Analisi e gestione del rischio cyber

Vincenzo Calabrò

PARTE 1 –
SCALDIAMO
I MOTORI

PARTE 2 –
E' TEMPO
DI 31000

PARTE 3 –
INFORMATION
SECURITY

PARTE 4 –IL
CISO (CHIEF INFORMATION
SECURITY MANAGER)

PARTE 3 – INFORMATION SECURITY

Information & co

Dati: insieme di singoli fatti, immagini e impressioni

Informazioni: dati organizzati e significativi

Conoscenza: informazioni recepite e comprese da un singolo individuo

Sapienza: conoscenze tra loro connesse che permettono di prendere decisioni

Le informazioni sono trasmesse e archiviate su dei supporti.

- I supporti possono essere digitali o analogici / non digitali (carta, fotografie su pellicola…)
- Un caso particolare di supporto non digitale è l'essere umano

Per la trasmissione si possono usare reti informatiche, posta tradizionale, telefono, conversazioni…

Information security (ISO/IEC 27000:2018)

preservation of confidentiality, integrity and availability of information

DEFINIZIONE

DEFINIZIONE

CIA (ISO/IEC 27000:2018)

Confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity

property of accuracy and completeness

Availability

property of being accessible and usable on demand by an authorized entity

DEFINIZIONE

Information security (ISO/IEC 27000:2018)

preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

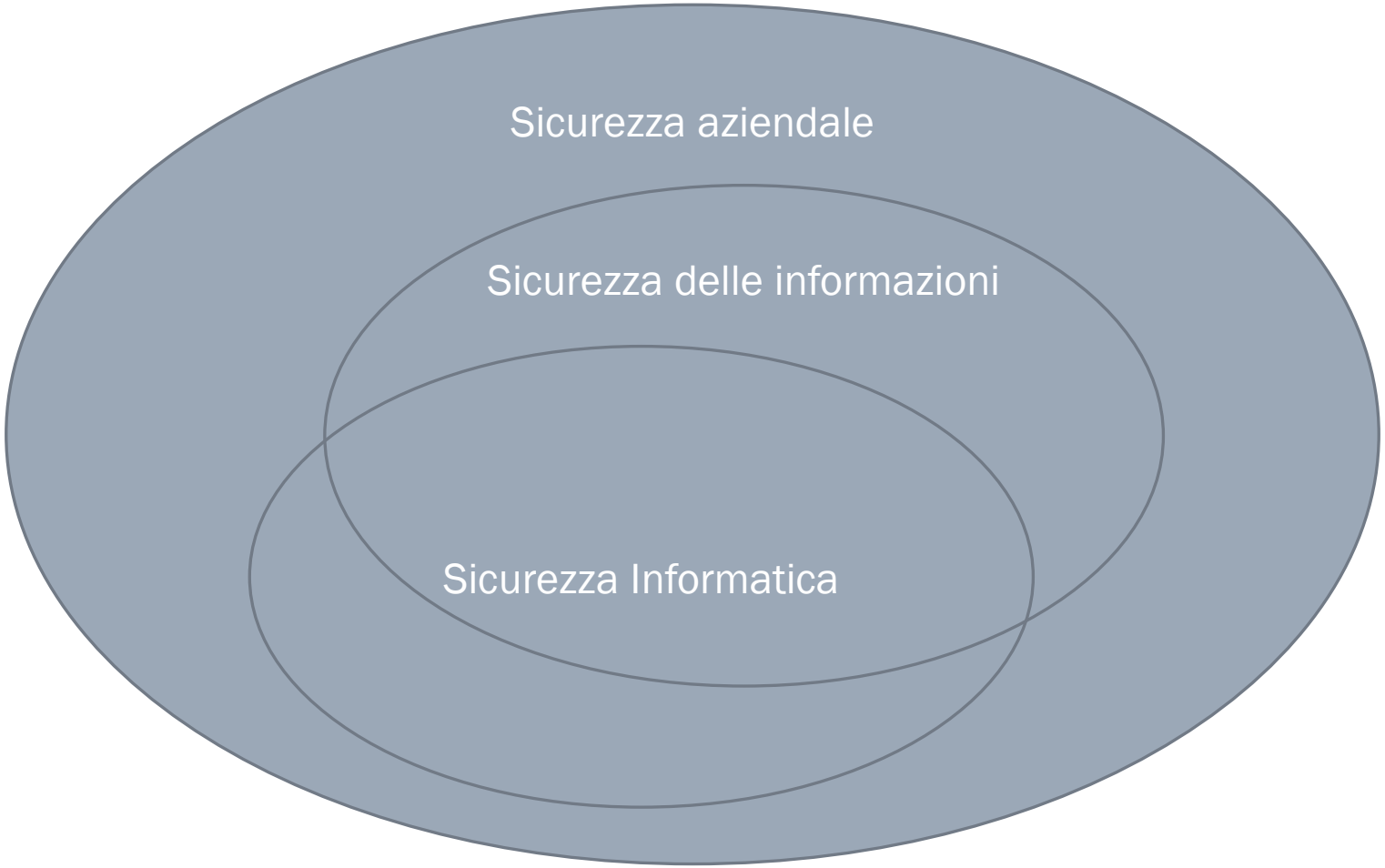
3.6
authenticity
property that an entity is what it claims to be

Non definito nella ISO/IEC 27000 ma (in modo diverso) in numerose altre norme. Riguarda la responsabilità e la possibilità di attribuire la responsabilità di un evento a un'entità

3.48
non-repudiation
ability to prove the occurrence of a claimed *event* (3.21) or action and its originating entities

3.55
reliability
property of consistent intended behaviour and results

Information security



DEFINIZIONE

Management system (ISO/IEC 27000:2018)

set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

Sistemi di gestione secondo le norme ISO

Con tale termine si intendono tutti i sistemi di gestione implementati nelle organizzazioni (imprese, società, enti o aziende pubbliche, studi professionali, associazioni, ecc.) nei diversi settori in cui operano (es. manifatturiero, commercio, agricoltura, servizi, costruzioni, istituzioni, ecc.) in riferimento ai requisiti espressi da una serie di norme internazionali ISO, tra le quali:

- ISO 9000 per i sistemi di gestione della qualità
- ISO 14000 per i sistemi di gestione ambientale
- UNI CEI EN ISO 50000 per i sistemi di gestione dell'energia
- ISO 45001 per i sistemi di gestione della sicurezza e della salute nei luoghi di lavoro
- SA 8000 impatto sull'etica e sul sociale (emessa dal SAI)
- ISO 27001 per i sistemi di gestione della sicurezza delle informazioni
- ISO 19600 per i sistemi di gestione della conformità (legislativa)

FONTE: https://it.wikipedia.org/wiki/Sistema_di_gestione

SGSI = Sistema di gestione per la sicurezza delle informazioni
ISMS = Information Security Management System

Cosa ci dicono i sistemi di gestione?

Per un certo ambito (disciplina), oppure per più ambiti, suggeriscono cosa fare

- in termini organizzativi
- di ruoli
- di responsabilità
- in merito alla pianificazione
- riguardo alle operazioni

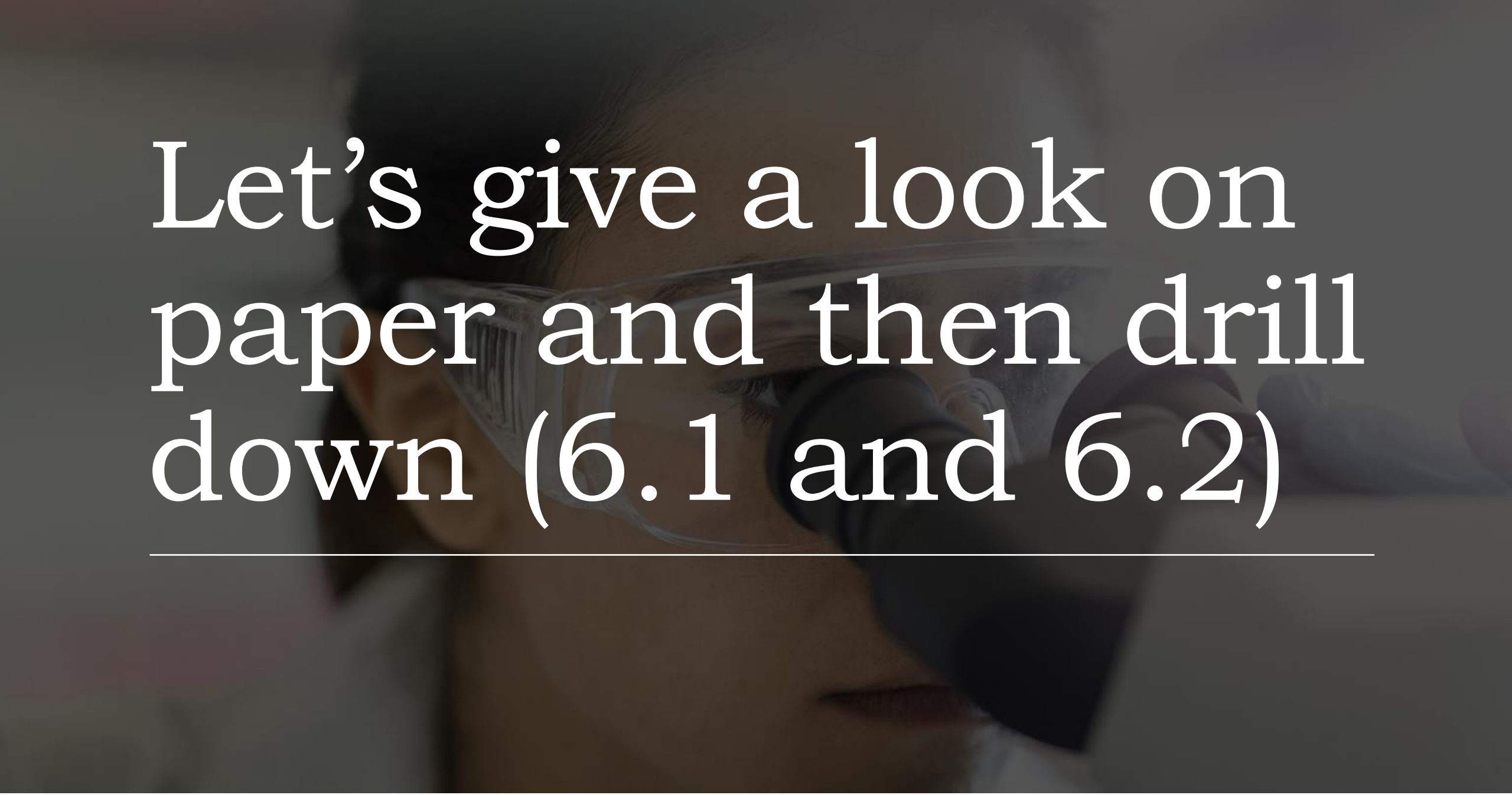
Ci possono essere delle sovrapposizioni tra diversi sistemi come, per esempio, nel caso della prevenzione degli incendi che è materia comune alla sicurezza delle informazioni, alla sicurezza fisica e alla sicurezza e salute del personale. Queste sovrapposizioni comportano delle opportunità «di riuso» ma anche rischi di sprechi e contrasto all'interno (e all'esterno) dell'organizzazione

In generale i sistemi di gestione sono un'opportunità per aiutare a fare bene le cose; inoltre, si può ottenere una certificazione che attesti che l'organizzazione stia facendo bene le cose.

