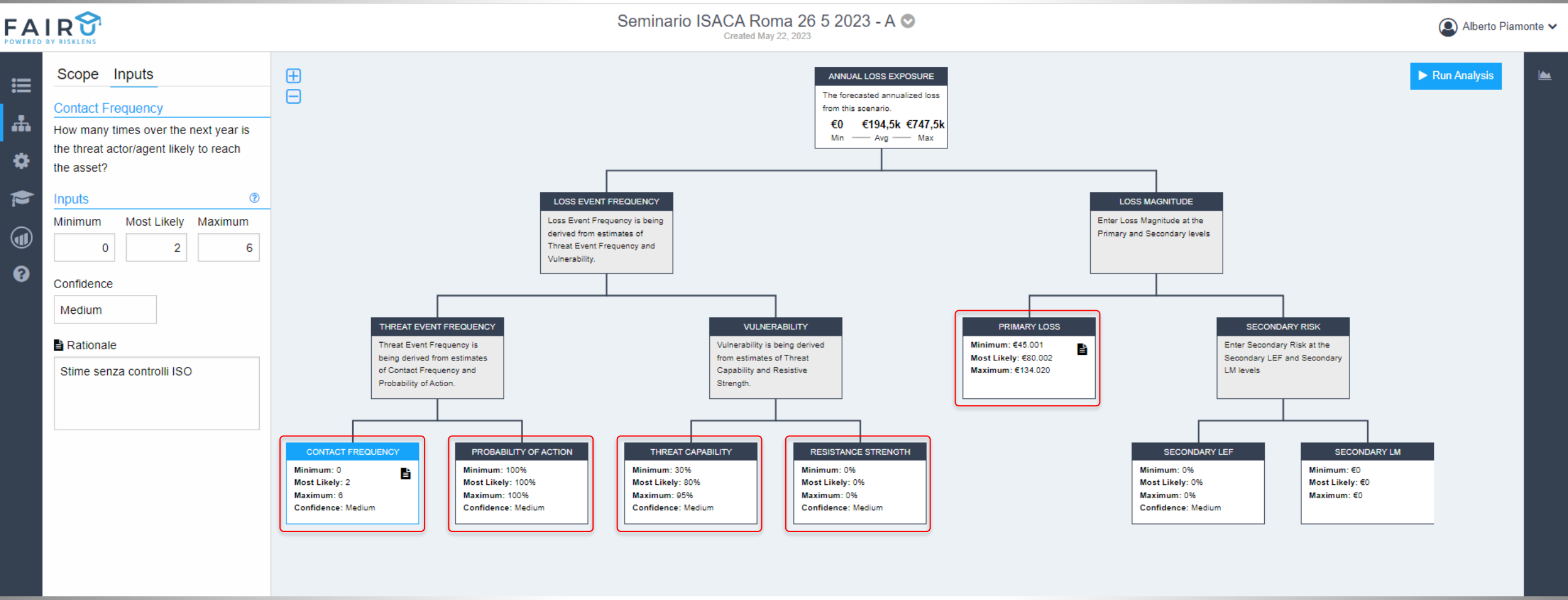
Authorized Users Conduct Unauthorized Actions

- A - Risk Scenario Description
- **B - Risk Scenario Components**
- C - Risk Scenario Scope and Extent
- **D - Controls to Mitigate the Risk Scenario**
- E - Key Risk Indicators



