



Analisi e gestione del rischio

PROF. ALESSANDRO VALLEGA

UNIVERSITÀ DEGLI STUDI DI MILANO

CORSI DI LAUREA MAGISTRALE IN SICUREZZA
INFORMATICA E IN INFORMATICA

Cosa imparerete in questo corso

PARTE 1 – SCALDIAMO I MOTORI



PARTE 2 – E' TEMPO DI 31000



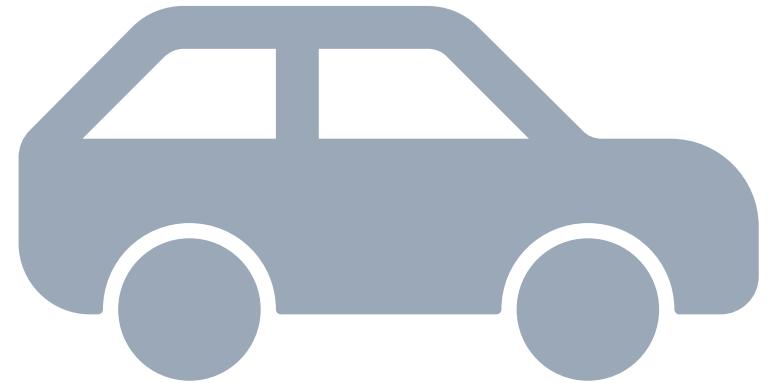
PARTE 3 – INFORMATION SECURITY



PARTE 4 -IL CISO (CHIEF INFORMATION SECURITY OFFICER)



PARTE 1 - SCALDIAMO I MOTORI



Argomenti

Mi presento

Vi presentate

Ricevimento

Ariel

Calendario delle lezioni

Libri

Esame



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Alessandro Vallega

Laurea in Scienze Politiche.

Lavoro in informatica dal 1984.

- Esperienze come programmatore, analista, project manager, program manager, business development, consultant in diverse società tra le quali Olivetti Information Services, Fiat, Oracle e Partners4Innovation.
- Ho lavorato principalmente in Italia e un po' all'estero (Spagna, Portogallo, Francia, Olanda, Belgio, Centro America).

Dal 2007 mi occupo di sicurezza informatica.

- Sono nel consiglio direttivo di Clusit
- Sono il fondatore e il chairman della Clusit Community for Security.
- Organizzo, modero e sono relatore a conferenze di CyberSecurity.

I libri e il materiale

<https://www.unimi.it/it/corsi/insegnamenti-dei-corsi-di-laurea/2025/analisi-e-gestione-del-rischio>

Questo ppt

Analisi e gestione del rischio



1



2

Parte 1 - scaldiamo i motori



3



4



5



6



7



8



9



10



11



12



13



14



15



16



17



18



19



20



21



22



23



24



25



26



27



28



29



30



31



32



33



34



35



36



37



38



39



40



41



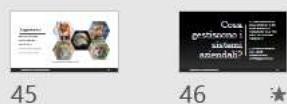
42



43



44



45



46



47



48



49



50



51



52



53



54



55



56



57



58



59



60



61



62



63



64



65



66



67



68



69



70



71



72

Questo ppt – Nota bene

Analisi e gestione del rischio

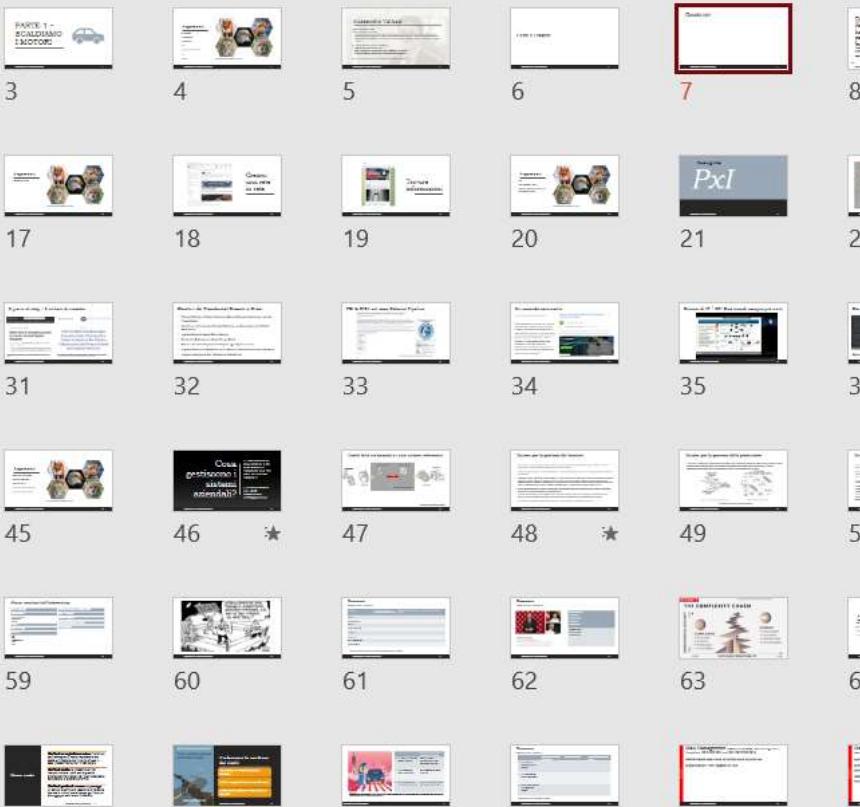


1



2

Parte 1 - scaldiamo i motori

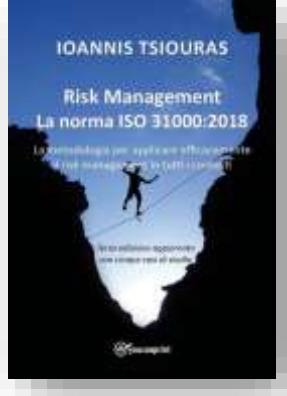
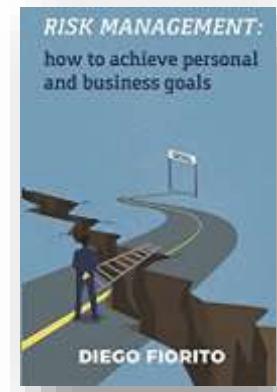


Alcune sezioni finali sono indicate con il nome «verticale» su «argomento»

Lo studente ne prepari almeno una a scelta e indichi quale/quali ha preparato

Testi di riferimento

1. Diego Fiorito; Risk management: how to achieve personal and business goals. ISBN 9798686535879 / Eccetto chapter III (pagine 59-70). In inglese.
 2. Risk Management – La norma ISO 31000. La metodologia per applicare efficacemente il risk management in tutti i contesti. Terza edizione aggiornata con 5 casi di studio. ISBN 8891149837. In italiano.
 3. ISO 31000:2018; Risk management – Guidelines.
<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en> In Inglese.
 4. ISO/IEC 27000:2018; Information technology – Security techniques – Information security management systems – Overview and vocabulary.
<https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html> In inglese
 5. Cesare Gallotti; Sicurezza delle informazioni (edizione del 2022). ISBN 9791220888196 (e-book) e 9791220388450 (cartaceo)
<https://www.cesaregallotti.it/libro.html> in italiano. Oppure Cesare Gallotti; Information Security (2022 edition). ISBN 9791220888851 (e-book) and 9791220388474 (hardcopy) <https://www.cesaregallotti.it/libro-ENG.html> (alternativa in inglese).



Testi di riferimento facoltativi (6-12)

- I primi 100 giorni del Responsabile della Sicurezza delle Informazioni (in italiano) o The first 100 days of the Information Security Manager (in inglese) scaricabili gratuitamente dal sito <https://c4s.clusit.it/>

Altri libri (in italiano) scaricabili gratuitamente dal sito <https://c4s.clusit.it/> e in particolare quelli più recenti come

- Rischio Digitale Innovazione e Resilienza
- Supply Chain Security
- Intelligenza Artificiale e Sicurezza
- IoT Security e Compliance
- Consapevolmente **Cloud**

Infine,

- Alan Calder; NIST Cybersecurity Framework. A pocket guide. ISBN 9781787780408 in inglese

Esercizi e challenges

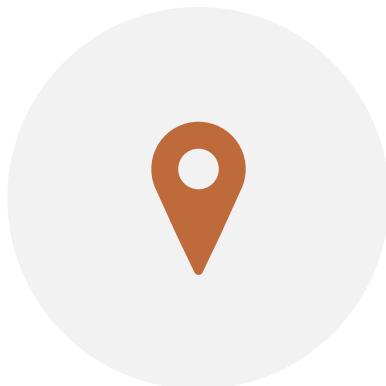
Nel PPT sono indicati alcuni (semplici) esercizi da sviluppare. Sono tutti facoltativi. Possono essere preparati durante il corso e presentati alla classe la lezione successiva a quella dove saranno spiegati. Si scrive una email al professore per prenotarsi

Lo studente ha così l'opportunità di parlare in pubblico. Inoltre, una delle domande di esame riprenderà eventualmente uno degli esercizi svolti.

Esercizio collettivo di analisi del rischio



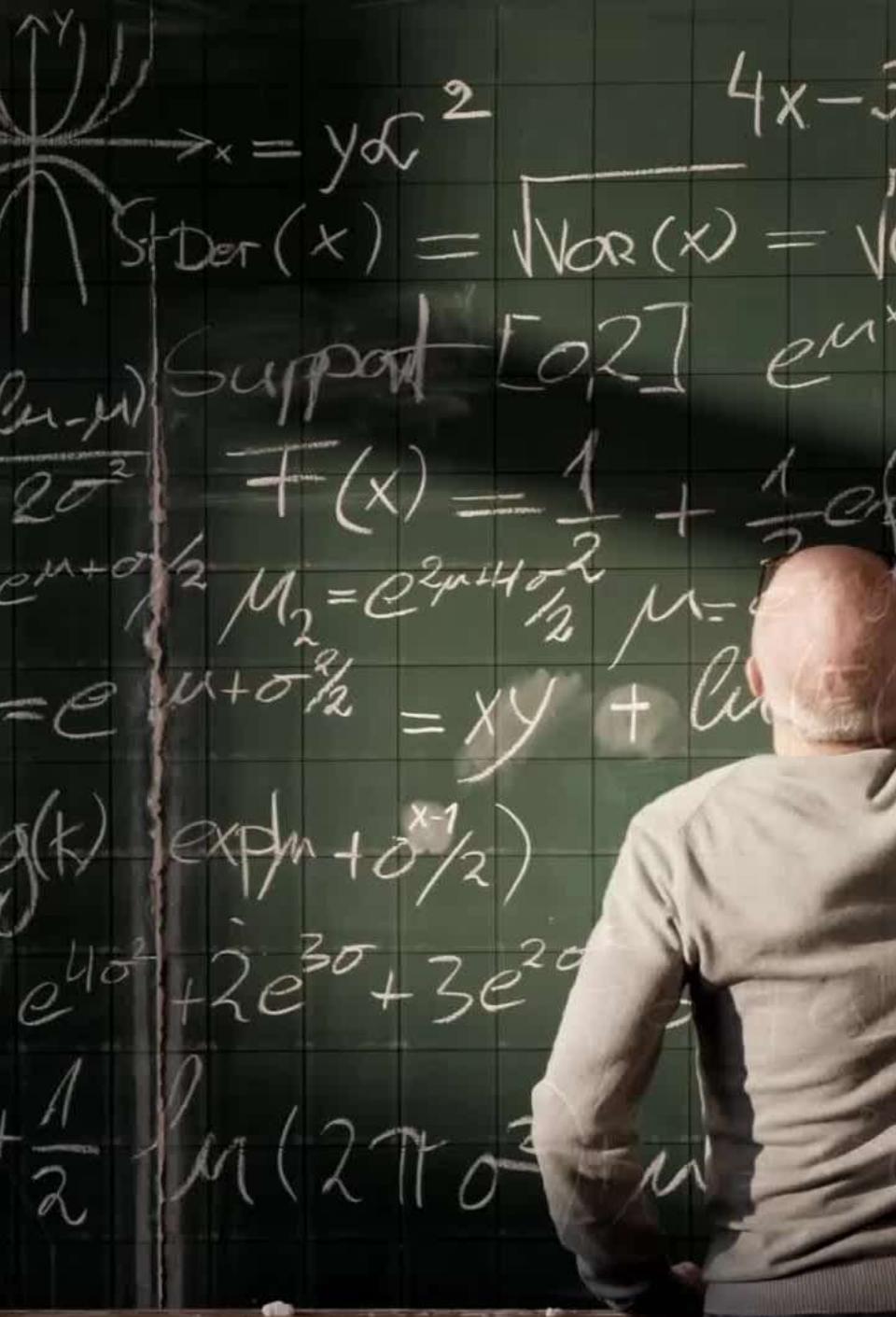
DURANTE IL CORSO FAREMO UN ESERCIZIO COLLETTIVO A PICCOLI GRUPPI DI STUDENTI PER CONDURRE UNA ANALISI DEL RISCHIO 31000.



AVVERrà NELLA SECONDA METÀ DEL CORSO E CI IMPEGNERÀ QUALCHE ORA PER 3 O 4 LEZIONI.



IN QUESTO MODO SI POTRANNO COMPRENDERE BENE I PROCESSI E LE DIFFICOLTÀ RELATIVE.



Ospiti esterni

Quasi tutte le lezioni vedranno le testimonianze (30-60 minuti massimo) dei professionisti che operano nel settore. Avrete la possibilità di capire che mestiere fanno il CISO e gli specialisti e ottenere importanti informazioni sul mondo del lavoro



Esame orale!

Paura!!

Argomenti

Quiz

Che succede la fuori?

Perché è importante l'analisi e la gestione del rischio



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Cosa significa

PXI

Rapporto Clusit

<https://clusit.it/rapporto-clusit/>

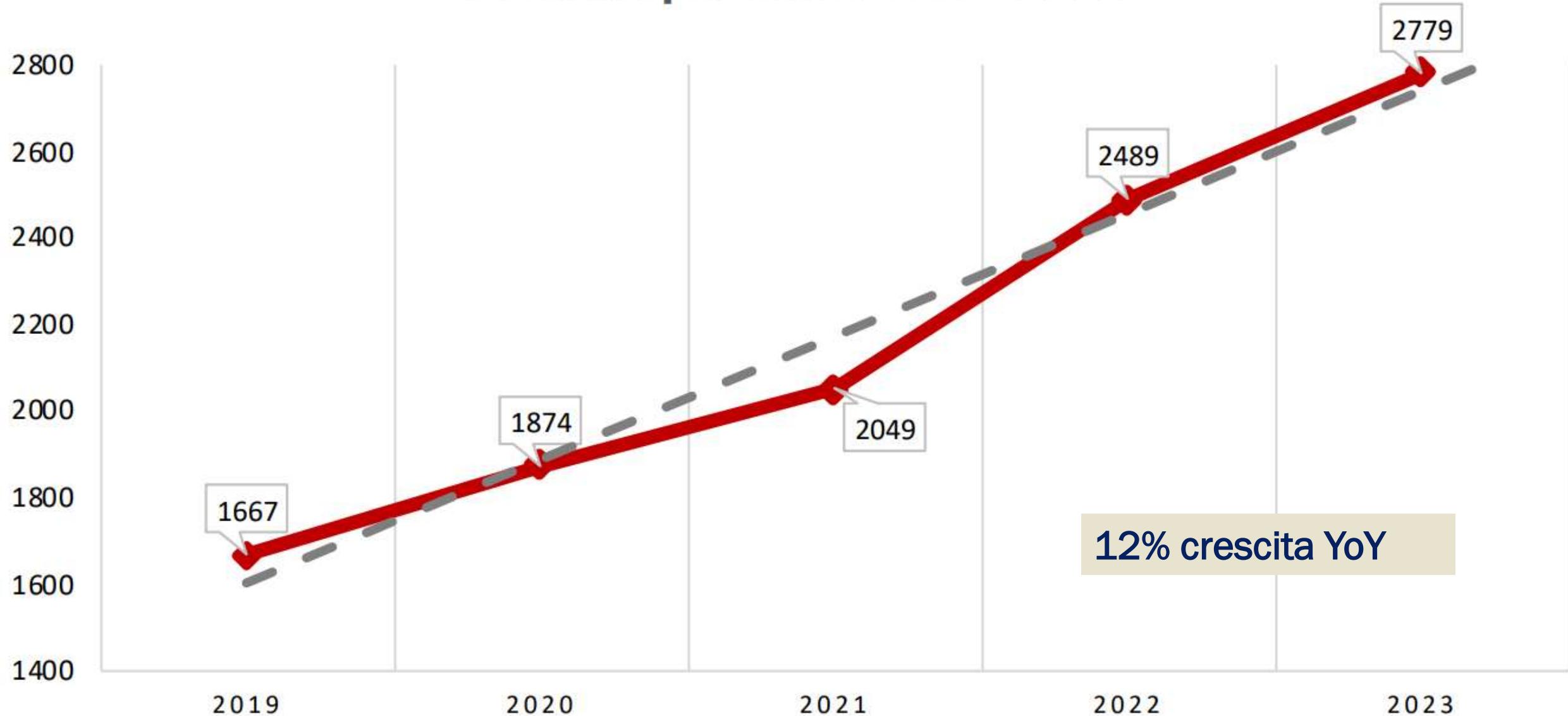


Rapporto Clusit

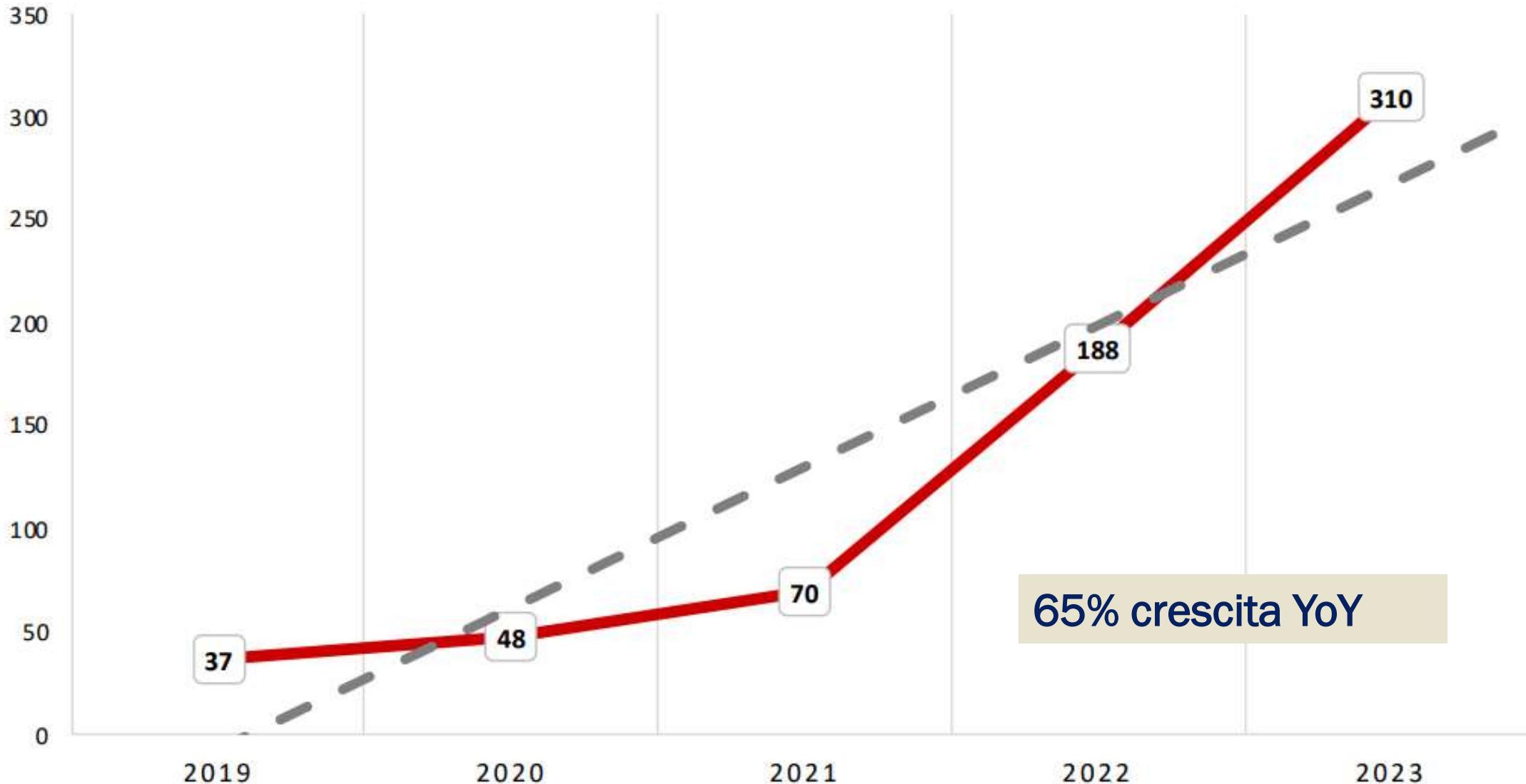
È importante per le analisi che svolge e l'opera di informazione verso il pubblico, la stampa e i decision maker

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

Attacchi per anno 2019 - 2023



Cyber attacchi in Italia 2019 - 2023





Inoltre

Molte altre informazioni e approfondimenti da parte degli esperti del settore e delle diverse autorità coinvolte o interessate al fenomeno cyber

Esercizio

<nome dello/degli studente/i>

- 1.Scaricare il Rapporto Clusit
- 2.Leggerne un capitolo a scelta
- 3.Raccontarlo in classe

Argomenti

Attacco Colonial Pipeline

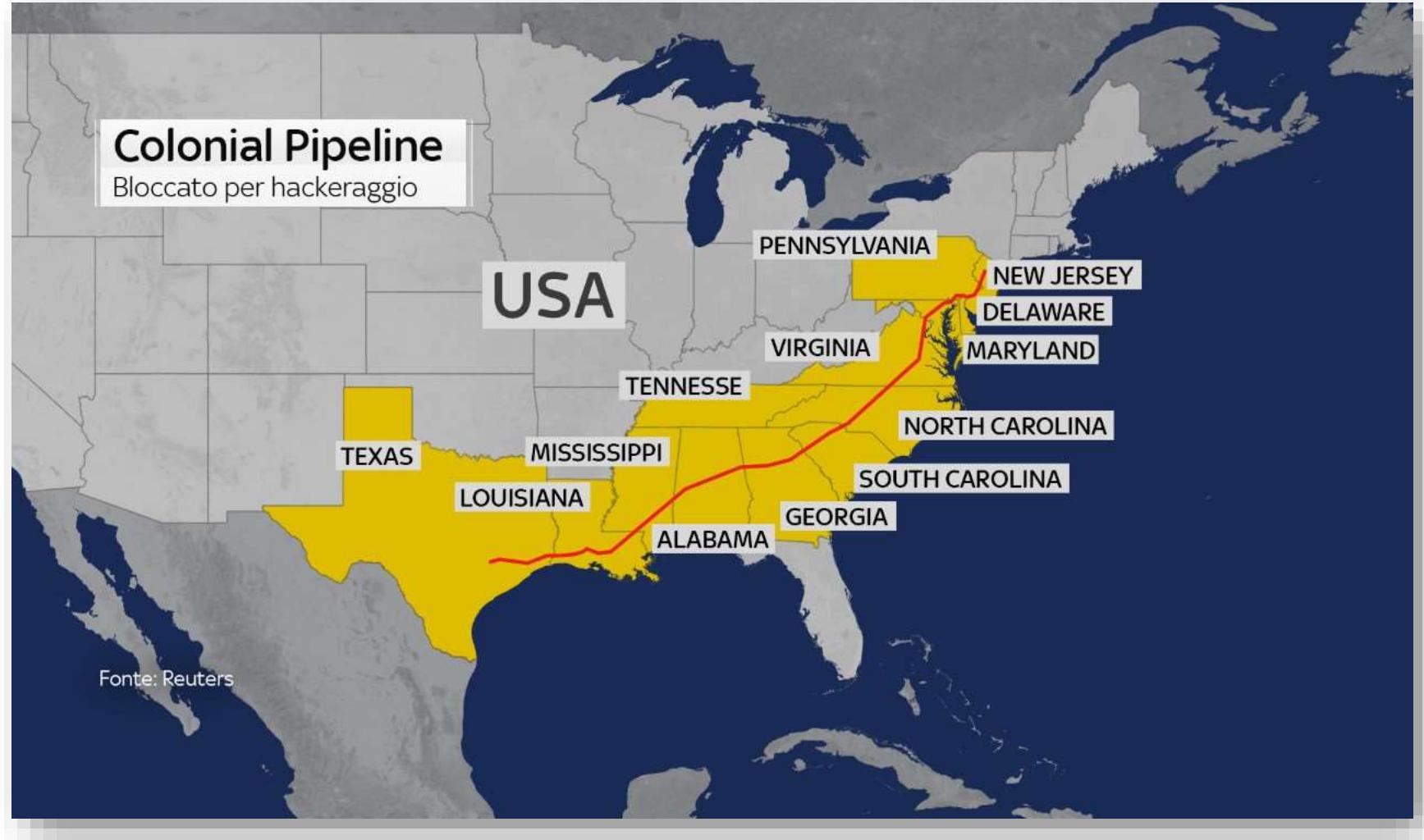
Attacco alla Regione Lazio



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Colonial pipeline cyberattack

- Il più grande oleodotto americano (8850 chilometri di condotte)
- Fornisce il 45% del carburante della East Coast



FONTE: SKY TG24

6 giorni di stop – 5 milioni di riscatto

Seeking Alpha 

Symbols, authors, keywords 

Premium My Portfolio My Authors Top Stocks Latest News Markets Stock Ideas Divide

Energy U.S. Economy Top News

Biden turns to emergency powers to counter Colonial Pipeline disruption

May 10, 2021 4:19 AM ET | Shell Midstream Partners, L.P. (SHLX) | By: Yoel Minkoff, SA News Editor | 517 Comments

- The U.S. government has declared a state of emergency to keep fuel supply lines open following the shutdown of Colonial Pipeline [on Friday](#).

FONTE: <https://seekingalpha.com/news/3693634-biden-turns-to-emergency-powers-to-counter-colonial-pipeline-disruption>

THE WHITE HOUSE 

Administration Priorities COVID-19 Briefin

BRIEFING ROOM

FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks

FONTE: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/>

Obiettivi del Presidential Executive Order

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector 
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government 
- Improve Software Supply Chain Security 
- Establish a Cybersecurity Safety Review Board
- Create a Standard Playbook for Responding to Cyber Incidents
- Improve Detection of Cybersecurity Incidents on Federal Government Networks
- Improve Investigative and Remediation Capabilities

FBI & CISA sul caso Colonial Pipeline

Cybersecurity and Infrastructure Security Agency

From Wikipedia, the free encyclopedia

The **Cybersecurity and Infrastructure Security Agency (CISA)** is a standalone [United States federal agency](#), an operational component under [Department of Homeland Security \(DHS\)](#) oversight.^[3] Its activities are a continuation of the National Protection and Programs Directorate (NPPD). CISA was established on November 16, 2018 when President Donald Trump signed into law the [Cybersecurity and Infrastructure Security Agency Act of 2018](#).^{[4][3]}

Former NPPD Under-Secretary Christopher Krebs was CISA's first Director, and former Deputy Under-Secretary Matthew Travis was its first Deputy Director.^{[5][6]} The expected role of CISA is to improve [cybersecurity](#) across all levels of government, coordinate cybersecurity programs with [U.S. states](#), and improve the government's cybersecurity protections against private and nation-state [hackers](#).^[3]

Contents [hide]

- 1 History
- 2 Role
- 3 Performance
- 4 Subcomponents
- 5 See also
- 6 References
- 7 Notes
- 8 External links

History



Cybersecurity and Infrastructure Security Agency



Agency overview

Formed	2018
Jurisdiction	United States
Headquarters	Rosslyn, Arlington, Virginia
Employees	3,374 (2017) ^[a]
Annual budget	\$3.16 billion (2020)
Agency executives	Brandon Wales, Director (acting) ^[1]

FONTE: https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency

Un secondo commento

280 stazioni pompaggio e controllo



"Many believe that this attack was a result of more engineers remotely accessing control systems for the pipeline from home using a remote desktop software such as TeamViewer and Microsoft Remote Desktop," said Troy Gill, manager of security research at security provider Zix. "The pandemic forces more employees to work from home, and unfortunately, many organizations are still trying to secure their devices, remote access points and overall networks."

How to prevent another Colonial Pipeline ransomware attack



by Lance Whitney in Security on May 12, 2021, 7:31 AM PST

Government and business both need to step up to combat ransomware attacks against critical systems before they spiral further out of control.



FONTE: <https://www.techrepublic.com/article/how-to-prevent-another-colonial-pipeline-ransomware-attack/>

Osmosi di IT / OT. Due mondi sempre più uniti

Premi **Esc** per uscire dalla modalità a schermo intero

IT / OT and the “in between” aka bridges for business / badness

- Attacks on corporate IT networks that pivot over trusted communications to resources in industrial DMZs
- Connections to partner networks that could extend impacts beyond target

The diagram illustrates the layers of network connectivity from External Network Hosts down to Sensors & Actuators, showing various protocol stacks and attack vectors:

- External Network Hosts (Business or Plant Network)**: Contains servers, mobile devices, and desktop computers connected via Common Protocols.
- DMZ Applications**: Contains web servers connected via Common Protocols.
- Supervisory Control Elements (Network, Applications, Servers)**: Contains Engineering Workstation, Alarm Servers, HMI, Application Servers, and Historian, connected via Common & Industrial Protocols.
- Control Elements (PLCs, RTUs, SIS)**: Contains PLCs, RTUs, and SIS, connected via Industrial Protocols.
- Sensors & Actuators**: Contains Sensors and Actuators connected via Fieldbus using Industrial Protocols.

A vertical yellow line on the left highlights the "in between" layers (DMZ Applications, Supervisory Control Elements, Control Elements) with a magnifying glass icon. A red circle highlights a connection point between the DMZ Applications and Supervisory Control Elements layers. A red box highlights a connection point between the Control Elements and Sensors & Actuators layers. A blue box highlights a connection point between the External Network Hosts and DMZ Applications layers. A blue square highlights a connection point between the DMZ Applications and Supervisory Control Elements layers. A blue square highlights a connection point between the Supervisory Control Elements and Control Elements layers. A blue square highlights a connection point between the Control Elements and Sensors & Actuators layers.

SANS | SANS ICS | sans.org/ics | 11 | 2021-05-13 11:20:25 | 48:02

Tim Conway

Darkside



We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.

We received millions of dollars profit by partnering with other well-known cryptolockers.

We created DarkSide because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.

Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.

You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will NEVER provide you decryptors.

We take our reputation very seriously, so if paid, all guarantees will be fulfilled.

If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

FONTE: Dark web; pagina del gruppo criminale

Organizzazione criminale; Malware as a Service

CYBERSECURITY360

Ransomware Darkside, organizz...

Home > Malware e attacchi hacker > Ransomware

Condividi questo articolo



La variante 2.0 del ransomware Darkside è l'occasione per analizzare l'evoluzione delle attività di organizzazione e affiliazione del malware, alla luce del core business dei nuovi attacchi informatici basato sul modello Ransomware-as-a-Service. Ecco il modus operandi e le soluzioni di mitigazione

13 Apr 2021

B Giorgia Benatti

Focus team Legal Tech SC Avvocati Associati e team Compliance&Corporate

C Vittorio Colombo

Avvocato esperto di diritto delle nuove tecnologie

FONTE: <https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-darkside-organizzazione-e-affiliazione-il-core-business-dei-nuovi-attacchi-informatici/>

'Majority' of ransom paid by Colonial Pipeline seized and returned by DOJ

Of the \$4.4 million the company paid, \$2.3 million was returned.