Table of contents

Argomenti della ISO 27001:2013

FONTE: https://www.iso.org/obp/ui#iso:std:iso-iec:27001:ed-2:v1:en

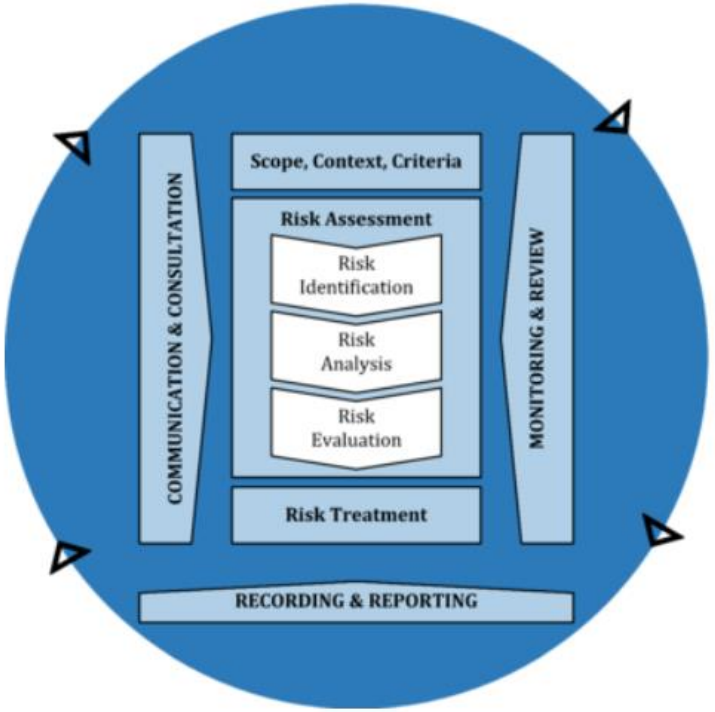


Let’s give a look on paper and then drill down (6.1 and 6.2)

Risk assessment and risk treatment #6.1

- 6 Planning
  - 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

Un parallelo tra 31000 e 27001



FONTE: ISO 3100:2018

FONTE: ISO/IEC 27001:2013

IDENTIFICATION

1. Identificare i rischi associati alla perdita di riservatezza, integrità e disponibilità — 6.1.2.C.1
2. Identificare i risk owner — 6.1.2.C.2

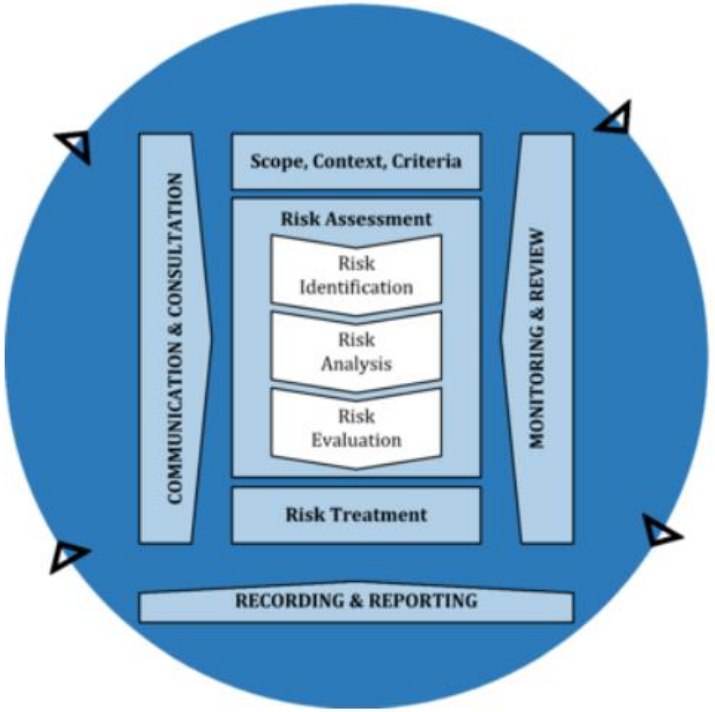
ANALYSIS

1. Analizzare l'impatto del rischio — 6.1.2.D.1
2. Analizzare le probabilità di accadimento — 6.1.2.D.2
3. Determinare il livello del rischio — 6.1.2.D.3

EVALUATION

1. Ponderare i rischi rispetto ai criteri di accettabilità — 6.1.2.E.1
2. Prioritizzare i trattamenti — 6.1.2.E.2

Un parallelo tra 31000 e 27001



FONTE: ISO 3100:2018

TREATMENT

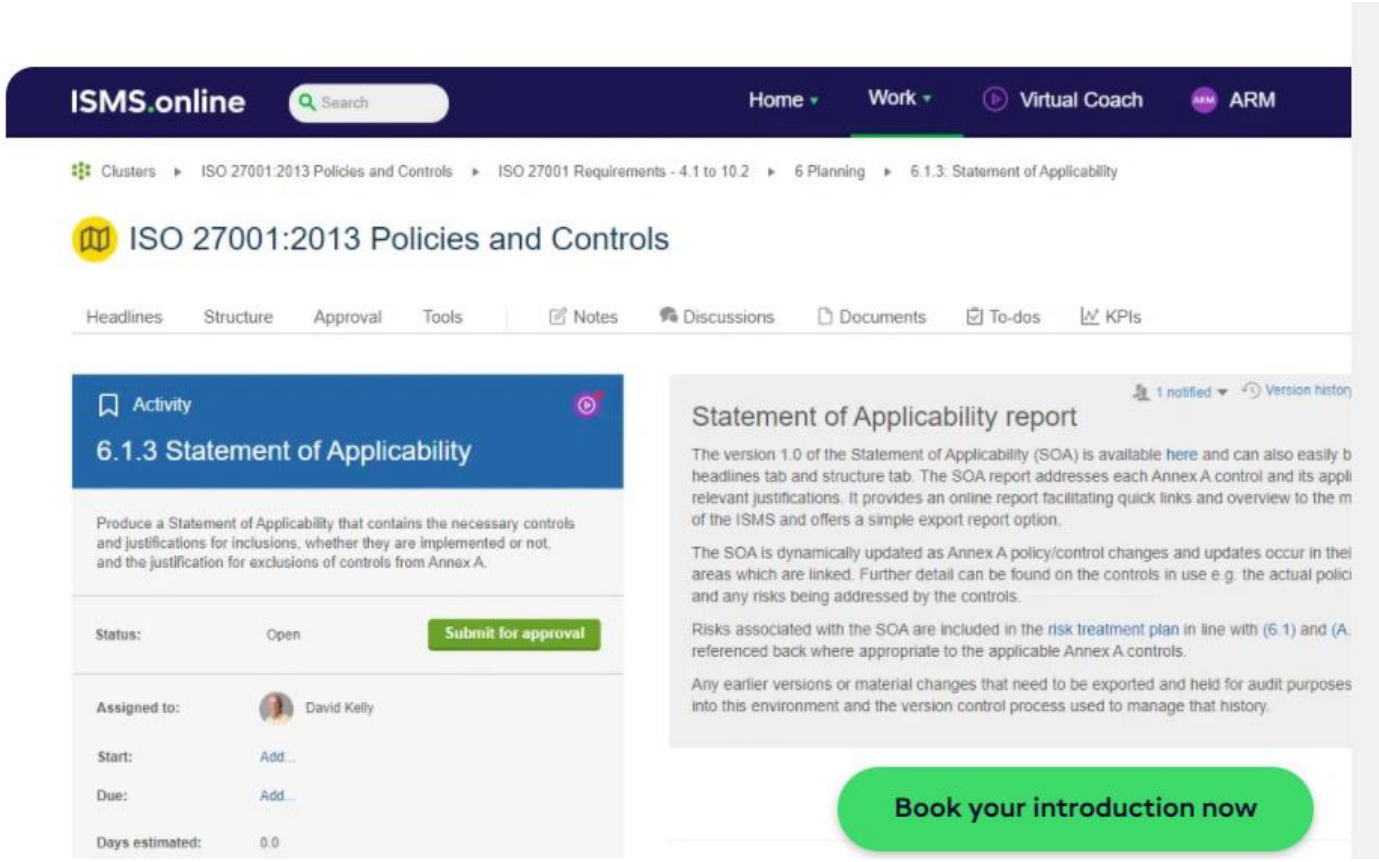
FONTE: ISO/IEC 27001:2013

1. Selezionare le opzioni di trattamento
2. Determinare i controlli necessari
3. Confrontare i controlli determinati con quelli dell'annesso A
4. Produrre lo Statement of Applicability
5. Formulare il piano di trattamento
6. Ottenere l'approvazione