https://app.fairu.net




FAIR
POWERED BY RISKLENS
Seminario ISACA Roma 26 5 2023 - A
Created May 22, 2023
Alberto Piamonte
Scope
Inputs
Contact Frequency
How many times over the next year is the threat actor/agent likely to reach the asset?
Inputs
Minimum
Most Likely
Maximum
0
2
6
Confidence
Medium
Rationale
Stime senza controlli ISO
Run Analysis
ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
€0
€194,5k
€747,5k
Min
Avg
Max
LOSS EVENT FREQUENCY
Loss Event Frequency is being derived from estimates of Threat Event Frequency and Vulnerability.
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
THREAT EVENT FREQUENCY
Threat Event Frequency is being derived from estimates of Contact Frequency and Probability of Action.
VULNERABILITY
Vulnerability is being derived from estimates of Threat Capability and Resistive Strength.
PRIMARY LOSS
Minimum: €45.001
Most Likely: €80.002
Maximum: €134.020
SECONDARY RISK
Enter Secondary Risk at the Secondary LEF and Secondary LM levels
CONTACT FREQUENCY
Minimum: 0
Most Likely: 2
Maximum: 6
Confidence: Medium
PROBABILITY OF ACTION
Minimum: 100%
Most Likely: 100%
Maximum: 100%
Confidence: Medium
THREAT CAPABILITY
Minimum: 30%
Most Likely: 80%
Maximum: 95%
Confidence: Medium
RESISTANCE STRENGTH
Minimum: 0%
Most Likely: 0%
Maximum: 0%
Confidence: Medium
SECONDARY LEF
Minimum: 0%
Most Likely: 0%
Maximum: 0%
Confidence: Medium
SECONDARY LM
Minimum: €0
Most Likely: €0
Maximum: €0

