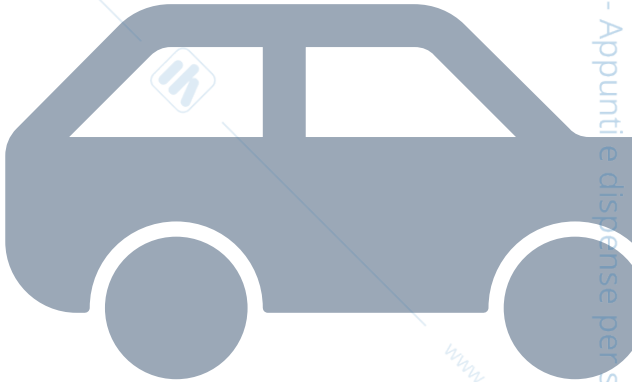
Analisi e gestione de rischio

PROF. ALESSANDRO VALLEGA

UNIVERSITÀ DEGLI STUDI DI MILANO

CORSI DI LAUREA MAGISTRALE IN SICUREZZA INFORMATICA E IN INFORMATICA

PARTE 1 – SCALDIAMO I MOTORI



Cosa significa

PxI

ALESSANDRO VALLEGA - UNIMI - ANALISI E GESTIONE DEL RISCHIO

Il Rapporto inizia con **una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel 2022**, confrontandoli con i dati raccolti nei 4 anni precedenti.

Ci siamo avvalsi anche in questa edizione dei dati relativi agli attacchi in Italia rilevati dal **Security Operations Center (SOC) di FASTWEB**.

L'analisi degli attacchi in Italia è poi completata dalle **rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni**, che ci hanno fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso degli ultimi 12 mesi.

Segue un'analisi realizzata da Libraesva sull'**evoluzione dell'e-mail security in Italia** ed un approfondimento sulla **Sanità, tra cyberattacchi e rischi per la salute**, realizzato dalle Women for Security.

Presentiamo a questo punto l'abituale capitolo dedicato al settore FINANCE, **con un'analisi sul Cyber-crime nel settore finanziario in Europa**, a cura di IBM, ed un contributo realizzato dagli **esperti del CERT di Banca d'Italia** sullo **scenario evolutivo della minaccia ransomware**.

Seguono tre survey.

– La prima, realizzata da Netwrix, che ha intervistato 720 professionisti **sul passaggio al Cloud e sulle problematiche di sicurezza riscontrate**.
– La seconda **sulla gestione del rischio cyber nelle grandi organizzazioni italiane**, realizzata dall'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano.
– La terza sulla **Cybersecurity nelle micro e piccole imprese**, una Survey di CNA Milano e dell'Unione Artigiani Milano.

Rapporto Clusit

https://clusit.it/rapporto-cl

Rapporto Clusit

È importante per le analisi che svolge e l'opera di informazione verso il pubblico, la stampa e i decision maker

Attacchi per anno nel mondo

Tipologia di attaccanti

Vittime per industry

Vittime per area geografica

Vittime per severity

Tecniche di attacco

Severity degli attacchi

Severity per classe di attaccanti

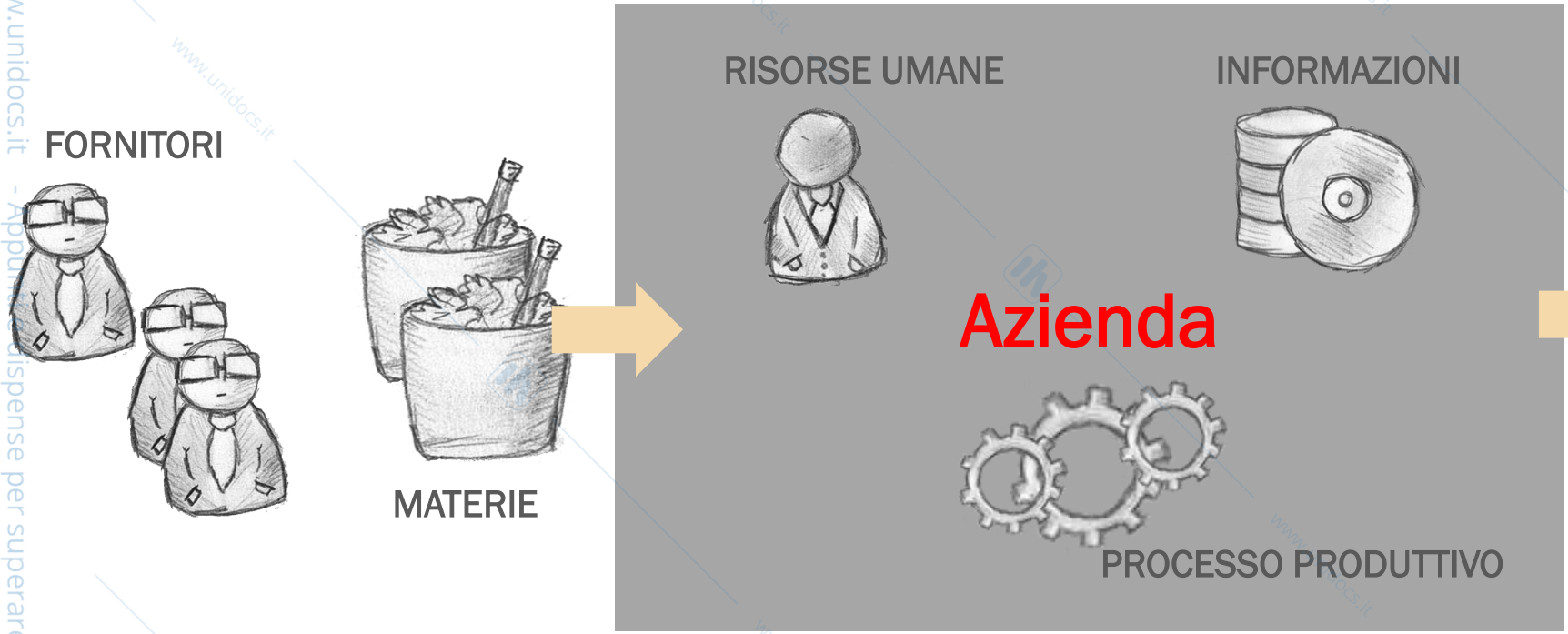
Analisi per l'Italia

Cosa gestiscono i sistemi aziendali?

LA COMPRENSION
DELL'AZIENDA E D
SUOI SISTEMI È
FONDAMENTALE P
OGNI ANALISI DEL
RISCHIO IT

(...E QUINDI SEGUE
UNA LORO
DESCRIZIONE
APPROSSIMATIVA)

Com’è fatta un’azienda e i suoi sistemi informa



Icone di Alexandra Olawolska http://handdr

Sistemi per la gestione dei fornitori

- L'ufficio acquisti tratta con i fornitori («vendor»), dopo aver raccolto le esigenze interne, ordinando i materiali necessari. In ing «purchasing». Vi lavorano i compratori / addetti dell'ufficio acquisti («buyer»).
- I materiali possono essere diretti (direttamente necessari alla produzione) oppure indiretti (tutto il resto, come le penne e l'a del presidente)
- I documenti principali sono l'ordine («purchase order»), la richiesta d'acquisto RDA («requisition») che serve internamente per le esigenze, la richiesta d'offerta RDO che viene mandata a diversi fornitori per chiedere informazioni su prezzi e condizioni («request for proposal»; «request for information» RFI). In alcune situazioni, soprattutto nella pubblica amministrazione al di so importi, si indicono delle gare tra fornitori («tender») più o meno formali a valle della preparazione del materiale di gara.
- Gli ordini possono essere chiusi («normali») oppure aperti («blanket order» cioè da fare man mano che serve il materiale) e po avere più articoli, consegne differenziate in luogo e tempi ecc.
- A fronte di alcune condizioni il fornitore emette fattura (elettronica) e questa viene pagata (dall'amministrazione; non dall'uff acquisti) se il materiale soddisfa certi requisiti di quantità e qualità (che sono verificati al ricevimento e dall'utilizzatore).
- I dati principali riguardano: le persone giuridiche (fornitori), i prezzi dei materiali e le condizioni di fornitura.

Sistemi per la gestione della produzione

- I sistemi per la gestione della produzione differiscono moltissimo a seconda del prodotto da produrre e delle scelte d
  Hanno lo scopo di rendere disponibili le giuste quantità di prodotto (non di meno e non di più) della qualità richiesta,
  producendo nel minor tempo possibile e usando nella maniera più efficiente possibile le risorse,

Figura 1.1: Classificazione dei sistemi di produzione.