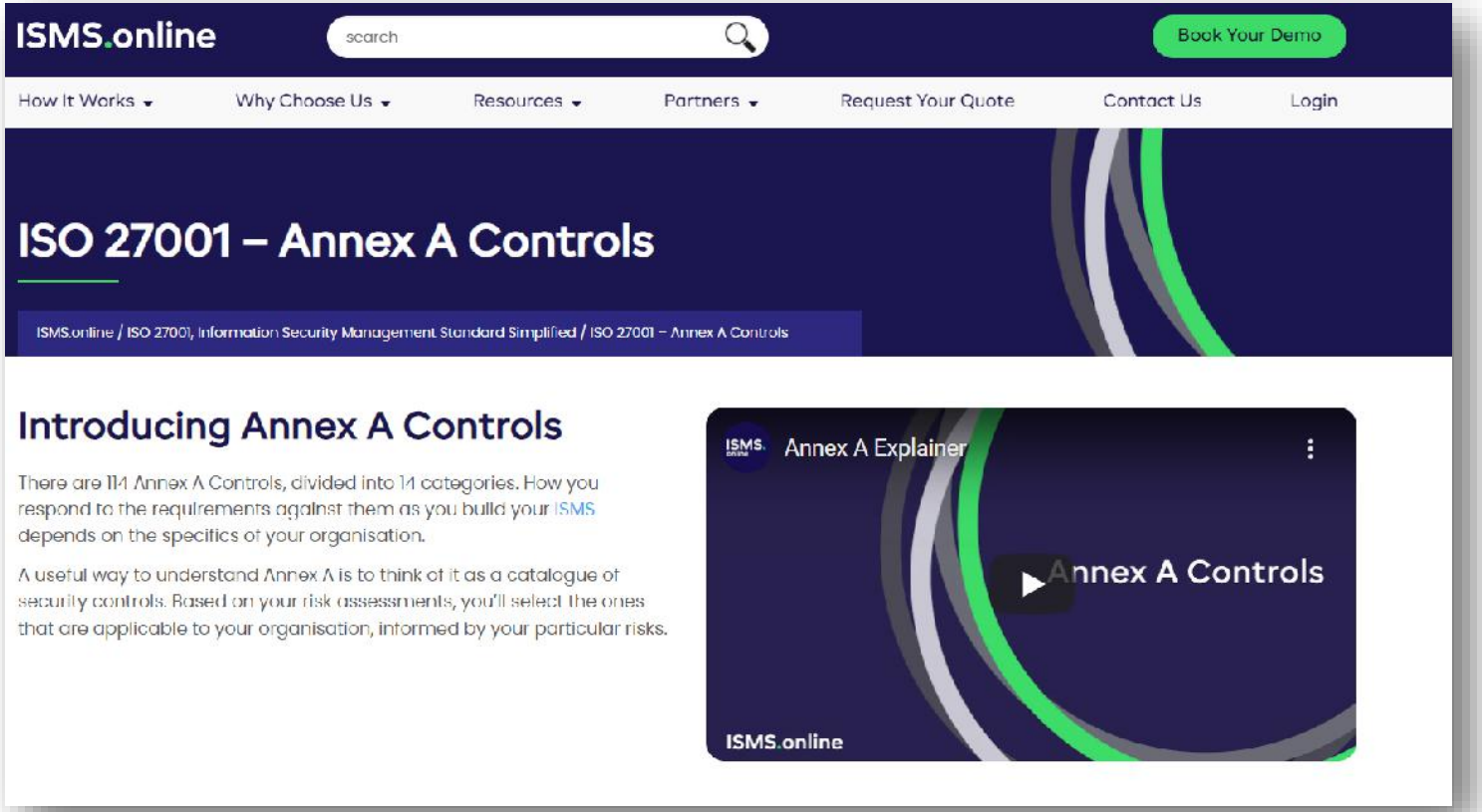
6.1.3 (A fino F)

Cosa è lo Statement of Applicability

The Statement of Applicability (SoA) forms a fundamental part of your information security management system (ISMS). The SoA is one of the most important documents you'll need to develop for ISO 27001:2013 certification. Put simply, in its quest to protect valuable information assets and manage the information processing facilities, the SoA states what ISO 27001 controls and policies are being applied by the organisation. It benchmarks against the Annex A control set in the ISO 27001 standard (described at the back of that ISO standards document as reference control objectives and controls). The statement of applicability is found in 6.1.3 of the main requirements for ISO 27001, which is part of the broader 6.1, focused on actions to address risks and opportunities. The SoA is therefore an integral part of the mandatory ISO 27001 documentation that needs to be presented to an external auditor when the ISMS is undergoing an independent audit e.g. by a UKAS audit certification body.



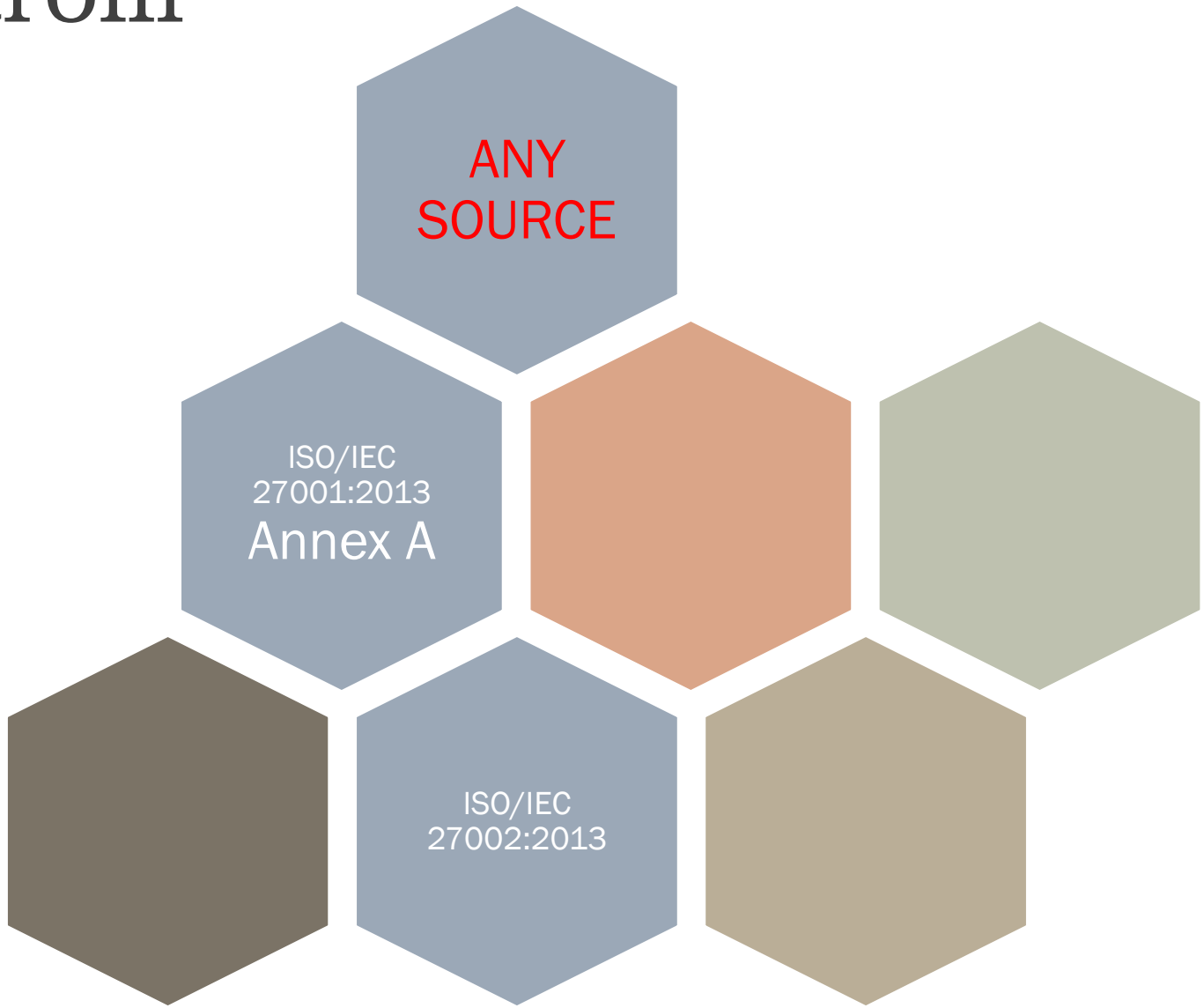
FONTE: https://www.isms.online/iso-27001/iso27001-statement-applicability-simplified/



Vediamo ISO 27001 - Annex A

https://www.isms.online/iso-27001/annex-a-controls/

Liste di controlli



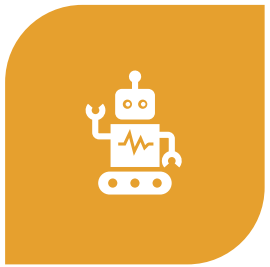
DEFINIZIONE

Control (ISO/IEC 27000:2018)

measure that is modifying risk

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.