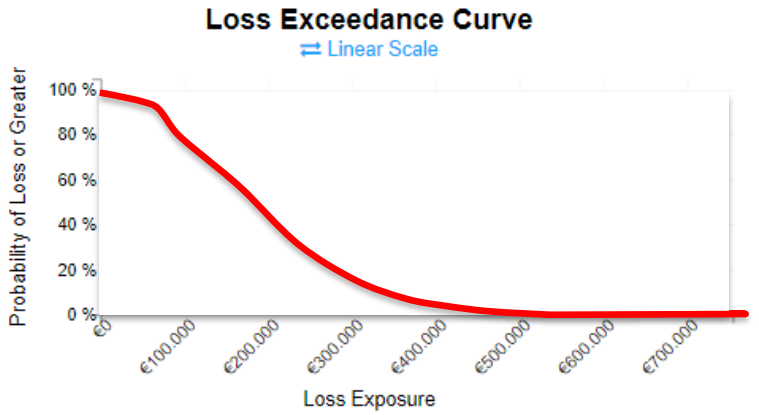
Nessun controllo ISO

Analysis Results

Risk **Senza controlli**

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

€0	€194,5k	€747,5k
Minimum	Average	Maximum



Summary of Simulation Results

Primary

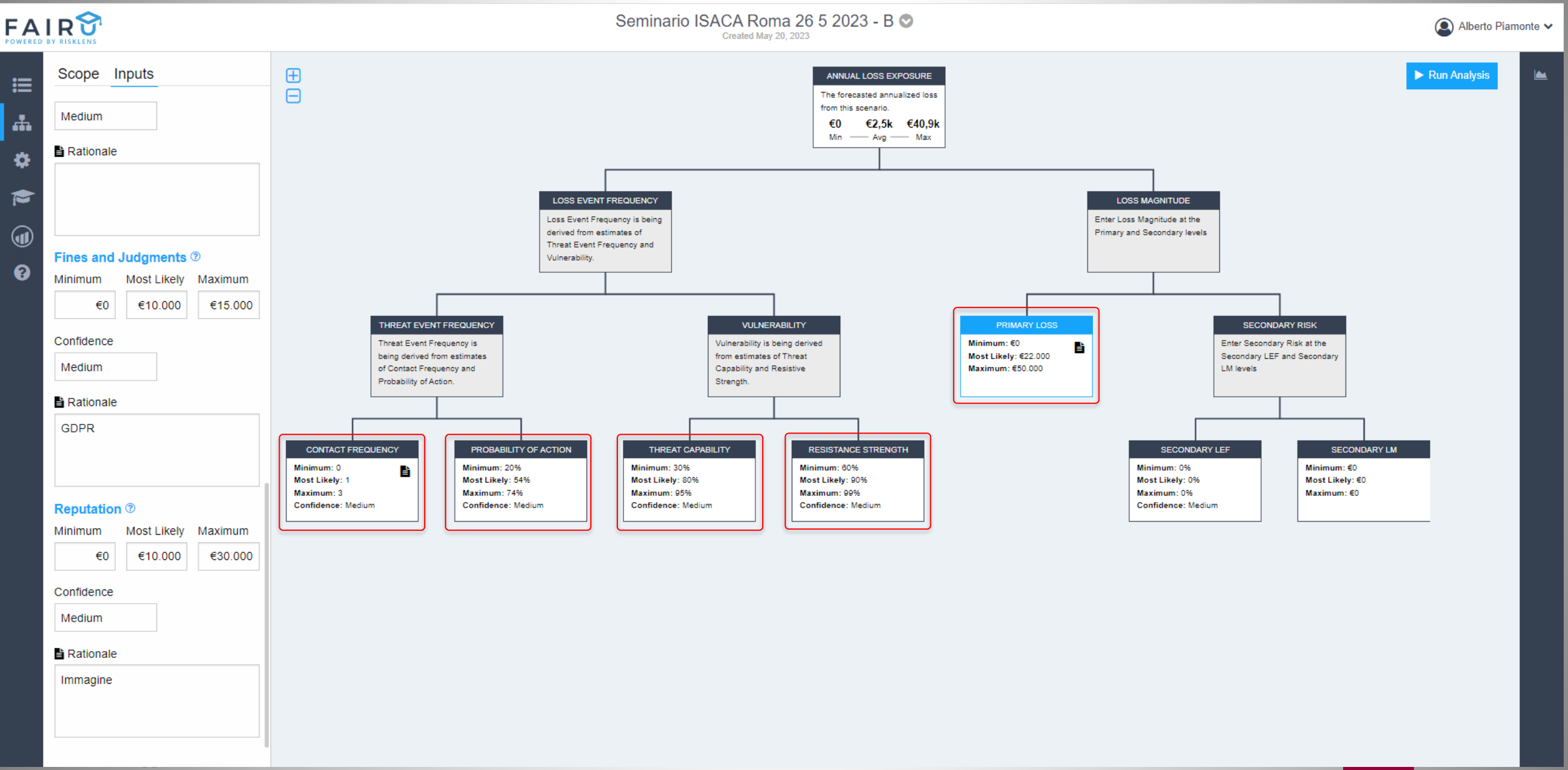
	Min	Avg	Max
Loss Events / Year	0	2,34	6
Loss Magnitude	€45,9k	€83,2k	€130,8k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0	0
Loss Magnitude	€0	€0	€0

Vulnerability 100%

Applichiamo i controlli previsti



Analysis Results

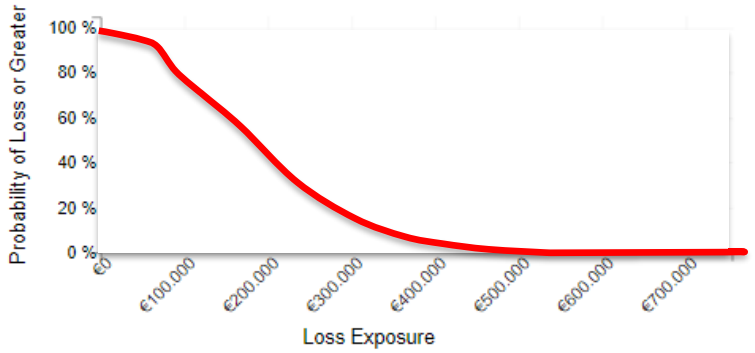
Risk — Senza controlli

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

€0	€194,5k	€747,5k
Minimum	Average	Maximum

Loss Exceedance Curve

Linear Scale



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	2,34	6
Loss Magnitude	€45,9k	€83,2k	€130,8k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0	0
Loss Magnitude	€0	€0	€0

Vulnerability 100%

Analysis Results

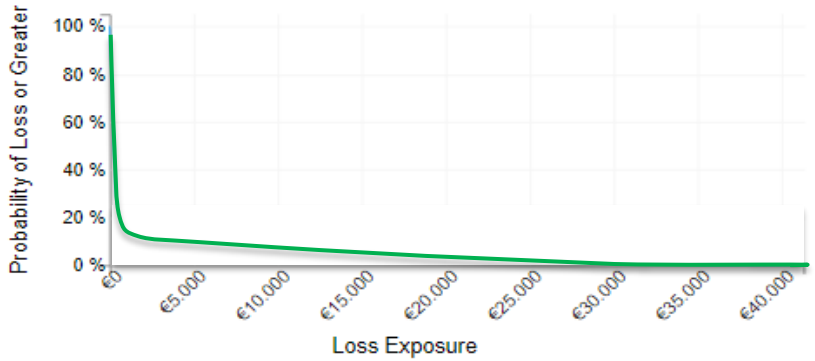
Risk — Con SoA definita

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

€0	€2,5k	€40,9k
Minimum	Average	Maximum

Loss Exceedance Curve

Linear Scale



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0,11	1
Loss Magnitude	€5,7k	€23,1k	€43,2k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0	0
Loss Magnitude	€0	€0	€0