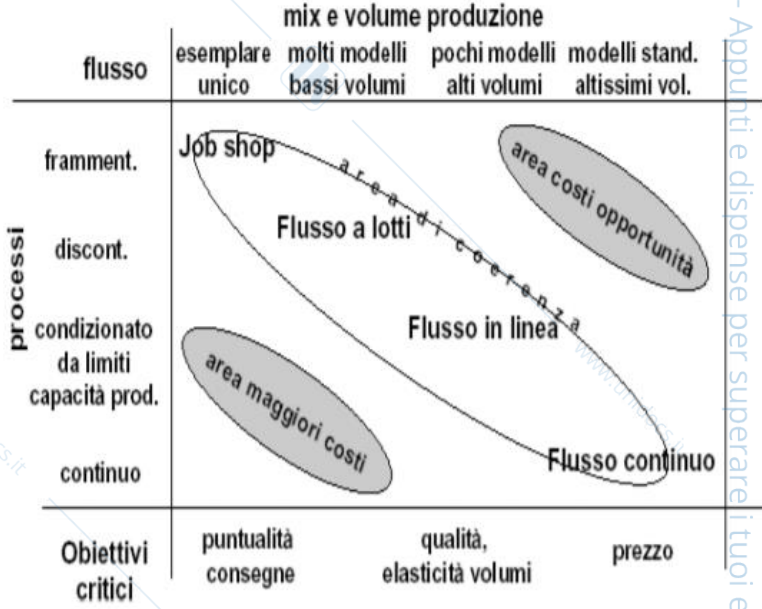


Figura 1.3: Matrice prodotto - processo.

FONTE: https://didattica-2000.archived.uniroma2.it/MSP/deposito/MSP_versione_2.pdf

Sistemi per la gestione dei clienti

- Il cliente è la chiave del successo dell'azienda. Si dice B2B (business to business) un'azienda i cui clienti siano a loro volta d e B2C (business to consumer) quella i cui clienti sono dei consumatori finali. I clienti sono gestiti dall'ufficio commerciale.
- L'organizzazione commerciale risente di questa caratterizzazione e delle scelte dell'azienda. La guida il direttore commercial essere presenti dei commerciali, degli agenti, dei rappresentanti, dei distributori. La retribuzione di questi soggetti è forteme agli obiettivi di vendita (accordi contrattuali, provvigioni e «compensation plan»).
- Se i prodotti da vendere sono sofisticati si affianca spesso una forza di prevendita (assistenza alla vendita) e/o una di post v (assistenza all'uso) eventualmente coadiuvata da una rete di partner (aziende terze che intervengono a monte e/o a valle de
- Il sistema informatico principe è il CRM (customer relationship management) che gestisce i contatti (persone che apparteng all'organizzazione del cliente), le trattative secondo il loro stato di avanzamento e gli ordini. Inoltre, una serie di elementi e in tendono a prevedere come stanno andando le vendite.
- I dati principali riguardano: le persone giuridiche per il B2B, le persone fisiche che vi lavorano, le persone fisiche per il B2C (consumatori finali), la situazione del venduto (complessivo e analiticamente per ogni cliente), le previsioni di vendita, la situ provvigionale

Sistemi per la gestione della ricerca e sviluppo

- Le aziende innovano per continuare a stare sul mercato. L'ufficio R&D (research and development) si occupa di ques processo.
- I software utilizzati sono di diverso tipo a seconda del business aziendale e i documenti possono essere disegni in bo disegni tecnici molto dettagliati, database di prove, documenti testuali, corrispondenza interna e documenti scambia partner e fornitori esterni, modelli in scala e prototipi materiali o immateriali ecc.
- Il lavoro realizzato a volte produce dei brevetti che consentono di ottenere l'esclusività relativamente ad un prodotto processo innovativo e permettono di sviluppare una posizione dominante sul mercato

Sistemi per il marketing

- Le attività dell'ufficio marketing possono essere molto diverse a seconda dell'azienda (B2B, B2C in primis) e delle sc aziendali. Possono includere lo studio del mercato di riferimento e l'analisi dell'interazione del mercato con l'azienda orientare le direzioni di lavoro della ricerca e sviluppo e le politiche dei prezzi dell'ufficio commerciale.
- Inoltre, al marketing viene data la responsabilità di promuovere il brand e la reputazione aziendale organizzando la p sui social network e i media (es. con la pubblicità) e altre attività (es. attività benefiche per la comunità e l'ambiente)
- Infine, può essere dato loro l'incarico di preparare brochure di prodotto e organizzare o partecipare a fiere e manifes
- I dati principali riguardano le analisi di mercato, dati sintetici e proiezioni di vendita e materiali relativi ai prodotti e al campagne (che sono riservati finché non saranno pubblici).

Sistemi per la gestione delle risorse umane

- L'ufficio delle risorse umane (HR «human resources») (o ufficio del personale) si occupa dell'amministrazione e della
del personale attraverso tutte le fasi del rapporto di lavoro (dalla candidatura, all'assunzione, alle dimissioni o pensio
- Si occupa degli stipendi e dei pagamenti ai lavoratori. Spesso approva gli aumenti di stipendio a fronte di un budget
definito con la direzione generale.
- Lavora in tandem con i manager delle varie linee per comprendere le necessità di nuovo personale («vacancy»), form
annunci di lavoro, fare la prima selezione dei candidati e procedere all'assunzione.
- Normalmente verifica anche le esigenze formative e organizza i corsi necessari e quelli obbligatori per legge.
- Organizza i processi annuali di valutazione del personale (competenze, prestazioni, potenziale) per decidere gli aspet
meritocratici e di carriera (carte di successione, alti potenziali ecc.)
- Gestisce le relazioni sindacali e i conflitti interpersonali e tra l'azienda e il lavoratore.
- I dati principali riguardano i dipendenti, retribuzione e valutazioni; tra gli altri, i dati relativi alla salute.

Sistemi per l'amministrazione, finanza e contro

- L'ufficio AFC ha molti compiti legati agli aspetti economici dell'azienda.
- Tiene la contabilità in partita doppia e redige il bilancio di esercizio composto da conto economico (costi e ricavi), sta patrimoniale (la ricchezza dell'azienda, attivo e passivo) e nota integrativa. Si occupa quindi del reporting di legge e v direzione.
- Oltre al reporting di legge provvede alla definizione del budget e della contabilità analitica e si occupa degli aspetti fi dell'azienda, come la registrazione delle fatture attive e passive e all'incasso o al pagamento.
- Tiene i rapporti con le banche, controlla i conti, si procura o cede la liquidità e si assicura contro i rischi di cambio se è internazionale.

Sistemi per la funzione legale

- Ogni grande azienda ha un ufficio legale e – vista l'ampiezza delle conoscenze richieste – si avvale di ulteriori profes specializzati in vari ambiti.
- La funzione legale gestisce il contenzioso di ogni tipo, i contratti particolari, gli obblighi relativi al dlgs. 231/01 (sulla responsabilità amministrativa delle persone giuridiche), a volte quelli al regolamento EU 2016/679 (il famoso GDPR alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di le questioni relative alla compagine aziendale (fusioni e acquisizioni, cessioni di ramo d'azienda, brevetti ecc.)
- Le informazioni che tratta in maniera digitale sono normalmente dei documenti di testo.

RID aka CIA

https://standards.iso.org/ittf/PubliclyAvailableStandards/ https://iso27001security.com/index.ht

DEFINIZIONE

Confidentiality (Riservatezza)

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

Integrity (Integrità)

property of accuracy and completeness

Availability (Disponibilità)

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

Alcuni mestieri dell'informatica

- Utente / manager
- Programmatore
  - Web programmer
  - Mobile apps
  - Server
- Analista
- Project Manager
- Sistemista
  - OS
  - DBA
  - Middleware vari
  - Rete
  - Disk
- Addetto alla sicurezza / CISO / CSO
- CIO / IT Manager
- System Integrator
- Indipendent Software Vendor
- Ufficio acquisti

Risk (ISO 31000:2018)

DEFINIZIONE

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and c
address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories and can be applied at differer