CONTROLLO

MISURA

CONTROMISURA

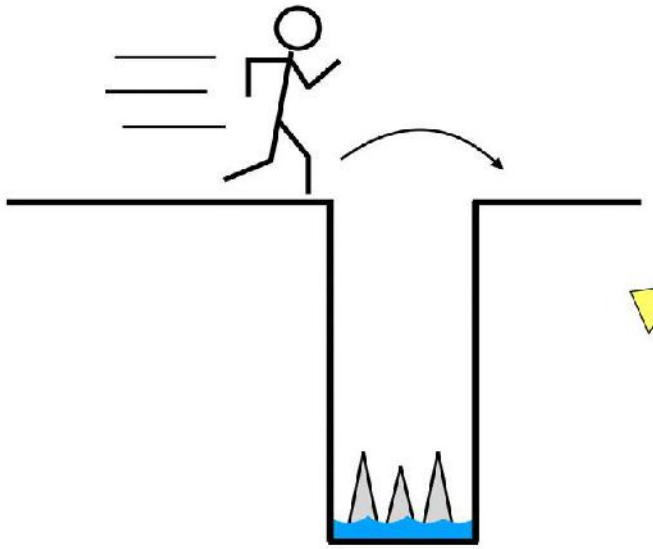
Sinonimi correntemente usati

Su cosa agiscono i controlli

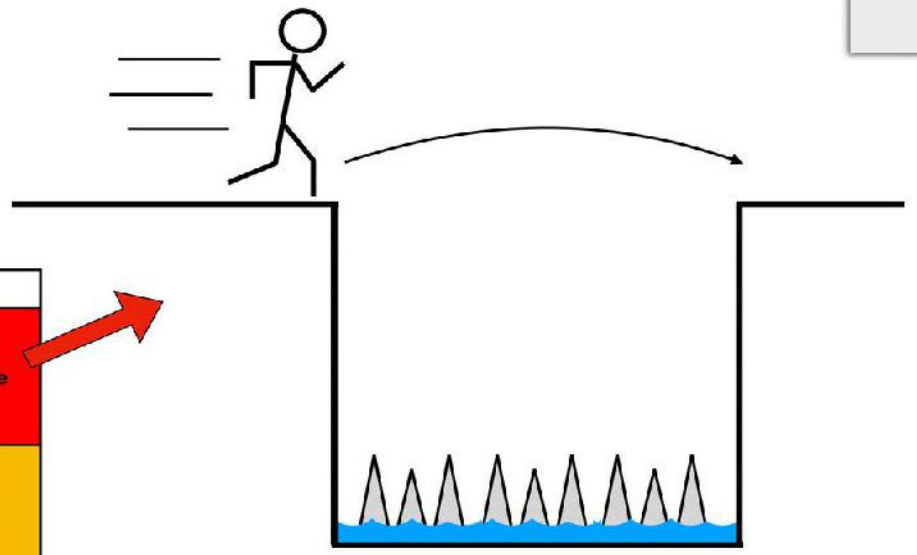
Risk Assessment Matrix				
Impact of Risk (Consequence)	Major Impact	**Medium**	**High**	**Extreme**
	Moderate Impact	**Medium**	**Medium**	**High**
	Minor Impact	**Low**	**Medium**	**Medium**
Risk Exposure = Impact x Probability		Unlikely (0-33%)	Moderately Likely (33%-66%)	Very Likely (66%+)
		Probability of Risk (Likelihood)		

Assessment of Risk Exposure = Risk Probability x Impact

(Severity = Likelihood x Consequence)

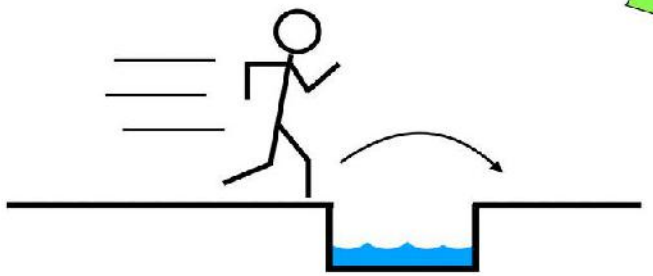


Low Probability & High Impact

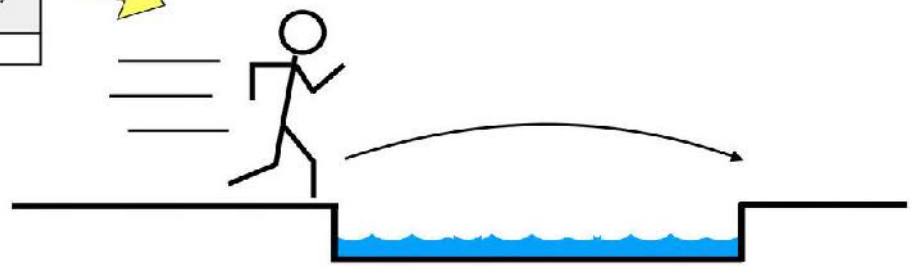


High Probability & High Impact

Risk Assessment Matrix				
Impact of Risk (Consequence)	Major Impact	Medium	High	Extreme
	Moderate Impact	Medium	Medium	High
	Minor Impact	Low	Medium	Medium
Risk Exposure = Impact x Probability		Unlikely (0-33%)	Moderately Likely (33%-66%)	Very Likely (66%+)
		Probability of Risk (Likelihood)		