Vulnerability 18,35%

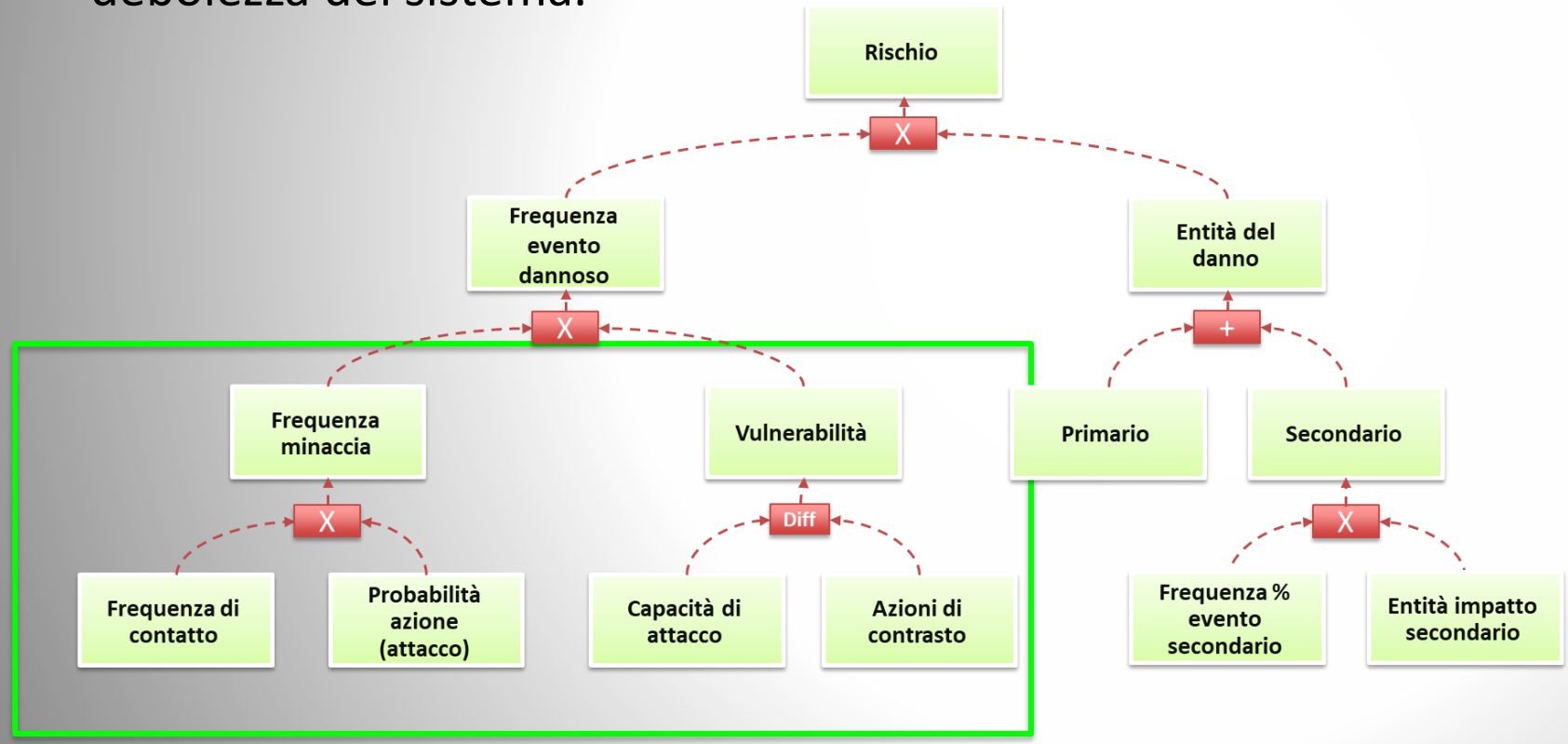
Agenda

- Introduzione: scenari e valutazione del rischio
- ISO27002 e 27005
- Gli scenari di rischio ISACA e l'utilizzo nel modello quantitativo FAIR
- Altri spunti: MITRE, DORA
- Considerazioni conclusive

Attacco vs difesa (threat vs resistance / control)

Negli approcci event-based, la stima della differenza di capacità di attacco e di resistenza, è un elemento centrale delle valutazioni.