By Jonathan Greig | June 7, 2021 – 20:29 GMT (21:29 BST) | Topic: Government , US

The Department of Justice announced on Monday that it managed to recover some of the ransom that was paid by Colonial Pipeline to the cybercriminals behind the DarkSide ransomware last month.

While this is not the first time the government has been able to get some money back to victims, Deputy Attorney General Lisa Monaco said during a press conference that this was a first for the new Ransomware and Digital Extortion Task Force that was created in April to address the growing number of cyberattacks.

FONTE: <https://www.zdnet.com/article/majority-of-ransom-paid-by-colonial-pipeline-seized-and-returned-by-doj/>

Colonial Pipeline sends breach letters to more than 5,000 after ransomware group accessed SSNs, more

Colonial Pipeline said the leaks involved the personal information of current and former employees.



By Jonathan Greig | August 16, 2021 – 20:46 GMT (21:46 BST) | Topic: Security

Colonial Pipeline is sending out breach notification letters to 5,810 current and former employees whose personal information was accessed by the DarkSide ransomware group during an attack in May.

The company admitted in an August 13 letter that on May 6, the ransomware group "acquired certain records" stored in their systems.

FONTE: <https://www.zdnet.com/article/colonial-pipeline-sends-breach-letters-to-more-than-5000-after-ransomware-group-accessed-ssns-more/>

E poi?

Attacco al sistema di prenotazione vaccinale della regione Lazio



CORRIERE DELLA SERA

ROMA / CRONACA

REGIONE LAZIO

Attacco hacker, ecco come sono stati «bucati» i sistemi della regione Lazio

Per l'attacco hacker che ha colpito la regione Lazio sono state usate le credenziali di un dipendente di Frosinone. Criptati milioni di dati dal ransomware. Gli esperti: «Senza chiave andrà tutto perso»

di Alessio Lana e Fiorenza Sarzanini



Il governatore Nicola Zingaretti

Hello, Lazio!

Your files were encrypted.

Please don't try to modify or rename any of encrypted files,
because it can result in serious data loss and decryption failure.

Here is your personal link with full information regarding this
accident (use Tor browser):

<http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion>
/ /

Do not share this link to keep this accident confidential.

Alleged Lazio ransom note

FONTE: <https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/>

Conseguenze

- Chiesto un riscatto di 5 milioni di euro in cryptovalute
- Sistemi regionali (in particolare quelli vaccinali e sanitari) bloccati dal primo al sei agosto
- Fortissimo interessamento dei media e grande confusione nella comunicazione



293



1

E' uscito poco fa dalla questura di **Frosinone** N. B., 61 anni, impiegato presso la Regione (Enti Locali) che è stato sentito in merito all'**attacco hacker** del sito regionale. Ai poliziotti ha detto che, stando a casa, in smart working, lavora spesso di sera per ultimare le pratiche a lui assegnate. Ha aggiunto anche di non essersi «accorto di nulla» nella notte in cui il sito è stato attaccato (si presume) attraverso il suo computer.

FONTE: https://www.ilmessaggero.it/roma/news/attacco_hacker_regione_lazio_interrogatorio_impiegato-6124289.html

1. Furto delle credenziali VPN



Cos'è Emotet?

Emotet è un programma malware originariamente sviluppato sotto forma di trojan bancario. L'obiettivo era quello di accedere a dispositivi stranieri e spiare i dati privati sensibili. Emotet ha ingannato i programmi anti-virus di base nascondendosi da essi. Una volta infettati i sistemi, il malware si diffonde come un worm cercando di infiltrarsi in altri computer nella rete.

Emotet si diffonde principalmente attraverso e-mail di spam. L'e-mail contiene un collegamento dannoso o un documento infetto. Scaricando il documento o aprendo il collegamento, vengono automaticamente scaricati altri malware nel computer. Le e-mail sono state create per sembrare molto autentiche e molte persone sono rimaste vittime di Emotet.

FONTE: <https://www.kaspersky.it/resource-center/threats/emotet>

2. Installazione di Emotet |

A

questo punto tutto era pronto per il **terzo passaggio**, il clou dell'operazione, **l'inserimento del ransomware**, il programma che ha **criptato i dati e chiesto il riscatto**. Insomma, una procedura che ricalca un copione già letto favorita però dall'assenza di una procedura di autenticazione a due fattori da parte del dipendente, quella misura che oltre a username e password chiede un secondo modo per confermare la propria identità come per esempio un sms sul telefono o un'app che rilascia un codice.

FONTE: https://www.corriere.it/cronache/21_agosto_03/attacco-hacker-lazio-vpn-5d4eb07e-f420-11eb-9680-9b12a81aa8eb.shtml

3. Inserimento del ransomware |

chiave che ti do io dietro pagamento. Per fare questa cosa **hanno cercato di eliminare tutte le copie di salvataggio, proprio per evitare che la vittima recuperasse i dati**. In questo caso i dati di salvataggio non sono stati cifrati perché anche questa sarebbe un'operazione troppo onerosa, ma sono stati **cancellati con una tecnica sofisticata sovrascrivendo nuovi dati e cifrando i dati primari**". "Peccato- ha proseguito- che questa operazione sia stata sventata dal sistema che gestiva questi dati di salvataggio, che non è un disco normale ma un'attrezzatura per data center che emula le vecchie librerie robotizzate a nastro e quindi ha un disaccoppiamento molto importante tra le funzioni di alto livello e lo strato fisico. **Le cancellazioni sono state soltanto logiche: i dati sono rimasti nel substrato delle memorie e con operazioni tecniche piuttosto sofisticate è stato possibile recuperarli**" ha concluso Giustozzi. (Fde/ Dire) 17:51 06-08-21 NNNN

14.4K 18:11

FONTE: Account ufficiale regione Lazio, 9 agosto. Attribuito a Corrado Giustozzi

Storia plausibile, dice **Paolo dal Checco, ingegnere forense e tra i massimi esperti del tema**: "Può succedere che i dati siano solo cancellati, anche se di solito i ransomware riescono a criptare anche i backup".

Plausibile, ma che lascia perplessi numerosi tecnici, in particolare su **Twitter** e su chat dedicate alla security su **Telegram**: Matteo Flora si è per esempio detto scettico rispetto all'annuncio del ritrovamento dei dati (presentato per la prima volta ieri sera da Corrado Giustozzi, che lavora sul caso e finora avrebbe sempre parlato autorizzato dalla Regione), ma "**sarà facile vedere se hanno pagato o meno il riscatto**. Se non escono i dati, hanno pagato".

Insomma, il sospetto è che i dati siano stati recuperati perché la Regione ha pagato il riscatto, **ipotesi fin dall'inizio scartata anche dal governo**. Comunque, la piattaforma vaccinale è già

FONTE:
https://www.repubblica.it/tecnologia/2021/08/06/news/l_attacco_alla_region_lazio_il_backup_che_salva_e_i_dubbi_sul_riscatto-313139323/

Risoluzione

Esercizio

<nome dello/degli studente/i>

The screenshot shows the Lawfare website's header with the title 'LAWFARE' and a yellow speech bubble icon. It includes navigation links for 'TOPICS', 'HOME', 'REVIEWS AND ESSAYS', 'FOB BLOG', 'AEGIS', 'RESOURCE PAGES', 'SPECIAL FEATURES', 'MORE', and social media links for Twitter and Facebook. Below the header, the date 'Sunday, September 26, 2021' is displayed. The main content area features the article title 'SolarWinds and the Holiday Bear Campaign: A Case Study for the Classroom' and author information 'By Robert Chesney Wednesday, August 25, 2021, 8:01 AM'.

CYBERSECURITY

SolarWinds and the Holiday Bear Campaign: A Case Study for the Classroom

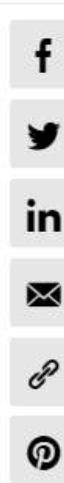
By Robert Chesney Wednesday, August 25, 2021, 8:01 AM



Robert Chesney is the **Charles I. Francis Professor in Law** and Associate Dean for Academic Affairs at the University of Texas School of Law. He also serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law. His scholarship encompasses a wide range of issues relating to national security and the law, including detention, targeting, prosecution, covert action, and the state secrets privilege; most of it is posted [here](#). Along with Ben Wittes and Jack Goldsmith, he is one of the co-founders of the blog.

Lettura interessante

FONTE: <https://www.lawfareblog.com/solarwinds-and-holiday-bear-campaign-case-study-classroom>



▲ Nikita Kuzmin a bordo della sua BMW Serie 6 cabriolet

FONTE: https://www.repubblica.it/esteri/2021/09/09/news/cybercrime_malware_e_i_reati_informatici_di_nikita_kuzman_il_mondo_di_gozzi-316873694/

Esercizio

<nome dello/degli studente/i>

- 1.Trovare sulla stampa la descrizione di un incidente di sicurezza
- 2.Fare 1-3 slide
- 3.Raccontarlo in classe

Argomenti

Il mondo del lavoro



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

The screenshot shows a LinkedIn feed page. At the top, there's a navigation bar with various icons and a search bar. Below it, the main content area displays a post by Davide Giribaldi. The post includes a profile picture of Davide Giribaldi, his name, title ('1st'), and a brief bio: 'I protect your company's value from crisis, threats and vulnerabilities.' It also mentions a post about ransomware that has affected the Region Lazio. A 'See translation' link is present. Below the post, there's a large image of a building with 'REGIONE LAZIO' written on it. Underneath the image, the text 'Service Unavailable' is displayed, followed by a message: 'The server is temporarily unable to service your request due to maintenance downtime or c...' and a smaller image of hands typing on a keyboard.



Crearsi una rete in rete



Trovare informazioni

Argomenti

Com'è fatta un'azienda

Esercizio (Coca Cola)

I mestieri dell'IT

Esercizio (l'errore più grave)

Voi siete James Quincey



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Cosa gestiscono i sistemi aziendali?

LA COMPRENSIONE
DELL'AZIENDA E DEI
SUOI SISTEMI È
FONDAMENTALE PER
OGNI ANALISI DEL
RISCHIO IT

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

Com'è fatta un'azienda e i suoi sistemi informativi



Icone di Alexandra Olawolska <http://handdrawing.olawolska.com/>

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 inglese «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'automobile del presidente)
- I documenti principali sono l'ordine («purchase order»), la richiesta d'acquisto RDA («requisition») che serve internamente per raccogliere le esigenze, la richiesta d'offerta RDO che viene mandata a diversi fornitori per chiedere informazioni su prezzi e condizioni (RFP «request for proposal»; «request for information» RFI). In alcune situazioni, soprattutto nella pubblica amministrazione al di sopra di certi importi, si indicano 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 possono 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'ufficio 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 dell'azienda. 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.

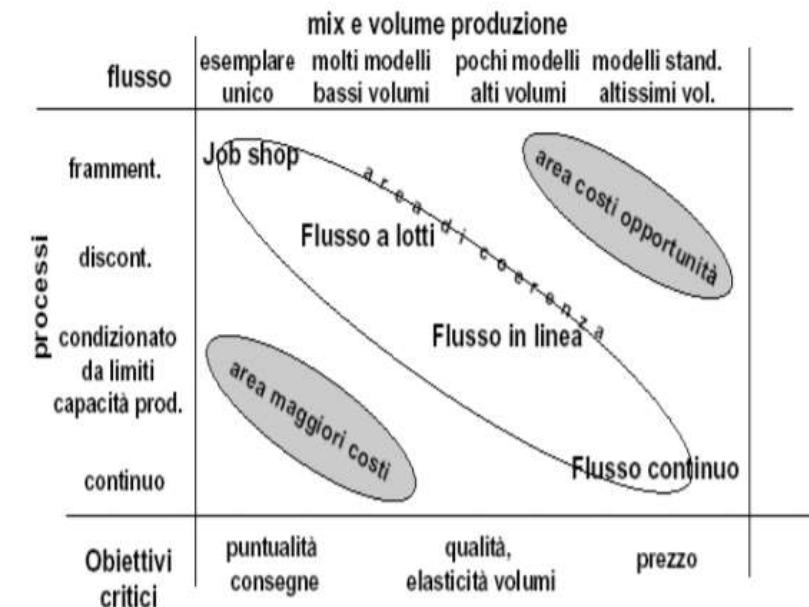


Figura 1.3: Matrice prodotto - processo.

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 delle aziende 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 commerciale. Possono essere presenti dei commerciali, degli agenti, dei rappresentanti, dei distributori. La retribuzione di questi soggetti è fortemente legata 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 vendita (assistenza all'uso) eventualmente coadiuvata da una rete di partner (aziende terze che intervengono a monte e/o a valle della vendita).
- Il sistema informatico principe è il CRM (customer relationship management) che gestisce i contatti (persone che appartengono all'organizzazione del cliente), le trattative secondo il loro stato di avanzamento e gli ordini. Inoltre, una serie di elementi e indicatori che 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 situazione 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 questo processo.
- I software utilizzati sono di diverso tipo a seconda del business aziendale e i documenti possono essere disegni in bozza, disegni tecnici molto dettagliati, database di prove, documenti testuali, corrispondenza interna e documenti scambiati con 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 o ad un 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 scelte aziendali. Possono includere lo studio del mercato di riferimento e l’analisi dell’interazione del mercato con l’azienda per 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 presenza 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 manifestazioni.
- I dati principali riguardano le analisi di mercato, dati sintetici e proiezioni di vendita e materiali relativi ai prodotti e alle 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 gestione del personale attraverso tutte le fasi del rapporto di lavoro (dalla candidatura, all'assunzione, alle dimissioni o pensionamento).
- Si occupa degli stipendi e dei pagamenti ai lavoratori. Spesso approva gli aumenti di stipendio a fronte di un budget di aumenti definito con la direzione generale.
- Lavora in tandem con i manager delle varie linee per comprendere le necessità di nuovo personale («vacancy»), formalizzarle in 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 aspetti 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 controllo



- 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), stato patrimoniale (la ricchezza dell'azienda, attivo e passivo) e nota integrativa. Si occupa quindi del reporting di legge e verso la direzione.
- Oltre al reporting di legge provvede alla definizione del budget e della contabilità analitica e si occupa degli aspetti finanziari 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 il business 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 professionisti 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 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) e 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.html>



Confidentiality (Riservatezza)

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

Integrity (Integrità)

property of accuracy and completeness

Availability (Disponibilità)

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



**Refreshing the World
and Making a
Difference**

Working together to create a better shared future for our people, our communities and our planet

**EXPLORE OUR 2020 BUSINESS &
ENVIRONMENTAL, SOCIAL AND
GOVERNANCE REPORT** ⓘ

Scroll

Esercizio



<nome dello/degli studente/i>

Sistema che gestisce i:	Riservatezza	Integrità	Disponibilità
Fornitori			
Produzione			
Clienti			
Ricerca e Sviluppo			
Marketing			
Risorse umane			
Amm. Finanza e Controllo			
Legale			

Per ogni riga scegliere R, I oppure D e nella cella descrivere le possibili conseguenze (per l'azienda e/o per terzi) di un incidente di sicurezza che comprometta la RID. Scegliere R, I oppure D in funzione della vostra opinione sulla maggior gravità del caso.

Alcuni mestieri dell'informatica

Utente / manager

Programmatore

- Web programmer
- Mobile apps
- Server

Analista

Project Manager

Sistemista

- OS
- DBA
- Middleware vari
- Rete
- Disk

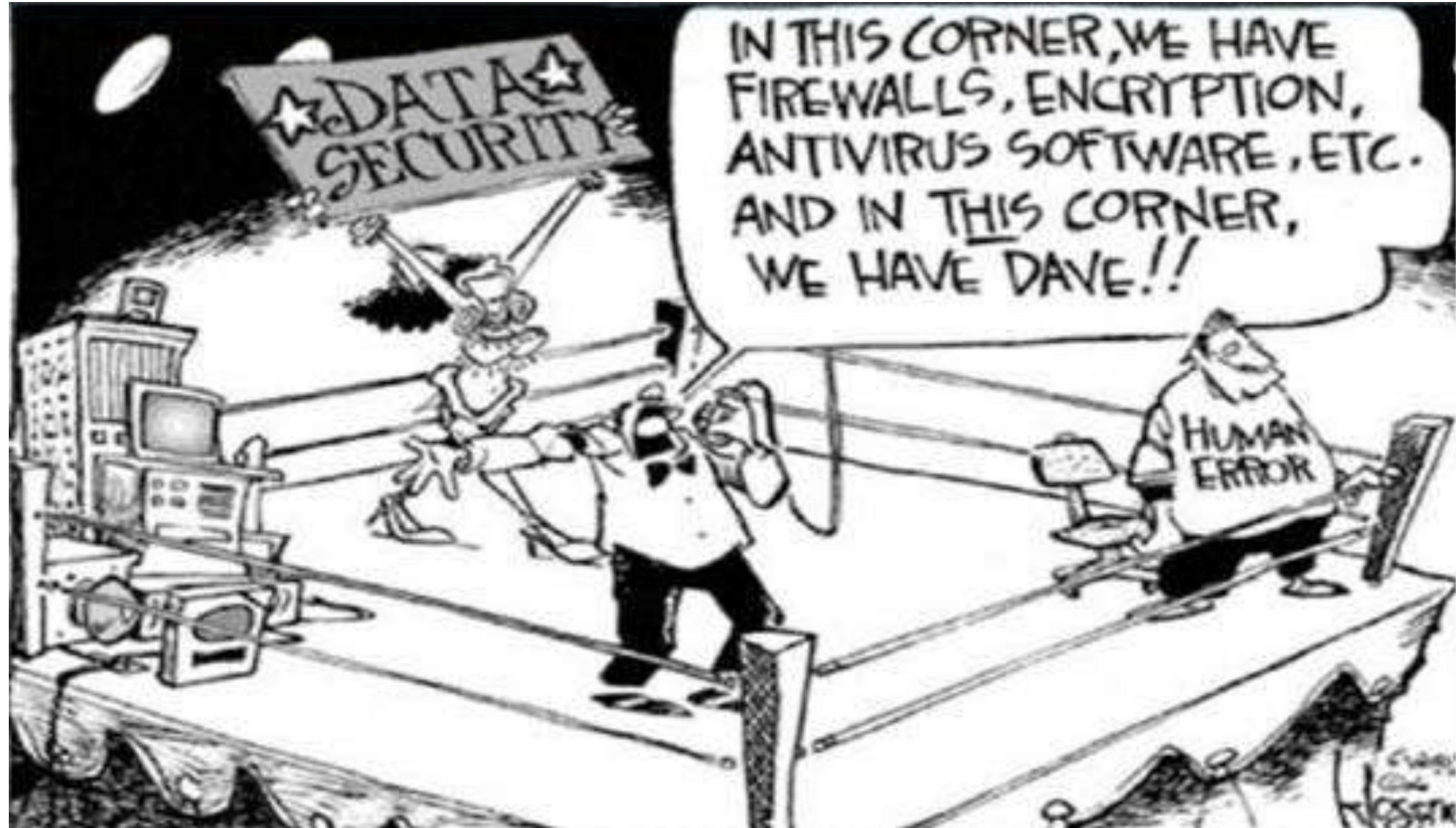
Addetto alla sicurezza / CISO / CSO

CIO / IT Manager

System Integrator

Indipendent Software Vendor

Ufficio acquisti



Esercizio

<nome dello/degli studente/i>

Mestiere	Ha responsabilità certe in merito alla sicurezza (SI / NO)?	Primo errore più grave che può fare	Secondo errore grave
Utenti			
Programmatori			
Analisti			
Project manager			
Sistemisti			
CISO, CSO			
CIO / IT manager			
Ufficio acquisti			

Per ogni riga indicare gli errori che possono fare quelle classi di utenza

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

Quanto denaro aggiuntivo usereste per aumentare la sicurezza informatica?

In quale area / per far cosa lo spendereste?

Argomenti

Com'è fatto il ginocchio umano

Risk

Risk Management

Risk Management Process



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



Ossa e superfici articolari [modifica | modifica wikistato]

L'articolazione del ginocchio è un ginglimo angolare, con un grado di libertà consente quindi il movimento di flessione-estensione; Prevede un secondo grado di mobilità, la rotazione su asse longitudinale della gamba, che si verifica solo a ginocchio flesso.

Sul piano frontale, grazie agli assi longitudinali del femore e della tibia, è possibile notare il comune fisiologico valgismo di circa 170°.

Le ossa coinvolte nell'articolazione del ginocchio sono il **femore**, la **rotula** (o patella) e la **tibia**.

La **patella** è il più grande **osso sesamoide** del corpo umano. È un osso piatto che possiede due superfici, una anteriore ed una posteriore, tre lati ed un apice diretto inferiormente ma la sua forma è molto variabile. La superficie anteriore è molto ricca di fori nutritizi (dove penetrano rami delle arterie genicolate e della ricci rilievi longitudinali che possono essere più o meno marcati a seconda dell'individuo e che sono le aree di inserzione del tendine del muscolo **quadriceps femorale**, dove si inseriscono i muscoli **vasto intermedio** e **retto del femore**. Lungo i lati mediale e laterale si inseriscono rispettivamente il retinacolo patellare mediale e il reti posteriore è invece più liscia di quella anteriore. La porzione superiore è divisa longitudinalmente da un rilievo, detto spigolo, in due faccette articolari, con la latera faccette la patella si articola con la superficie patellare del femore. La porzione inferiore sino all'apice è invece molto scabra, qui infatti si inserisce il tendine patella costituita da una lamina di osso compatto superficiale che ricopre una più spessa porzione trabecolare, con le trabecole parallele alla superficie dell'osso nella porzione posteriore.

La superficie articolare del femore è costituita dalla sua epifisi distale espansa. L'epifisi distale del femore è costituita dai due condili, mediale e laterale, che anteriormente posteriormente divergono lateralmente; lo spazio che ne deriva è la fossa intercondiloidea. Superiormente e lateralmente ad esso, ciascun condilo possiede superiore dell'epicondilo mediale forma una sporgenza detta tubercolo adduttore, poiché vi si inserisce una parte del tendine del muscolo grande adduttore. La superiore le due linee sopracondiloidee (mediale e laterale), detta poplitea, è scabra appena superiormente ai condili. Scabra è anche la superficie anteriore dei condili e condili e nella fossa intercondiloidea. Anteriormente all'epifisi distale vi è un'area triangolare liscia, la superficie patellare che si articola con la patella; è concava tra superficie articolare del femore, costituita dalla superficie inferiore dei due condili è liscia ed ha la forma di una "U" rovesciata, essa si articola con il piatto tibiale, ciò prossimale della tibia, mentre non prende contatto con il perone.

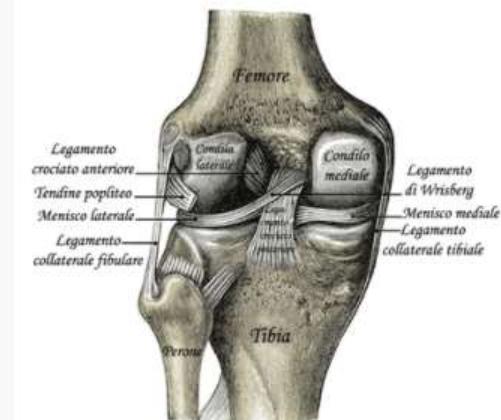
Capsula articolare [modifica | modifica wikistato]

Come ogni diartrosi, il ginocchio è circondato da una capsula articolare, formata da membrane fibrose, separate da depositi di grasso. La capsula è costituita da un sacco che costituisce la **membrana sinoviale**, che delimita una cavità dove è presente **liquido sinoviale**. Anteriormente la membrana sinoviale è attaccata al margine delle carni capsule che non sono comunicanti con questa, presenti tra la cute e la patella.

Menischi [modifica | modifica wikistato]

I dischi articolari del ginocchio sono chiamati **menischi**.^[4] I menischi sono costituiti da **tessuto connettivo** con fibre di **collagene** contenente cellule cartilaginee, hanno

Ginocchio



Vista posteriore del ginocchio sinistro



Vista laterale del ginocchio destro

Anatomia del Gray (EN) Pagina 839

Nome latino *articulatio genus*

Cos'è il rischio?

Risk (ISO 31000:2018)



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 can address, create or result in opportunities and threats.

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

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 operativi. Si parla 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 dipendenti, la felicità della comunità di riferimento**

Possono essere espressi in modi diversi e con parole diverse (obiettivo, target, goal ecc.) in maniera formale (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 e conseguenze.

Non sappiamo chi vincerà le elezioni, come fluttuerà il tasso di cambio, se mi ammalerò di influenza, se viene 7 dalla somma del lancio di due dadi, se il nuovo guardiano si addormenterà durante il turno notturno, se 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 disciplina generale del risk management e la ISO 31000 lo prevedono.

Risk (ISO/IEC 27000:2018)

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, understanding or 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 73:2009, 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 (including 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 can be 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 vulnerabilities of an 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 potential “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), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including 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 can be 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 vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Alcuni rischi

Rischio di contagio di coronavirus: finché non sarò contagiato è molto improbabile che abbia un'infezione. Se rimango chiuso in casa probabilmente non mi contagerò

Rischio di credito: la probabilità di non ricevere indietro i soldi dati a prestito dipende da molti fattori tra i quali la capacità del debitore e le garanzie fornite

Rischio di perdita di un asset: se posseggo un bene c'è sempre la possibilità di perderlo, che me lo rubino, che si rompa per l'uso o si distrugga per certi eventi (incendio)

RISK MANAGEMENT: how to achieve personal and business goals



DIEGO FIORITO

Uniformare la scrittura dei rischi

As a result of <defined cause / causes>,

<this unexpected event> could occur,

which could produce <this effect on targets>



	Pedestrian crossing the road being distracted
1. As a result of <defined cause / causes>,	Come risultato di attraversare la strada guardando il cellulare
2. <this unexpected event> could occur,	Un'automobile potrebbe investirmi
3. which could produce <this effect on targets>	e causarmi morte o ferite e conseguenti costi medici

Fonte dell'immagine:

https://www.dreamstime.com/search.php?securitycheck=3592561f791a84f63f3595d615730338&firstvalue=&lastsearchvalue=&srh_field=pedestrian+accident+vector+illustration+man+smartphone+crosswalk+danger+road+careless+young+dangerous+way+safety+internet+image11892738&s_ph=y&s_il=y&s_video=y&s_audio=

Esercizio

<nome dello/degli studente/i>

	Rischio di contagio di coronavirus	Rischio di credito	Rischio di perdita di un asset
1. As a result of <defined cause / causes>,			
2. <this unexpected event> could occur,			
3. which could produce <this effect on targets>			

Completare la tabella seguendo lo schema

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

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

Risk Management Process

(ISO Guide 73:2009, “Risk management – Vocabulary, and ISO/IEC 27000:2018)

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

My account

Search

Search results ×

5 results for

risk management process



Orientation:



ALL LANGUAGES

View:

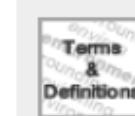
FULL ENTRY

GROUPED

Results per page: 300 ▾

✖ Terms & Definitions

Sort by: RELEVANCE ↓ TERM

**risk management process**systematic application
establishing the context

Note 1 to entry: The pro

ISO 13131:2021(en), 3.

Available in: EN

Un tool utile:
<https://www.iso.org/obp/ui#search>

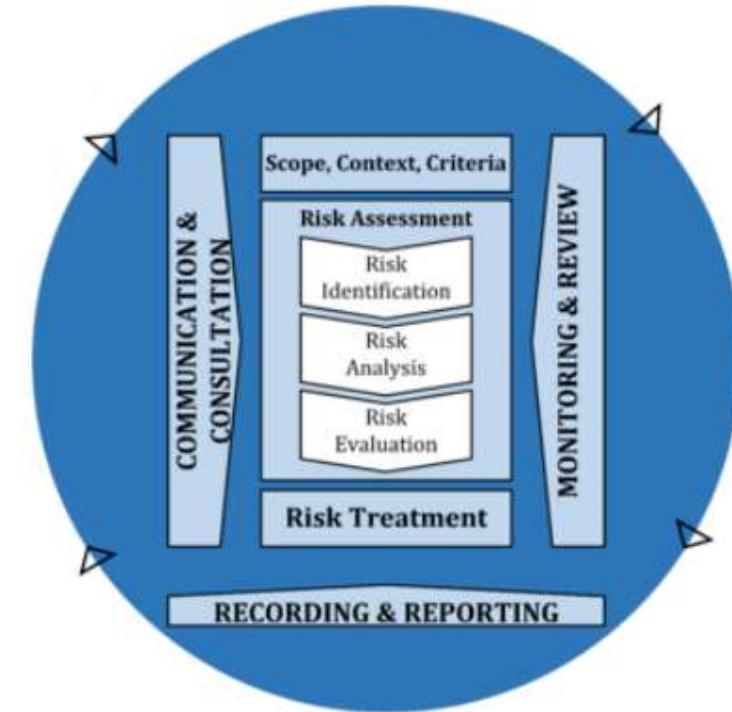
**risk management process**systematic application of management **policies** (3.53), procedures and practices to the activities of communicating,
consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing **risk** (3.61)Note 1 to entry: ISO/IEC 27005 uses the term “*process*” (3.54) to describe risk management overall. The elements within the
risk management (3.69) process are referred to as “activities”.

[SOURCE: ISO Guide 73:2009, 3.1, modified — Note 1 to entry has been added.]

Perché il termine Risk Management Process (che è definito nella ISO/IEC 27000:2018) non è definito nella ISO 31000:2018?