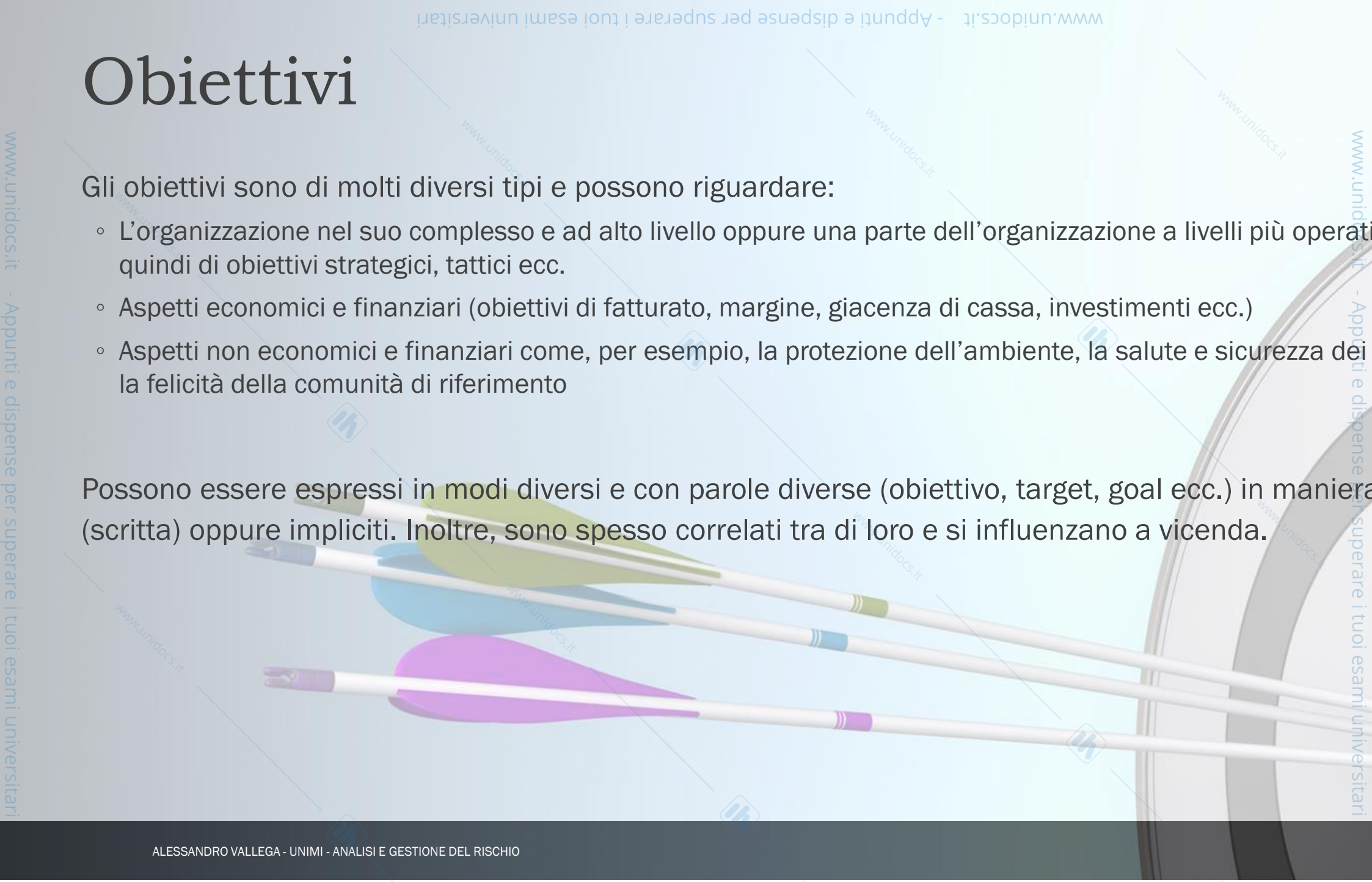
Note 3 to entry: Risk is usually expressed in terms of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7).

Obiettivi

Gli obiettivi sono di molti diversi tipi e possono riguardare:

- L'organizzazione nel suo complesso e ad alto livello oppure una parte dell'organizzazione a livelli più operati quindi di obiettivi strategici, tattici ecc.
- Aspetti economici e finanziari (obiettivi di fatturato, margine, giacenza di cassa, investimenti ecc.)
- Aspetti non economici e finanziari come, per esempio, la protezione dell'ambiente, la salute e sicurezza dei la felicità della comunità di riferimento

Possono essere espressi in modi diversi e con parole diverse (obiettivo, target, goal ecc.) in maniera (scritta) oppure impliciti. Inoltre, sono spesso correlati tra di loro e si influenzano a vicenda.



Incertezza

Rappresenta il deficit che abbiamo della conoscenza del mondo, degli eventi, delle loro probabilità conseguenze.

Non sappiamo chi vincerà le elezioni, come fluttuerà il tasso di cambio, se mi ammalerò di influenza 7 dalla somma del lancio di due dadi, se il nuovo guardiano si addormenterà durante il turno nottur degli hacker prenderanno di mira la nostra Università...

Effetto dell'incertezza

Corrisponde a mancare l'obiettivo di un piccolo o grande margine.

Nota: Anche se è controintuitivo vedere realizzati dei rischi che producono effetti positivi, la disciplir generale del risk management e la ISO 31000 lo prevedono.

Risk (ISO/IEC 27000:2018)

DEFINIZIONE

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understandir knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73 3.5.1.3) and “consequences” (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (inclu changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks ca expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabi information asset or group of information assets and thereby cause harm to an organization.

Risk (effect of uncertainty on objectives

ISO 31000:2018

[...]

Note 3 to entry: Risk is usually expressed in terms of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7).

«Risk source» non è definito nella 27000

Nella 27000 troviamo spesso al suo posto «threat» (minaccia) perché, contrariamente alla 31000, il rischio, nell'Information Security, è spesso considerato negativo.

ISO/IEC 27000:2018

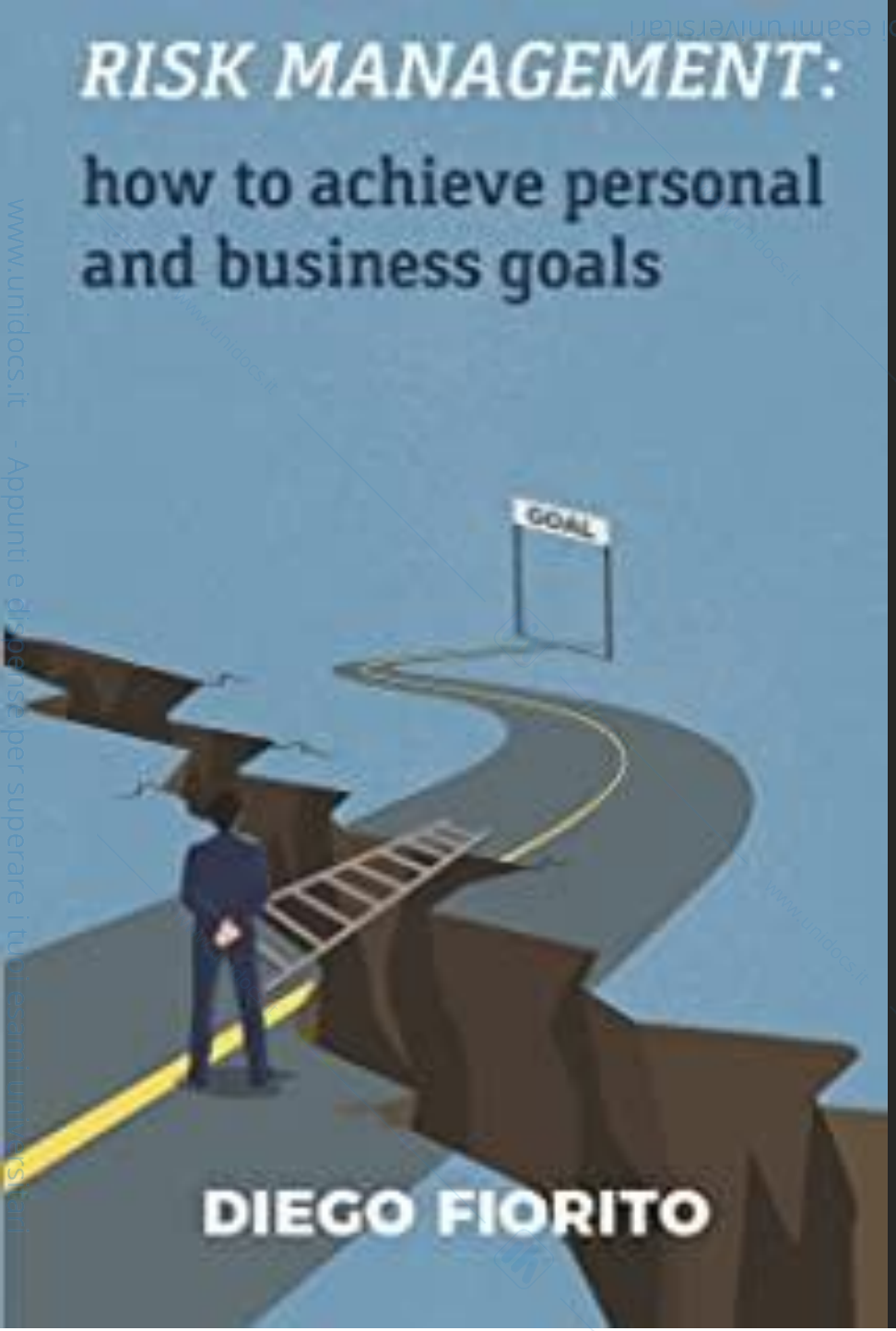
[...]

Note 3 to entry: Risk is often characterized by reference to "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3 combination of these.

Note 4 to entry: Risk is often expressed in terms of a combi consequences of an event (including changes in circumstar associated "likelihood" (as defined in ISO Guide 73:2009, 3 occurrence.