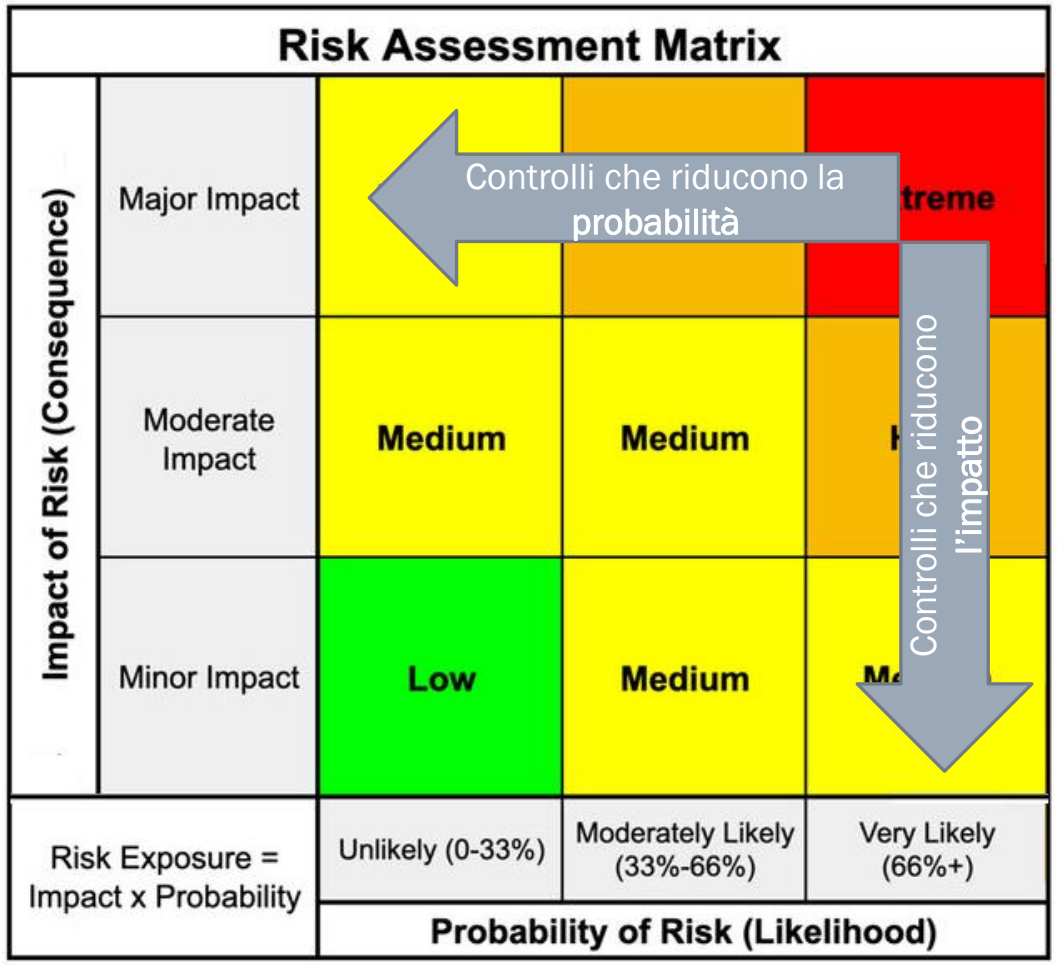


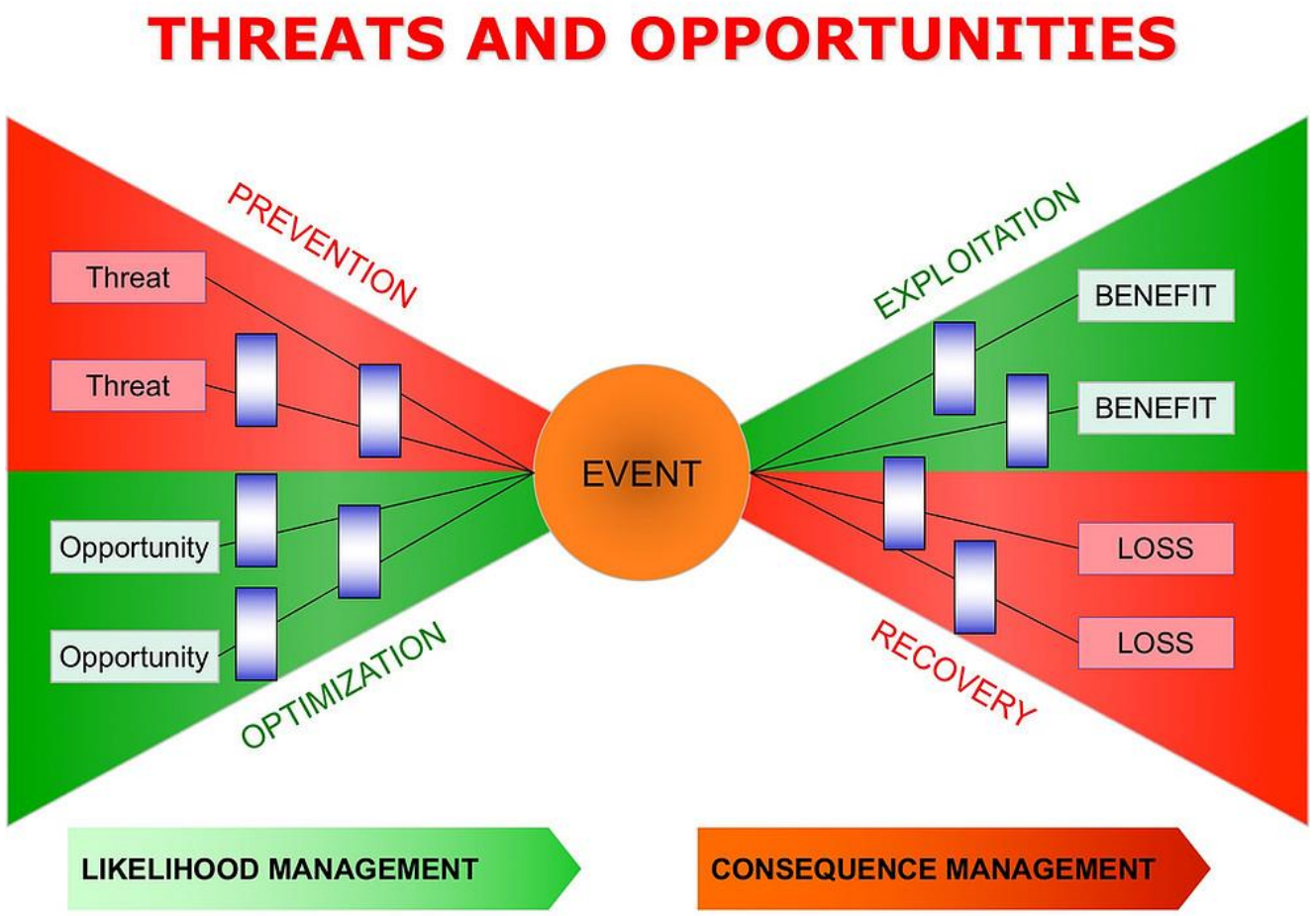
Low Probability & Low Impact



High Probability & Low Impact

Tipi di controlli



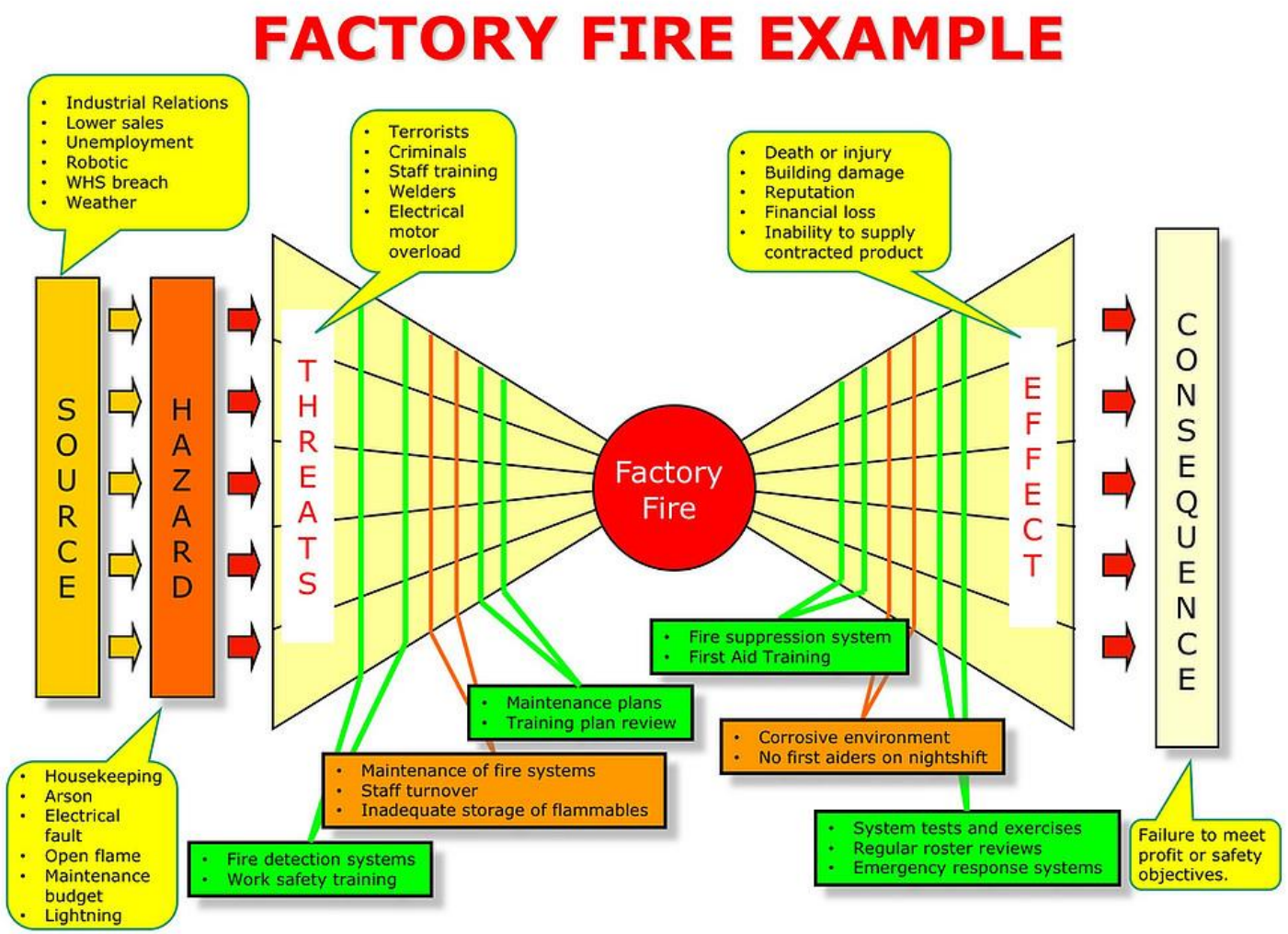


FONTE: https://www.juliantalbot.com/post/risk-bow-tie-method

JULIAN TALBOT

HOME BOOKS DOWNl

Bow tie analysis (farfallino)

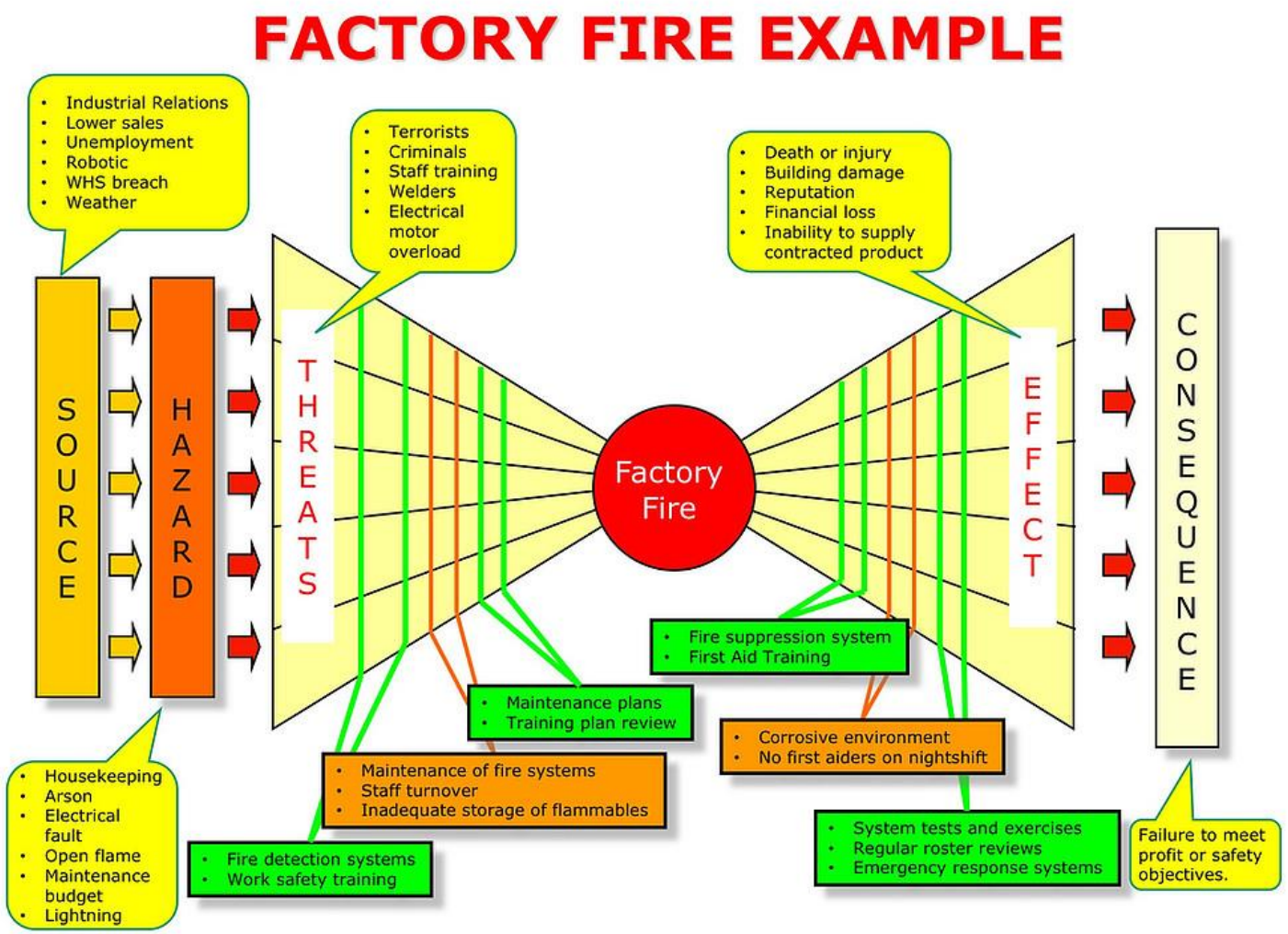


FONTE: https://www.juliantalbot.com/post/risk-bow-tie-method

JULIAN TALBOT

HOME BOOKS DOWNl

Esempio



FONTE: https://www.juliantalbot.com/post/risk-bow-tie-method

JULIAN TALBOT

HOME BOOKS DOWNl

Un controllo può introdurre altri rischi

Tipi di controlli

Tecnici

basato sulla tecnologia, di norma automatico, che funziona a prescindere dall'intervento attivo dell'uomo