Perché la 31000 descrive come si fa il processo di risk manager, quindi non posso metterlo nella definizione, è il contenuto della norma (sarebbe ricorsivo)

Risk Management Process as ISO 31000:2018



Process (clause 6)

Argomenti

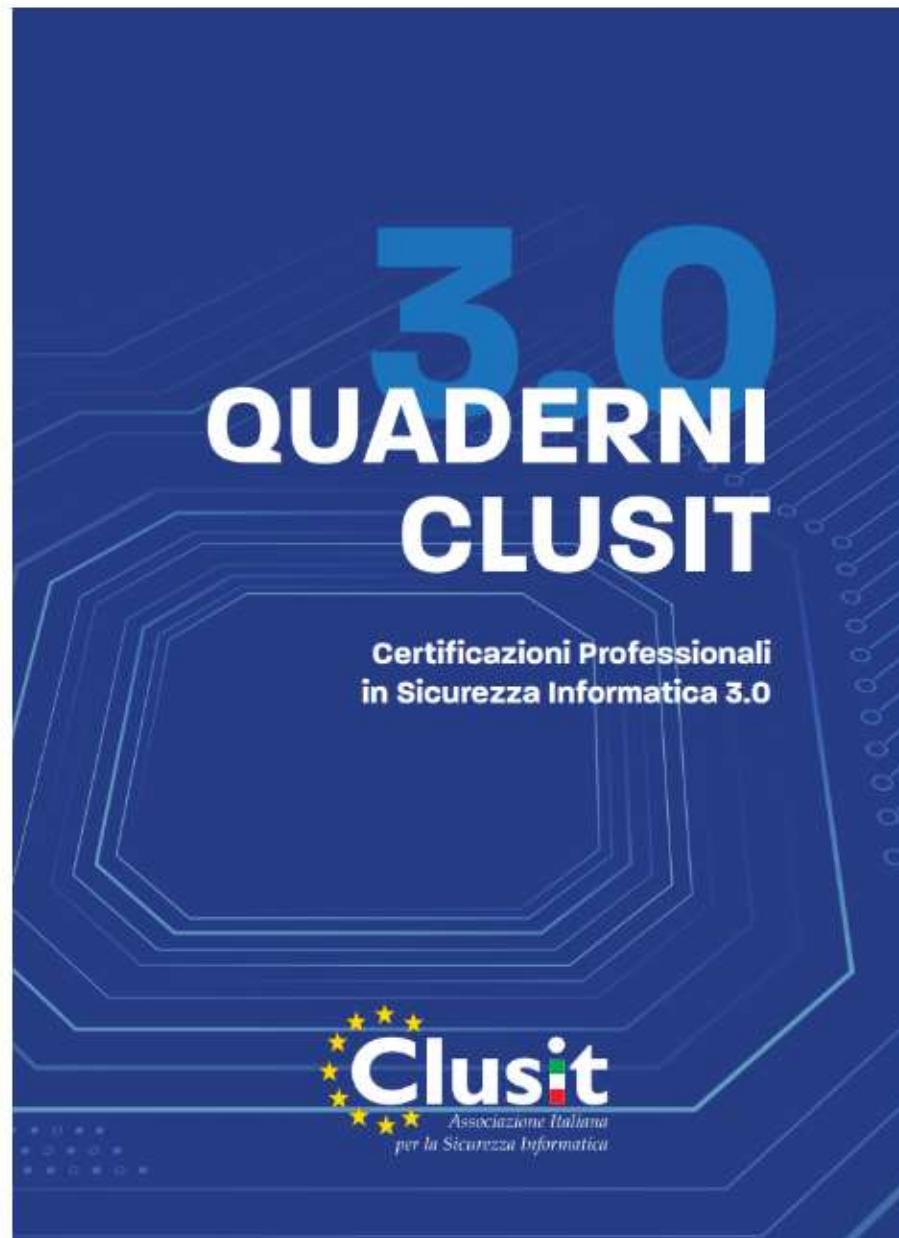
Le certificazioni professionali

Classificazione del rischio in
funzione dell'impatto

Esercizio



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



Cesare Gallotti, Federico Gozzi, Fabio Guasconi
<https://clusit.it/blog/quaderni-clusit-certificazioni-professionali-in-sicurezza-informatica-3-0-giugno-2023/>

Le certificazioni professionali sono lo strumento per eccellenza con cui dimostrare la propria competenza in un certo settore al di là o a rafforzamento delle referenze individuali.

L'edizione 2023 è un aggiornamento e revisione dei quaderni pubblicati nel 2005 e nel 2013 da Clusit, al fine di tenerlo al passo con le dinamiche di mercato.

Nel quaderno sono descritte certificazioni che dimostrano competenze tecnologiche accanto a quelle che dimostrano competenze principalmente organizzative. Abbiamo preferito non riportare le certificazioni relative a prodotti specifici, essendo queste troppo numerose.

Si è cercato di schematizzare il più possibile le specifiche di ogni certificazione, in modo da aiutare coloro che selezionano il personale, o scrivono bandi di gara, a stabilire quali certificazioni corrispondono alle caratteristiche richieste e nel contempo i professionisti che vogliono certificare e far riconoscere le proprie competenze in un determinato settore ed essere inseriti in una comunità di professioniste e professionisti con cui scambiare competenze ed esperienze.

Per segnalare mancanze, incompletezze o per proporre nuovi schemi da inserire nel quaderno, si invita a scrivere a qcrt@clusit.it in modo che siano prese in carico per la prossima edizione del quaderno.

Classificazione secondo impatto



Strategic



Operational (processes and procedures)



Projects



Products

Rischi strategici

Sono legati agli aspetti strategici dell'azienda come mission, vision e obiettivi aziendali

(qui si trovano esempi di vision e mission:
<https://www.clearvoice.com/blog/difference-between-mission-vision-statement-examples/>)

Sono di altissimo livello e quindi comprensibili anche dal «pubblico» (stakeholder esterni)

Rischi strategici di Coca Cola Femsa (Mexico) nel 2020

Tabella derivata dal libro Risk management: how to achieve personal and business goals (Diego Fiorito) – la fonte originale non è disponibile

Risk	Description	Impact
Strategic relationship	Loss of the strategic relationship with the distributors	Economic and reputational losses
Demand	Change in consumer preferences	Reduction in demand. Lower income
Patents	Patent violation	Damage to company's brand and reputation
Competition	Aggressive position from the competition	Loss of income, profit or business
Cyber risk	Loss of service or loss of information	Loss of information. Impact on brand reputation
Economic, politic or social conditions	Changes in countries where the company operates	Loss of income. Lower demand. Lower prices. Decrease in profitability
Regulations	New taxes or regulations	Increase in costs. Restrictions. Lower income.
Legal	Adverse results of legal proceedings	Financial impact. Investigations related to taxes, consumer protection, environment or work-related issues
Acquisitions	Little or low ability to integrate acquisitions or fewer synergies than expected	Liabilities. Higher costs
FX (foreign exchange)	FX movement and volatility	Lower profitability due to devaluation of local currencies. Increase of raw material (prices). Lower profitability
Climate change	Unfavorable climate conditions	Loss of operations. Lower sales
Social media	Negative or inaccurate information about the company in the media	Reputational impact
Water	Lack of water	Reduced production
Raw materials	Increase in price or lower availability	Higher costs. Difficulties in production. Reduced profitability

Rischi relativi a processi e procedure (operational)

Sono legati agli aspetti di processo e procedurali dell'azienda

Per essere identificati e compresi richiedono la conoscenza di dettaglio dei processi e/o procedure

Process (ISO 9000:2015)

set of interrelated or interacting activities that use inputs 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 on the 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 inputs to other 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 value.

Note 5 to entry: A process where the conformity (3.6.11) of the resulting output cannot be readily or economically validated is frequently 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 in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified to prevent circularity between process and output, and Notes 1 to 5 to entry have been added.

Procedure

(ISO 9000:2015)

specified way to carry out an activity or a process

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

DEFINIZIONE

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

Risks of «opening of bank accounts»

Due to weaknesses in the design and / or execution of the controls, an error could be generated in the request for transfer of resources (account, amount, bank, etc.), incurring economic losses for the organization.

Due to weakness in the controls or non-application of the controls, or ignorance of the procedures, accounts could be opened in the name of the organization improperly (eg, unauthorized personnel), incurring economic losses.

Due to the lack of a bank analysis or due diligence, an account may be opened at an institution that has high credit risks or financial risks, which could create greater credit exposure and / or image effects for the organization.

Due to the lack of controls or criteria, many accounts could be created (which could not be used), which lead to operational risks and costs associated with their administration.

Due to the absence of personnel, or personnel without specific experience or knowledge in the activities of the process, etc., the procedure could not be executed, affecting the normal flow of operations (partial or total) of the organization.

Due to external events, etc., the procedure could not be executed (unavailability of personal, systems, etc.), affecting the normal flow of operations (partial or total) of the organization.

Rischi relativi ai progetti

Sono relativi ai progetti di ogni tipo,
inclusi i progetti di realizzazione /
integrazione di software

Per essere identificati e compresi
richiedono la conoscenza del progetto,
ma alcune caratteristiche sono comuni

Project (ISO 21502:2020 (and PMBOK – Project Management Institute))

temporary endeavour to achieve one or more defined objectives

I progetti



Li gestisce un project manager che deve equilibrare i costi, i tempi e l'ambito (scope)

Esercizio

<nome dello/degli studente/i>

Risk	Description	Impact

Identificare e descrivere una decina di rischi di progetto. Nella descrizione e nell'impatto usare frasi complete

Rischi di prodotto

Sono legati alla progettazione,
produzione, commercializzazione e
manutenzione di prodotti materiali o
immateriali

L'enfasi è sulla realizzazione di qualcosa
che verrà prodotto in grandi quantità

Risk management di prodotto



Nella fase di design, il risk management deve focalizzarsi sui difetti del processo di produzione e del prodotto in grandi quantità.

Se coinvolti dei fornitori esterni (molto probabile) si devono identificare eventuali criticità (variazioni della qualità attesa, variazioni dei prezzi e delle disponibilità, ritardi di approvvigionamento, fallimento del fornitore, prodotti / fornitori alternativi).

Si devono raccogliere e utilizzare i feedback del mercato per controllare e modificare il processo di produzione (difetti) e le strategie commerciali (prezzi, sconti, bundle ecc.)



Argomenti

Classificazione del rischio in funzione della tipologia



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

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

Esercizio

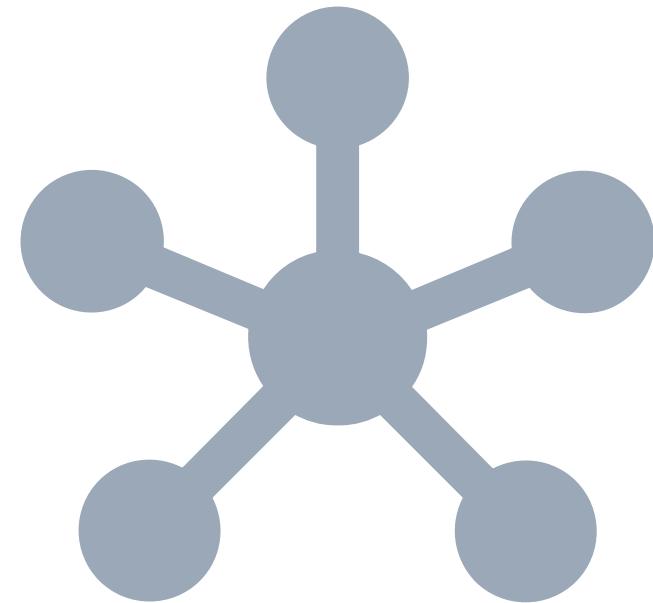
<nome dello/degli studente/i>



Risk	Descrizione
di credito	
di mercato	
relativo alle risorse umane	
legale	
ambientali	
sociali	
di compliance	
di salute e sicurezza sul lavoro	

Descripire i rischi elencati. Usare frasi complete

PARTE 2 – E' TEMPO DI 31000



Argomenti

Introduzione

Processo



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Esercizio

<nome dello/dagli 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 2011 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, perseguiendo i suoi obiettivi, corre molti e diversi rischi.

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

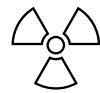
Il risk management aumenta la razionalità delle decisioni.

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

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

ISO 31000:2018

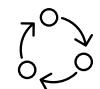
<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>



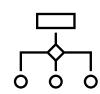
This document is **for use by people** who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.



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



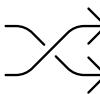
Managing risk is **iterative** and assists organizations in setting strategy, achieving objectives and making informed decisions.



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...

... trattare il rischio

... ma per farlo
abbiamo bisogno di
valutarlo

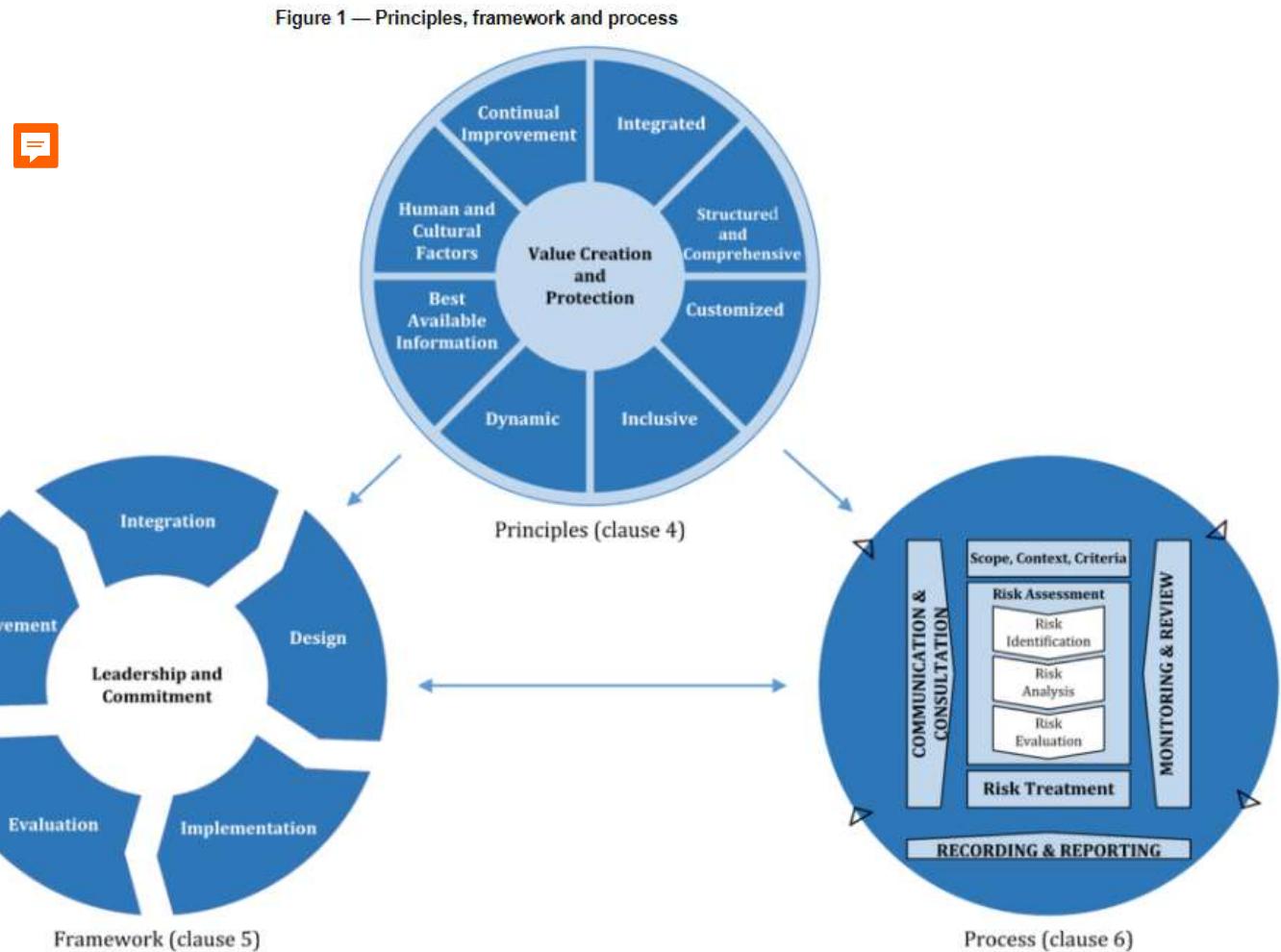
... e prima ancora, di
comprendere in che
contesto siamo

... e, inoltre, dobbiamo
organizzarci per avere
successo

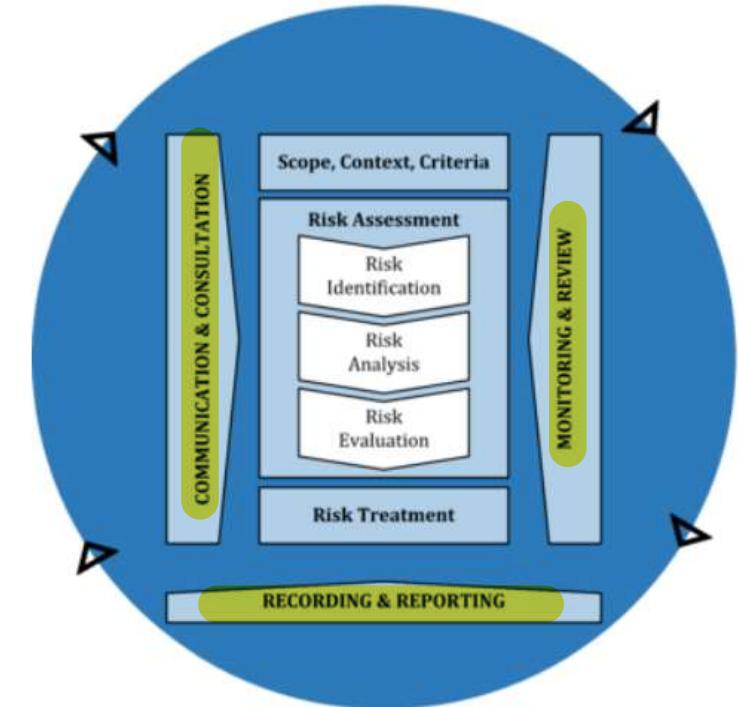


Principi, framework e processo

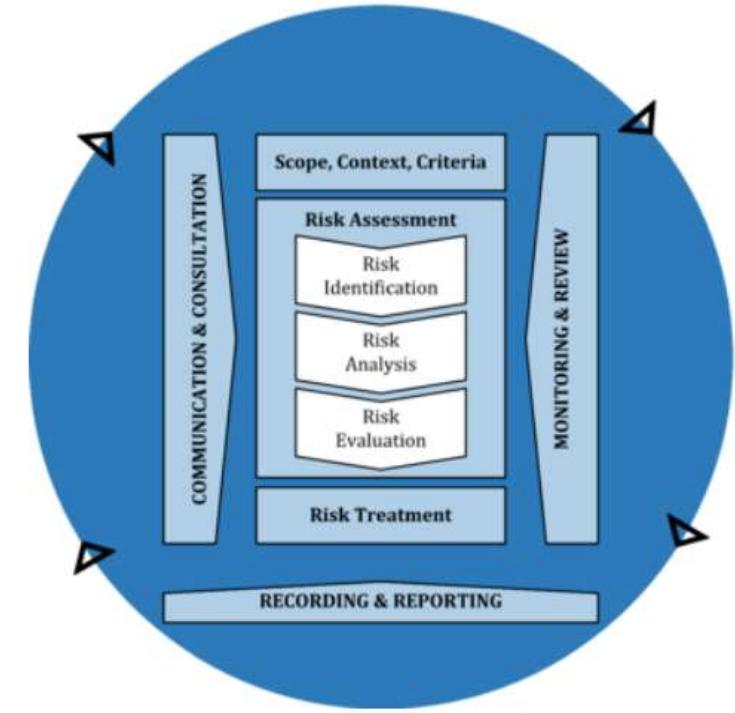
Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.



Risk Management **Process** as ISO 31000:2018



Cosa sono i 4 triangolini sul perimetro?



Communication and consultation

6.2 Communication and consultation



Questo processo ha lo scopo di allineare costantemente gli stakeholders e ottenere feedback e informazioni utili per prendere le decisioni.

E' un processo cruciale e garantisce nel tempo il commitment aziendale ed è un prerequisito per il successo dell'iniziativa di risk management

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

Stakeholder (ISO 31000:2018)

person or organization that can affect, be affected by, or 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”.

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 lo scopo di assicurare la qualità dell'intero processo di risk management e di migliorarlo nel tempo. In pratica risponde alla domanda «Stiamo facendo bene? Si può migliorare?»

Queste domande bisognerebbe porsele in ogni fase e momento dell'intero processo e bisognerebbe pianificarle e assegnare delle chiare responsabilità di esecuzione. Il risultato di queste analisi dovrebbe essere incorporato nel sistema di gestione 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 tramite appropriati meccanismi come, per esempio, la stesura di documenti e la loro archiviazione in modi e luoghi appropriati affinché siano disponibili a chi ne ha o potrebbe avere bisogno. Questi decisioni devono tenere a mente anche gli aspetti di riservatezza e i diversi stakeholder (es. esterni). Lo scopo di questo processo è quello comunicare, fornire informazioni a 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



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



6.6 Monitoring and review

6.7 Recording and reporting

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



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



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 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 process è quello di aumentare la razionalità delle decisioni organizzative. In un certo senso, quello di applicare il «metodo scientifico» all'analisi del rischio. **Quindi si devono definire criteri e misure il più possibile oggettive e ripetibili nel tempo e da persone diverse per dare istruzioni alle fasi di assessment e treatment che seguono.** In questa fase si cerca quindi di definire cose come la risk capacity dell'organizzazione o quando classificare un rischio come alto o basso, eccetera. Si capirà meglio in seguito.

Visto che il risk management ha a che fare con l'incertezza e l'esecuzione del processo stesso fa cambiare nel tempo la maturità aziendale sarà necessario adeguare le decisioni prese 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 trovare, comprendere e descrivere i rischi. Per farlo è necessario avere delle informazioni rilevanti e aggiornate. Per redigere questa 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



Nella fase di risk analysis si cerca di comprendere la natura del rischio e le sue caratteristiche incluso, se appropriato, il livello di rischio. L'analisi considera gli eventi di rischio (event), le risk source, le conseguenze (consequences), le probabilità (likelihood), i controlli (control) e le relazioni tra eventi che possono avere molteplici cause e conseguenze su diversi obiettivi...

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

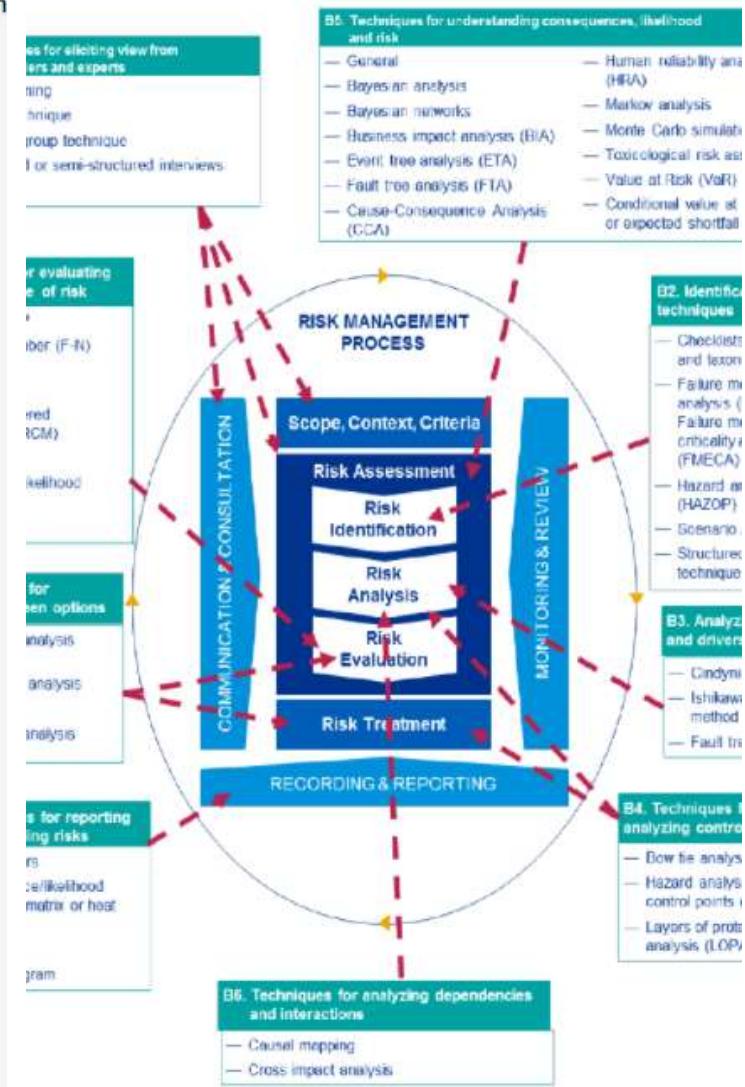
Lo scopo della fase di analisi è quello di dare informazioni alla fase successiva (evaluation) per decidere se il rischio dovrà essere trattato o meno e come.

6.6 Monitoring and review

6.7 Recording and reporting

Elenco 31 Tecniche di Valutazione del rischio (Tabella A) edizioni

1. Brainstorming
2. Structured or semi-structured interviews
3. Delphi
4. Check-lists
5. Primary hazard analysis
6. Hazard and operability studies (HAZOP)
7. Hazard Analysis and Critical Control Points (HACCP)
8. Environmental risk assessment
9. Structure «What if? (SWIFT)
10. Scenario analysis
11. Business impact analysis
12. Root cause analysis
13. Failure mode effect analysis
14. Fault tree analysis
15. Event tree analysis
16. Cause and consequence analysis
17. Cause-and-effect analysis
18. Layer protection analysis (LOPA)
19. Decision tree
20. Human reliability analysis
21. Bow tie analysis
22. Reliability centred maintenance
23. Sneak circuit analysis
24. Markov analysis
25. Monte Carlo simulation
26. Bayesian statistics and Bayes Nets
27. FN curves
28. Risk indices
29. Consequence/probability matrix
30. Cost/benefit analysis
31. Multi-criteria decision analysis (MCDA)



ISO 31010:2019 guida alle tecniche di valutazione del rischio

FONTE: <https://www.certifico.com/id/4040>

Esercizio

<nome dello/degli studente/i>

Descrivere (insegnare a usare) una delle tecniche di valutazione del rischio presentate nella slide precedente cercando su internet. Vedere anche
<https://www.certifico.com/id/4040>

Presentare il risultato con una o più slide di ppt.

Event (ISO 31000:2018)



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 (3.6).

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.

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

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 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.



Considerazioni sulle conseguenze

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

- 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 secondo le conseguenze. La classificazione può essere una misura precisa e quantitativa (esempio denaro perso) 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 infrastrutturale



Likelihood (ISO 31000:2018)

chance of something happening

Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general 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 equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.



Considerazioni sulle probabilità

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

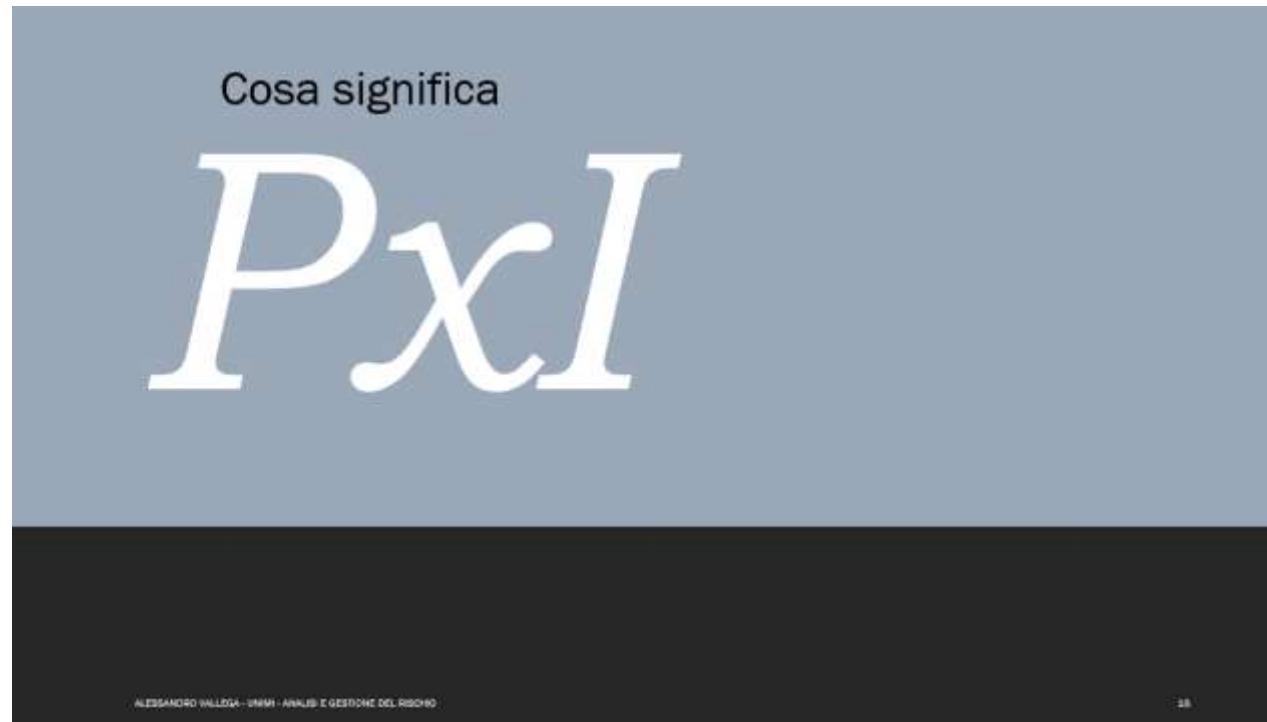
Definizione dei criteri per la gestione del rischio (un esempio)

 La **Probabilità (P)** con la quale si manifesta l'evento sfavorevole (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 ($5\% \leq P < 20\%$)
4	Alta	Probabile	Avviene in una buona parte dei casi ($20\% \leq P \leq 50\%$)
5	Molto alta	Quasi certo	Avviene nella maggior parte dei casi ($P > 50\%$)

Considerazioni su conseguenze e probabilità

Inoltre ci è sicuramente utile combinare le due valutazioni in un unico indicatore di rischio (livello di rischio).



Level of risk (ISO/IEC 27002:2018)

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
Medio (3)	3	6	M	9	15
Alto (4)	4	8	12	16	A
Molto Alto (5)	5	10	15	20	25

Quando si definiscono queste scale e criteri?

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 Molti basso	Insignificante
2 Bassi	Bassi
3 Medio	Moderato
4 Alto	Elevato
5 Molto alto	Catastrofico

Alcune note:

- Nessun danno alle persone o alla produzione. Bassissimo impatto economico.
- Intervento di pronto soccorso. Alcune attività bloccate senza danni alla produzione. Basso impatto economico.
- Rischio infernante medio. Molte attività bloccate con moderati danni alla produzione. Alto impatto economico.
- Danni estesi alle persone. Alcuni processi bloccati con elevati danni alla produzione. Massimo impatto economico anche a livello sistematico (sistemi informatici).
- Casi di morte. Rischio-gas tossici con effetti dannosi. Massimo impatto economico a livello sia sistematico che infrastrutturale.

Risk Management - IAU 31000:2018/pag. 84 - Rischio Totale

rischiocollage - analisi e gestione del rischio

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

La Probabilità (P) con la quale si manifesta l'evento sfavorevole (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	Modesta	Più 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 certa	Avviene nella maggior parte dei casi ($P > 50\%$)

Risk Management - IAU 31000:2018/pag. 83 - Rischio Totale

rischiocollage - analisi e gestione del rischio

Definizione dei criteri per la gestione del rischio

Criteri di valutazione del Rischio

Il **Rischio** (R) (come funzione della probabilità (P) e dell'impatto/Danno/Conseguenze (D); $R = f(P \times D)$)

Conseguenze (D)	Probabilità (P)				
	Molto Bassa (1)	Bassa (2)	Media (3)	Alta (4)	Molto Alta (5)
Molto Bassa (1)	1	3	3	4	5
Bassa (2)	B	4	6	8	10
Media (3)	1	5	M	12	15
Alta (4)	4	8	13	16	18
Molto Alta (5)	3	10	17	20	A

Risk Management - IAU 31000:2018/pag. 82 - Rischio Totale

rischiocollage - analisi e gestione del rischio

Risk assessment

ERAVAMO QUI

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

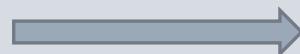
- 6.4.2 Risk identification
- 6.4.3 **Risk analysis**
- 6.4.4 Risk evaluation

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 natura del rischio e le sue caratteristiche incluso, se appropriato, il livello di rischio. L'analisi considera gli eventi di rischio (event), le risk source, le conseguenze, le probabilità, i controlli (control) e le relazioni tra eventi che possono avere molteplici cause e conseguenze su diversi obiettivi...

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

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

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 decisionale del processo. Prendendo in input le informazioni prodotte dall'analisi e i criteri di accettabilità (identificati nella fase scope, context and criteria) permette di decidere se e come 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 o 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, dei benefici, degli obblighi contrattuali e di legge, della diversa opinione dei diversi stakeholder ecc.