Note 5 to entry: In the context of information security mana systems, information security risks can be expressed as eff uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with that threats will exploit vulnerabilities of an information ass information assets and thereby cause harm to an organizat



Uniformare la scrittura dei rischi

As a result of <defined cause / causes>,

<this unexpected event> could occu

which could produce <this effect on targets>

Risk Management (ISO Guide 73:2009, “Risk managem
Vocabulary, ISO 31000:2018 and ISO/IEC 27000:2018)

DEFINIZIONE

coordinated activities to direct and control an organization with regard to risk

Risk Management Process (ISO Guide 73:2009, "I
management – Vocabulary, and ISO/IEC 27000:2018)

DEFINIZIONE

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, monitoring reviewing risk

Process (ISO 9000:2015)

DEFINIZIONE

set of interrelated or interacting activities that use in to deliver an intended result

Note 1 to entry: Whether the “intended result” of a process is called output (3.7.5), product (3.7.6) or service (3.7.7) depends c context of the reference.

Note 2 to entry: Inputs to a process are generally the outputs of other processes and outputs of a process are generally the inp processes.

Note 3 to entry: Two or more interrelated and interacting processes in series can also be referred to as a process.

Note 4 to entry: Processes in an organization (3.2.1) are generally planned and carried out under controlled conditions to add

Note 5 to entry: A process where the conformity (3.6.11) of the resulting output cannot be readily or economically validated is referred to as a “special process”.

Note 6 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given i the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified to prevent circula process and output, and Notes 1 to 5 to entry have been added.

Procedure (ISO 9000:2015)

DEFINIZIONE

specified way to carry out an activity or a process

Note 1 to entry: Procedures can be documented or not.

The difference between process and procedure is that processes are gen
activities to achieve a goal and procedures are specific steps that must be followe
complete a task.

Project (ISO 21502:2020 (and PMBOK – Project Management Ins

temporary endeavour to achieve one or more define objectives

DEFINIZIONE

I progetti

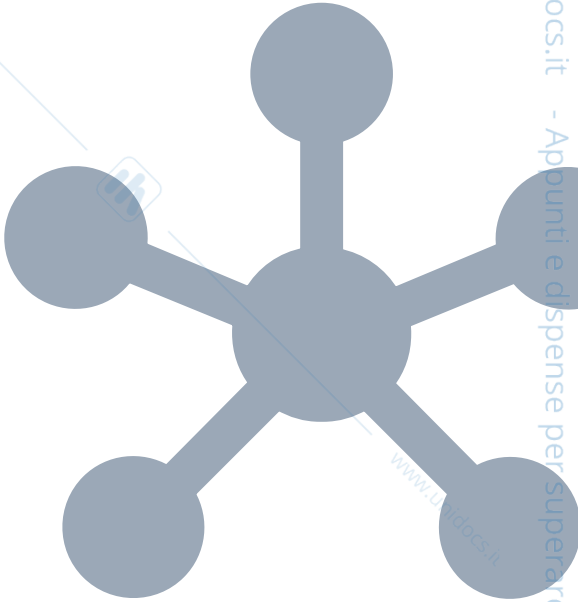
- Hanno un obiettivo specifico da raggiungere
- Sono limitati nel tempo ed hanno una data di inizio e una di fine
- Utilizzano risorse (umane, economiche, materiali, equipaggiamento)
- Hanno un budget e limitazioni di spesa

Li gestisce un project manager che dev
equilibrare i costi, i tempi e l'ambito (sc

Una possibile classificazione dei rischi

- Rischio di credito
- Rischio di mercato
- Rischio operativo
- Rischio relativo alle risorse umane
- Rischio IT e cyber security
- Rischio legale
- Rischio di compliance
- Rischio di crimine finanziario
- Rischio ambientali
- Rischio sociale
- Rischio di salute e sicurezza sul lavoro

PARTE 2 – E' TEMPO DI 31000



Esercizio

<nome dello/degli studente/i>

James Quincey

Chairman and Chief Executive Officer

James Quincey is Chairman and CEO of The Coca-Cola Company. Quincey, who first joined the company in 1996, has held a number of leadership roles around the world. He became CEO in 2017 and Chairman of the Board in

Voi siete James Quincey

Quanto denaro «aggiuntivo» usereste per aumentare la sicurezza informatica?

In quale area / per far cosa lo spendereste?

Ogni organizzazione, perseguendo i suoi
corre molti e diversi rischi.

Il risk management aumenta la possibilit
dell'organizzazione di affrontare i rischi i
migliore, aumentando così la propria pos
avere successo.

Il risk management aumenta la razionali
decisioni.

Il risk management process aiuta l'orgar
ad attuare il risk management

La ISO 31000:2018 Risk management —
Guidelines standardizza nomenclatura e a

ISO 31000:2018

https://www.iso.org/obp/ui/#iso:std:iso:31000:

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.

Organizations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.

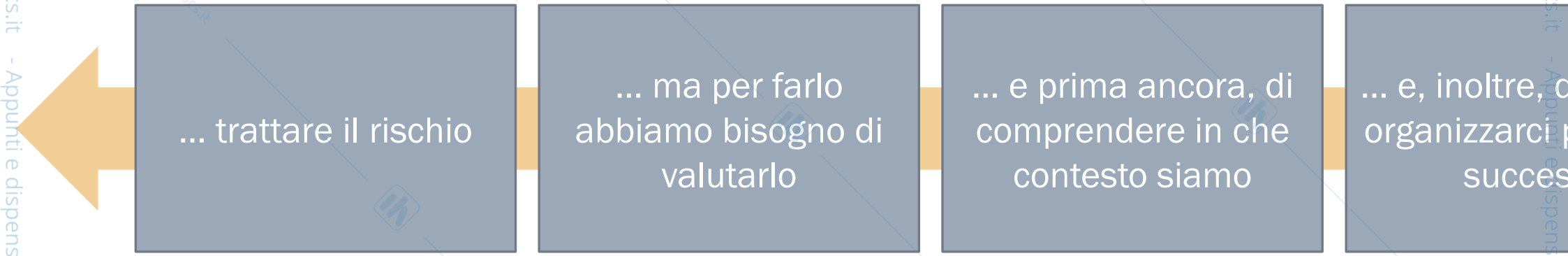
Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.

Managing risk is part of all activities associated with an organization and includes interaction with stakeholders.

Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

La ISO 31000:2018 ci aiuta a…



Communication and consultation

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Questo processo ha lo scopo di allineare costantemen
stakeholders e ottenere feedback e informazioni utili p
prendere le decisioni.

E' un processo cruciale e garantisce nel tempo il comr
aziendale ed è un prerequisito per il successo dell'iniz
risk management

Stakeholder (ISO 31000:2018)

person or organization that can affect, be affected by, perceive themselves to be affected by a decision or activity

Note 1 to entry: The term “interested party” can be used as an alternative to “stakeholder”.

DEFINIZIONE

Monitoring and review

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Il monitoraggio continuo e le review periodiche hanno
di assicurare la qualità dell'intero processo di risk ma
e di migliorarlo nel tempo. In pratica risponde alla don
«Stiamo facendo bene? Si può migliorare?»

Queste domande bisognerebbe porsele in ogni fase e
dell'intero processo e bisognerebbe pianificarle e asse
delle chiare responsabilità di esecuzione. Il risultato d
analisi dovrebbe essere incorporato nel sistema di ges
delle performance e nel reporting aziendale.

Recording and reporting

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Il processo stesso di risk management e i suoi output dovrebbero essere documentati e resi disponibili tram appropriati meccanismi come, per esempio, la stesura documenti e la loro archiviazione in modi e luoghi app affinché siano disponibili a chi ne ha o potrebbe avere Questi decisioni devono tenere a mente anche gli aspe riservatezza e i diversi stakeholder (es. esterni). Lo sc questo processo è quello comunicare, fornire informaz supporto delle decisioni, migliorare le attività di risk management e interagire con gli stakeholder.

Scope context and criteria

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Scope significa «ambito» ed è molto importante definir chiarezza in anticipo. Lo scope può essere limitato geograficamente (es. le consociate spagnole), second (strategico, operativo, progetto, prodotto) o altri criteri

Scope context and criteria

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

E' importante conoscere e stabilire il contesto interno esterno in cui opera l'organizzazione e nel quale essa raggiungere i propri obiettivi perché creano il contesto quale il processo di risk management deve operare. Ritroveremo questo tema nel framework – design

Scope context and criteria

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Come abbiamo visto, lo scopo del risk management pr
quello di aumentare la razionalità delle decisioni orga
In un certo senso, quello di applicare il «metodo scient
all'analisi del rischio. Quindi si devono definire criteri e
più possibile oggettive e ripetibili nel tempo e da perso
diverse per dare istruzioni alle fasi di assessment e tre
che seguono. In questa fase si cerca quindi di definire
come la risk capacity dell'organizzazione o quando cla
un rischio come alto o basso, eccetera. Si capirà megl
seguito.

Visto che il risk management ha a che fare con l'incert
l'esecuzione del processo stesso fa cambiare nel temp
maturità aziendale sarà necessario adeguare le decisi
in questa fase nel tempo.