Organizzativi

regole e procedure che le persone devono seguire

Tipi di controlli

Confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity

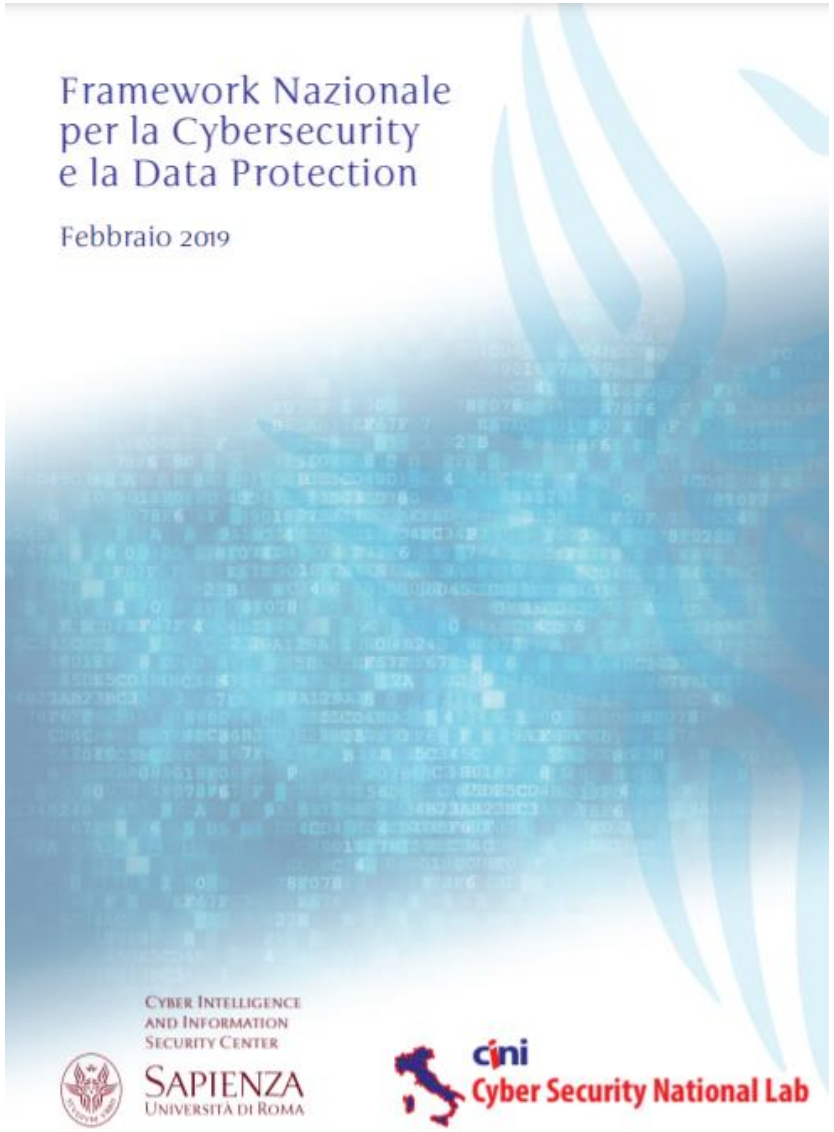
property of accuracy and completeness

Availability

property of being accessible and usable on demand by an authorized entity

Framework Nazionale per la Cybersecurity e la Data Protection

https://www.cybersecurityframework.it/



Framework Nazionale Cyber Security

Il Framework Nazionale Cyber Security (FNCS) pubblicato nel 2015 dal CIS Sapienza e dal Laboratorio Nazionale di Cybersecurity del CINI, viene divulgato nel Febbraio 2016 con l'obiettivo principale di fornire a tutte le aziende - inizialmente il target erano le PMI - un ausilio operativo di Cyber Risk Management Strategy, adattabile alla realtà nazionale ed alla tipologia/criticità specifica di ogni business.
Il FNCS, pur riprendendo i concetti fondamentali di cyber threats e la struttura del Framework Core del Cyber Security Framework NIST da cui è stato derivato, si differenzia da esso introducendo, già nella sua prima implementazione, importanti strumenti di modellazione che avrebbero facilitato la contestualizzazione allo specifico settore di business.

FONTE: Prossimo libro sul rischio della Clusit Community for Security

FONTE: https://docs.google.com/document/d/1fc1RL36_5zW-2bUxBnQjMr-rrf5382ysj07D-EAiI3Q/edit

DBSec Most Common Mistakes

Brussels October 2016

Alessandro Vallega
Security Business Development Oracle Europe WCEs
Clusit Board of Directors
Oracle Community for Security Chairman
Founder of EuroPrivacy.info

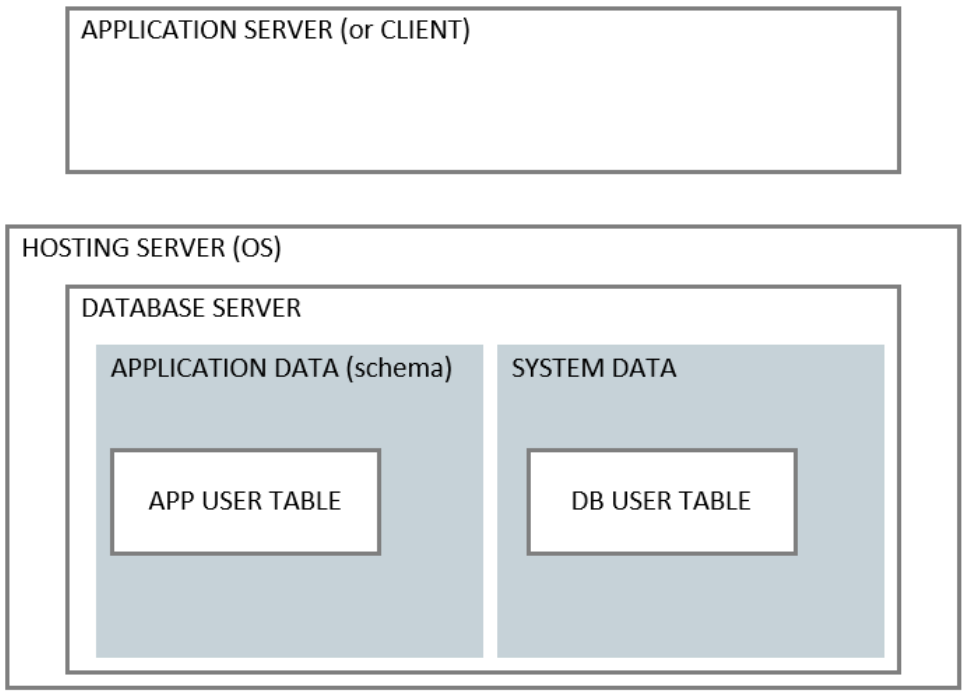
ORACLE

Database Security Maturity Knowledge Areas

DB Security	DB Access Control	Monitoring / Blocking and Audit	Data Protection	Secure Configuration
	Ability to assure access only to authorized users and to control when/where/how the data are accessed 	Ability to analyze the transactional activities (threats/blocks) and to view current transactional activities and historical information 	Processes and controls to secure storage, transmission and accessing of an organization's data throughout its lifecycle 	Process and controls to assure DB configuration for security and compliance 