Il trattamento di un rischio può modificare o creare altri rischi 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 saranno implementate le opzioni scelte di modo che siano ben chiari i compiti di chi è coinvolto e il progresso del piano possa essere monitorato.

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

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

Control (ISO 31000:2018)

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 actions 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

Argomenti

Framework

Principi



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Risk Management **Framework** as ISO 31000:2018



Framework = struttura di riferimento

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 responsabili della 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 governo, e nelle operations. Deve essere ovunque e ognuno nell'organizzazione ha la responsabilità di gestire il rischio. Le responsabilità di gestione del rischio e la responsabilità di controllo della gestione del rischio devono essere assegnate con precisione.

Design

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

- Comprendere molto bene l'organizzazione e il suo contesto
- Articolare il commitment continuo verso il risk management tramite delle policy (documenti strategici), dichiarazioni o 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 — Vocabulary)

person or entity with the accountability and authority to manage a risk

Implementation

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

Evaluation

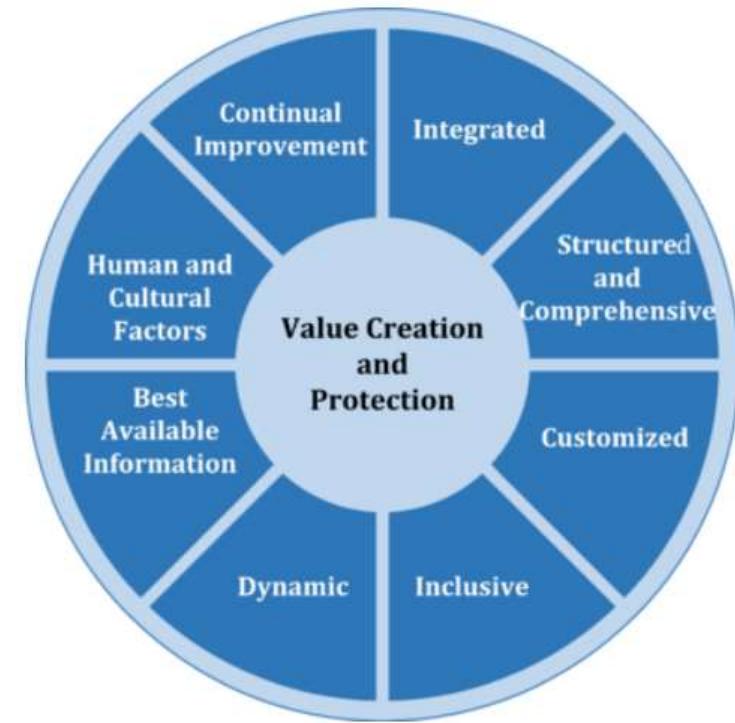
Per valutare l'efficacia del quadro di gestione del rischio, l'organizzazione dovrebbe:

- 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 vengono identificate delle aree o delle opportunità di miglioramento bisogna sviluppare dei piani e assegnare le responsabilità per la loro esecuzione.

Risk Management Principles as ISO 31000:2018



Principles

- a) **Integrated:** Risk management is an integral part of all organizational activities.
- b) **Structured and comprehensive:** A structured and comprehensive approach to risk management contributes to consistent and comparable results.
- c) **Customized:** The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.
- d) **Inclusive:** Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
- e) **Dynamic:** Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
- f) **Best available information:** The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
- g) **Human and cultural factors:** Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
- h) **Continual improvement:** Risk management is continually improved through learning and experience.



Considerazioni finali sulla ISO 31000:2018

La linea guida aiuta le organizzazioni a strutturare il processo di risk 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'incertezza correlata, è normale che varie decisioni e disposizioni vengano corrette ed emendate nel tempo

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

PARTE 3 – INFORMATION SECURITY



Argomenti

Information

Security



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Information security (ISO/IEC 27000:2018)

preservation of confidentiality, integrity and availability of information

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...

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

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



Esercizio

<nome dello/degli studente/i>

Fare un esempio di un incidente di	
Sicurezza aziendale (che non sia anche di sicurezza informatica e di sicurezza delle informazioni)	
Sicurezza informatica (che non sia anche di sicurezza delle informazioni)	
Sicurezza delle informazioni	

Argomenti

Sistemi di gestione

Sistemi di gestione per la
sicurezza delle informazioni



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

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 9001 per i sistemi di gestione della qualità
- ISO 14001 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

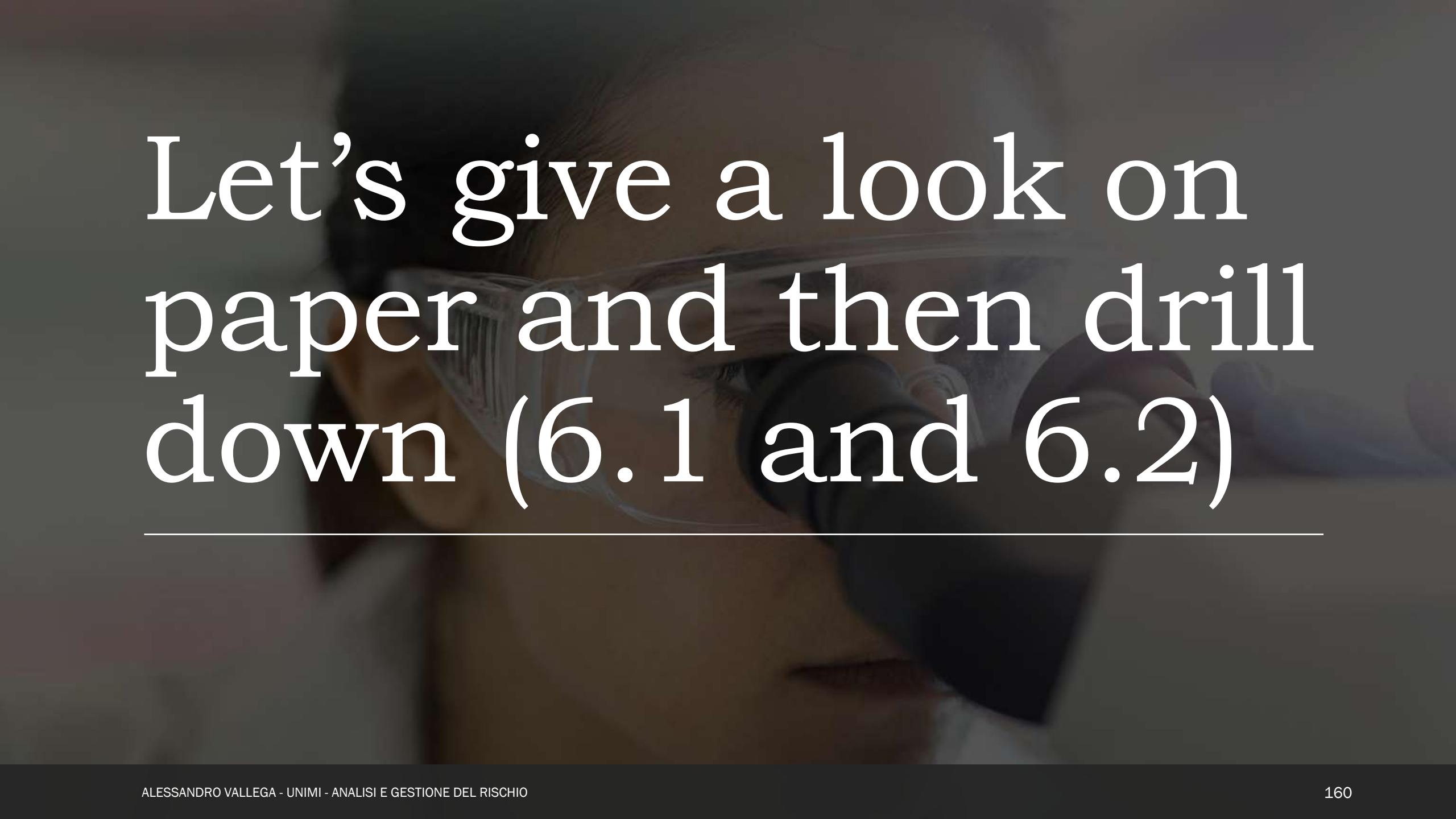
In generale i sistemi di gestione sono un'opportunità per aiutare a fare bene le cose; inoltre, si può ottenere una certificazione che attesti che l'organizzazione stia facendo bene le cose.

Table of contents

- Foreword
- 0 Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- ▼ 4 Context of the organization
 - 4.1 Understanding the organization and its context
 - 4.2 Understanding the needs and expectations of interested parties
 - 4.3 Determining the scope of the information security management system
 - 4.4 Information security management system
- ▼ 5 Leadership
 - 5.1 Leadership and commitment
 - 5.2 Policy
 - 5.3 Organizational roles, responsibilities and authorities
- ▼ 6 Planning
 - 6.1 Actions to address risks and opportunities
 - 6.2 Information security objectives and planning to achieve them
- ▼ 7 Support
 - 7.1 Resources
 - 7.2 Competence
 - 7.3 Awareness
 - 7.4 Communication
 - 7.5 Documented information
- ▼ 8 Operation
 - 8.1 Operational planning and control
 - 8.2 Information security risk assessment
 - 8.3 Information security risk treatment
- ▼ 9 Performance evaluation
 - 9.1 Monitoring, measurement, analysis and evaluation
 - 9.2 Internal audit
 - 9.3 Management review
- ▼ 10 Improvement
 - 10.1 Nonconformity and corrective action
 - 10.2 Continual improvement
- Annex A Reference control objectives and controls
- Bibliography

Argomenti della ISO 27001:2013

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

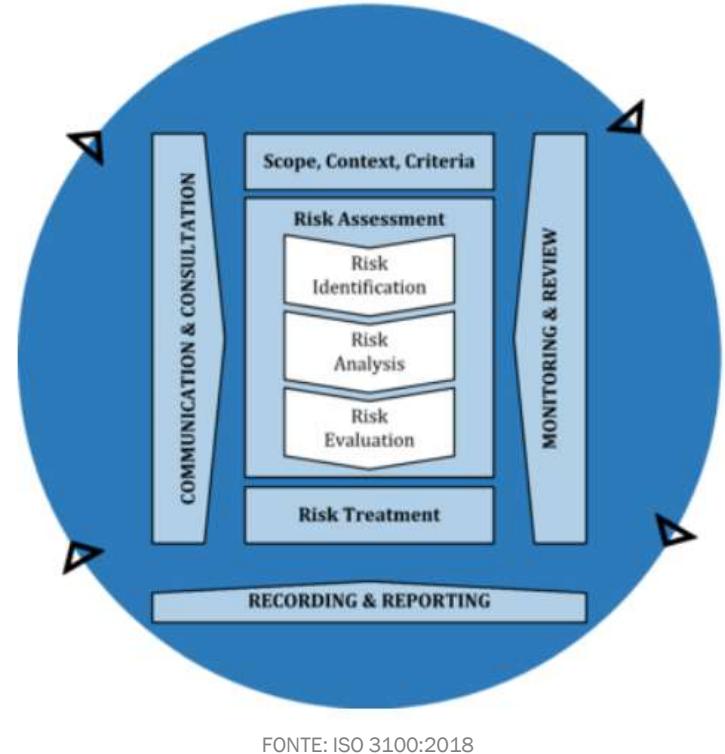
A dark, slightly blurred background image of a person wearing a white hard hat and safety glasses, looking down at something off-camera.

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



IDENTIFICATION

ANALYSIS

EVALUATION

1. Identificare i rischi associati alla perdita di riservatezza, integrità e disponibilità
 2. Identificare i risk owner
 1. Analizzare l'impatto del rischio
 2. Analizzare le probabilità di accadimento
 3. Determinare il livello del rischio
 1. Ponderare i rischi rispetto ai criteri di accettabilità
 2. Prioritizzare i trattamenti

FONTE: ISO/IEC 27001:2013 e 2022

6.1.2.C.1

6.1.2.C.2

6.1.2.D.1

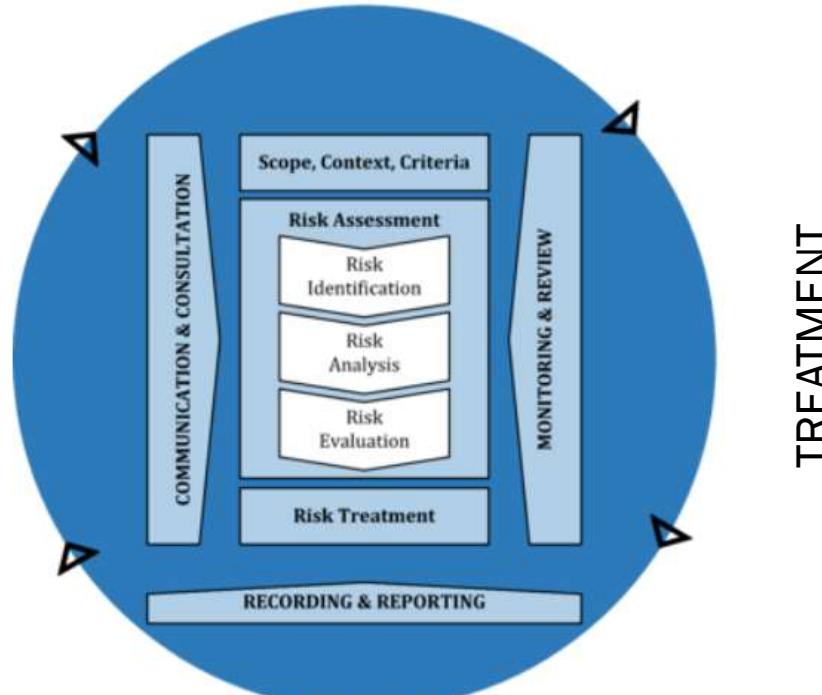
6.1.2.D.2

6.1.2.D.3

6.1.2.E.1

6.1.2.E.2

Un parallelo tra 31000 e 27001



FONTE: ISO/IEC 27001:2013 e 2022

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.

The screenshot shows the ISMS.online platform interface. At the top, there's a navigation bar with 'ISMS.online' logo, a search bar, and links for 'Home', 'Work', 'Virtual Coach', and 'ARM'. Below the navigation, a breadcrumb trail shows the path: Clusters > ISO 27001:2013 Policies and Controls > ISO 27001 Requirements - 4.1 to 10.2 > 6 Planning > 6.1.3: Statement of Applicability. The main content area has a title 'ISO 27001:2013 Policies and Controls' with a 'Statement of Applicability' sub-section. This sub-section includes a sub-headline '6.1.3 Statement of Applicability' and a detailed description: 'Produce a Statement of Applicability that contains the necessary controls and justifications for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A.' Below this, there's a table with fields: 'Status' (Open), 'Assigned to' (David Kelly), 'Start' (Add...), 'Due' (Add...), and 'Days estimated' (0.0). A green button labeled 'Submit for approval' is visible. To the right, there's a sidebar titled 'Statement of Applicability report' with a note about version history and a 'Book your introduction now' button.

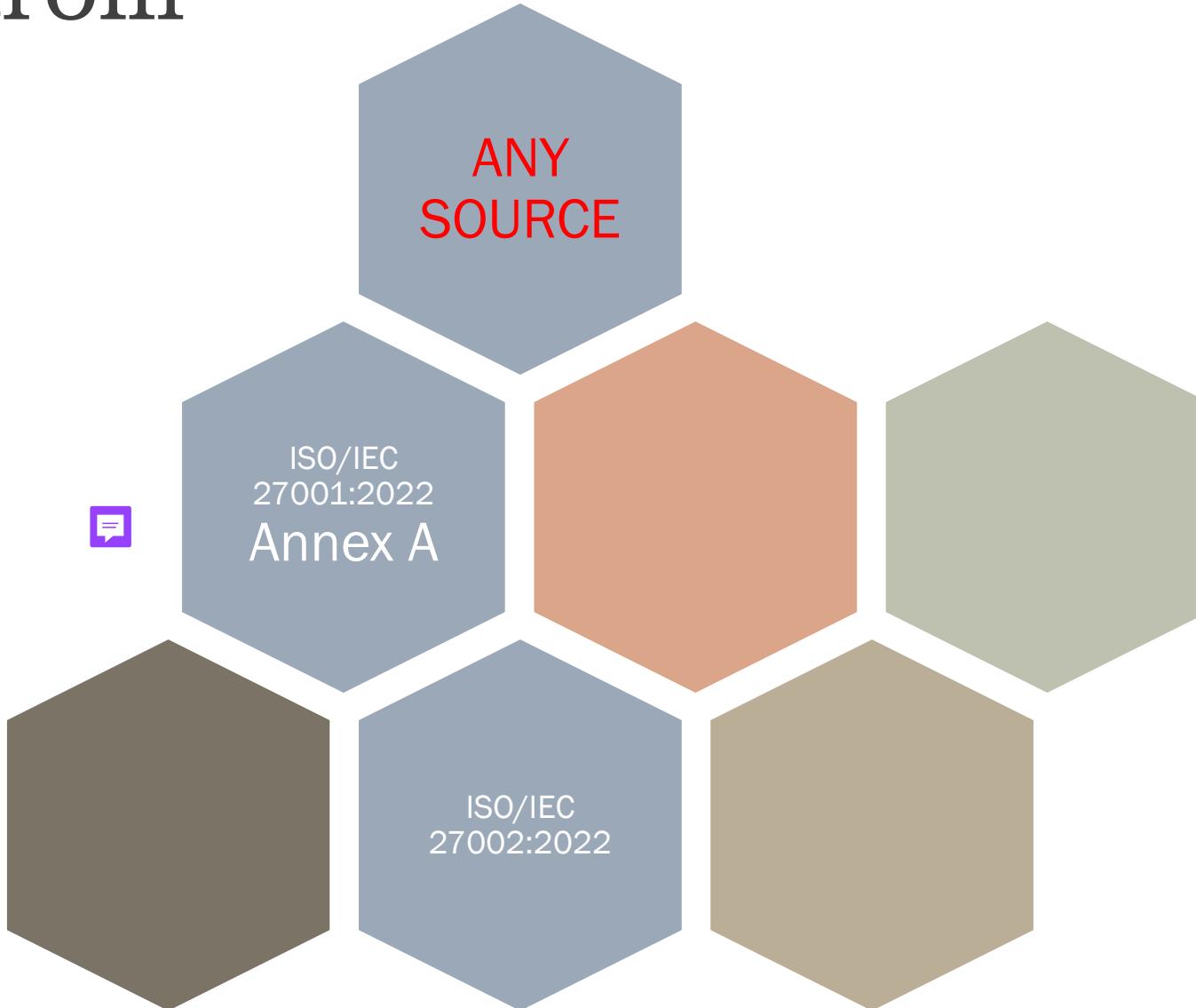
FONTE: <https://www.isms.online/iso-27001/iso27001-statement-applicability-simplified/>

The screenshot shows the ISMS.online website homepage. At the top, there is a dark header bar with the logo "ISMS.online" on the left, a search bar in the center, and a green "Book Your Demo" button on the right. Below the header, there are several navigation links: "How It Works", "Why Choose Us", "Resources", "Partners", "Request Your Quote", "Contact Us", and "Login". The main content area has a dark blue background with the title "ISO 27001 – Annex A Controls" in white. Below the title, there is a breadcrumb navigation: "ISMS.online / ISO 27001, Information Security Management Standard Simplified / ISO 27001 – Annex A Controls". The main content section is titled "Introducing Annex A Controls". It contains two paragraphs of text and a video player. The first paragraph states: "There are 114 Annex A Controls, divided into 14 categories. How you respond to the requirements against them as you build your ISMS depends on the specifics of your organisation." The second paragraph states: "A useful way to understand Annex A is to think of it as a catalogue of security controls. Based on your risk assessments, you'll select the ones that are applicable to your organisation, informed by your particular risks." To the right of the text is a video player interface with the title "ISMS. Annex A Explainer" and a play button labeled "Annex A Controls".

Vediamo ISO 27001 - Annex A

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

Liste di controlli



Argomenti

Ancora sui controlli



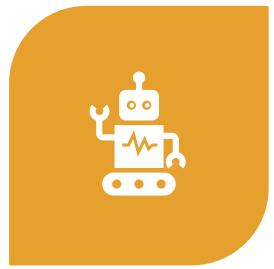
[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

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

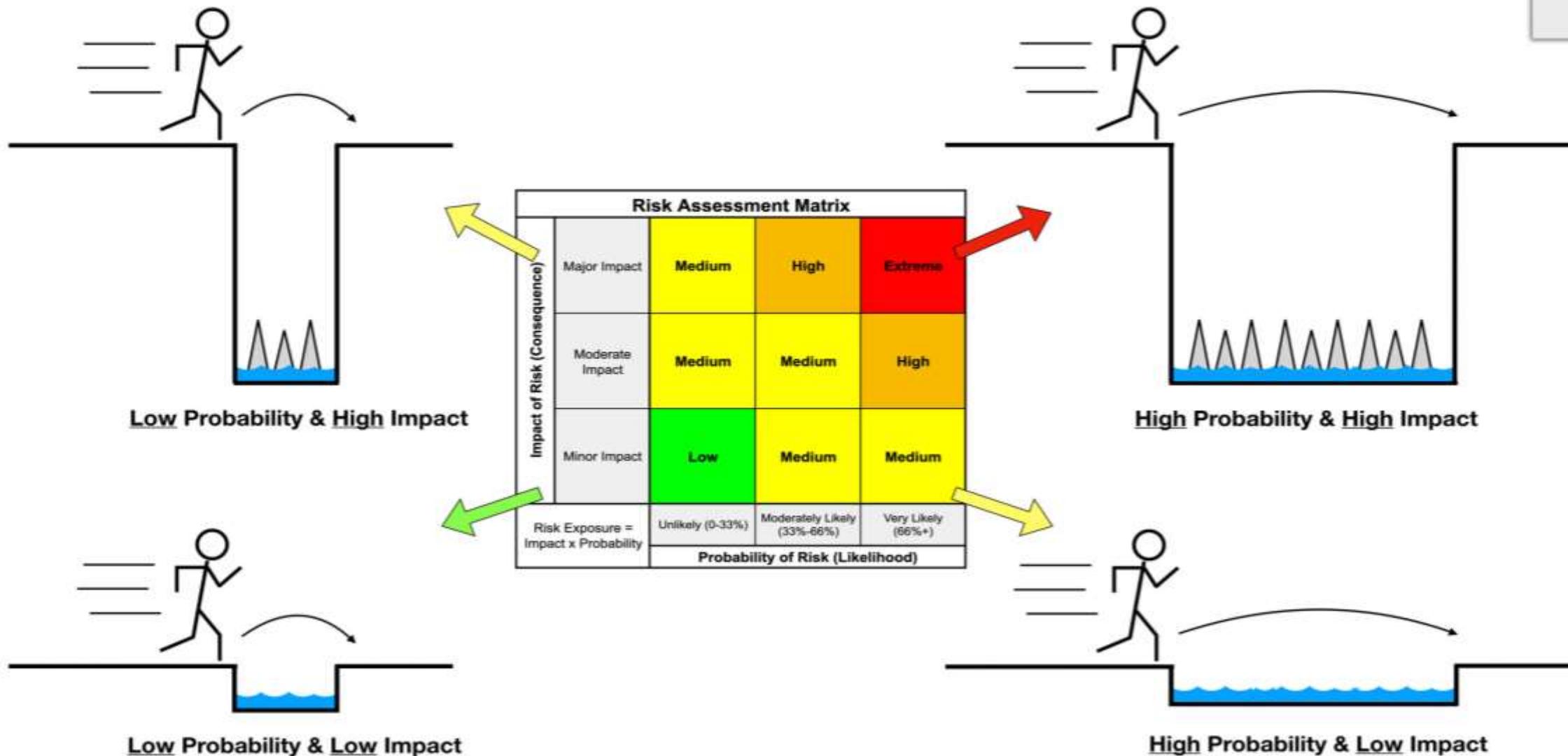
Sinonimi
correntemente
usati

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

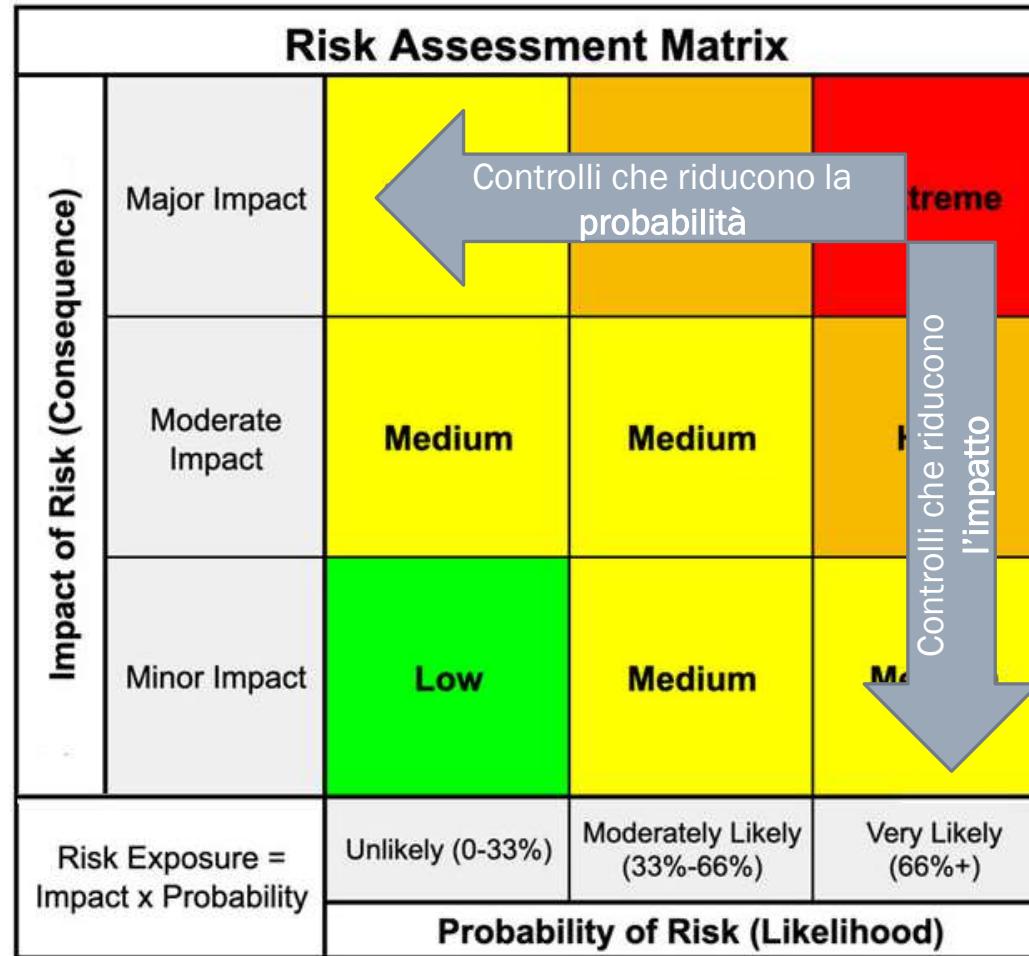
(Severity = Likelihood x Consequence)



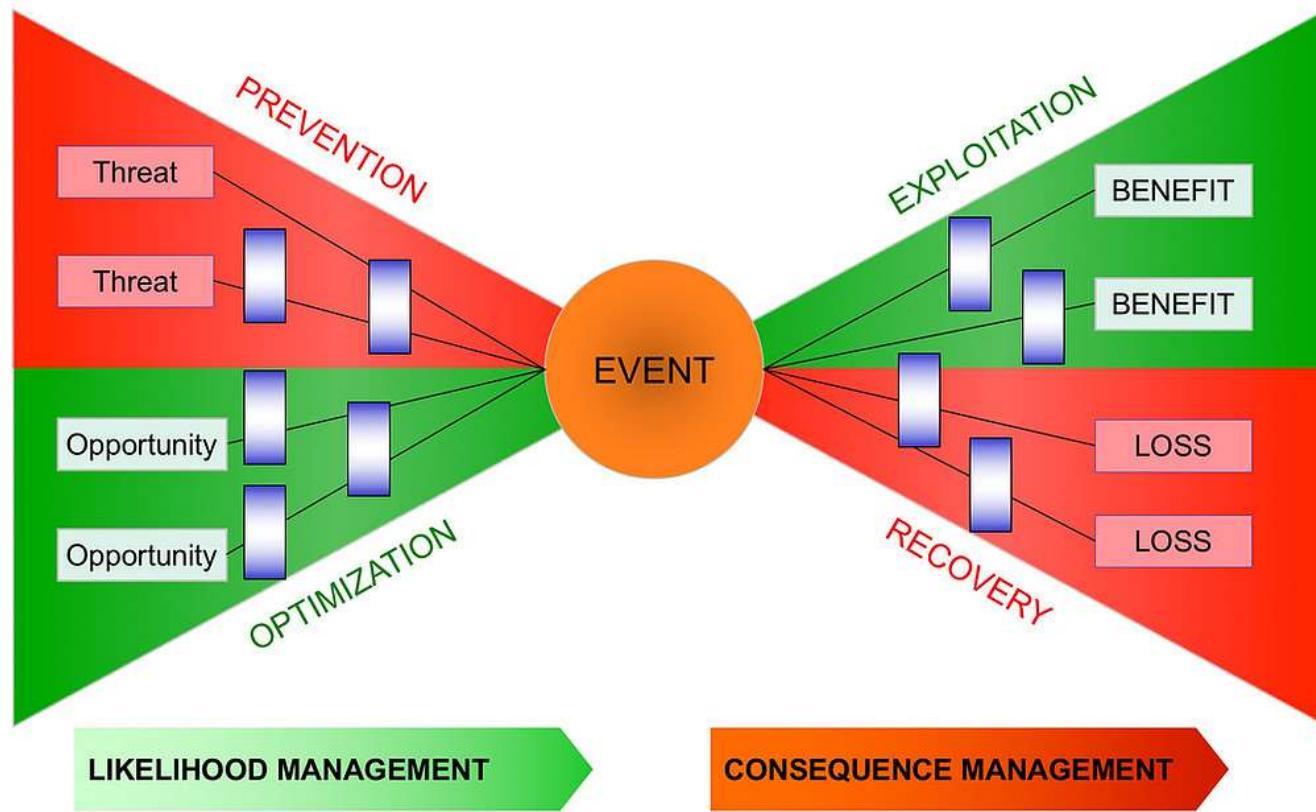
Copyright © 2017-2019 | Mark Warner | TheProjectManagementBlueprint.com

FONTE: <https://www.theprojectmanagementblueprint.com/blog/risk-management/risk-exposure-equals-probability-times-impact>