Risk assessment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Lo scopo della fase di risk identification è quello di tro
comprendere e descrivere i rischi. Per farlo è necessar
delle informazioni rilevanti e aggiornate. Per redigere c
lista si devono considerare molti elementi, come:

— tangible and intangible sources of risk;

— causes and events;

— threats and opportunities;

— vulnerabilities and capabilities;

— changes in the external and internal context;

— indicators of emerging risks;

— the nature and value of assets and resources;

— consequences and their impact on objectives;

— limitations of knowledge and reliability of information;

— time-related factors;

— biases, assumptions and beliefs of those involved.

Risk assessment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Nella fase di risk analysis si cerca di comprendere la n
rischio e le sue caratteristiche incluso, se appropriato,
di rischio. L'analisi considera gli eventi di rischio (*even*
source, le *conseguenze (consequences)*, le probabilità
(*likelihood*), i controlli (*control*) e le relazioni tra eventi
possono avere molteplici cause e conseguenze su dive
obiettivi...

La fase di analisi è prona ad errori (di valutazione, lega
tecniche di analisi ecc.) e soggetta punti di vista anche
diversi; quindi è meglio usare molteplici tecniche per v
rischi con conseguenze gravi.

Lo scopo della fase di analisi è quello di dare informaz
fase successiva (evaluation) per decidere se il rischio
essere trattato o meno e come.

Event (ISO 31000:2018)

DEFINIZIONE

occurrence or change of a particular set of circumsta

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several consequences (

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expec
does happen.

Note 3 to entry: An event can be a risk source.

DEFINIZIONE

Consequence (ISO 31000:2018)

outcome of an event (3.5) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects or

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

Considerazioni sulle conseguenze

Visto che si dovranno valutare molti rischi, ognuno con le sue proprie eterogenee conseguenze, per

- Causare morte o ferite e conseguenti costi medici
- Sversare più di 100.000 litri di inquinante nel fiume
- Comportare un esborso di denaro di 10.000 € per le riparazioni
- Ricevere una multa del 4% del fatturato mondiale annuo
- Apparire nei social con alcuni / molti messaggi negativi per la reputazione

E’ necessario classificare le conseguenze in qualche modo al fine di compararle e ordinare i rischi s conseguenze. La classificazione può essere una misura precisa e quantitativa (esempio denaro per oppure per range e qualitativa (esempio lieve / grave).

Definizione dei criteri per la gestione del rischio (un esempio)

L'**Impatto/Danno/Conseguenze (D)** dovute all'evento sfavorevole (incidente), valutata secondo la scala qualitativa.

Impatto/Danno/Conseguenze (D)			
1	Molto basso	Insignificante	Nessun danno alle persone e alla produzione. Basso impatto economico
2	Basso	Basso	Intervento del primo soccorso. Alcune attività bloccate senza danni alla produzione. Medio impatto economico
3	Medio	Moderato	Richiesto intervento medico. Molte attività bloccate con moderati danni alla produzione. Alto impatto economico
4	Alto	Elevato	Danni estesi alle persone. Alcuni processi bloccati con elevati danni alla produzione. Massimo impatto economico anche a livello sistemistico (sistema informatico
5	Molto alto	Catastrofico	Casi di morte. Rilascio gas tossici con effetti dannosi. Massimo impatto economico a livello sia sistemistico che infrastrut

Risk Management - ISO 31000:2018/pag. 34 - © Ioanis Tsiouras

Likelihood (ISO 31000:2018)

chance of something happening

DEFINIZIONE

Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happe whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivale term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. T risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the “probability” has in many languages other than English.

Considerazioni sulle probabilità

Analogamente alle conseguenze, abbiamo lo stesso bisogno di valutare la probabilità di accadimen
realizzazione di un rischio ai fini di classificazione e ordinamento.

Definizione dei criteri per la gestione del rischio (un esempio)

La **Probabilità** (P) con la quale si manifesta l'evento sfavorevol (incidente), valutata secondo la scala qualitativa.

Probabilità (P)			
1	Molto bassa	Rara	Accade solo in circostanze eccezionali (P<1%)
2	Bassa	Improbabile	È improbabile che accada (1%<P<5%)
3	Media	Moderata	Può accadere in un certo numero di casi (5%<=P<20%)
4	Alta	Probabile	Avviene in una buona parte dei casi (20%< =P<=50%)
5	Molto alta	Quasi certo	Avviene nella maggior parte dei casi (P>50%)

Risk Management - ISO 31000:2018/pag. 33 - © Ioanis Tsiouras

Level of risk (ISO/IEC 27002:2018)

DEFINIZIONE

magnitude of a risk, expressed in terms of the combination of consequences and their likelihood

Definizione dei criteri per la gestione del rischio (un esempio)

Criteri di valutazione del Rischio

Il **Rischio** (R) (come funzione della probabilità (P) e dell'impatto/Danno/Conseguenze (D): *R=f(PxD)*

Conseguenze (D)	Probabilità (P)				
	Molto bassa (1)	Bassa (2)	Media (3)	Alta (4)	Molto Alta (5)
Molto Basso (1)	1	2	3	4	5
Basso (2)	2 B	4	6	8	10
Medio (3)	3	6	9 M	12	15
Alto (4)	4	8	12	16 A	20
Molto Alto (5)	5	10	15	20	25

Risk Management - ISO 31000:2018/pag. 2 - © Ioanis Tsiouras

Risk assessment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

La valutazione del rischio è un punto di snodo decisior processo. Prendendo in input le informazioni prodotte dall'analisi e i criteri di accettabilità (identificati nella f scope, context and criteria) permette di decidere se e procedere con il trattamento del rischio.

— do nothing further;

— consider risk treatment options;

— undertake further analysis to better understand the risk;

— maintain existing controls;

— reconsider objectives.

Il risultato della valutazione dovrebbe essere registrato formalmente, comunicato e validato dal management

Risk treatment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Il rischio può essere trattato in molti modi.

Più specificamente:
- Si può evitare rinunciando all'attività che origina il rischio
- Si può modificare il rischio rimuovendo la fonte di rischio riducendo la probabilità e l'impatto tramite delle misure
- Si può condividere o trasferire a terzi (es. assicurazione)
- Si può accettare così com'è

Sono scelte complesse che tengono conto dei costi, de benefici, degli obblighi contrattuali e di legge, della div opinione dei diversi stakeholder ecc.

Il trattamento di un rischio può modificare o creare alt che dovranno quindi essere a loro volta gestiti.

Risk treatment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

I piani di trattamento del rischio specificano come sara implementate le opzioni scelte di modo che siano ben compiti di chi è coinvolto e il progresso del piano possa monitorato.

I piani dovranno essere integrati nei piani di gestione a e nei relativi processi in accordo con gli stakeholder in

Le informazioni a corredo devono comprendere il perc state scelte quelle opzioni di trattamento, i benefici att l'indicazione dei responsabili (approvazione ed esecuz azioni proposte, le risorse disponibili, i criteri di misura risultato, i vincoli, le regole di reporting, le date previst svolgimento e completamento del compito).

Control (ISO 31000:2018)

DEFINIZIONE

measure that maintains and/or modifies risk

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or a which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

Considerazioni sui controlli

I controlli possono essere organizzativi o tecnologici, per esempio:

- Ogni sera passare a controllare tutte le porte per verificare che siano chiuse
- Prima di decollare con il parapendio svolgere i 5 controlli del manuale di sicurezza della FIVL
- Installare l'antivirus su ogni nuovo PC consegnato ai dipendenti e rimuovere la password di amministrazione

Parleremo moltissimo dei controlli quando andremo sulla ISO 27000:2018

Leadership and commitment

Il top management deve assicurarsi che il risk management sia integrato in tutte le attività dell'organizzazione e dimostrare la propria leadership e il proprio commitment in diversi modi

— customizing and implementing all components of the framework;

— issuing a statement or policy that establishes a risk management approach, plan or course of action;

— ensuring that the necessary resources are allocated to managing risk;

— assigning authority, responsibility and accountability at appropriate levels within the organization.

Il top management è responsabile di gestire il rischio, mentre gli organi di controllo sono responsab
supervisione della gestione del rischi. In particolare:

— ensure that risks are adequately considered when setting the organization's objectives;

— understand the risks facing the organization in pursuit of its objectives;

— ensure that systems to manage such risks are implemented and operating effectively;

— ensure that such risks are appropriate in the context of the organization's objectives;

— ensure that information about such risks and their management is properly communicated.

Integration

Il risk management deve essere integrato nell'organizzazione, nel suo scopo, nei meccanismi di gov
nelle operations. Deve essere ovunque e ognuno nell'organizzazione ha la responsabilità di gestire
Le responsabilità di gestione del rischio e la responsabilità di controllo della gestione del rischio dev
essere assegnate con precisione.