Questo a differenza dei modelli asset-based, dove spesso la vulnerabilità indica una debolezza del sistema.



Altri approcci che analizzano queste dimensioni?

MITRE e MITRE ATT&CK

- Società americana no profit, con fondi federali di R&S; nasce come spin-off del MIT Lincoln Laboratory.

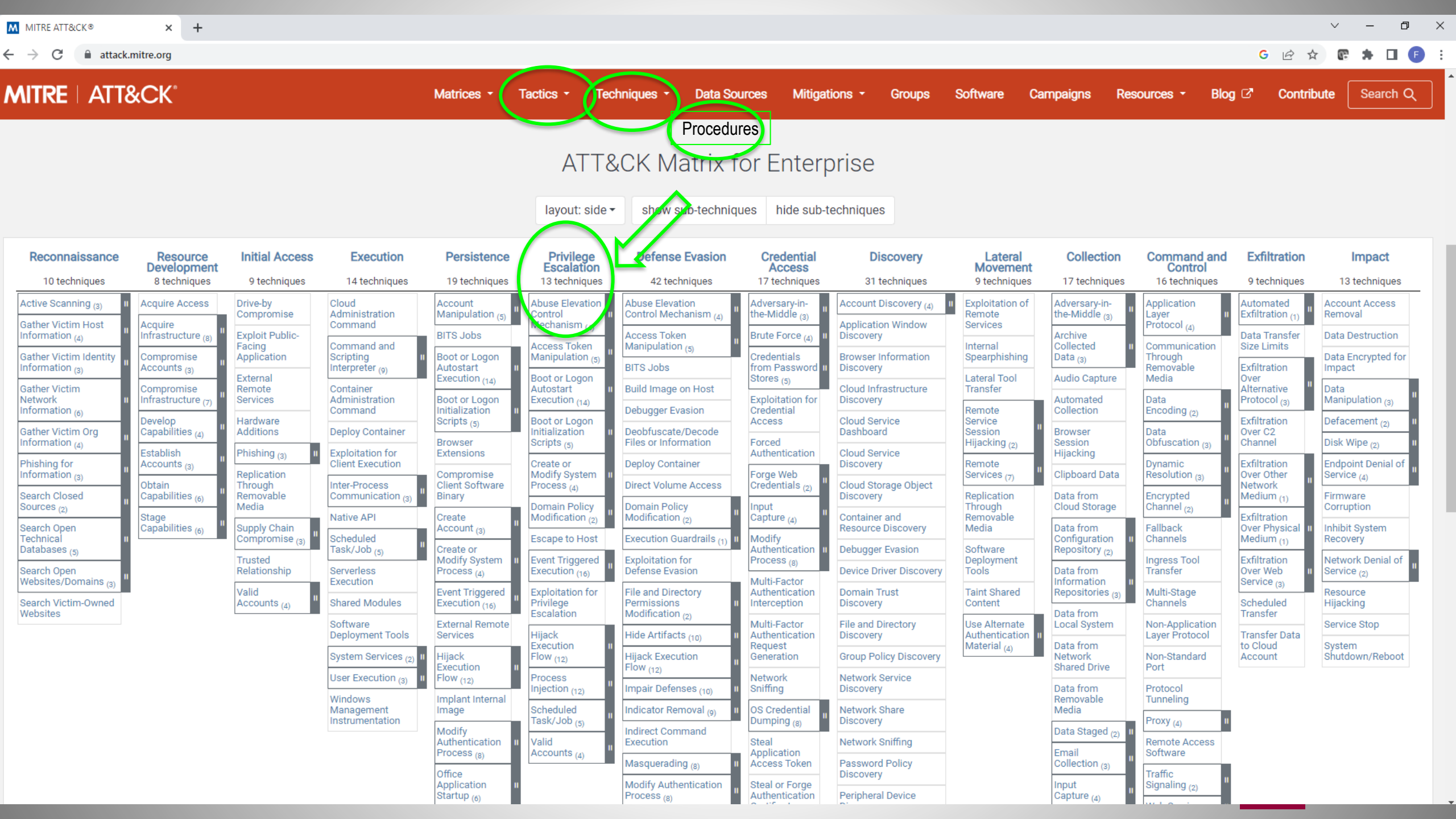
- ATT&CK inizia nel 2013 per documentare tattiche, tecniche e procedure (tactics, techniques, and procedures o TTPs) utilizzati in APT contro ambienti Windows, in framework MITRE ATT&CK viene lanciato nel 2015. Da poco è stata rilasciata la v13.
  - *According to a 2020 study published by the University of California, Berkeley and security software company McAfee, 80 percent of companies use the framework for cybersecurity.*
  - *The Structured Threat Information eXchange (STIX) was developed by MITRE and the Department of Homeland Security.*