Tipi di controlli



THREATS AND OPPORTUNITIES



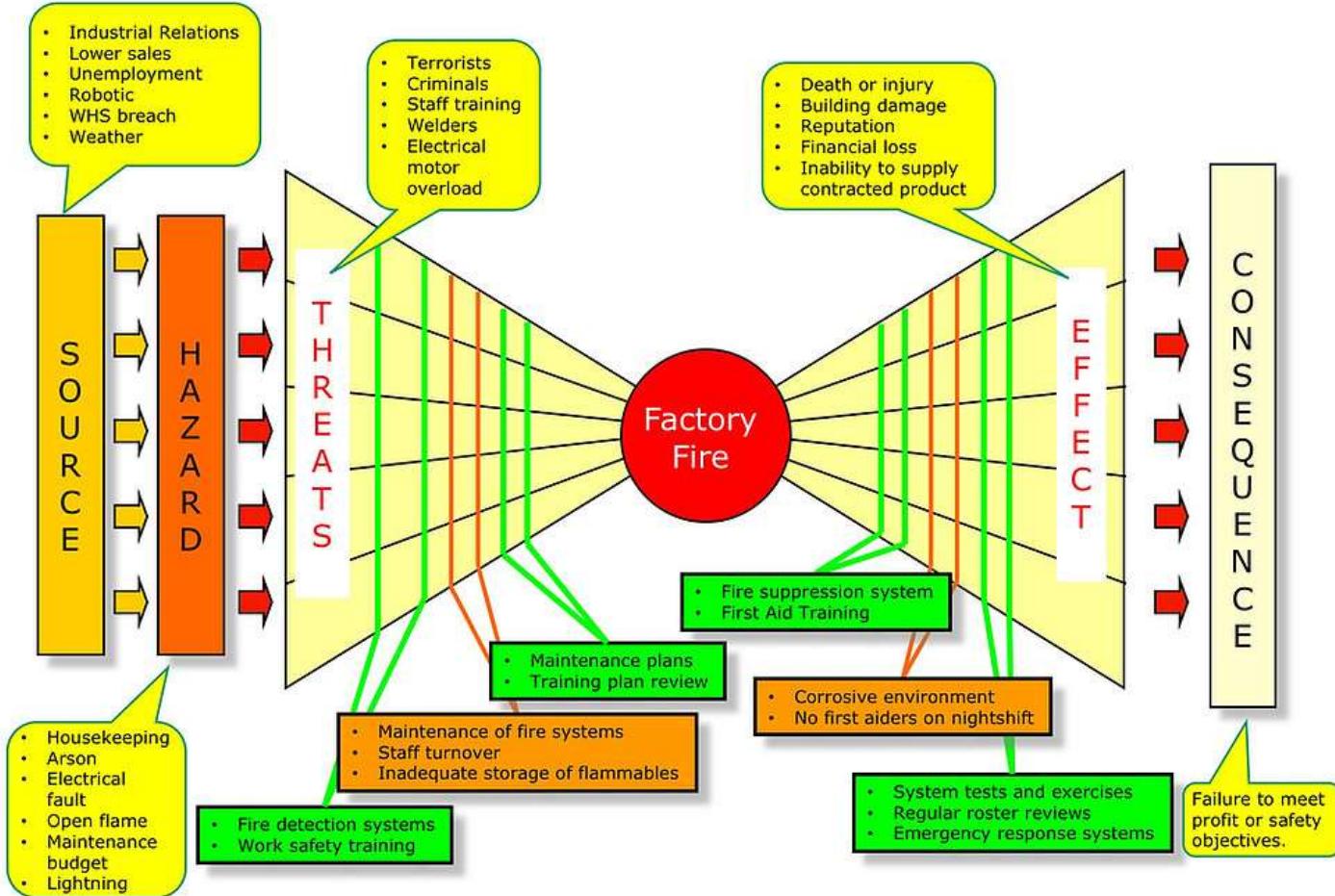
FONTE: <https://www.juliantalbot.com/post/risk-bow-tie-method>



JULIAN TALBOT

HOME BOOKS DOWNLOAD

FACTORY FIRE EXAMPLE



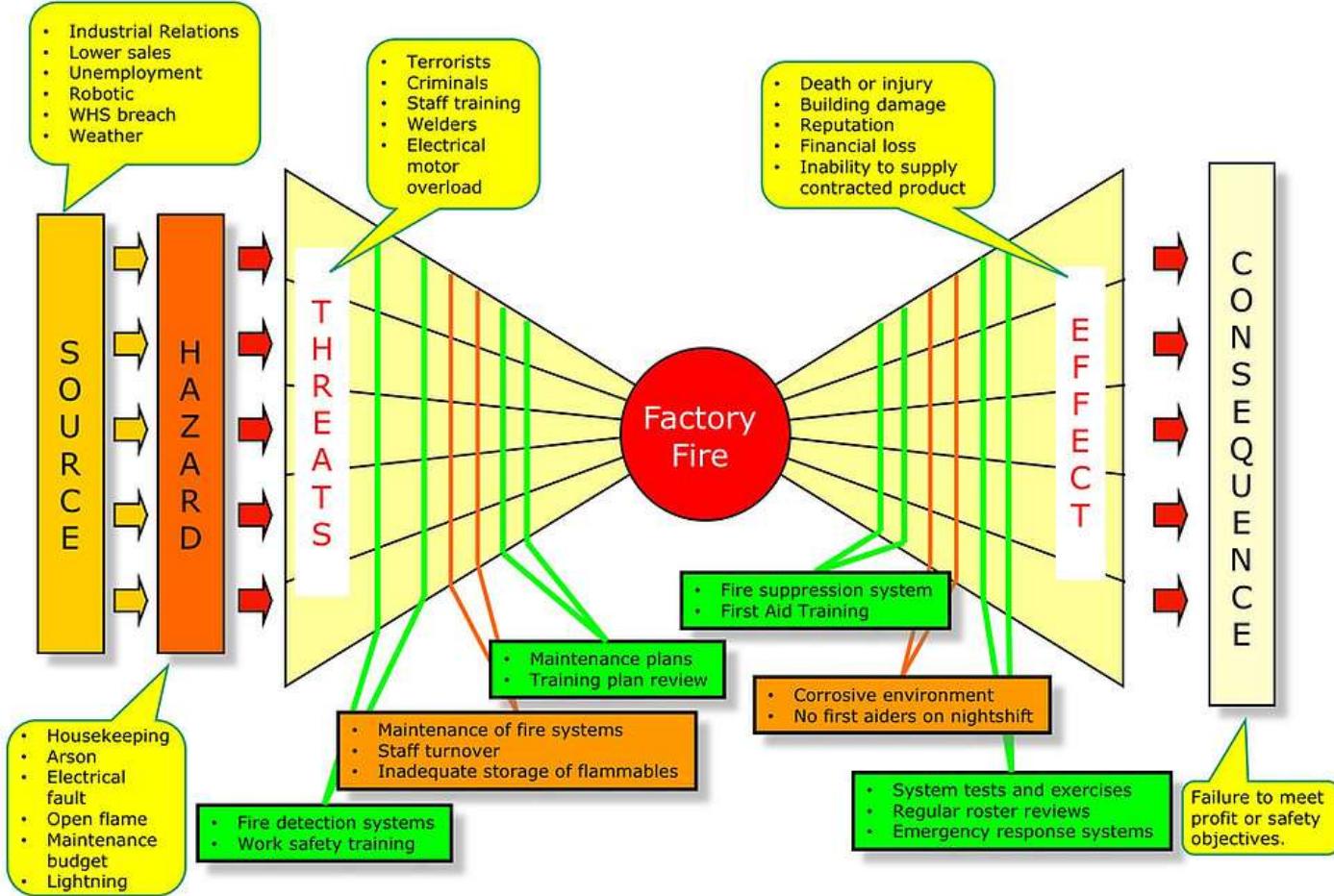
FONTE: <https://www.juliantalbot.com/post/risk-bow-tie-method>



JULIAN TALBOT

HOME BOOKS DOWNLOADS

FACTORY FIRE EXAMPLE



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



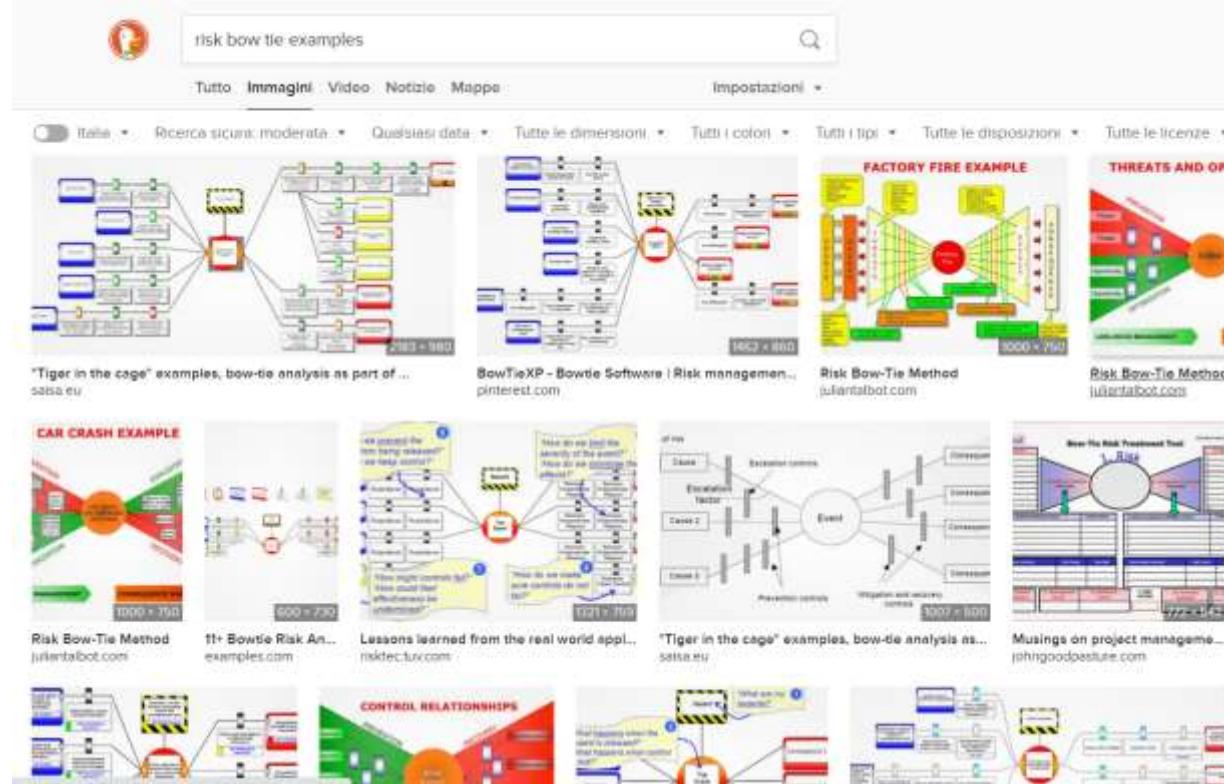
JULIAN TALBOT

HOME BOOKS DOWNLOADS

Un controllo
può
introdurre
altri rischi

Esercizio

<nome dello/degli studente/i>



Link

Motivazioni

Cercare su internet risk bow tie examples (immagini) e scegliere un diagramma interessante da condividere. Fornire il link e spiegare le motivazioni

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

Controlli che agiscono sulla
riservatezza

Controlli che agiscono
sull'integrità

Controlli che agiscono sulla
disponibilità

Esercizio

<nome dello/degli studente/i>

Controllo	Probabilità	Impatto	Tecnici	Organizzativi	Riservatezza	Integrità	Disponibilità
1							
2							
3							
4							
5							
6							
7							
8							

Nominare 8 controlli e classificarli (Y / null) per tipo (assegnazioni multiple sono possibili)

Argomenti

Il Framework Nazionale per la Cybersecurity e la Data Protection



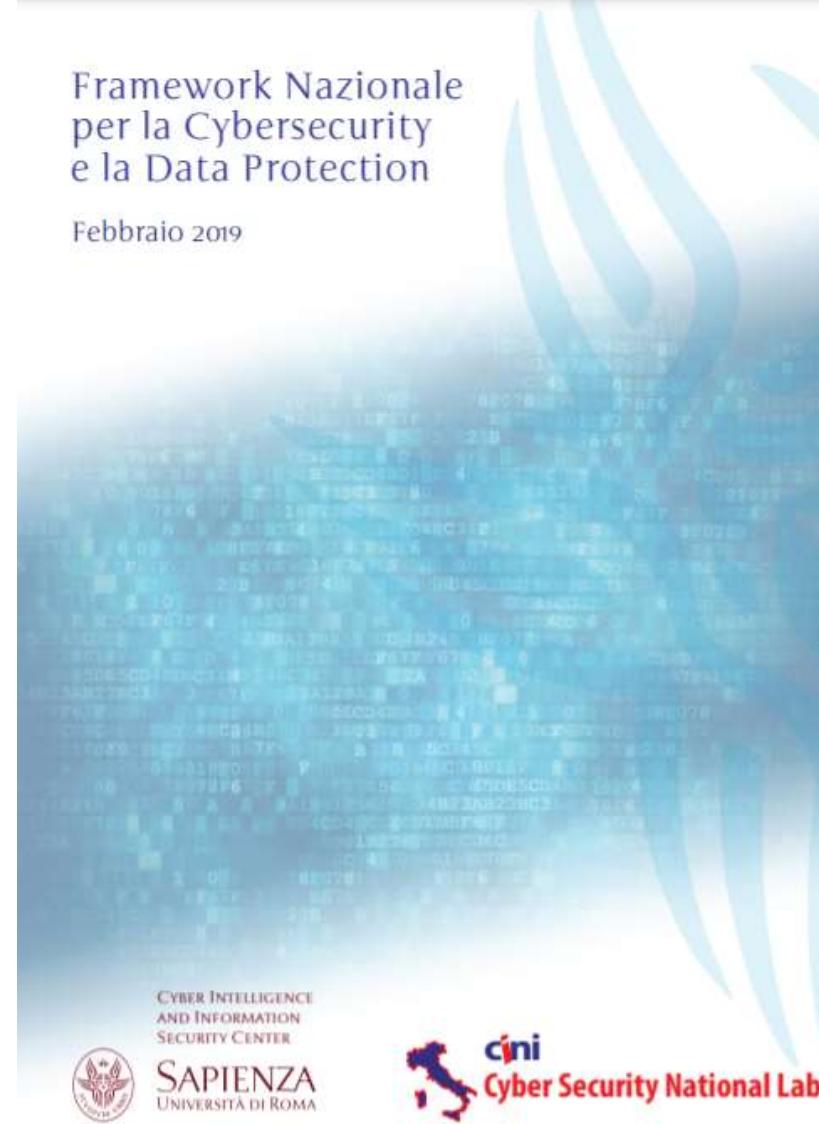
[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Framework Nazionale per la Cybersecurity e la Data Protection

<https://www.cybersecurityframework.it/>

Framework Nazionale
per la Cybersecurity
e la Data Protection

Febbraio 2019



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

Esercizio

<nome dello/degli studente/i>

Descrivere il framework nazionale di cybersecurity

Esercizio

<nome dello/degli studente/i>

Spiegare alcuni dei controlli del framework nazionale di cybersecurity

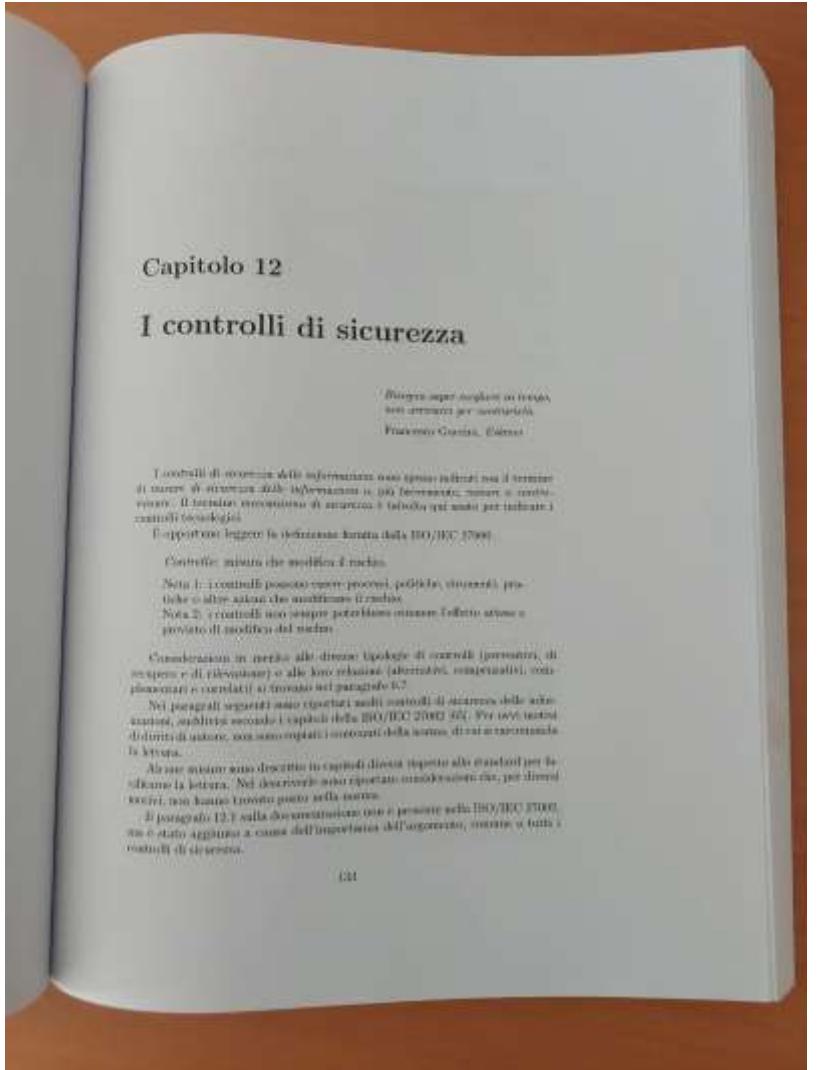
Argomenti

I controlli di Cesare



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Seguiamo il capitolo 12 del libro di Cesare Gallotti



12.1 Documenti

Politiche, procedure, registrazioni

Come scrivere, approvare e distribuire i documenti

Come archiviare le registrazioni

Tempi di conservazione

Verifica e manutenzione

Documenti di origine esterna

12.2 Politiche di sicurezza delle informazioni

Politica = policy (regole, principi o norme)

Politica generale (politica per la sicurezza delle informazioni)

Politiche di dettaglio (es. politica sull'antivirus)

12.3 Organizzazione per la sicurezza delle informazioni

Direzione

Governance e management

Responsabile della sicurezza

Altri ruoli

Coordinamento

Gestione dei progetti

Separazione dei ruoli

Rapporti con le autorità

12.4 Gestione del personale

Inserimento del personale

Competenze

Consapevolezza e sensibilizzazione

Lavoro fuori sede

12.5 Gestione degli asset

Informazioni (classificazione, etichettatura, trattamento)

Identificazione e censimento

12.6 Controllo accessi

Credenziali (principi: identificazione, autenticazione; password; consegna delle credenziali; istruzioni agli utenti; affidabilità degli strumenti biometrici; smart card; strumenti e credenziali condivise)

Autorizzazioni (principi: minimum privilege, need to know, segregation of duties; assegnazione e ritiro delle autorizzazioni; riesame delle utenze; chiavi tradizionali; amministratori di sistema; installazione di programmi)

12.7 Crittografia

Algoritmi simmetrici e asimmetrici

Protocolli crittografici

Normativa applicabile alla crittografia

12.8 Sicurezza fisica

Sicurezza della sede

Sicurezza delle apparecchiature

Archivi fisici

12.9 Conduzione dei sistemi informatici

Documentazione

Gestione dei cambiamenti

Malware

Backup

Monitoraggio e logging

Dispositivi portatili e personali

12.10 Sicurezza delle comunicazioni

Servizi autorizzati

Segmentazione della rete

Protezione degli apparati di rete

Scambi di informazioni

12.1.1 Acquisizione, sviluppo e manutenzione

Sistemi operativi, apparecchiature, appliance, programmi di amministrazione e supporto, meccanismi di sicurezza, programmi per le attività degli utenti, software e librerie, free and open source, pacchetti commerciali

12.12 Gestione fornitori

Tipi di fornitori, processo, requisiti di fornitura

Accordi e contratti

Selezione dei fornitori

Monitoraggio dei fornitori

Due parole sul cloud

12.13 Gestione degli incidenti

Processo di gestione degli incidenti

Controllo delle vulnerabilità

Gestione dei problemi

Gestione delle crisi

Digital forensic

12.14 Continuità operativa

Business Impact Analysis

Valutazione del rischio per la continuità operativa

Obiettivi e strategie di ripristino

Piani di continuità

Test e manutenzione

12.15 Conformità

Normativa vigente

Audit

Vulnerability assessment (e penetration test)

Argomenti

Verticale su Identity and Access Management



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Identity and Access Management Made Simpler

Alessandro Vallega

Consiglio Direttivo Clusit (Associazione Italiana per la Sicurezza Informatica)
Security Business Development, Oracle Europe WCE South
Founder and Chairman of Oracle Community for Security
Founder and Coordinator of EuroPrivacy.info

19 Settembre 2015

In collaborazione con:



*Clusit
Education*

Control complexity, increase productivity

```

jmp start
;*****
;* Program to read in two    *
;* numbers and add them    *
;* and print out the result *
;*****
        number db 7 dup(0)           ; string which will store input and output
        n1     dw 0                  ; two input variables
        n2     dw 0
        res    dw 0                  ; one output variable
        cr     dw 13,10,"$"
start:
        mov dx,offset number
        mov bx,dx
        mov b[bx],5                 ; maximum 5 characters to read
        mov ah,0ah
        int 21h                     ; read in a string from keyboard
        mov bx,offset number +1
        mov cx,00
        mov cl,[bx]                 ; cl now contains number of digits
        mov ax,00                   ; ax will contain the number input
usedigit:
        inc bx                      ; get next digit
        shl ax,1                   ; multiply by 10 using 2 shift ops and an add.
        mov dx,ax                  ; ... x*8 + x*2 = x*10 is the principle.
        shl ax,2
        add ax,dx
        mov dx,00
        mov dl,[bx]
        sub dx,48
        add ax,dx
loop usedigit
        cmp n1,00
        jnz second
        mov n1,ax
        jmp start
second:
        mov n2,ax
print_cr:
        mov ah,09
        mov dx,offset cr
        int 21h                     ; print out a carriage return character
addnos:
        mov ax,n1
        ; move numbers to registers

```

Control complexity, increase productivity

```

jmp start
;*****
;* Program to read in two    *
;* numbers and add them    *
;* and print out the result *
;*****
number db 7 dup(0)           ; 8
n1    dw 0                   ; two input variables
n2    dw 0
res   dw 0                   ; one output variable
cr    db 10,13,10,13          ; return, line feed

start
mov ax, 0
mov bx, 0
mov cx, 0
mov dx, 0
mov si, 0
mov di, 0
mov ah, 09h
mov offset cr, dx
int 21h
add n1, n2
add res, n1
mov dx, offset res
int 21h

```

CUT AND PASTE

and output

MODERN LANGUAGES

```

protected Object mapRow(ResultSet rs, int rowNum, Object[] parameters, Map context) throws SQLException {
    Customer customer = new Customer();
    customer.setId(rs.getLong("id"));
    customer.setFirstName(rs.getString("last_name"));
    customer.setLastName(rs.getString("first_name"));
    customer.setLastLogin(rs.getDate("last_login"));
    if (rs.wasNull()) customer.setLastLogin(null);
    if (context != null) {
        if (context.containsKey(LAST_LOGIN_DATE)) customer.setLastLogin((Date) context.get("lastLogin"));
    }
    return customer;
}

```

FUNCTIONAL SPECIALIZATION

- database management system
- business intelligence
- workflow management system
- service oriented architecture
- identity and access management
- database security
- etc.

```

loop usedigit
cmp n1,00
jnz second
mov n1,ax
jmp start
second:
mov n2,ax
print_cr:
mov ah,09
mov dx,offset cr
int 21h
add n1, n2
add res, n1
mov dx, offset res
int 21h

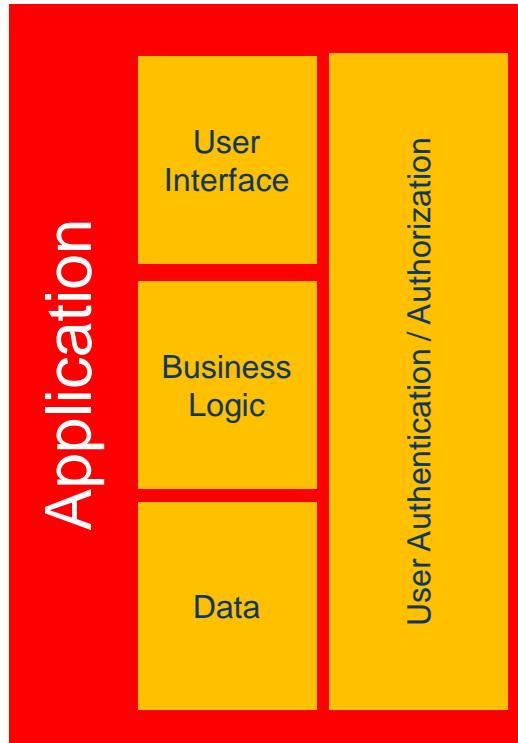
```

Agenda

- Identity Management and Governance
- Directory Services
- Access Management
- Conclusions

IDENTITY MANAGEMENT AND GOVERNANCE

IT systems have a long history



- Years ago each application, for example the Payroll, had its own:
 - ◆ User interface (salary increase form),
 - ◆ Business logic (for example algorithm to compute the monthly pay),
 - ◆ Data (salary table) and
 - ◆ **User authentication and authorization mechanisms**
- ... mixed and merged in the application itself

What is authentication and authorization

- Authentication “is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program”
 - ◆ Think to “user and password”
- Authorization “is the function of specifying access rights to resources”
 - ◆ Think to the fact that your HR manager can look at your salary but your colleagues not.
 - ◆ The sales manager can update only the forecast related to the customers of her group

Auth and AuthZ were embedded in the Application

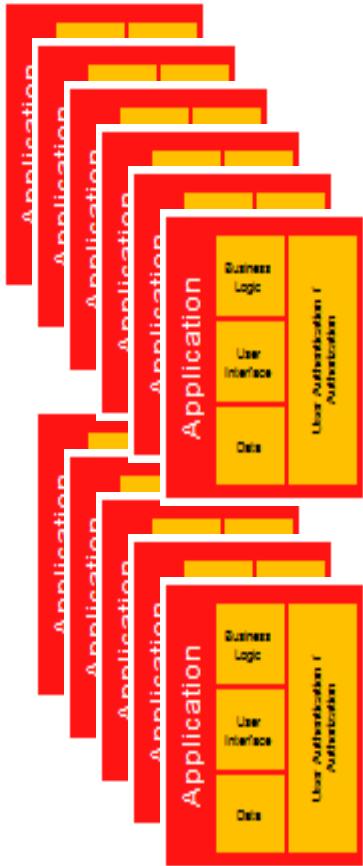
- It simply worked!
And up to a certain point it still does
- Each application store user and password in custom tables
- And also user authorization attributes (what he can do; his privileges)

AUTHENTICATION (user name and password)

AUTHORIZATION ATTRIBUTES (for example which menu item the user has)

Responsibility	Application	Description	Security Group	From	To
XMLP_ADMIN	Payables		Standard	27-FEB-2012	
XMLP_DEVELOPER	Payables		Standard	27-FEB-2012	
XMLP_SCHEDULER	Payables		Standard	27-FEB-2012	
XMLP_ANALYZER_EXCEL	Payables		Standard	27-FEB-2012	
XMLP_ANALYZER_ONLINE	Payables		Standard	27-FEB-2012	

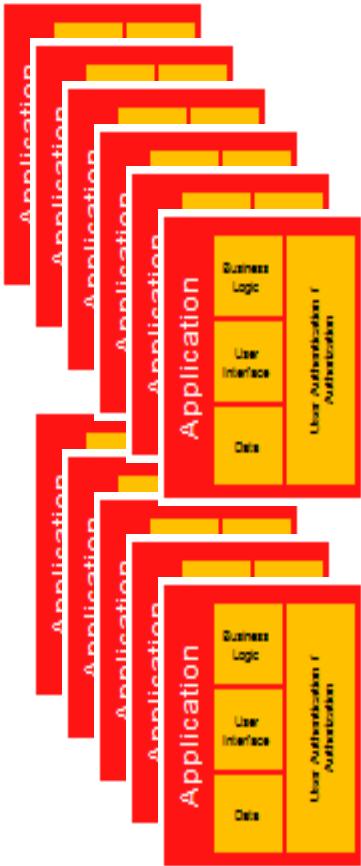
But Applications are not alone



- Real companies have tens of applications, each one with its own user and password tables



But Applications are not alone



- When a new employee join the company somebody in the company must create some records in the all application authentication and authorization tables
 - ◆ Normally it's the hep desk or the application management team that receive a phone call from his manager or a ticket in a the "ticketing" application
- And when an employee leave the company somebody must do the reverse
- And the same when a user change the role and his authorizations

But Applications are not alone



Security problem

- When a new employee join the company somebody in the company must create some records in the all application authentication and authorization tables
- Normally it's the help desk or the application management team that receive a phone call from his manager or a ticket in the “ticketing” application
- And when an employee leave the company somebody must do the reverse
- And the same when a user change the role and his authorizations

Efficiency problem

Both problems

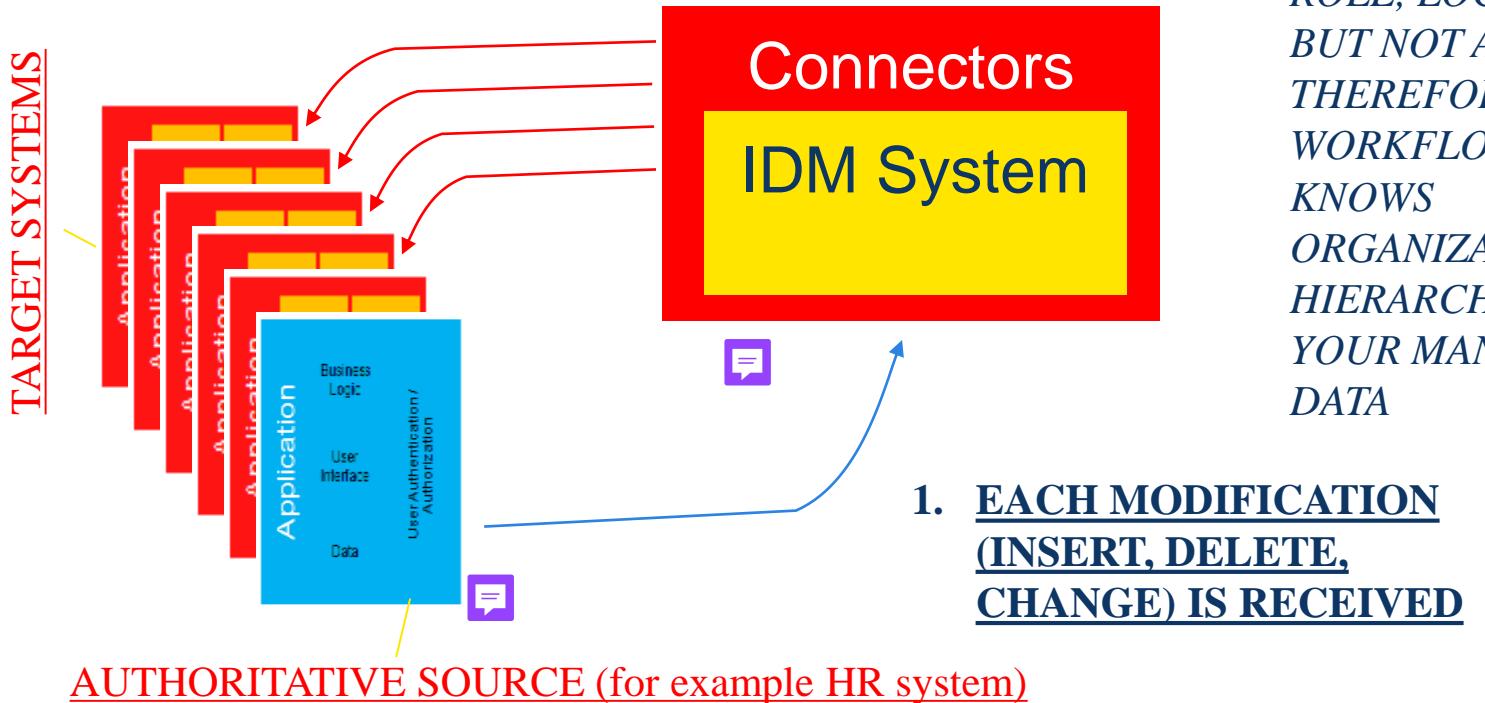
Identity Governance

- Address the problem of creation, deleting and changing the user data in each application
- It works making things automatic, avoid manual work from the help desk and application management teams
- Increase security giving and removing user accounts as soon as needed
- Address the problem of knowing who has (and had) the possibility to access to any application and with what level of privileges (entitlements)
- Support attestation, role mining, separation of duties and auditing
- Respond to Audit and Compliances including PCI-DSS, Privacy, SOX ...