Design

Quando si progetta il framework (la struttura di riferimento organizzativa) bisogna fare una serie di c

- Comprendere molto bene l'organizzazione e il suo contesto
- Articolare il commitment continuo verso il risk management tramite delle policy (documenti strategici), dichi altro spiegandone il bisogno e i meccanismi di funzionamento nell'organizzazione
- Assegnare ruoli organizzativi, autorità, responsabilità e competenze. Evidenziare chi sono i *risk owner*
- Allocare le risorse umane, organizzative, tecnologiche
- Stabilire i meccanismi di comunicazione e di consultazione

Risk owner (ISO Guide 73:2009 Risk management — Vocabu

person or entity with the accountability and authority
manage a risk

DEFINIZIONE

Implementation

Durante l'implementazione del risk management framework bisogna sviluppare un piano che includ
risorse, identificare nel dettaglio il processo decisionale e modificare il processo decisionale se nec
assicurarsi che le disposizioni prese per gestire il rischio siano ben comprese.

Evaluation

Per valutare l'efficacia del quadro di gestione del rischio, l'organizzazione dovrebbe:

- Misurare periodicamente le prestazioni del risk management framework rispetto al suo scopo, ai piani di implementazione, agli indicatori e al comportamento atteso
- Determinare se rimane adatto a sostenere il raggiungimento degli obiettivi dell'organizzazione

Improvement

In una logica di miglioramento continuo, l'organizzazione deve adattarsi e migliorarsi. Appena vengo identificate delle aree o delle opportunità di miglioramento bisogna sviluppare dei piani e assegnare responsabilità per la loro esecuzione.

Considerazioni finali sulla ISO 31000:201

La linea guida aiuta le organizzazioni a strutturare il processo di management

Nonostante questa presentazione faccia altrimenti, i principi, il framework e i processi vengono illustrati in quest'ordine

Anche se non si fa esplicito riferimento al PDCA si prevede una continua retroazione (feedback) tra le varie fasi del processo

Visto che il risk management cerca di ridurre i rischi e l'incertezz correlata, è normale che varie decisioni e disposizioni vengano corrette ed emendate nel tempo

Il risk management (di successo) è un processo continuativo ch deve accompagnare l'evoluzione organizzativa negli anni; è per sempre

ALESSANDRO VALLEGA - UNIMI - ANALISI E GESTIONE DEL RISCHIO

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 archiv
dei supporti.

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

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

Information security (ISO/IEC 27000:2018)

preservation of confidentiality, integrity and availabil
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 availabil information

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

Management system (ISO/IEC 27000:2018)

DEFINIZIONE

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 opera

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

Sistemi di gestione secondo le norme IS

Con tale termine si intendono tutti i sistemi di gestione implementati nelle organizzazioni (imprese, 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 requisit 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/Sist

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

Cosa ci dicono i sistemi di gestione?

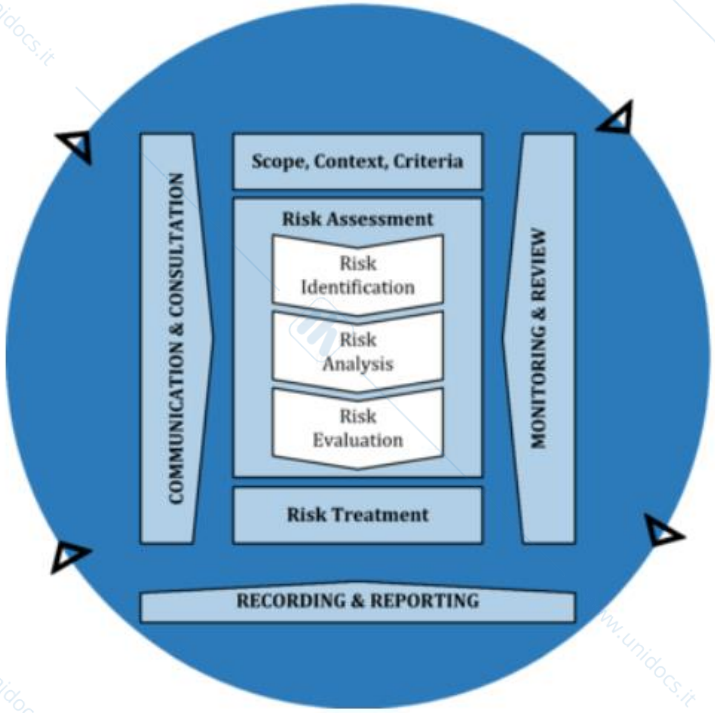
Per un certo ambito (disciplina), oppure per più ambiti, suggeriscono cosa fare

- 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 incendi che è materia comune alla sicurezza delle informazioni, alla sicurezza fisica e alla sicurezza e sal personale. Queste sovrapposizioni comportano delle opportunità «di riuso» ma anche rischi di sprechi e c 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 otten certificazione che attesti che l'organizzazione stia facendo bene le cose.

Un parallelo tra 31000 e 27001



FONTE: ISO 3100:2018

IDENTIFICATION

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

ANALYSIS

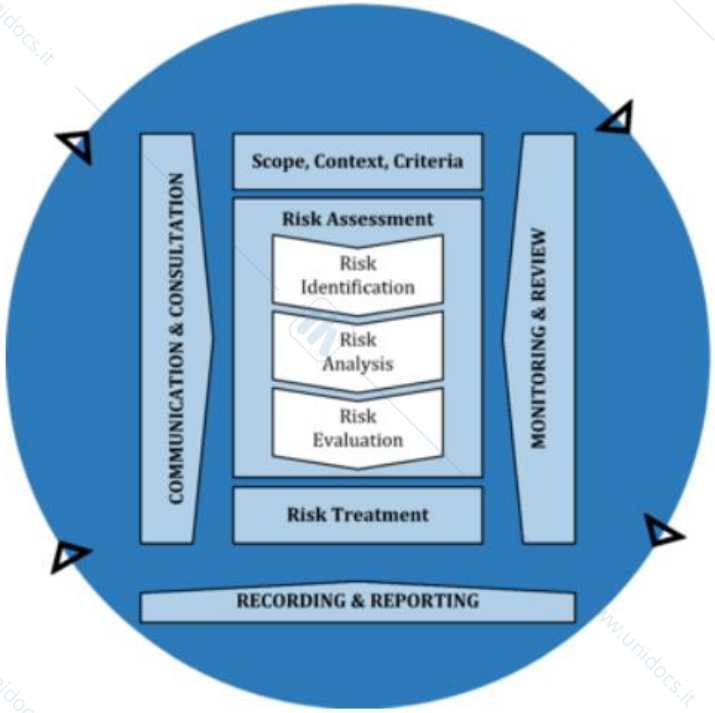
1. Analizzare l'impatto del rischio
2. Analizzare le probabilità di accadimento
3. Determinare il livello del rischio

EVALUATION

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

FONTE: 6.1.2 6.1.2 6.1.2 6.1.2 6.1.2 6.1.2

Un parallelo tra 31000 e 27001



FONTE: ISO 3100:2018

FONTE: ISO/IEC 27001:2013 e 2022

TREATMENT

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

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.