- Regole di utilizzo
  - *ATT&CK is open and available to any person or organization for use at no charge. If you decide to use ATT&CK, then follow the terms of use.*

MITRE ATT&CK

ATT&CK è:

- Una **knowledge base** di cyber **adversary** behavior
- Una **tassonomia** per le azioni avversarie nel corso del loro ciclo di vita


MITRE ATT&CK®
attack.mitre.org
MITRE | ATT&CK
Matrices
Tactics
Techniques
Data Sources
Mitigations
Groups
Software
Campaigns
Resources
Blog
Contribute
Search
Procedures
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (3)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (7)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (6)
Stage Capabilities (6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (9)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation
Persistence
19 techniques
Account Manipulation (5)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (16)
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (8)
Office Application Startup (6)
Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)
Defense Evasion
42 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (10)
Hijack Execution Flow (12)
Impair Defenses (10)
Indicator Removal (9)
Indirect Command Execution
Masquerading (8)
Modify Authentication Process (8)
Credential Access
17 techniques
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (8)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication
Discovery
31 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (7)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Adversary-in-the-Middle (3)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (2)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (3)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

TECHNIQUES
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Abuse Elevation Control Mechanism
Setuid and Setgid
Bypass User Account Control
Sudo and Sudo Caching
Elevated Execution with Prompt
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Mobile
ICS

Abuse Elevation Control Mechanism

Sub-techniques (4)

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

ID: T1548
Sub-techniques: T1548.001, T1548.002, T1548.003, T1548.004
Tactics: Privilege Escalation, Defense Evasion
Platforms: Linux, Windows, macOS
Permissions Required: Administrator, User
Version: 1.1
Created: 30 January 2020
Last Modified: 21 April 2023

Version Permalink

Mitigations

ID	Mitigation	Description
M1047	Audit	Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.[1]
M1038	Execution Prevention	System settings can prevent applications from running that haven't been downloaded from legitimate repositories which may help mitigate some of these issues. Not allowing unsigned applications from being run may also mitigate some risk.
M1028	Operating System Configuration	Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised. Additionally, the number of programs with setuid or setgid bits set should be minimized across a system. Ensuring that the sudo tty_tickets setting is enabled will prevent this leakage across tty sessions.
M1026	Privileged Account Management	Remove users from the local administrator group on systems. By requiring a password, even if an adversary can get terminal access, they must know the password to run anything in the sudoers file. Setting the timestamp_timeout to 0 will require the user to input their password every time sudo is executed.
M1022	Restrict File and Directory Permissions	The sudoers file should be strictly edited such that passwords are always required and that users can't spawn risky processes as users with higher privilege.
M1052	User Account Control	Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL Search Order Hijacking.