How Identity (De)Provisioning works

*CONNECTORS MAKE THE PROJECT
SIMPLER BECAUSE THEY KNOW THE
TARGET SYSTEMS*

2. AND PROPAGATED IN THE TARGET



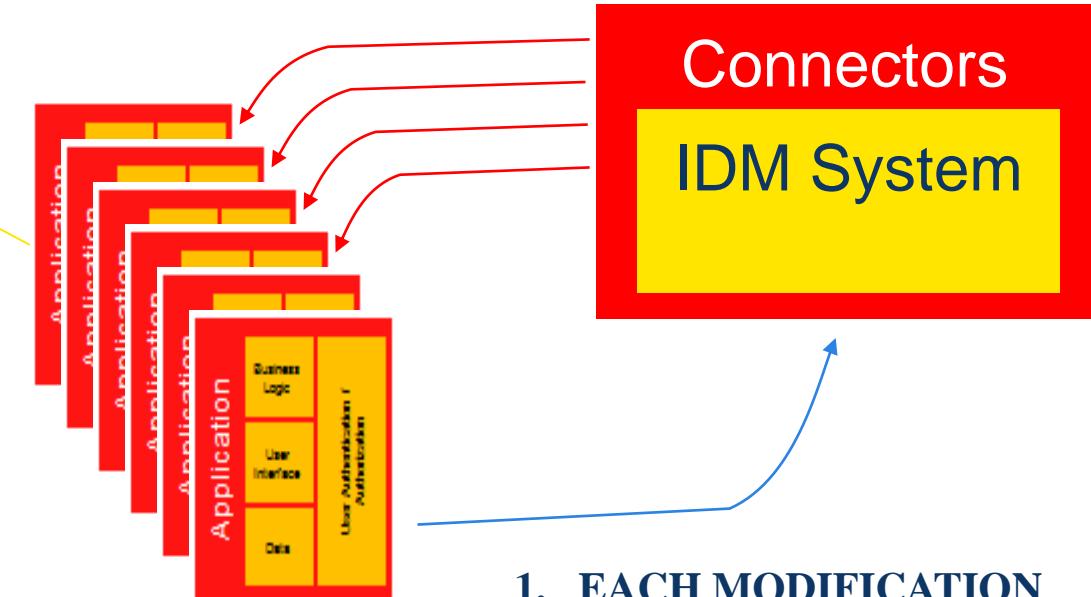
*THE AUTHORITATIVE
SOURCE KNOWS MUCH
(EXAMPLE USER, JOB,
ROLE, LOCATION ETC.)
BUT NOT ALL
THEREFORE IDM HAS
WORKFLOWS AND
KNOWS
ORGANIZATIONAL
HIERARCHY TO ASK TO
YOUR MANAGER EXTRA
DATA*

1. EACH MODIFICATION (INSERT, DELETE, CHANGE) IS RECEIVED

When this works... you

- ... you are enforcing an important **security principle**: everybody has no more privileges than he needs

2. AND PROPAGATED IN THE TARGET



1. EACH MODIFICATION (INSERT, DELETE, CHANGE) IS RECEIVED

Good Principles for Security and Compliance

- **Principle of least privilege** means giving a user account only those privileges which are essential to that user's work. For example if you don't have to install software than you cannot install software.

Good Principles for Security and Compliance

- **Separation of duties (SoD)** is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task (for example approve an invoice and pay) is an internal control intended to prevent fraud and error.

Good Principles in the reality

- In any medium to large company with hundreds of users, tens of applications and databases, many different privileges per each application and so on, is practically impossible to manually enforce the least privilege and separation of duties principles.

Good Principles in the reality

- Traditional approaches uses excel spreadsheets and manual entry ... A big matrix with one line per person, one column per application and some text in the cells to document accessibility.
- These excel are prone to errors, long to be produced and ineffective when used.

Application / Users

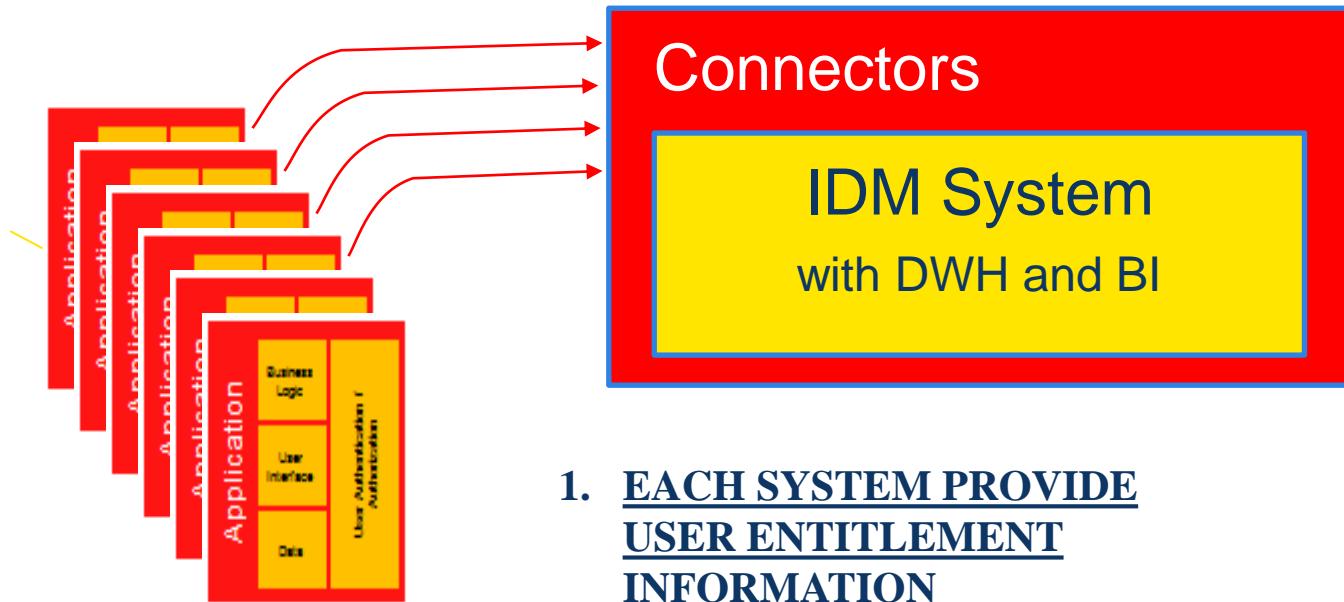
	MORETTI - 10926	BARBIERI - 10651	FONTANA - 10629	SANTORO - 10429	MARIANI - 10066	RINALDI - 10066	COSTA - 10066
SAP x34 Talamona	Buyer-Direct Material	Head Buyer	No	No	No	Buyer-Direct Material & Indirect Talamona	No
eMail MS Server Base	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Oracle HRMS Self Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HRMS Manager Self Service	No	Yes	No	No	No	Yes	No
Siebel	No	No	No	No	No	No	Yes (Manager)
Ticketing (Remedy)	No	Approver	No	Base User	Admin	No	No
Administrator	No	No	No	No	No	No	No



The other way around...

Make automatic data collection

2. THE CONNECTORS WORK THE OTHER WAY AROUND



THE ANALYTIC COMPONENT PROVIDE ALL INFORMATION (FOR REPORTING AND DECISIONS) RELATED TO USERS AND THEIR ENTITLEMENTS

THE INFORMATION DATABASE IS AN EXTENSION AND INTEGRATED WITH IDM

Identity analytics to control complexity

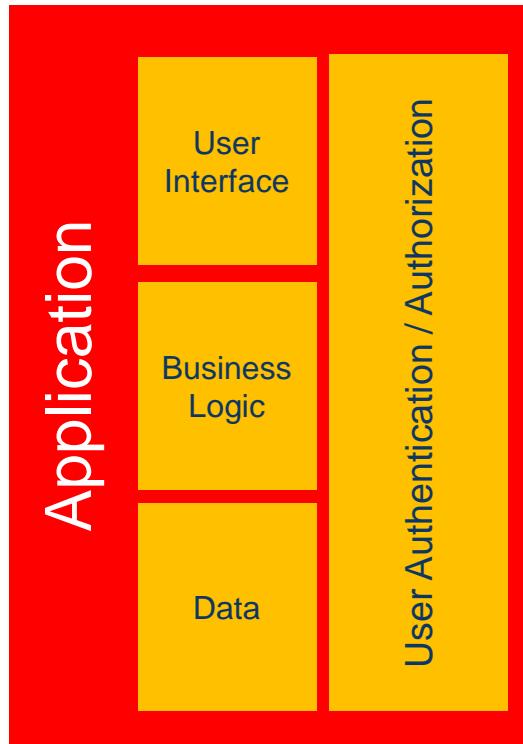
- Identity warehouse collects all users information
 - ◆ Who
 - ◆ Has / had
 - ◆ Which privilege (entitlements)
 - ◆ In which system / application

Identity analytics enables new processes

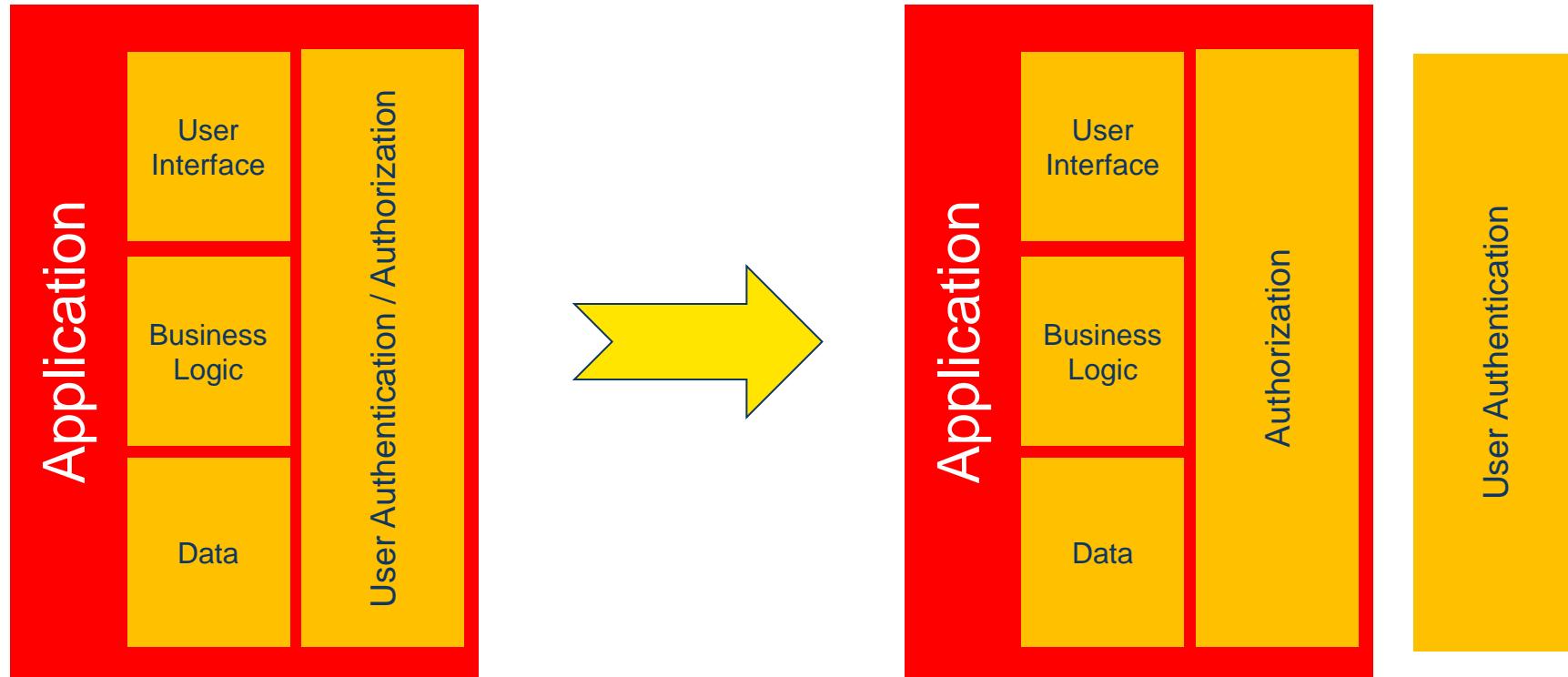
- **Attestation:** the system ask your manager if you have to have a certain privilege
- **Segregation of Duties:** let you define and enforce prohibited combination of entitlements
- **Role Mining:** help you to define IT Roles and connect them to Business Roles and to simplify everything else
- **Auditing:** answer all questions of your auditors

DIRECTORY SERVICES

A more modern approach

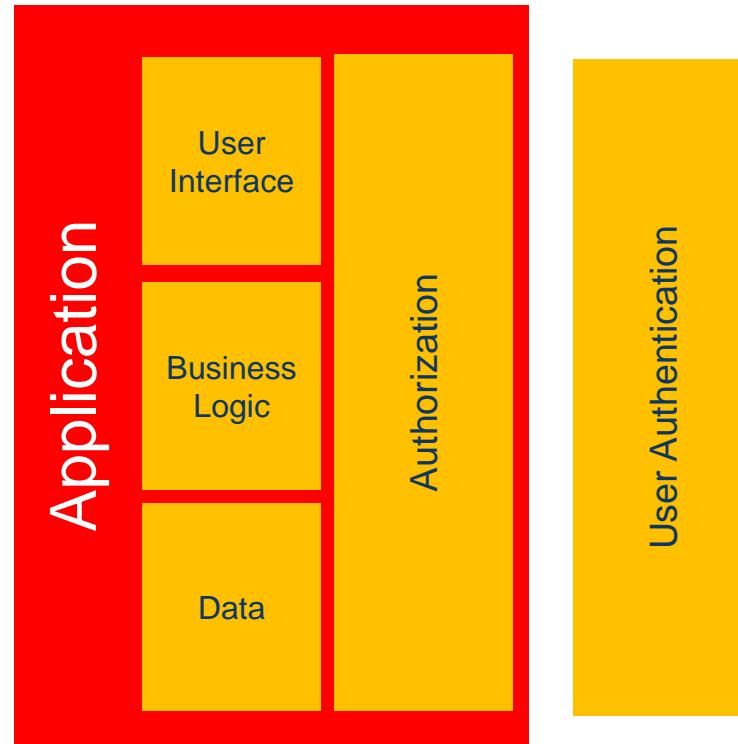


A more modern approach



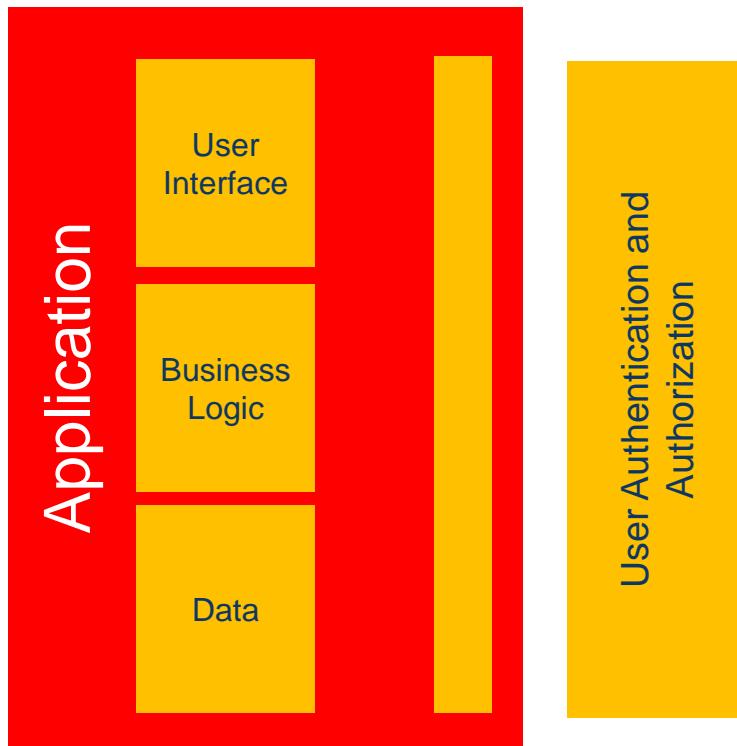
A more modern approach

- Modern applications and packages have the ability to use external authentication
- The application requests to the external authentication system (Directory) if the user is known and if the password is correct.

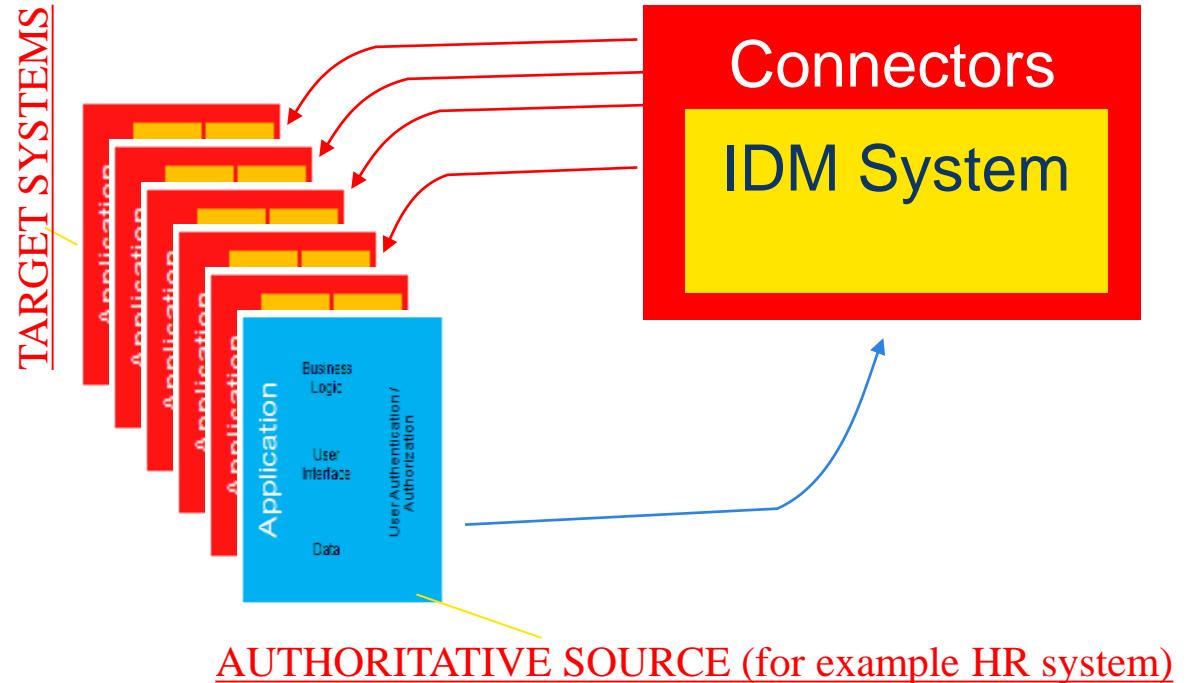


A more modern approach

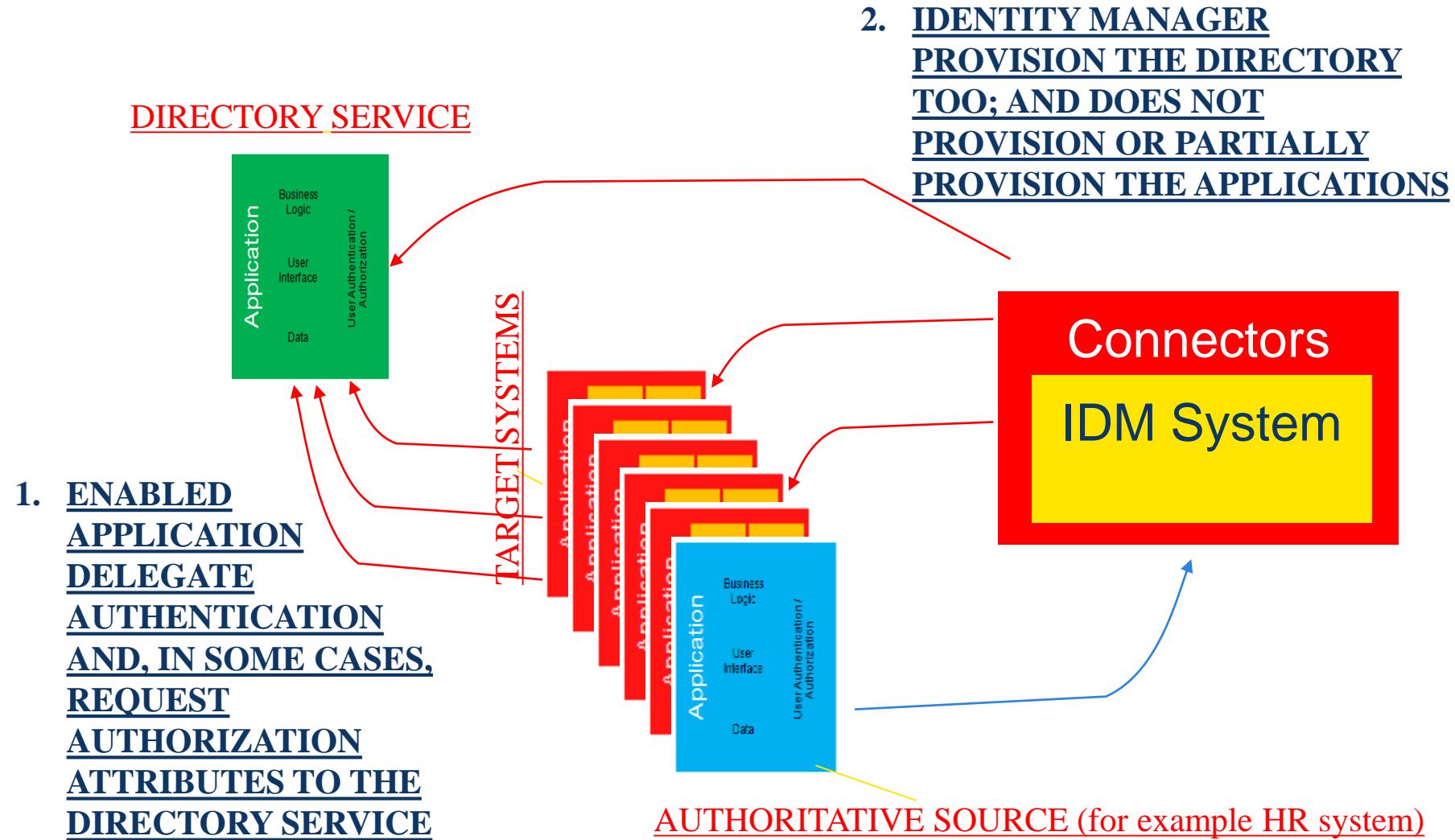
- Sometimes also (some or all) authorization attributes are removed from the application
- The application requests authorization attributes to the Directory
- If all attributes are in the directory the provisioning process has nothing to do but to integrate just one target system: the Directory



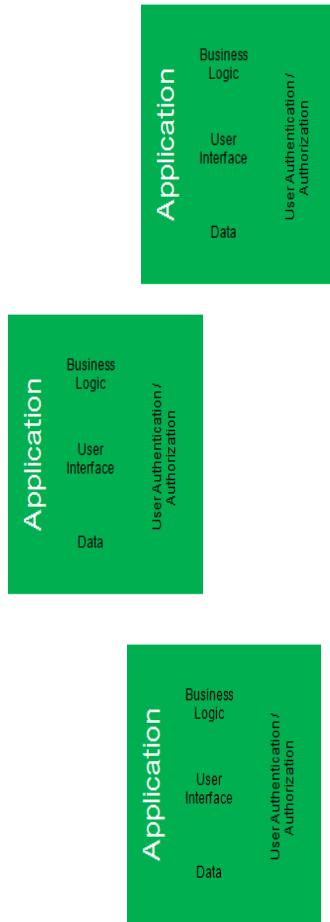
Do you remember this?



The directory is the new component in this architecture

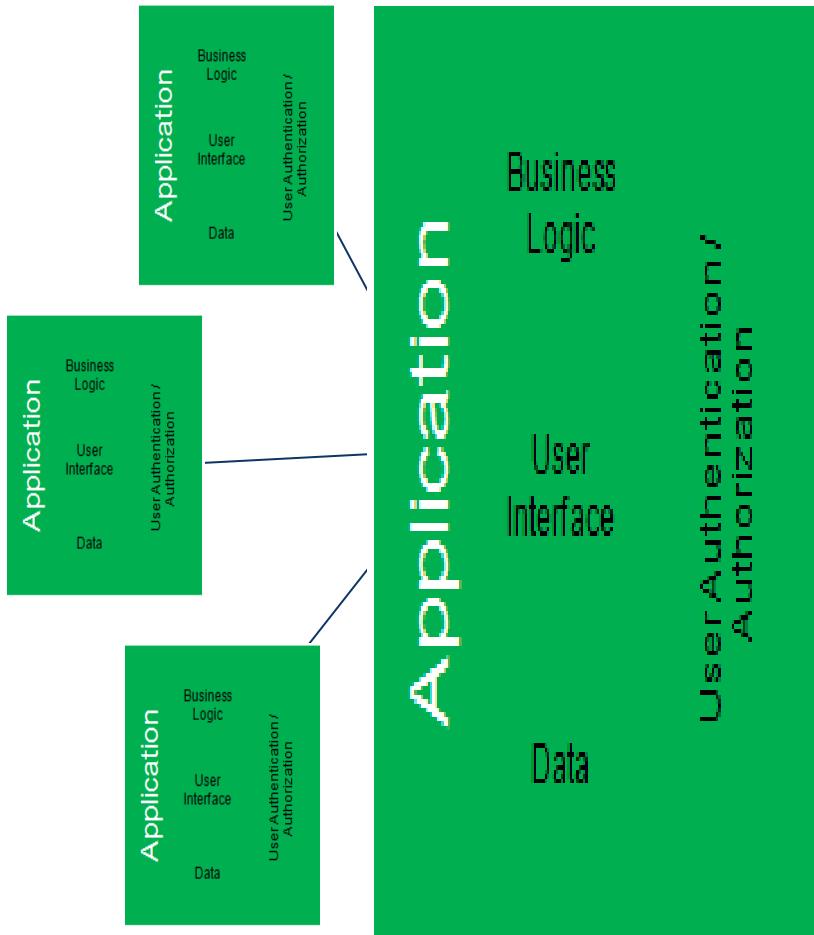


Directories proliferation



- Sometimes IT systems are grown chaotically like companies do. In case of merger and acquisitions, remote plants and opportunistic decisions you may have more directories!
- They also might be heterogeneous solutions mixing different technologies and standards

New challenges for Directory Services



- **Rationalization:** need to have single point of access, identity + data aggregation, and integration with non LDAP systems
- **High Volumes:** B2C companies are extending IT systems to their customers and prospect customers or citizens
- **Fast write:** new services need to write fast in the directory (example geodata for Mobile Apps)

Directory Services

- Directories are a very key component of any IT modernization strategy
- They provide simpler IT infrastructure, more control, efficiency and security
- They work with the identity provisioning to smoothly transition to the future applications

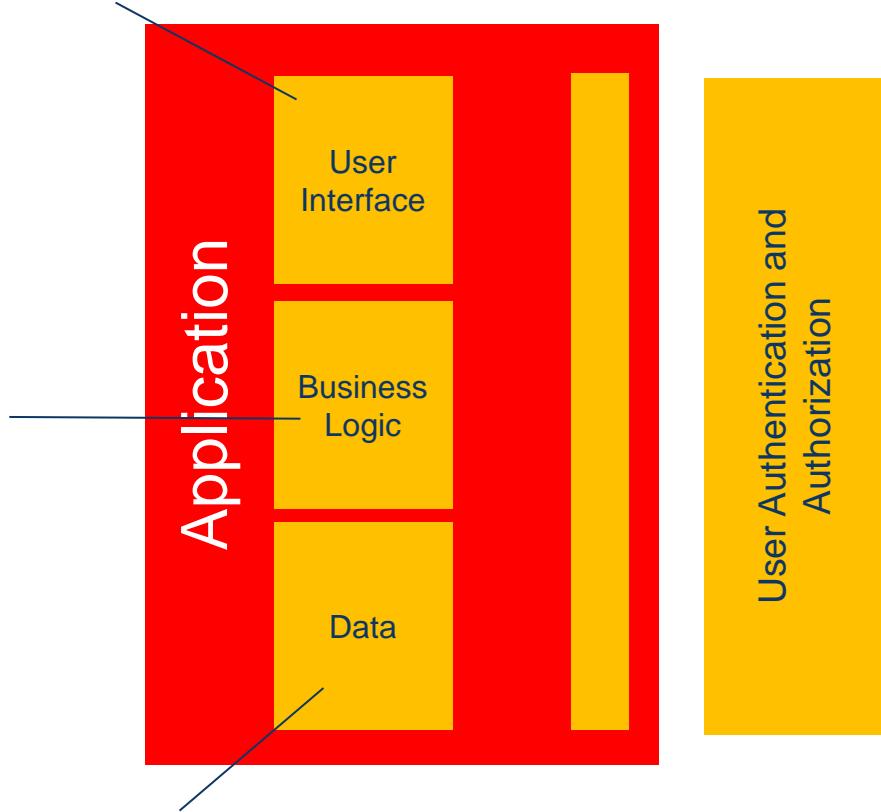
- They support the digital transformation of a company to better engage their (B2C) customers
- They allow the authentication / authorization rationalization for a better security and to reduce costs

ACCESS MANAGEMENT

Nowadays we have the web...