DEFINIZIONE

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

Controlli che agiscono sulla **riservatezza**

Integrity

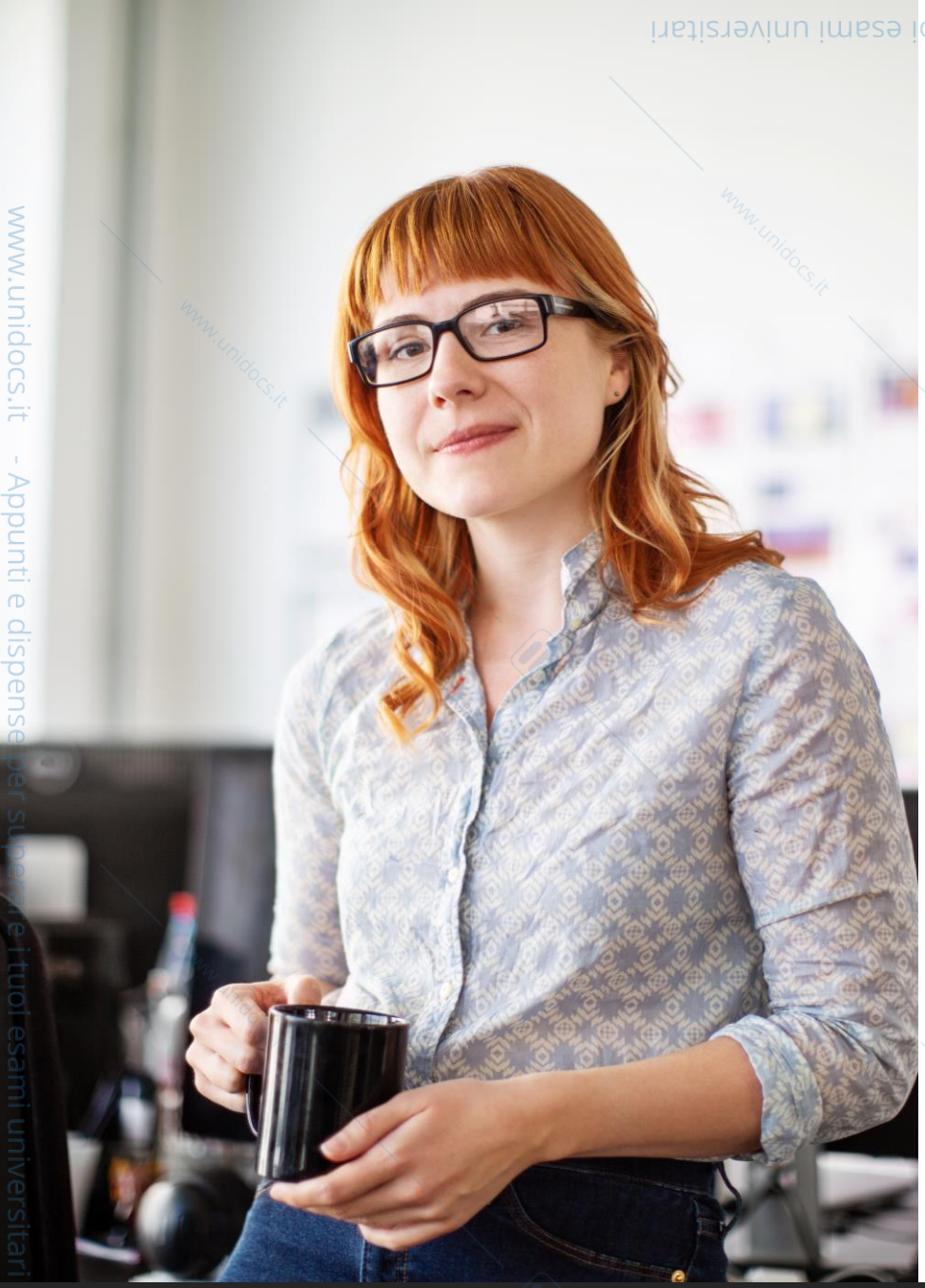
property of accuracy and completeness

Controlli che agiscono sull'**integrità**

Availability

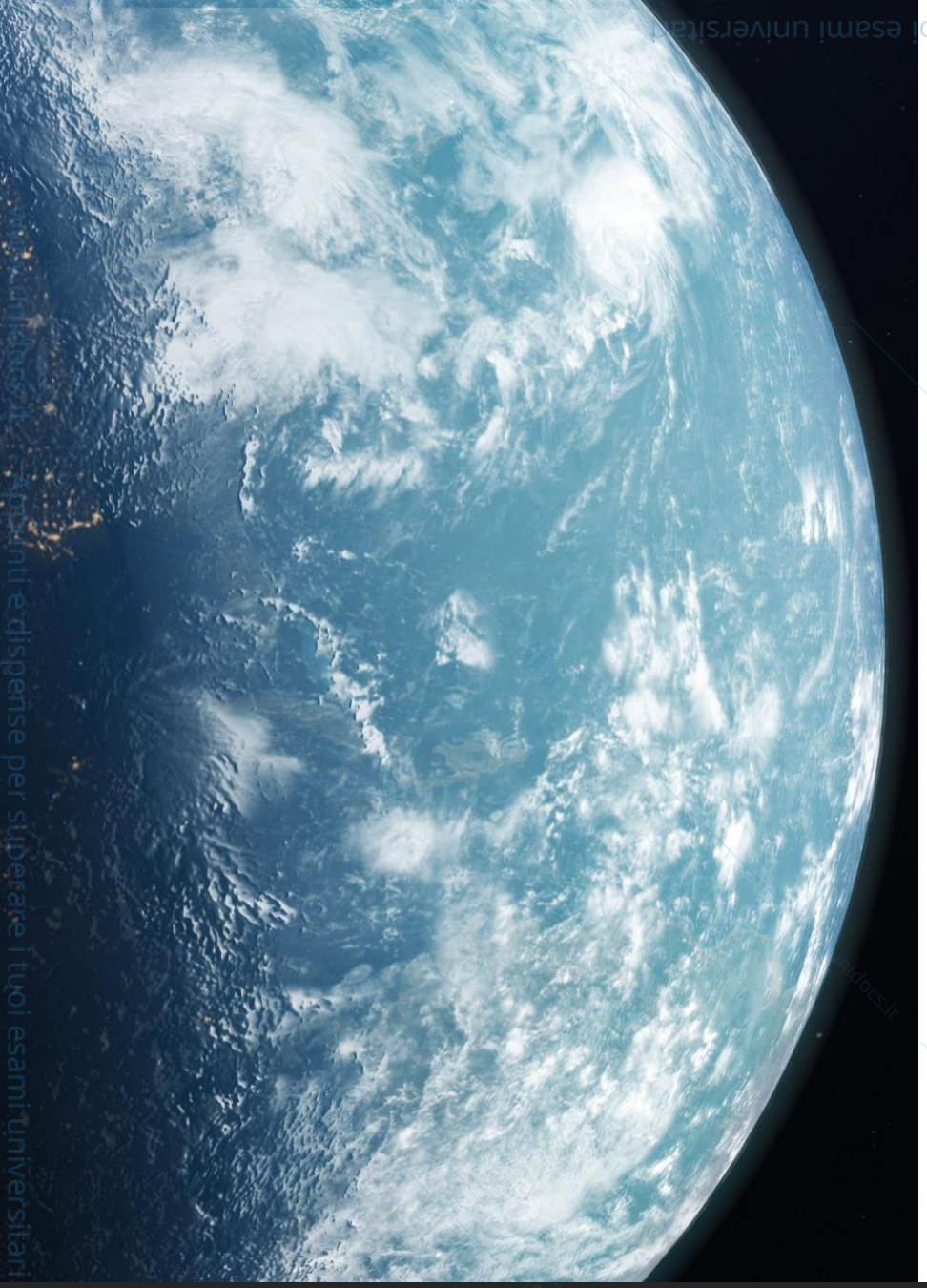
property of being accessible and usable on demand by an authorized entity

Controlli che agiscono sulla **disponibilità**



Il CISO

Il Chief Information Security Officer ha un compito non facile: quello di garantire che le informazioni siano opportunamente protette, pur essendo allo stesso tem fruibili.



Contesto macroeconomico, tecnologico e sociale

La globalizzazione, l'esternalizzazione di processi aziendali, la digitalizzazione e la regolamentazione crescente producono dei cambiamenti che impattano sull'azienda, sulla sua capacità di stare sul mercato, s innovazioni realizzabili, sulle informazioni da produrre da proteggere.

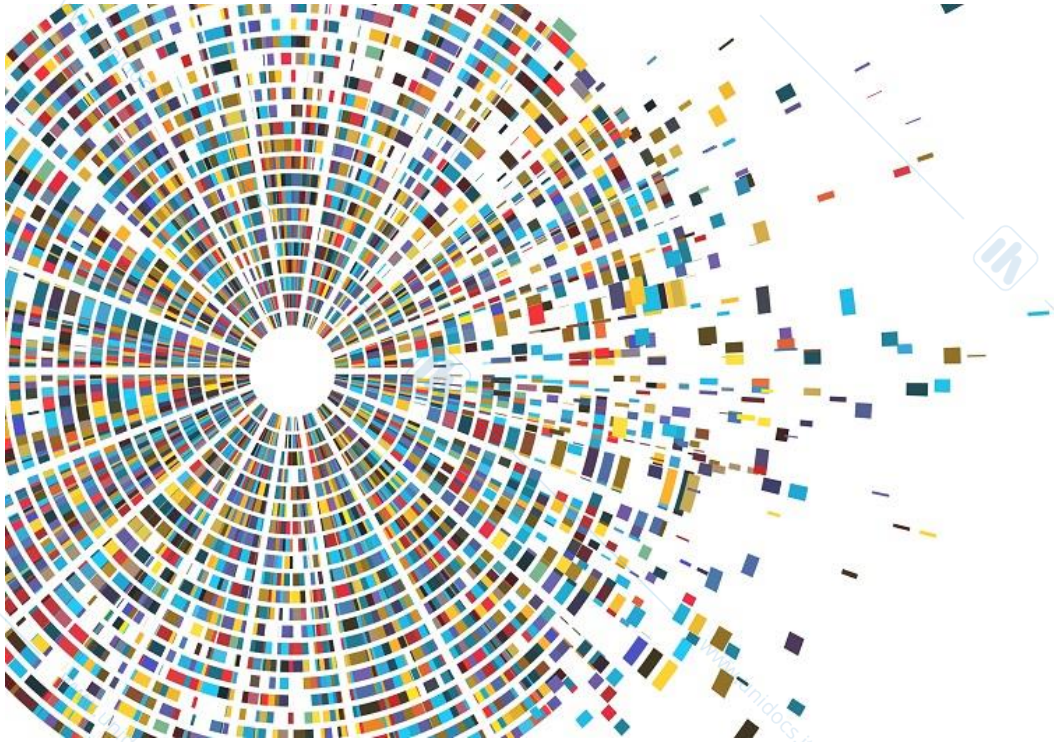
Il CISO arriva ultimo e il suo operato tiene insieme tutt pezzi.