Detection

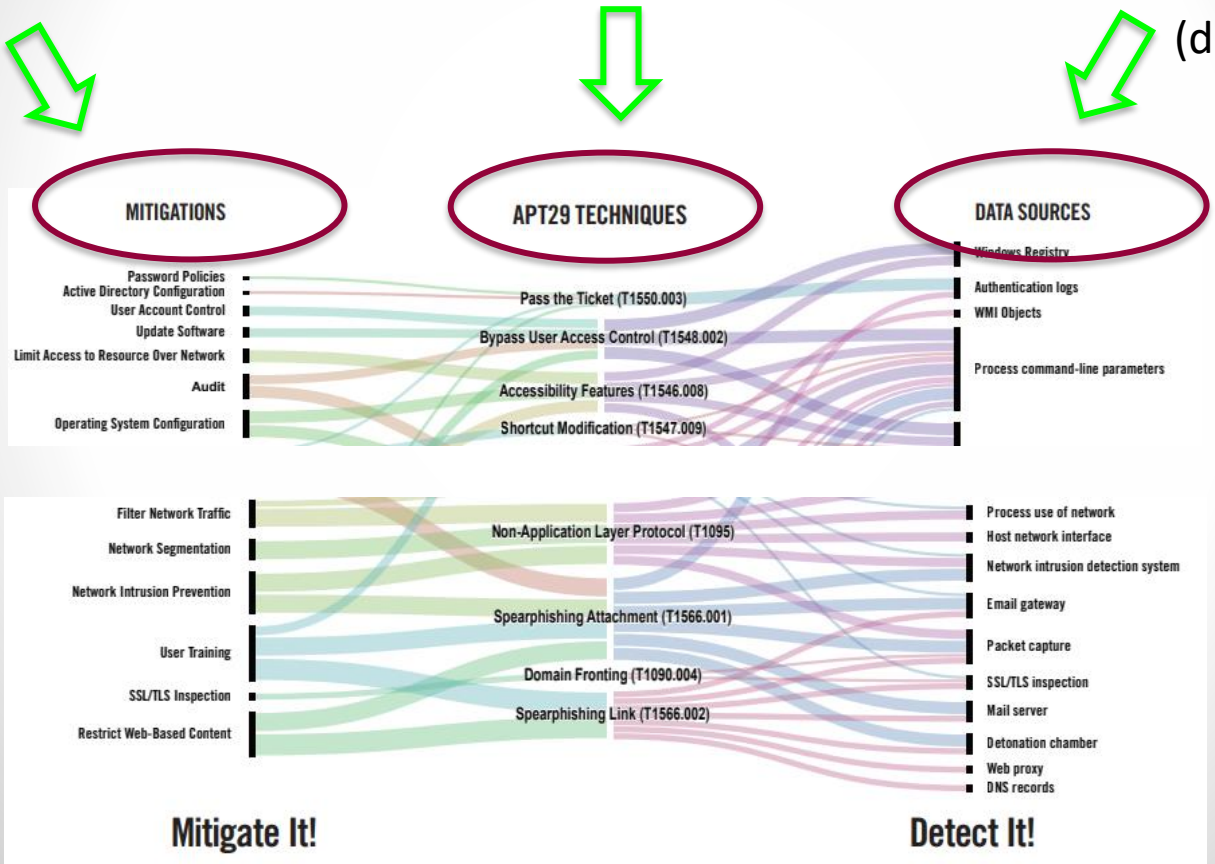
ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions.
DS0022	File	File Metadata	Monitor the file system for files that have the setuid or setgid bits set. On Linux, auditd can alert every time a user's actual ID and effective ID are different (this is what happens when you sudo).
		File Modification	On Linux, auditd can alert every time a user's actual ID and effective ID are different (this is what happens when you sudo). This technique is abusing normal functionality in macOS and Linux systems, but sudo has the ability to log all input and output based on the `LOG_INPUT` and `LOG_OUTPUT` directives in the `/etc/sudoers` file. Consider monitoring for `/usr/libexec/security_authtrampoline`

Elementi ricorrenti

- (behavioral) group profiling
- Attack strength

Control strength

Loss event reduction (detection)



From “attack roadmap”

Livello di astrazione

- A mid-level adversary model like ATT&CK is necessary to tie these various components together. The tactics and techniques in ATT&CK define adversarial behaviors within a lifecycle to a degree where they can be more effectively mapped to defenses.