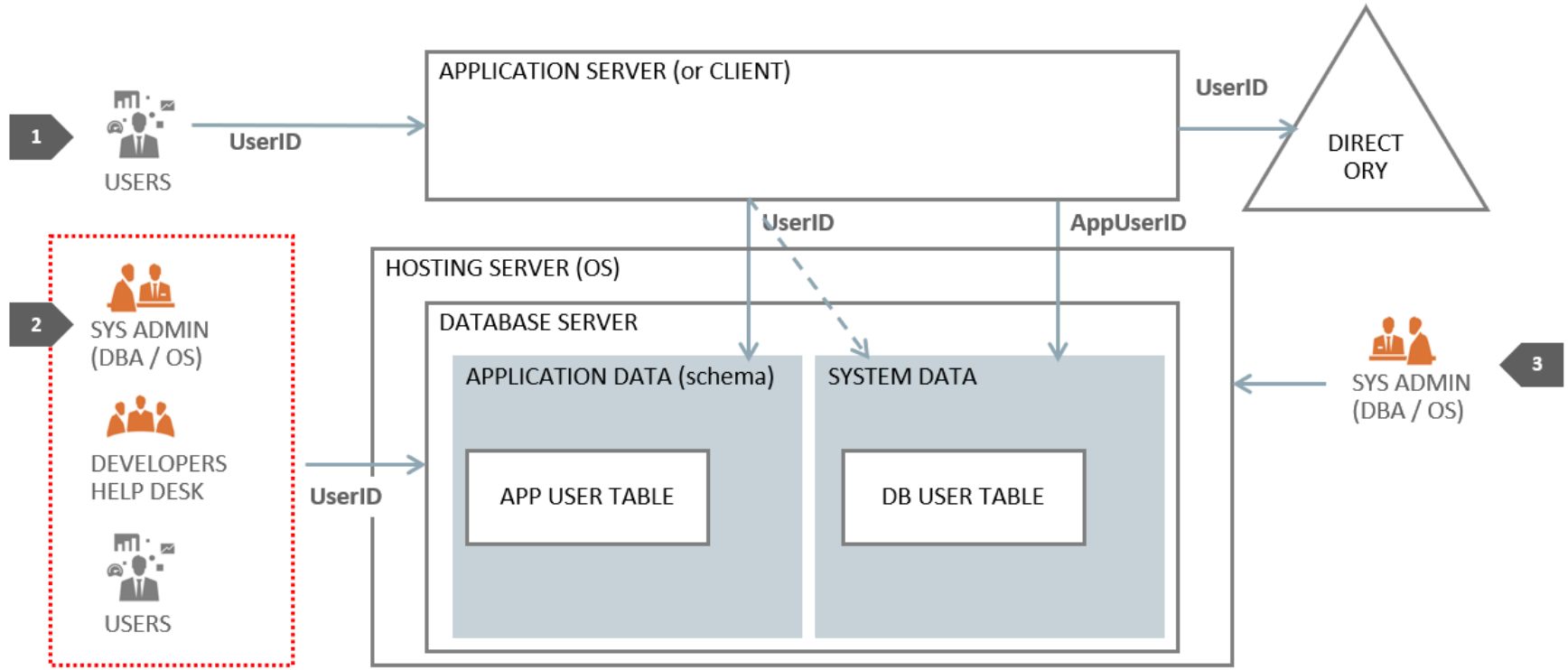
DB Access Control

Authentication and authorization



DB Access Control

Authentication and authorization from 3 different point of views

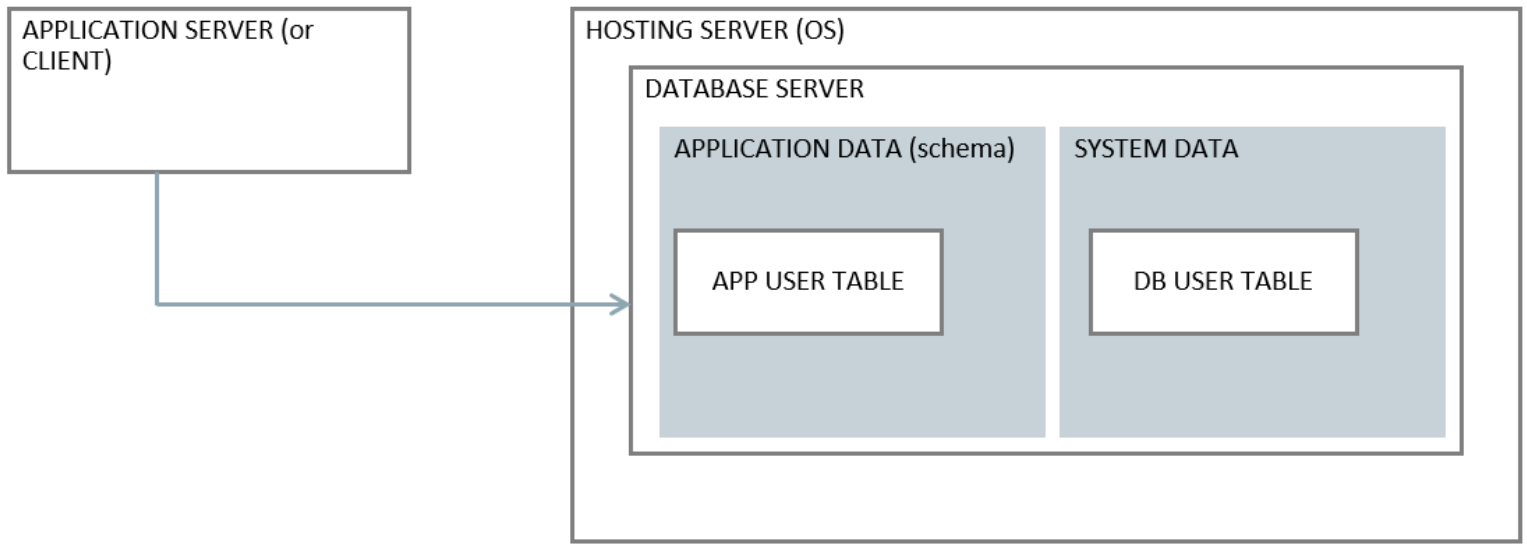


Alcuni errori area DB Access Control

1. Le credenziali dell'applicazione non sono protette nell'application server
2. Gli sviluppatori conoscono e usano le credenziali dell'applicazione
3. I DBA non hanno account personali
4. Le password dei sistemi sono definite in maniera algoritmica e non sono mai cambiate
5. Gli utenti accedono direttamente al DB per fare reporting estemporanei
6. I DBA hanno privilegi eccessivi (DDL **e DML**)

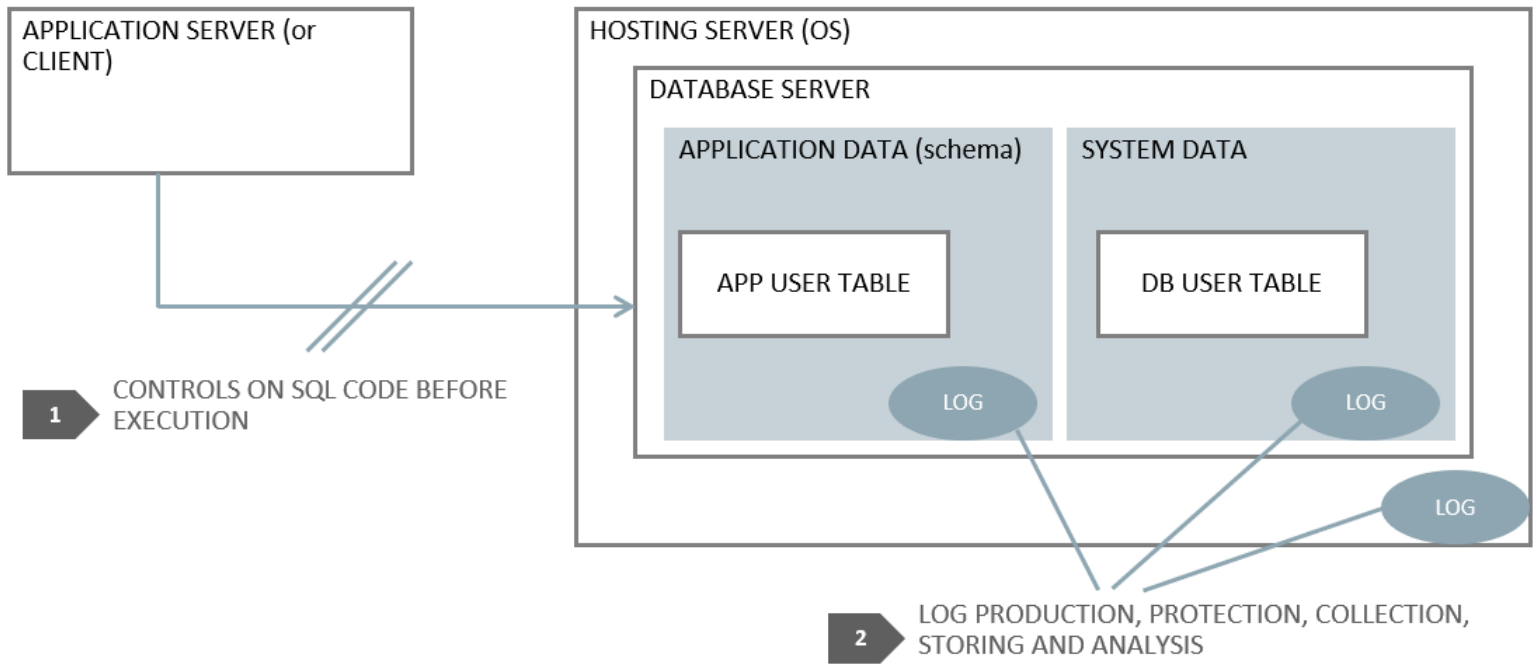
Monitoring, Blocking and Auding

Pre and post execution SQL controls



Monitoring, Blocking and Auding

Pre and post execution SQL controls

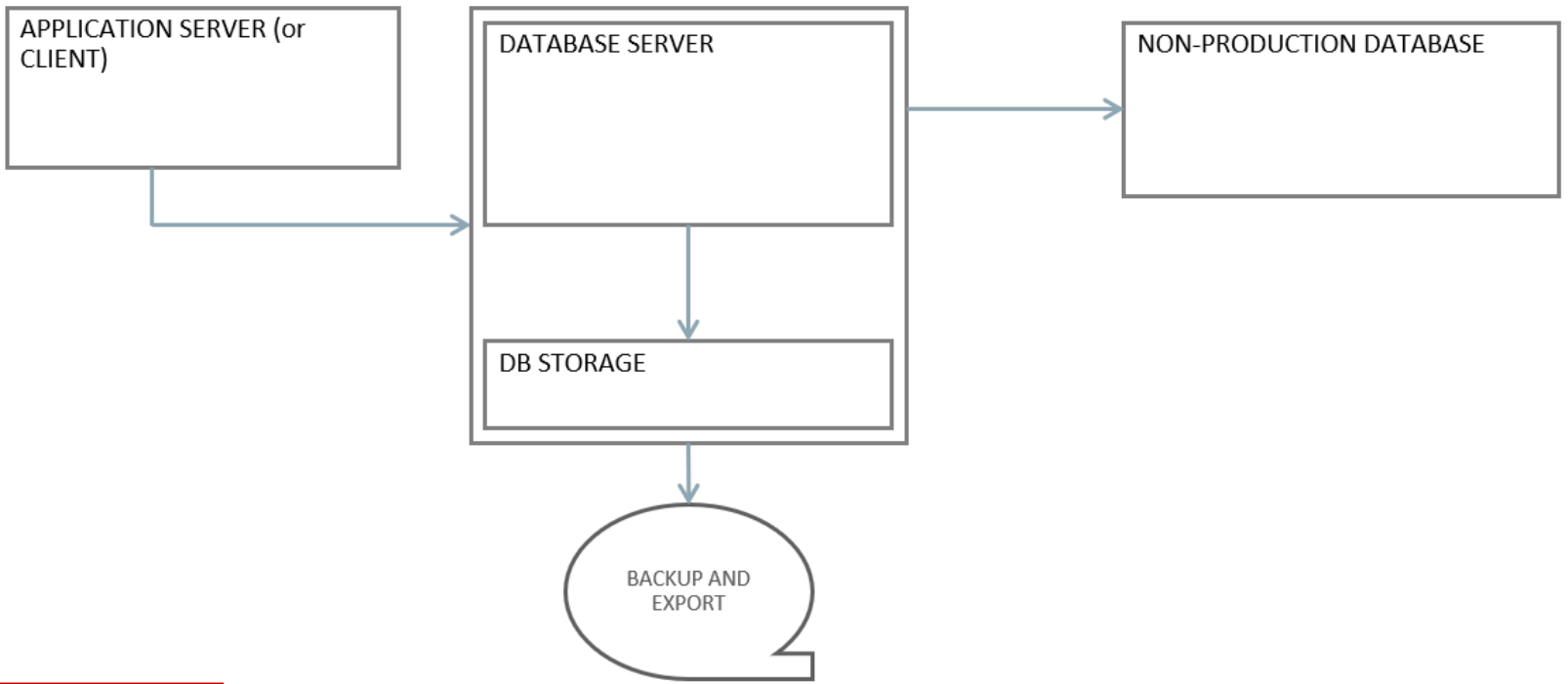


Alcuni errori area Monitoring, Blocking and Audit

1. Non ci sono controlli sull'SQL in input
2. Non vengono prodotti (o conservati) i log
3. I log non vengono analizzati proattivamente
4. I log non contengono l'identificazione degli operatori