Il cambiamento è molto rapido.

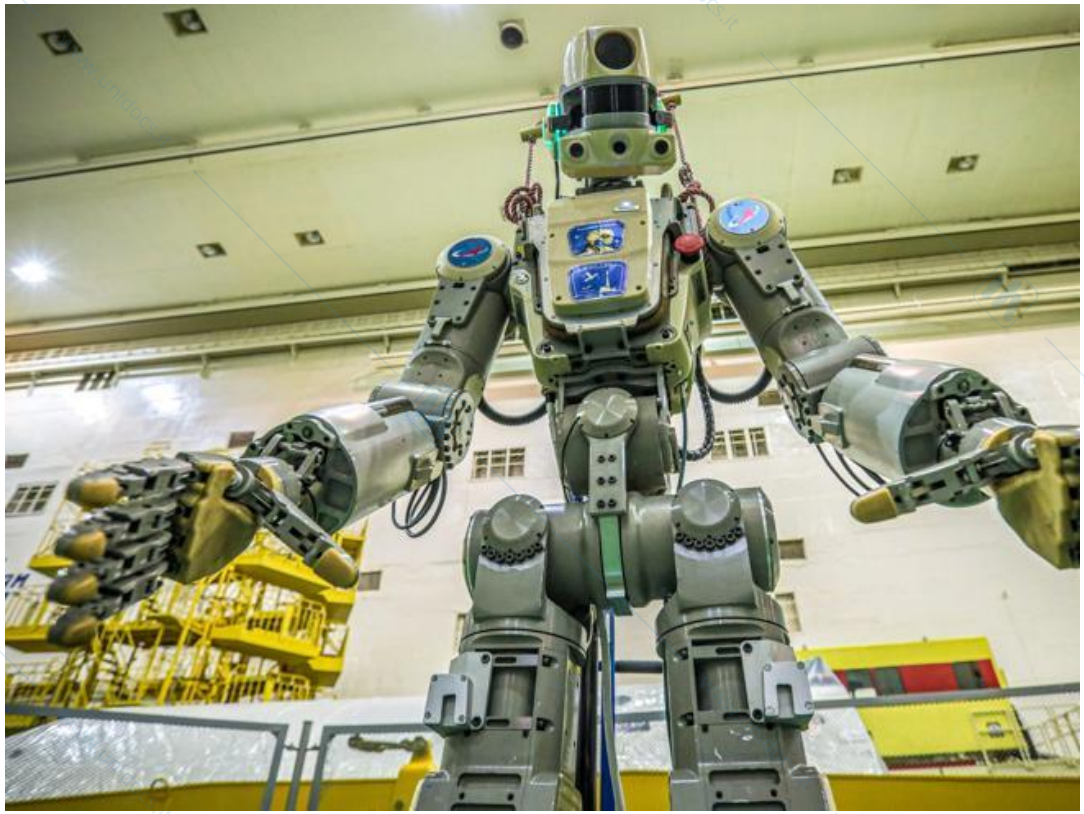
Gli utilizzatori consegna
ai social grandi quantit
dati utili alla profilazion

Lo fanno tramite tecnol
mobile lavorando e in
generale interagendo c
ogni luogo e in ogni ora

L'IoT vi aggiunge i dati arrivano tramite senso dal mondo delle cose



Tali quantità di dati sor
raccolte e rese gestibili
tramite tecnologie di bi
data



L'intelligenza artificiale analizza i dati tramite reti neurali e vari algoritmi e permette a programmi, ag software e robot di agire n mondo reale

L’IT si ibrida con l’OT estendendo il dominio dell’informatica nel mo di produrre e gestire

Tutto questo si basa su
cloud, che unifica, abili
garantisce: senza di es
niente sarebbe possibi

La trasformazione digitale per competer

Fatturato in miliardi di $ e data di fondazione di:

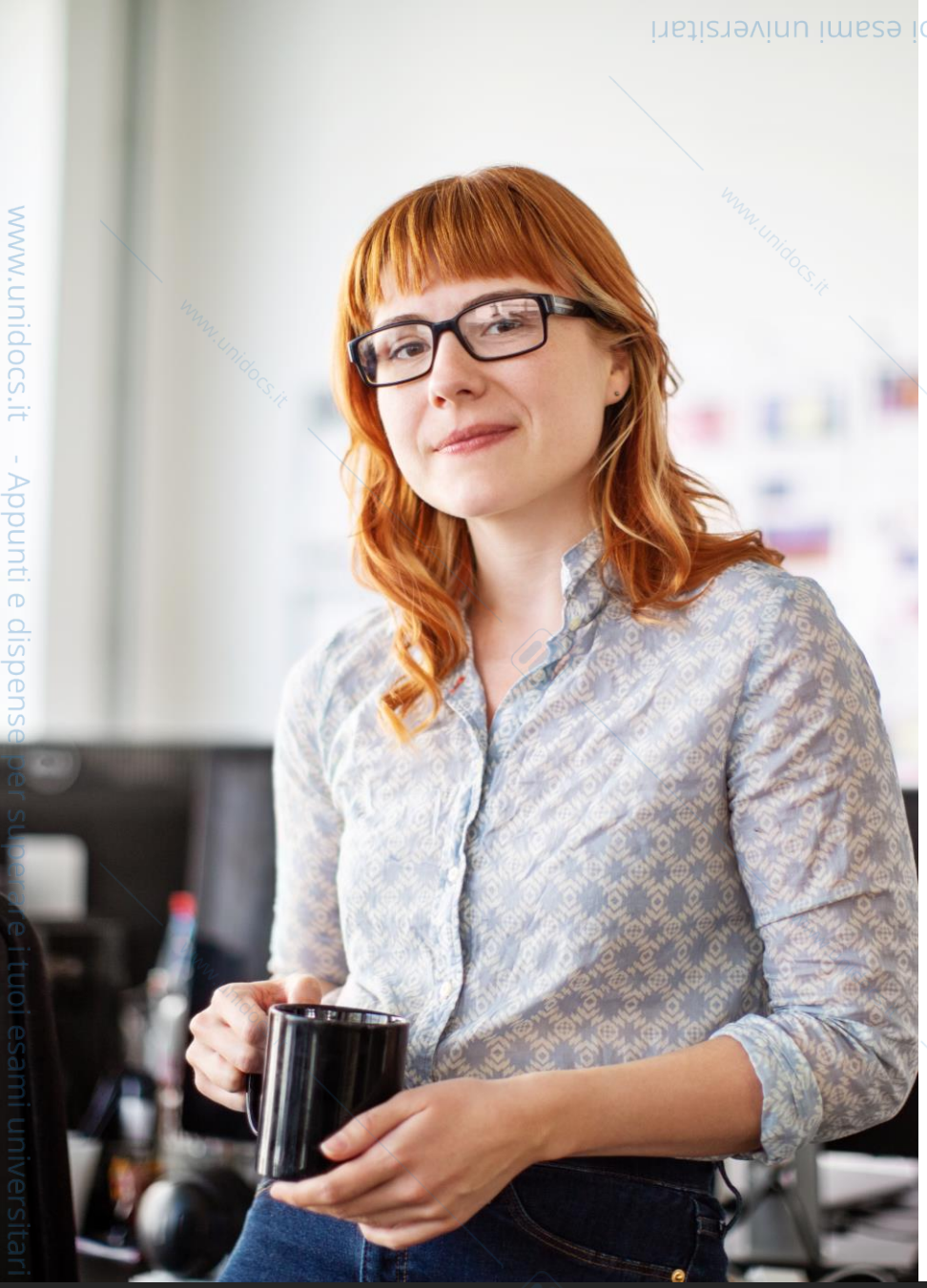
- Apple 274 (1976)
- Amazon 386 (1994)
- Facebook 86 (2004)
- Alphabet 182 (1998)

FONTE: Wikipedia e Internet

Complessivamente 1000 miliardi di dollari; aziende che hanno 25 anni di vita!

Il successo di queste e altre azie che fanno del digitale la loro lev competitiva è dovuto al fatto che

- Hanno i dati
- Collegano la domanda e l'offerta
- Integrano i prodotti con i servizi



Il CISO

Non frena queste innovazioni ma le facilita e aiuta a metterle in sicurezza

Il CISO

Collabora con il business e fa da «mediatore culturale» tra il business e i tecnici sugli aspetti di security

- Comprende il rischio e collabora con il risk manager
- Comprende le norme leggi e regolamenti e collabora con le funzioni di compliance
- Comprende l'IT e collabora con questa funzione
- Comprende le catene di fornitura e collabora con i fornitori
- Comprende i bisogni dei clienti e li aiuta a soddisfarli
- Conosce di tutto un po' - sa chi sa e si avvantaggia dell'esperienza altrui