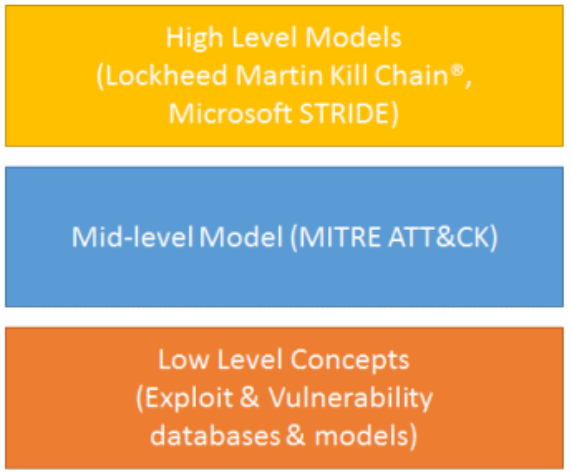


Figure 5. Abstraction Comparison of Models and Threat Knowledge Databases

Utilizzi:

- Creazione di scenari di simulazione di attacco, per testare le difese contro tecniche di attacco comuni (adversary simulation)
- Valutazione del gap delle capacità di difesa – individuazione delle componenti aziendali con deficit in controlli (difese) o in visibilità
- Valutazione delle maturità dei processi di rilevazione e risposta alle minacce (SOC)
- Valutazione delle postura di sicurezza rispetto ad un gruppo avversario specifico

Digital Operational Resilience Act (DORA)

- The Digital Operational Resilience Act (Regulation (EU) 2022/2554) solves an important problem in the EU financial regulation.
- Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience.
- After DORA, they must also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.
- DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring

https://www.digital-operational-resilience-act.com/

Digital Operational Resilience Act (DORA)

Cinque pillar:

- ICT Risk Management
- ICT Incident Reporting
- Digital Operational resilience testing
- Information and intelligence sharing
- ICT third-party risk management

1.1

a) obblighi applicabili alle entità finanziarie in materia di:

- i) gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC);
- ii) segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC e notifica, su base volontaria, delle minacce informatiche significative;
- iii) segnalazione alle autorità competenti, da parte delle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), di gravi incidenti operativi o relativi alla sicurezza dei pagamenti;
- iv) test di resilienza operativa digitale;
- v) condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche;
- vi) misure relative alla solida gestione dei rischi informatici derivanti da terzi;

DORA 1.1

Cinque pillar:

- ICT Risk Management
- ICT Incident Reporting
- Digital Operational resilience testing
- Information and intelligence sharing
- ICT third-party risk management

- 8.2 Le entità finanziarie identificano costantemente tutte le fonti di rischio relative alle TIC, in particolare l'esposizione al rischio da e verso altre entità finanziarie, e valutano le minacce informatiche e le vulnerabilità in materia di TIC pertinenti per le loro funzioni commerciali supportate dalle TIC, per i loro patrimoni informativi e per i loro risorse TIC. Le entità finanziarie riesaminano periodicamente, e almeno una volta all'anno, gli scenari di rischio che esercitano un impatto su di loro.
- in Art. 11: Continuità operativa, BIA, scenari

Consid. (56)
Per conseguire un elevato livello di resilienza operativa digitale, e in linea sia con le pertinenti norme internazionali (ad esempio, gli elementi fondamentali del G7 per i test di penetrazione basati su minacce) che con i quadri applicati nell'Unione, come TIBER-EU, le entità finanziarie dovrebbero sottoporre periodicamente a test i propri sistemi di TIC e il proprio personale con responsabilità connesse alle TIC per valutare l'efficacia delle relative capacità di prevenzione, individuazione, risposta e ripristino, allo scopo di scoprire e affrontare le potenziali vulnerabilità in materia di TIC
Articolo 26
Test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (TLPT)

Agenda

- Introduzione: scenari e valutazione del rischio
- ISO27002 e 27005
- Gli scenari di rischio ISACA e l'utilizzo nel modello quantitativo FAIR
- Altri spunti: MITRE, DORA
- Considerazioni conclusive

Considerazioni conclusive

- Descrizione delle scenario corrisponde al modello scelto (non viceversa)
- Focalizzarsi sui dati statistici può portare al overreliance sul passato
- Scenari strategici e operative: non solo ISO27005
- Relazione scenari di rischio – monitoraggio
- Importanza del “time”