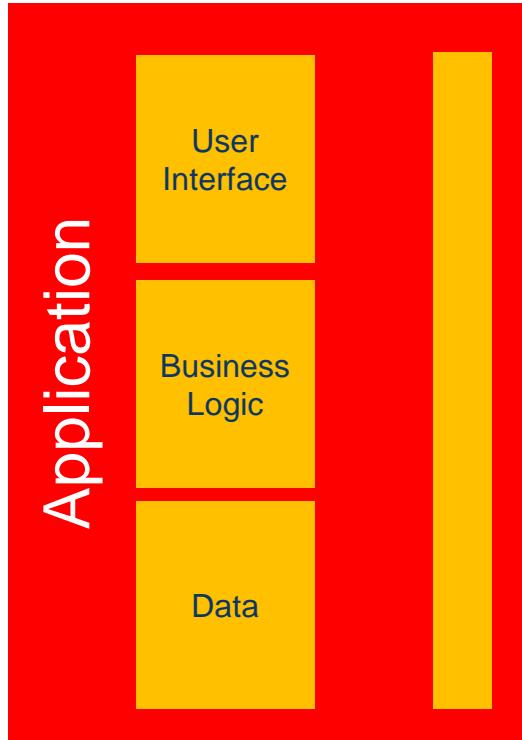
THIS GOES ON THE WEB BROWSER

THIS IN THE
APPLICATION
SERVER



THIS STAYS ON THE DATABASE SERVER

... we cannot control users

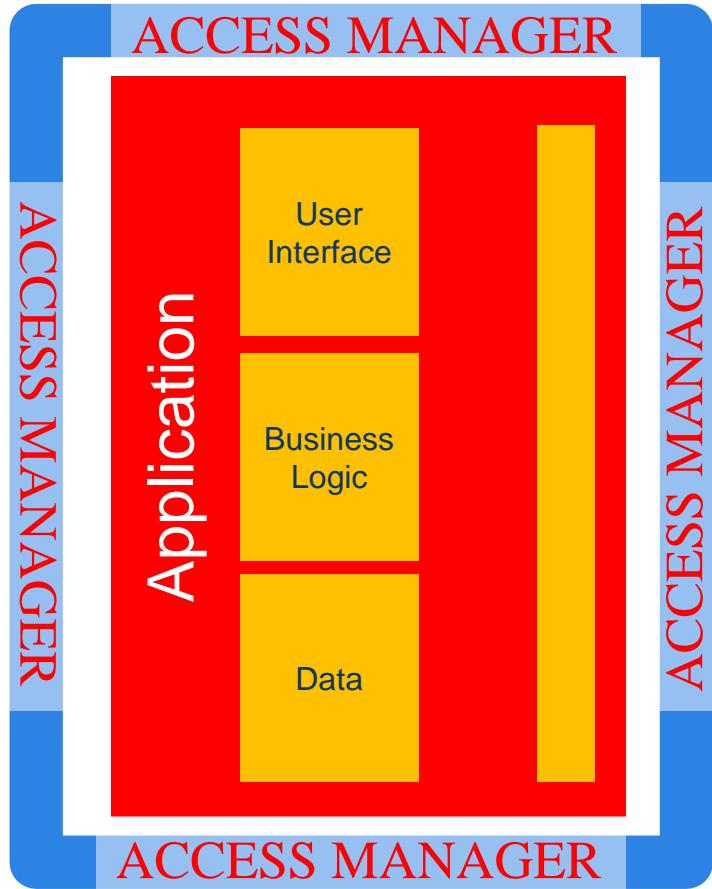


- Users have the browser back-button
- User can save applications URL and jump in the middle of the application days later
- URL often brings parameters with them
- Attackers can tamper URL (parameters) and session cookies....

Web applications must do a lot of things

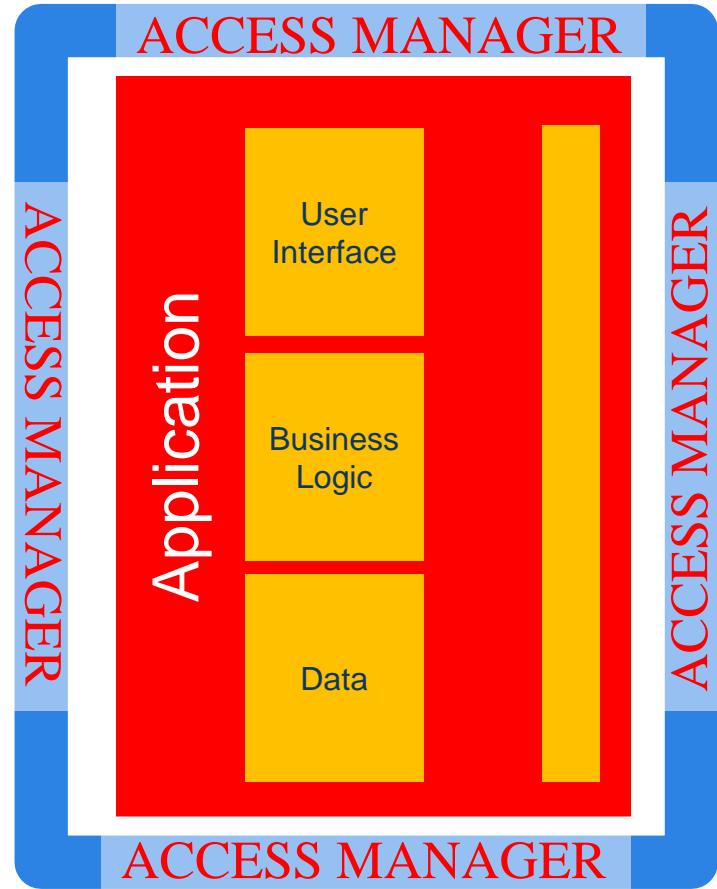
- All web applications must check every **single page** for user authentication and authorization
 - ◆ Is the user authenticated? Is the user authorized?
 - ◆ Is the session cookie still valid?
- The simpler solution is to use middleware: Access Manager

Increase user experience



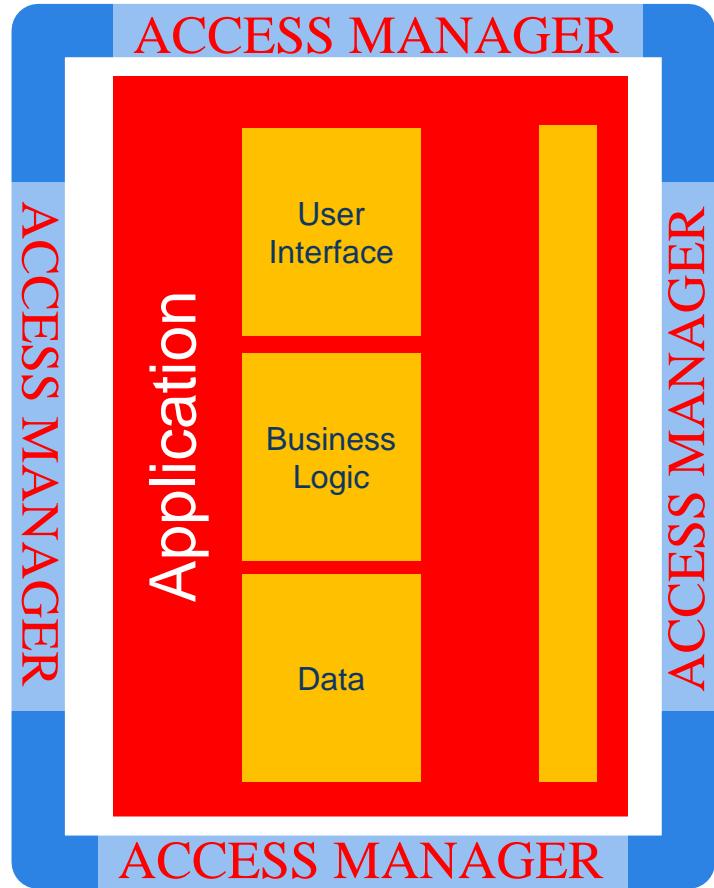
- If the user is authenticated he passes; if not, he is requested to enter his login...
- But then, the transaction continue with the requested resource without breaks, no interruption, reducing abandoned transactions, and a better customer experience

Increase security



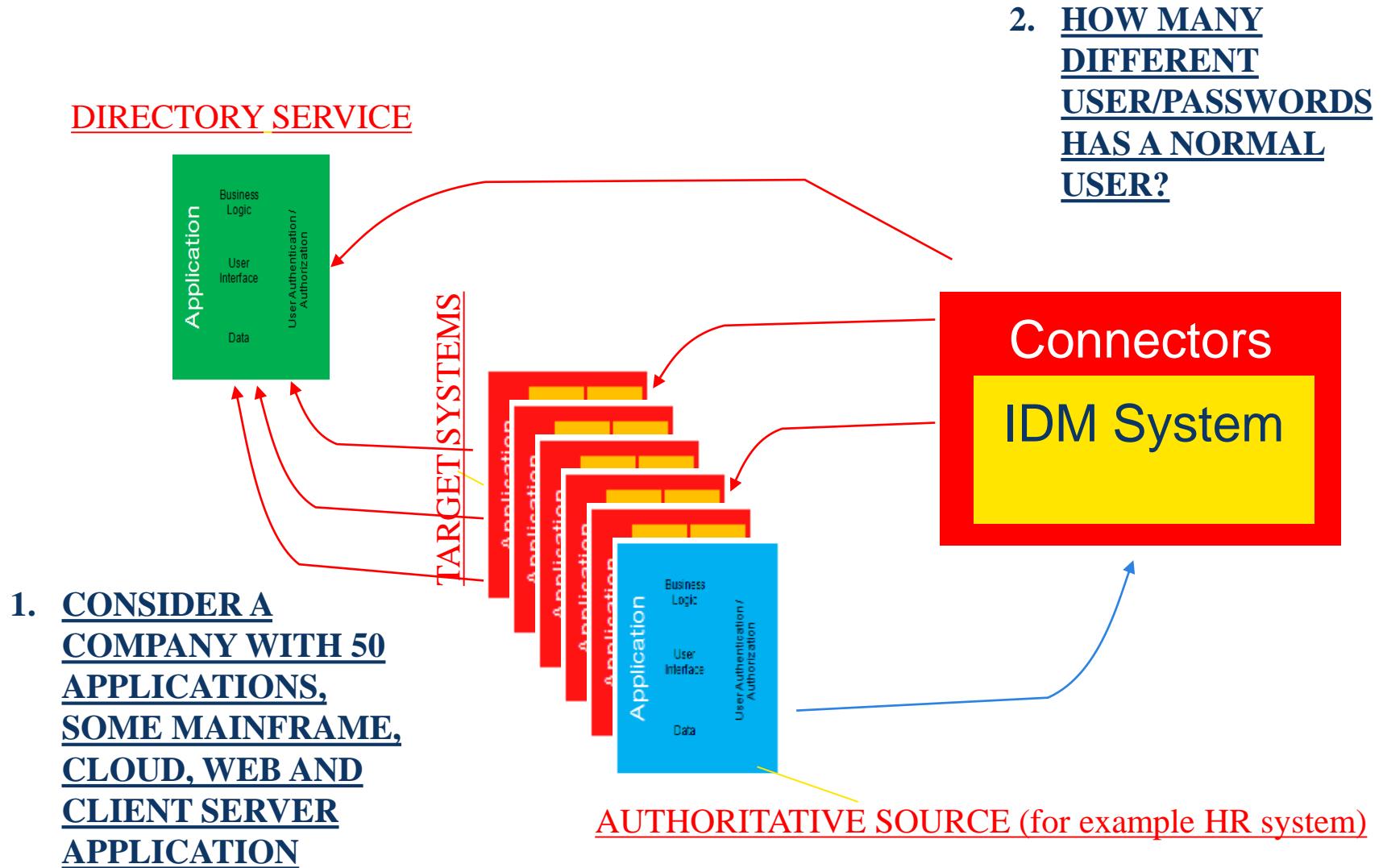
- All web resources (pages) are protected from unauthorized access
- Additional security features are available such as access fraud prevention controls, OTP and strong authentication
- Access logs can provide evidences in case of incidents

Increase productivity



- Out of the box security and user experience features
- Configuration versus development
- Extensible to Mobile, Cloud, Web Services, and Fine Grained Authorization

One final remarks: how many password do you have?



Answer: Many, even more than 20

- It depends on many factors, however it is possible that all web applications share the same authentication mechanism and all other applications have their proper ones.
- Also consider that (some normally old) applications might require multiple user/passwords for a single user if she plays different roles in the process (for example when she is a manager and also a contributor)
- And also consider that a normal user have his own accounts on systems external to the company for personal use...

Passwords and yellow post-it

Severe security problem

How do a person remember >5 passwords?



- **He uses the same password in all systems**
- **He uses simplistic passwords**
- **He never changes the passwords or cyclically reuses the same short set of passwords**

Give them only a single password (directory, federation) or make any trick to let them use only one master password (single sign on)

Access Management

- Addresses the problem of checking user authentication and authorization of cloud, mobile and web applications
- Reduces the programming efforts
- Increases user experience
- Supports “strong” authentication such as OTP (one time password delivered for example via SMS) and biometry
- Extends authentication to external contexts (business partners and cloud)
- Address the problem of knowing who had access to an application in a specific moment
- Enables other important features such as access frauds prevention, single sign on etc.

CONCLUSIONS

Identity and Access Management is:

Technically speaking

- Complex because of the historical evolution of IT
- It is an ineluctable part of our future
- There is still a lot of technical evolution for cloud, mobile, performance, and extended processes
- Better to use platforms

Business speaking

- A key technology to prevent frauds, breaches and security incidents
- Guarantee audit and compliance
- Enables modern business transformations where we need to know the identity of our customers and we have to provide a fantastic and seamless user experience to them

Argomenti

Verticale su Database Security



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

I più comuni errori di gestione di un'infrastruttura database

Lessons learned durante la pratica del DB Security Maturity Evaluation

Alessandro Vallega

Security Business Development Director, Oracle Europe WCE South
Responsabile del Programma DB Security Maturity Evaluation

Consiglio Direttivo Clusit (Associazione Italiana per la Sicurezza Informatica)

Founder and Chairman of Oracle Community for Security

Coordinatore di EuroPrivacy.info

Socio AIEA

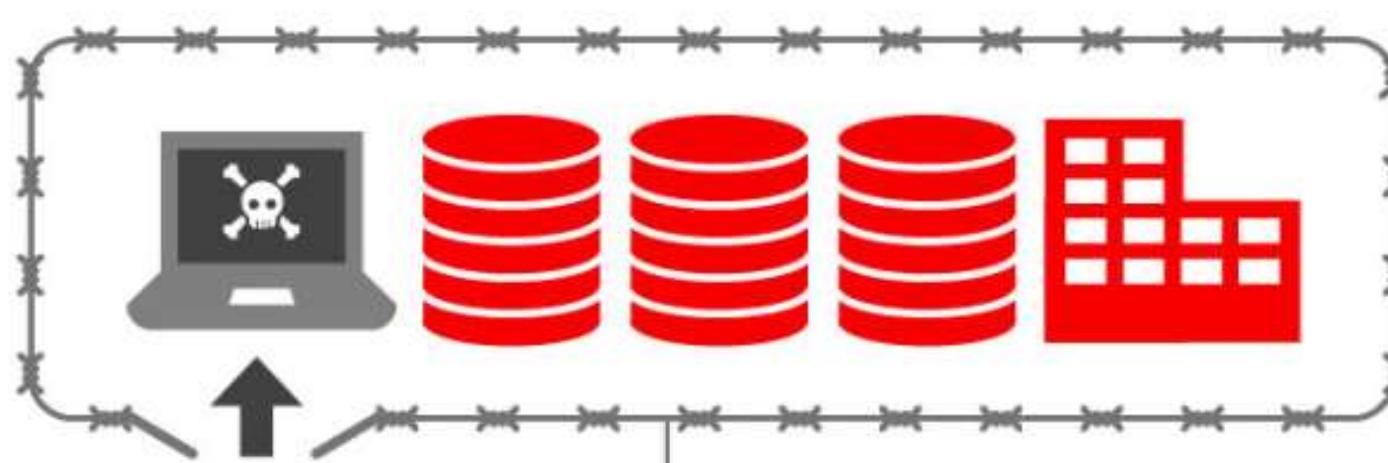
Milano, Dicembre 2015



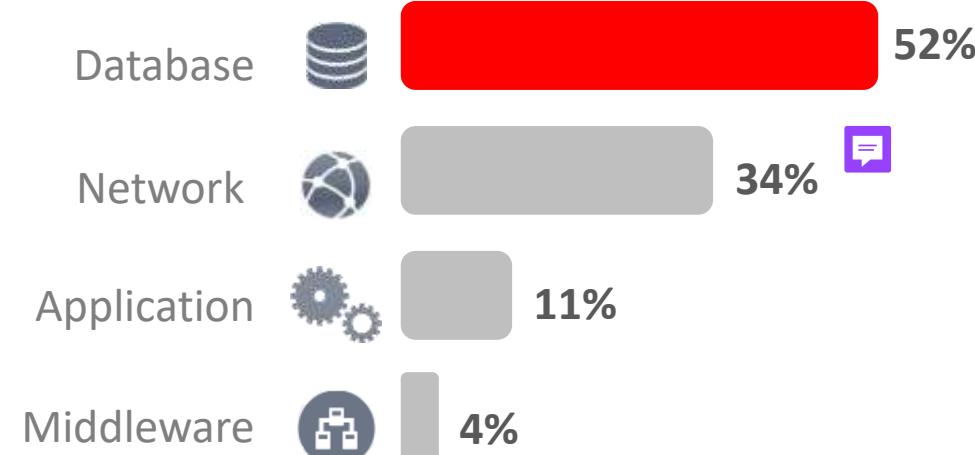
Program Agenda

- 1 ➤ Introduction
- 2 ➤ Most Common Mistakes in DB Management
- 3 ➤ Conclusion

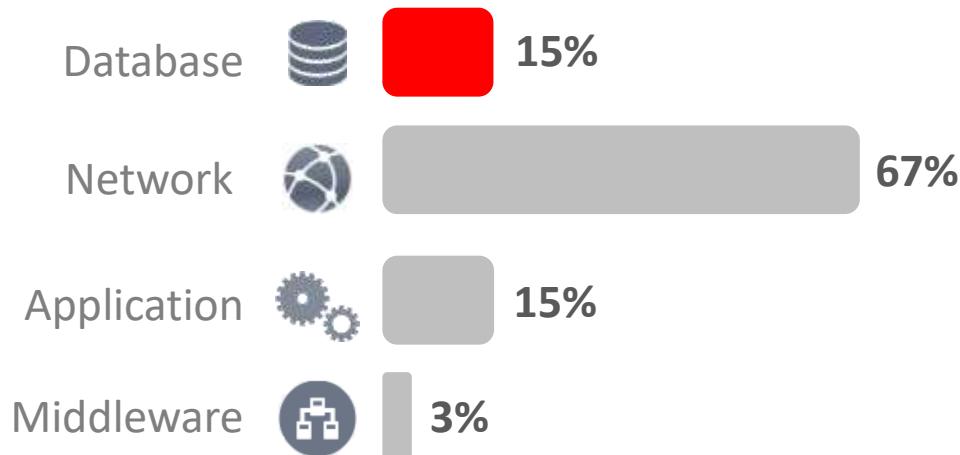
Introduction



IT Layers Most Vulnerable To Attacks



Allocation of Resources To Secure IT Layer



Source: CSO Online MarketPulse, 2013

What are the
consequences in
practice?

I can share our
direct
experience...

Security Maturity Evaluation



Oracle Europe best practice

Executed at 30+ Oracle largest customers in all sectors:

- Banks
- Insurances
- Telco
- Oil and Gas
- Utilities
- Hospitals
- Public Sector
- Defense



Our tool is your people!

Database Security Maturity Knowledge Areas

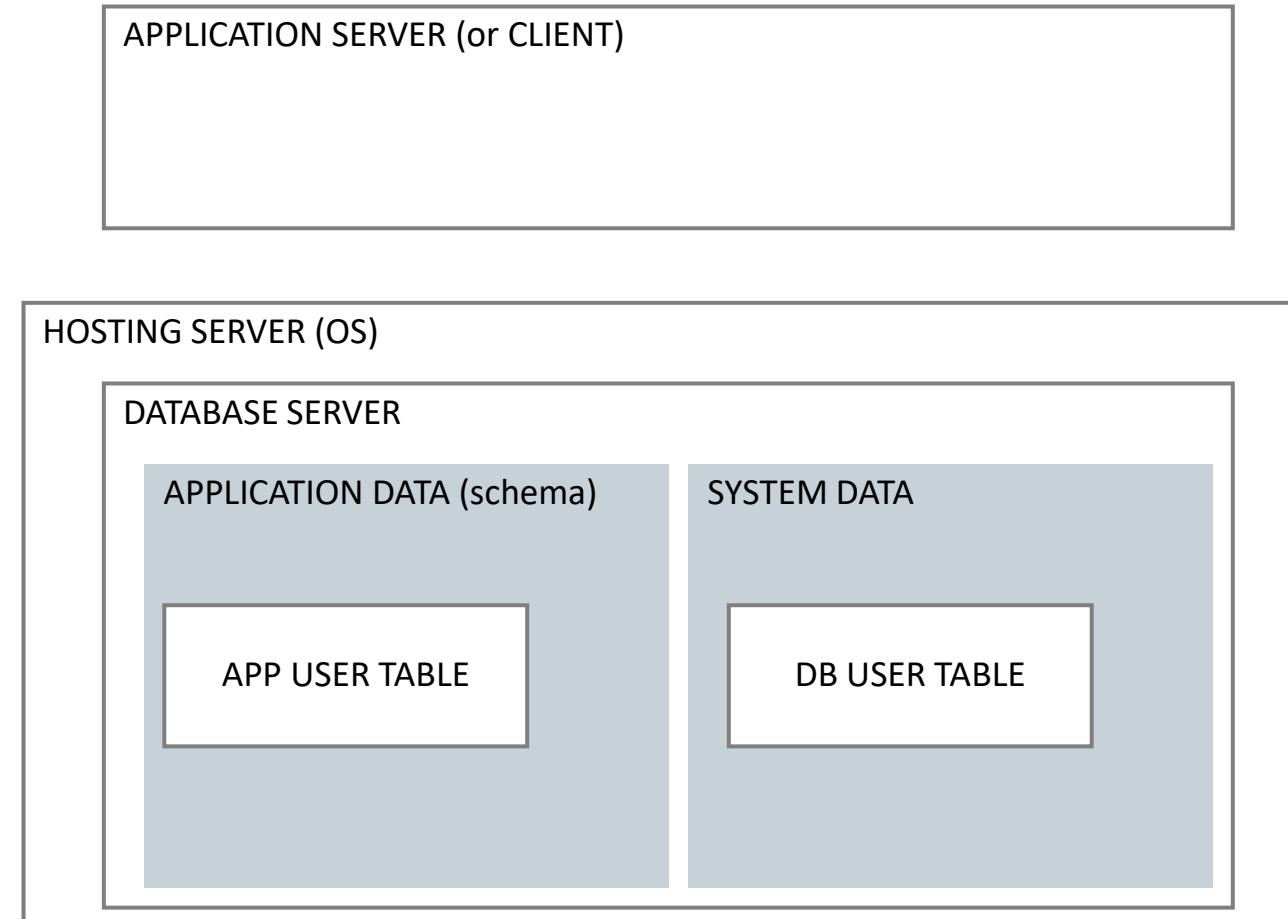
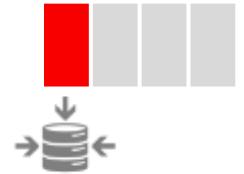
DB Security	DB Access Control	Monitoring / Blocking and Audit	Data Protection	Secure Configuration
	<p>Ability to assure access only to authorized users and to control when/where/how the data are accessed</p> 	<p>Ability to analyze the transactional activities (threats/blocks) and to view current transactional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



Database INsecurity Practices

DB Access Control

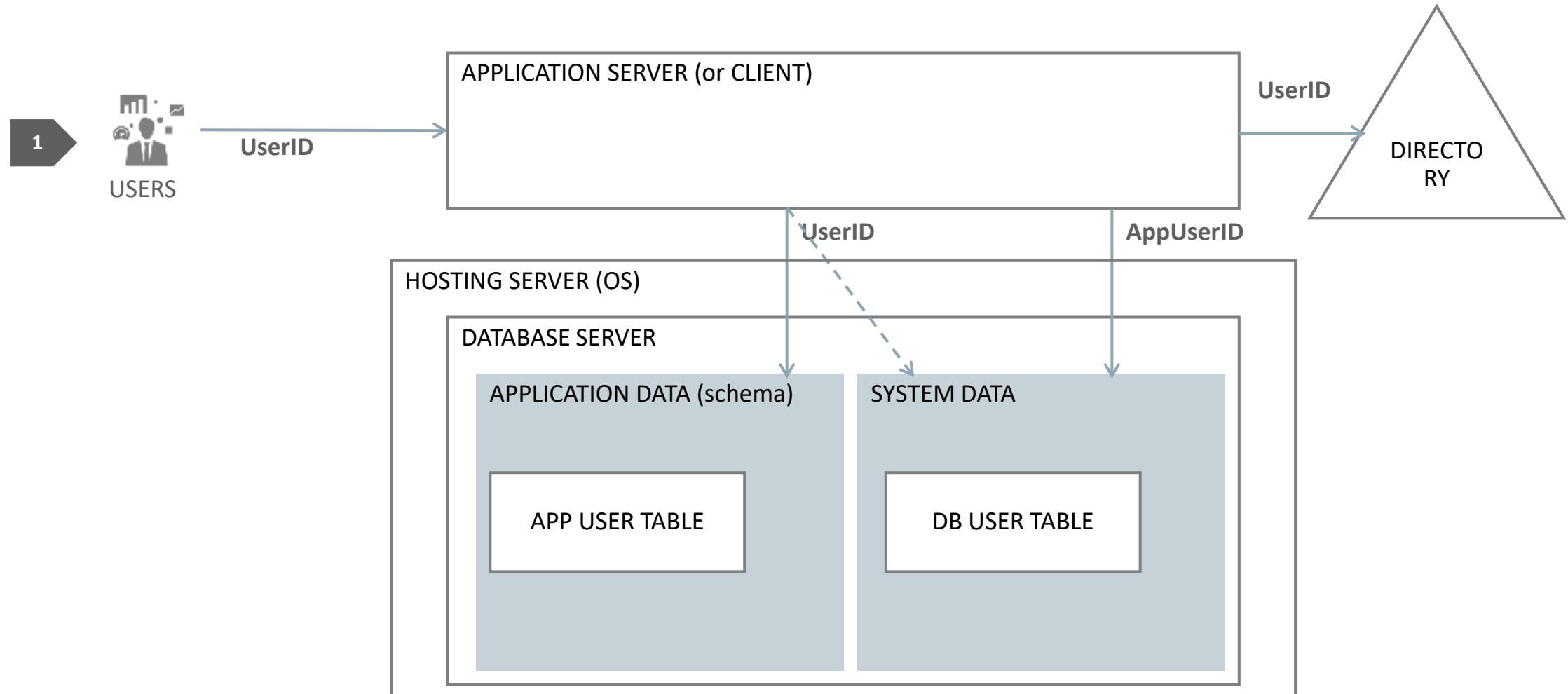
Authentication and authorization



DB Access Control



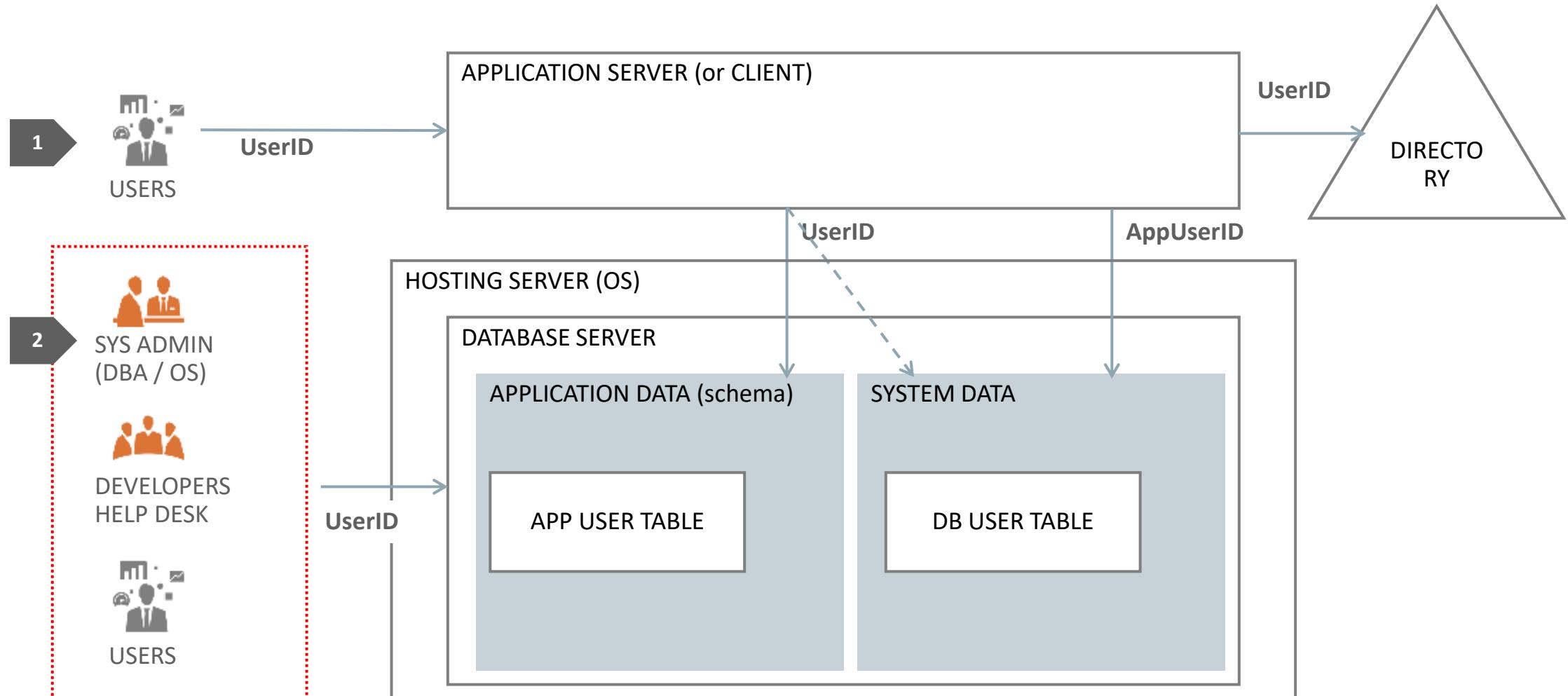
Authentication and authorization from 3 different point of views



DB Access Control



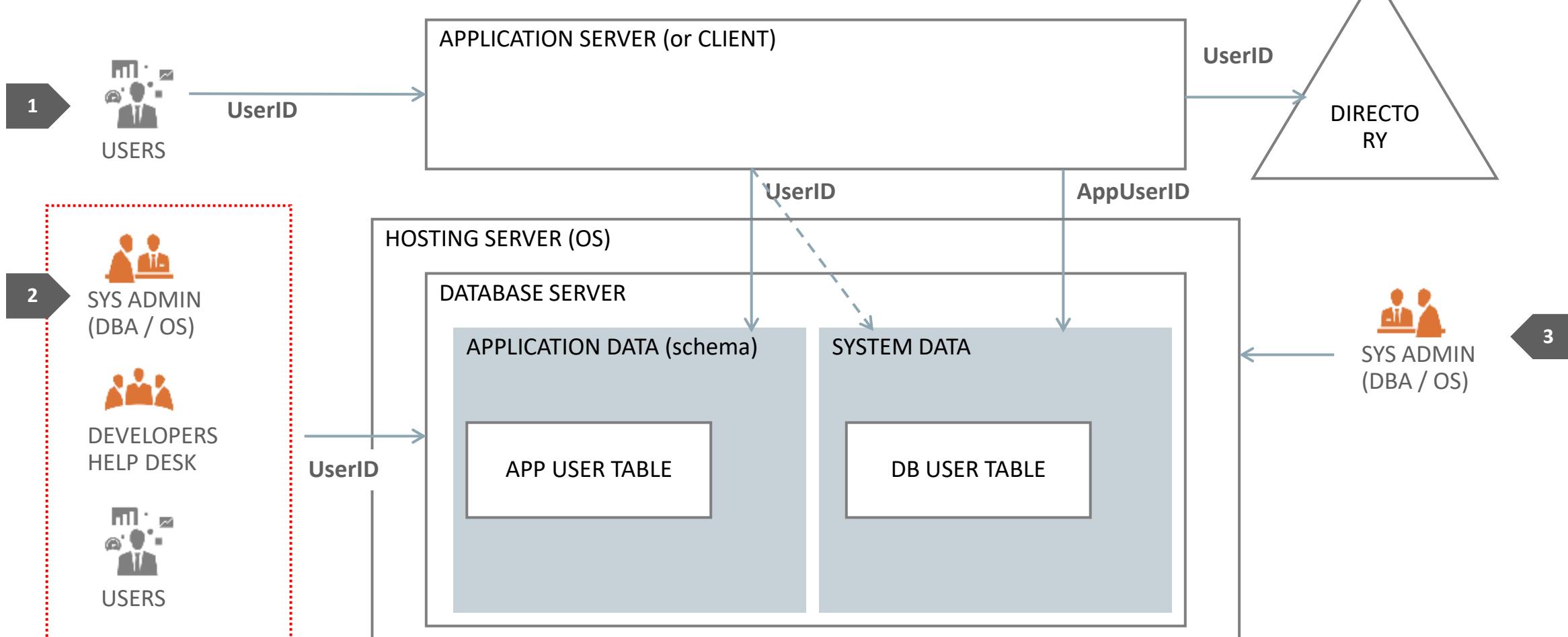
Authentication and authorization from 3 different point of views