Data Protection

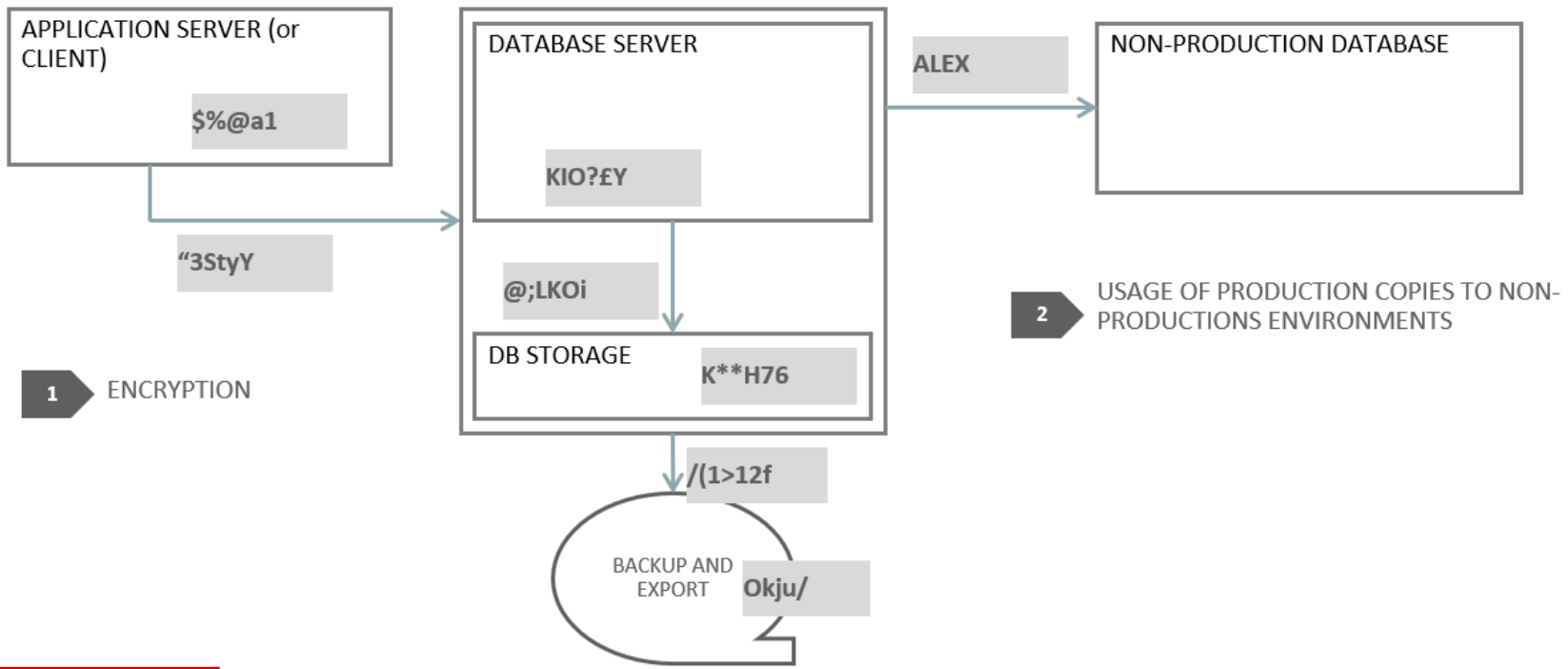
Usage of encryption and indiscriminated production copies



ORACLE

Data Protection

Usage of encryption and indiscriminated production copies

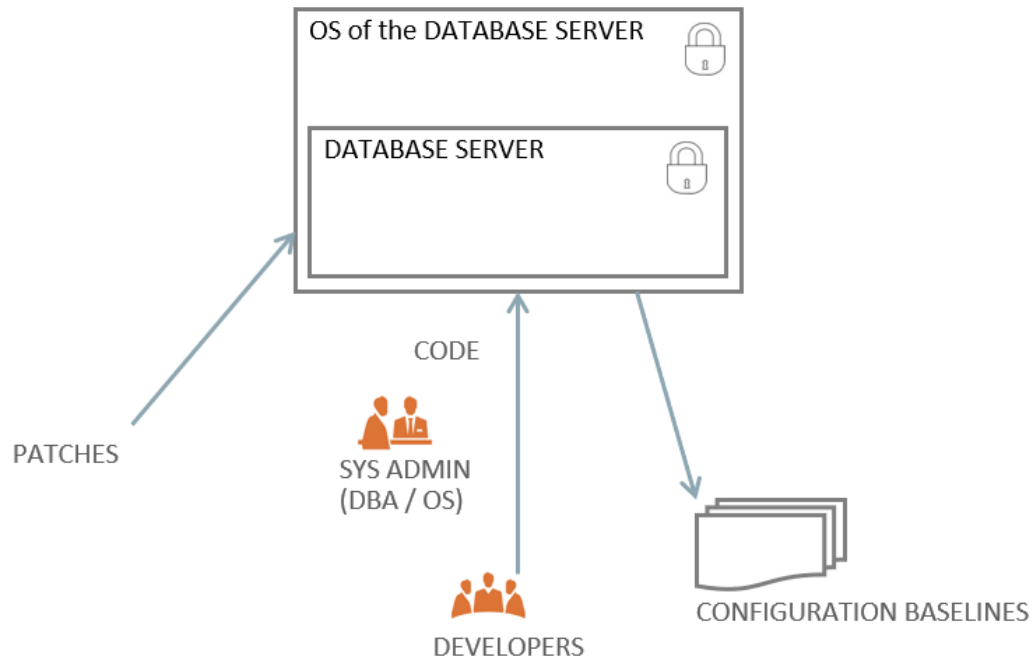


Alcuni errori area Data Protection

1. Non c’è nessun livello di cifratura in produzione (dischi, database, rete, applicazioni)
2. I dati dei backup non sono cifrati
3. I dati di produzione sono copiati nei sistemi di test e sviluppo

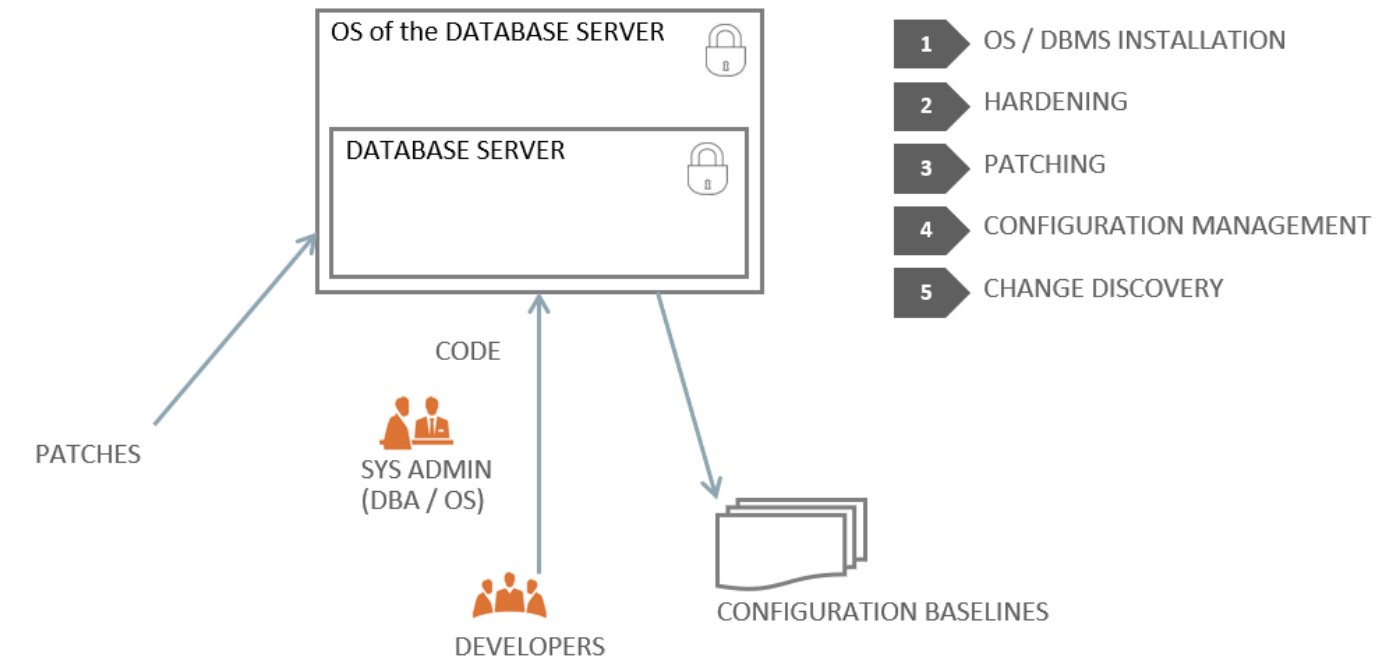
Secure Configuration

Installation, hardening, patching, configuration management...



Secure Configuration

Installation, hardening, patching, configuration management...



Alcuni errori area Secure Configuration

1. Hardware e sistemi operativi obsoleti
2. Patching tardiva o assente
3. VA/PT frammentaria e incostante
4. Scarsi controlli sul software development life cycle