DB Access Control



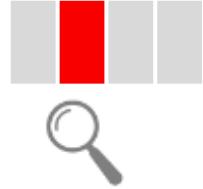
Authentication and authorization from 3 different point of views



DB Access Control – MCM

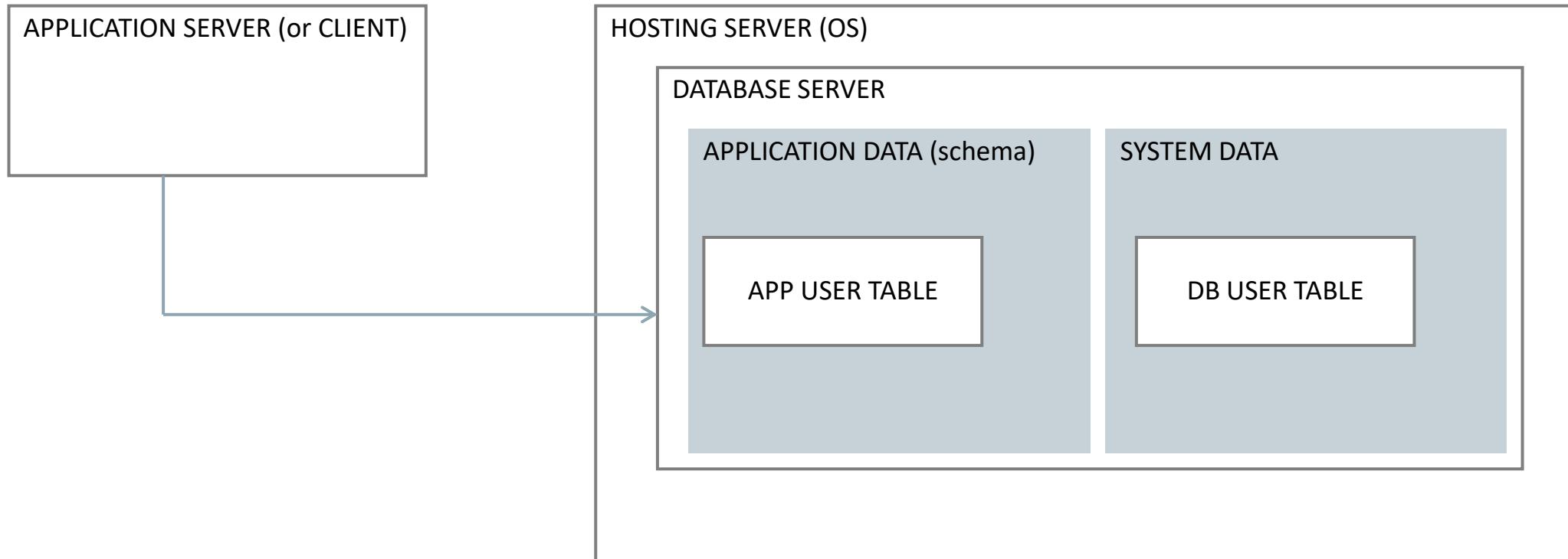
- No distinction between Application User and Schema Owner (AC1)
- Application user credential not protected in the application server (AC2)
- Developers use application user credential (AC3)
- DBA do not have personal accounts and use technical accounts (AC4)
- Technical accounts defined with a human algorithm and never changed (AC5)
- End users have direct access to the DB bypassing the application (AC6)
- ~~No lifecycle management for DB users (AC7)~~
- ~~OS administrators can escalate their privileges to DBA (AC8)~~
- ~~DBA have full access to DML (AC9)~~

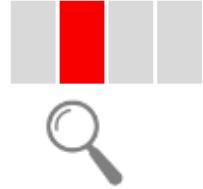




Monitoring, Blocking and Auditing

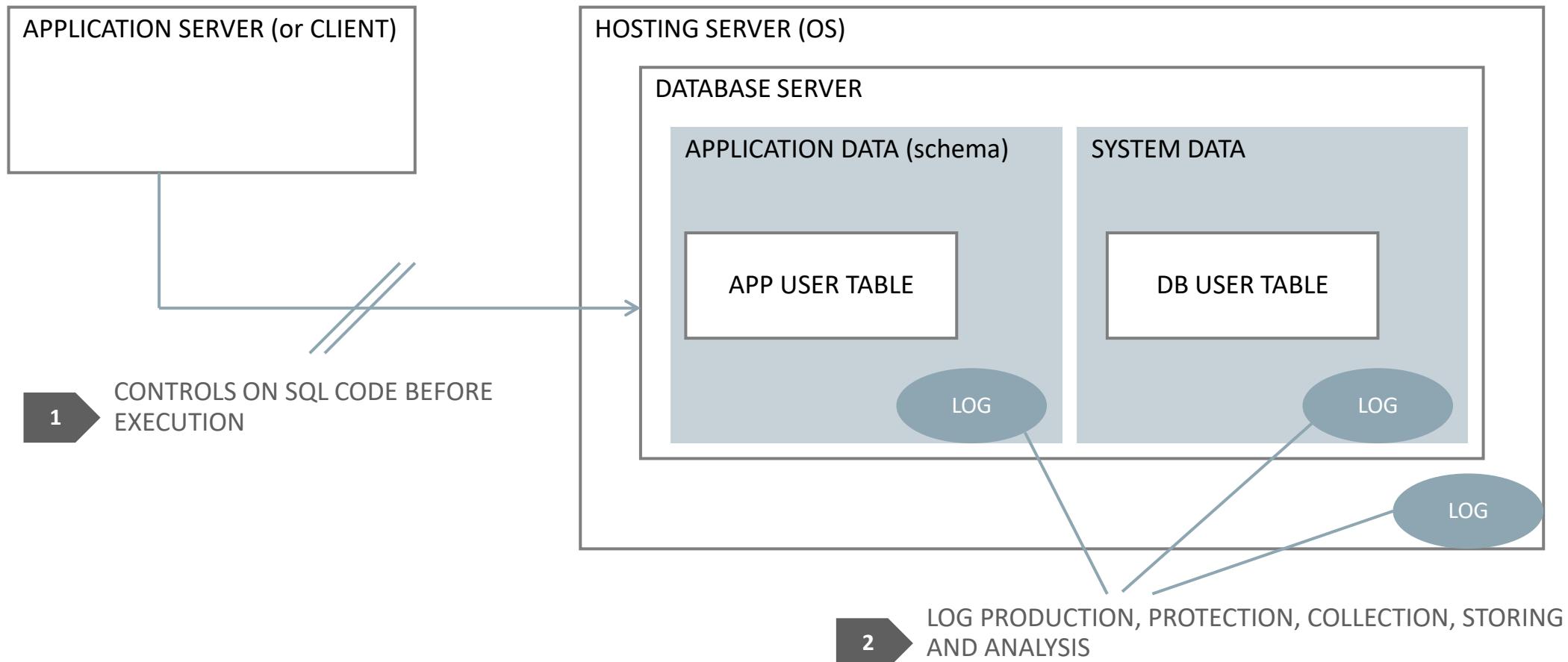
Pre and post execution SQL controls





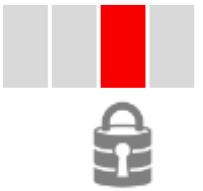
Monitoring, Blocking and Auditing

Pre and post execution SQL controls



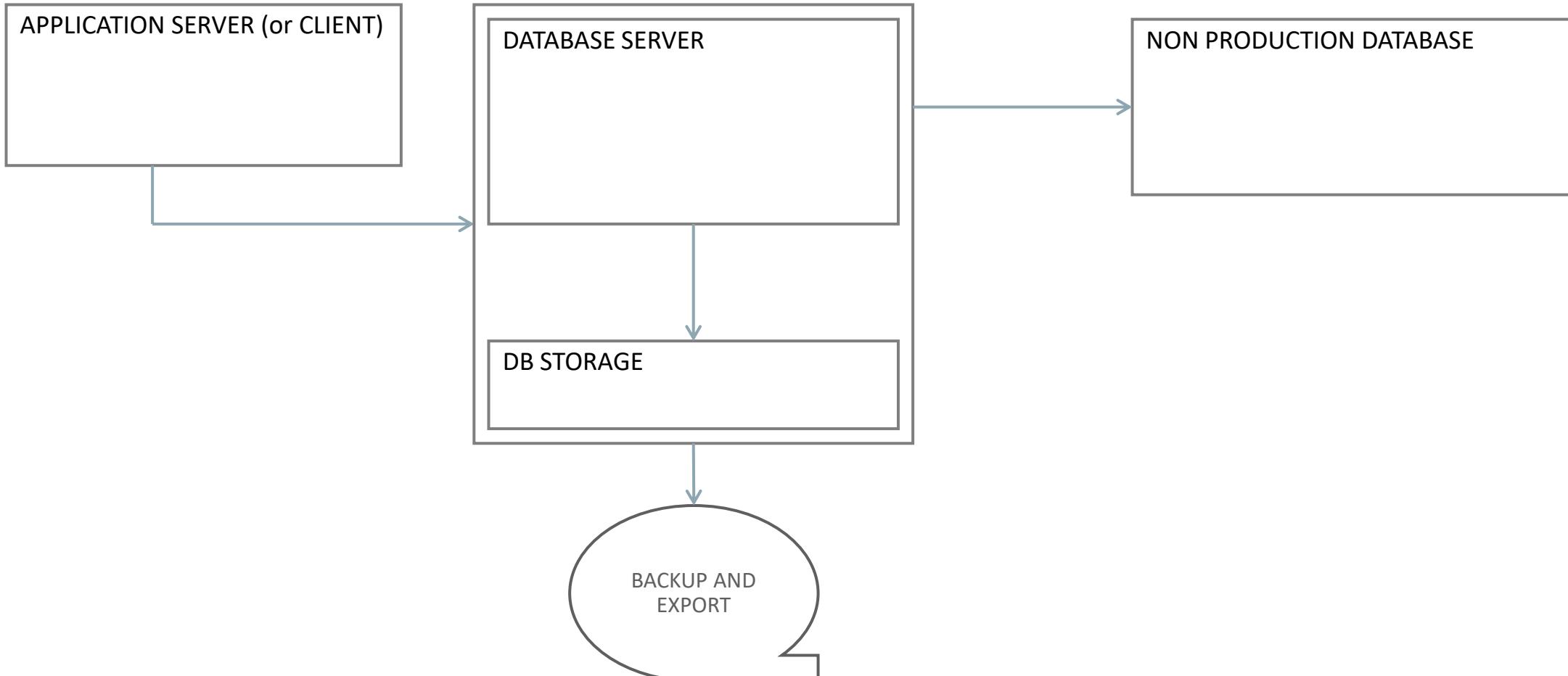
Monitoring, Blocking and Auditing – MCM

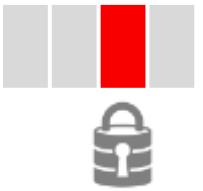
- No preventive SQL controls (LG1)
- No or partial and inconsistent logs (LG2)
- Logs are not analyzed (LG3)
- Logs are not managed (LG4)
- No DB user accountability (LG5)
- No end user accountability (LG6)



Data Protection

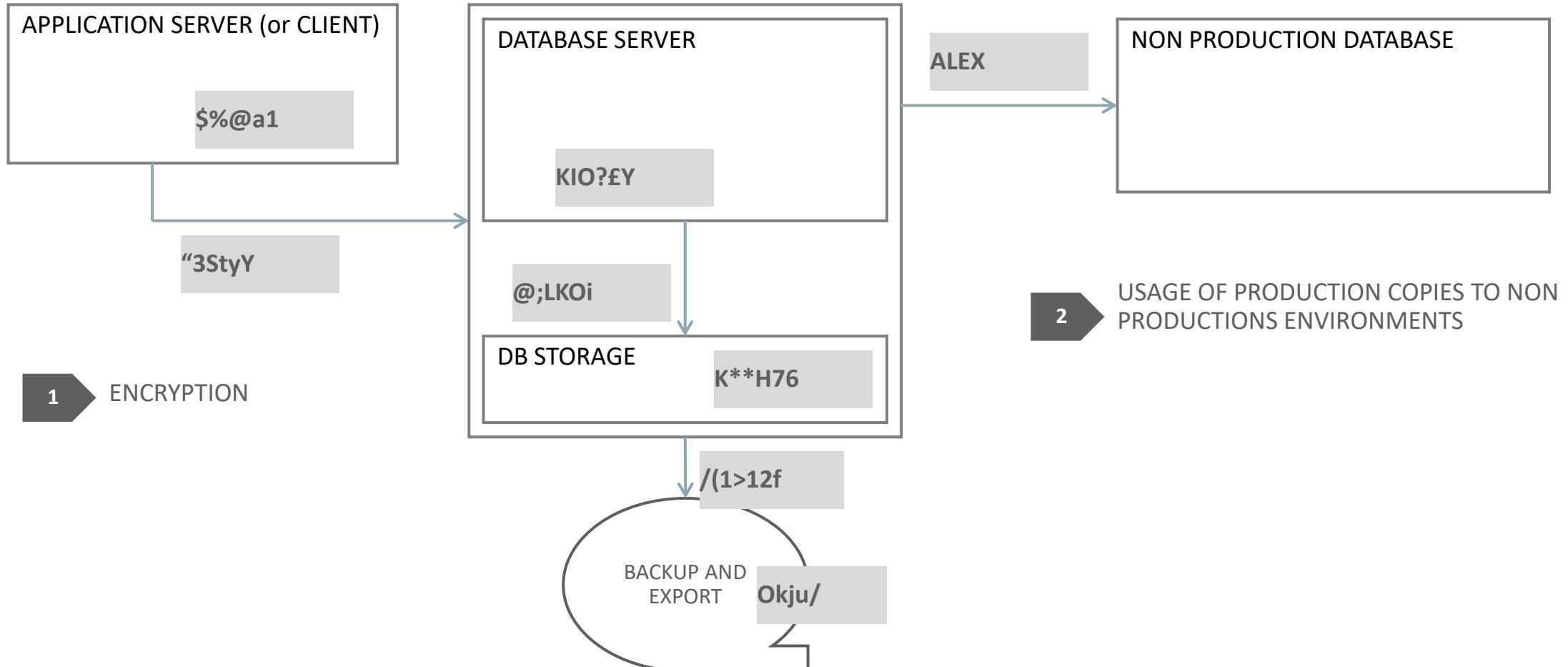
Usage of encryption and indiscriminated production copies





Data Protection

Usage of encryption and indiscriminated production copies



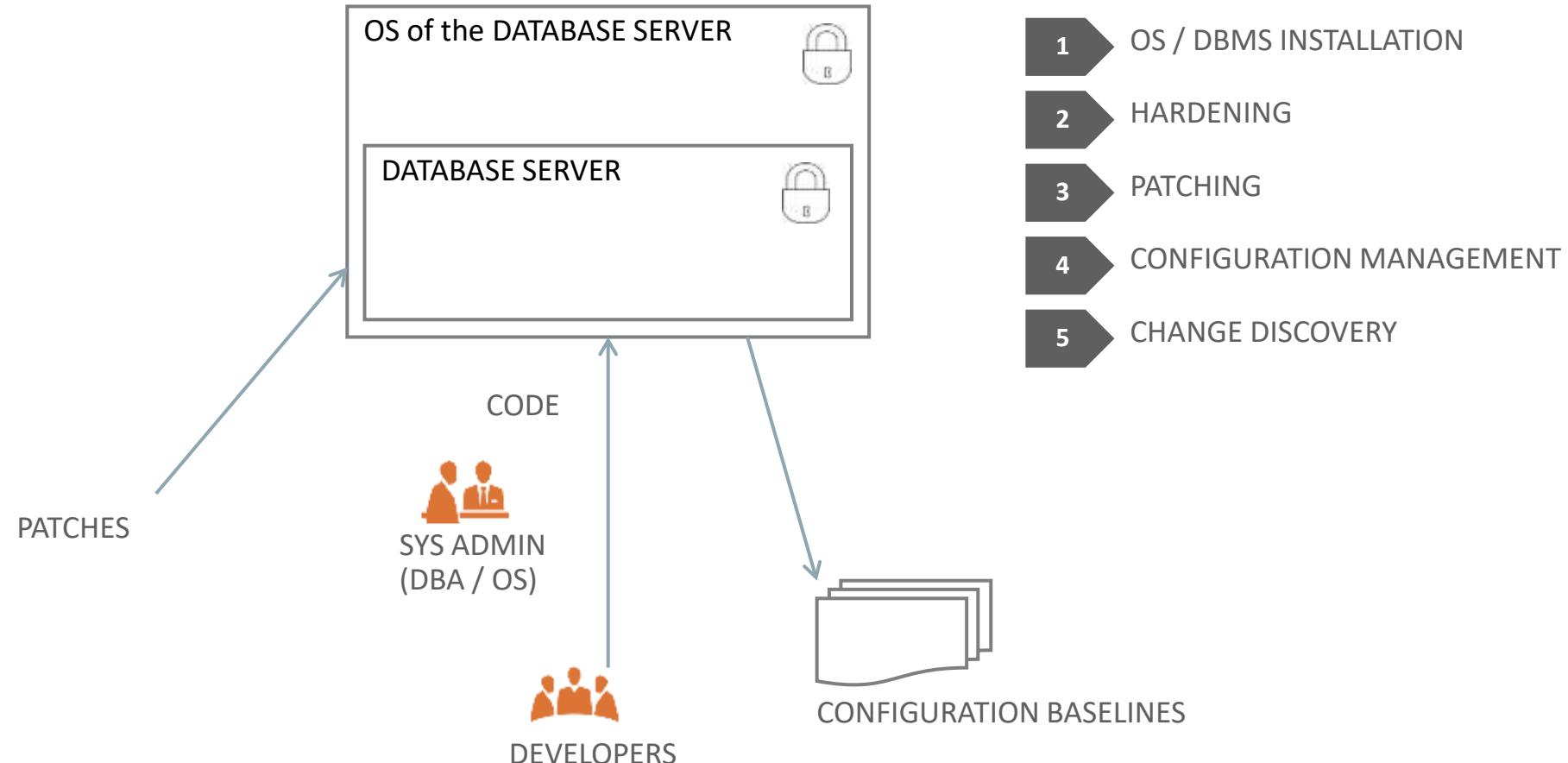
Data Protection – MCM

- Applications do not encrypt (DP1)
- No datafile encryption (DP2)
- No storage encryption (DP3)
- No network encryption (DP4)
- No backup / export encryption (DP5)
- Production data copied to development environments (DP6)



Secure Configuration

Installation, hardening, patching, configuration management...



Secure Configuration – MCM

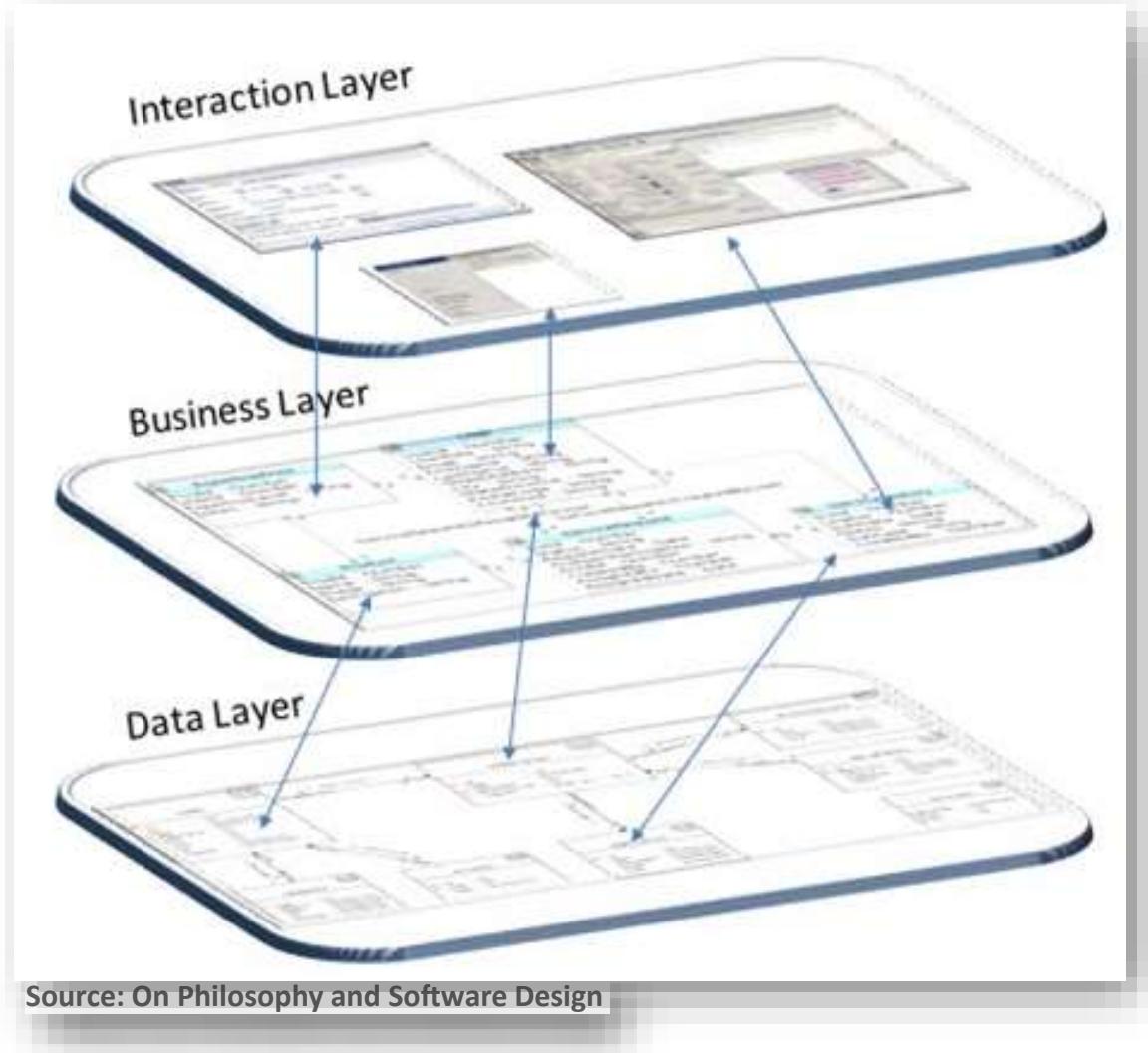
- Obsolete DB / OS releases (SC1)
- No DB / OS hardening (SC2)
- No patching (SC3)
- Poor SDLC production promotion and SoD (SC4)
- No production user, privileges, db objects change control (SC5)

Conclusion

Conclusion

- We need better DB security
- Most of the problems are related to carelessness
- Less than 50% of the improved controls requires new products provided by a vendor
- We need to follow Security best practices and principles
 - Need to know
 - Segregation of Duties
 - Accountability
- Defense in Depth
- Security in the Architecture

Security in the Architecture



- Each layer has its own security
- Each layer relies on the next one
- The deeper security controls are pushed the better it is
- More security at a less cost

Contact me



[LinkedIn](#)

[Twitter.com/U3L4](#)

alessandro.vallega@oracle.com

Integrated Cloud Applications & Platform Services

ORACLE®

Argomenti

Verticale sui rischi del cloud



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT



10.11.23
Webinar





Alessandro Vallega

Founding Partner Rexilience S.r.l.

Fondatore e Chairman Clusit Community for
Security

Comitato Scientifico Clusit

Professore a contratto @UNIMI - corso di Analisi e
gestione del rischio, laurea magistrale di sicurezza
informatica

alessandro.vallega@rexilience.eu



- | | | |
|-------------------|----------|---|
| 17/03/2023 | ■ | ▶ Il mercato della Cybersecurity e lo scenario in Italia e a livello internazionale |
| 21/03/2023 | ■ | ▶ Dall'incidente alla gestione della crisi |
| 30/03/2023 | ■ | ▶ Lo scenario dei cyber attacchi: evoluzione delle minacce e principali trend |
| 26/04/2023 | ■ | ▶ Il contesto generale della cybersecurity: cyber war e cambiamento della situazione a livello geopolitico |
| 28/04/2023 | ■ | ▶ Vulnerabilità, Vulnerability Assessment e Penetration Test: cosa sono e come gestirli |
| 10/05/2023 | ■ | ▶ Come affrontare praticamente la sicurezza della fornitura |
| 05/06/2023 | ■ | ▶ Trend digitali e nuove tendenze per la cybersecurity |
| 14/06/2023 | ■ | ▶ Rafforzare la "Security culture" per ridurre il rischio legato al fattore umano |
| 07/07/2023 | ■ | ▶ La gestione del rischio cyber e dei rischi connessi alla filiera aziendale |
| 12/07/2023 | ■ | ▶ Digital Operational resilience Act (DORA): struttura, principali novità introdotte e raccordo con altre normative in ambito |
| 22/09/2023 | ■ | ▶ Mutua autenticazione e affidabilità informativa in ambito smart mobility |
| 09/10/2023 | ■ | ▶ Internet of Military Things tra Cybersecurity e AI |
| 10/10/2023 | ■ | ▶ Principali cyber minacce e contromisure adeguate |
| 07/11/2023 | ■ | ▶ Le competenze per la cybersecurity e la gestione del fattore umano |
| 10/11/2023 | ■ | ▶ Introduzione al Cloud e rischi da considerare nell'adozione |
| 21/12/2023 | ■ | ▶ La certificazione di prodotto e la cyber security |

Il Cloud viene adottato dalle aziende in maniera crescente da molti anni, ma molte di esse devono ancora capirne l'uso migliore e i rischi che possono derivare da un utilizzo scorretto.

In questo webinar si fornisce la definizione di Cloud, come lo si può utilizzare e quali accorgimenti è meglio adottare per evitare eventuali pericoli in termini di sicurezza e compliance.



Come indicato nel programma, risponderemo a queste domande:

- Cos'è il Cloud e come evolverà nel futuro?
- Quali sono i benefici del Cloud?
- Quale percorso bisogna seguire per adottare delle soluzioni Cloud?
- Quali sono i rischi del Cloud?
- Quali misure di sicurezza ricadono nella propria responsabilità?
- Dove è possibile trovare altre informazioni per approfondire il tema?



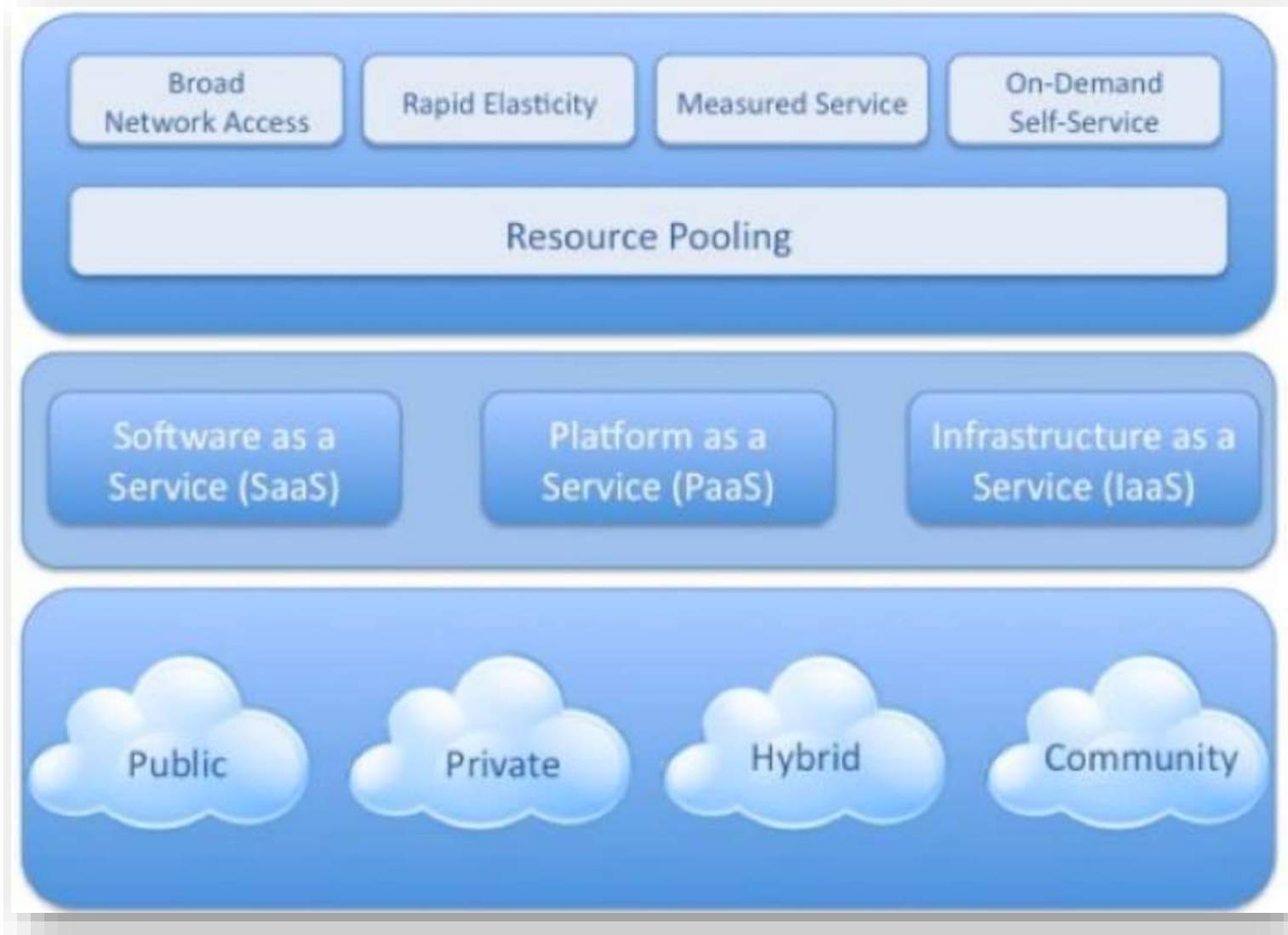
Introduzione



La definizione moderna di Cloud Computing è del
NIST e risale al 2010



Q Questa figura originale comprende tutti i suoi elementi



Essential
characteristics

Service models

Deployment models

[SP 800-145, The NIST Definition of Cloud Computing | CSRC](#)

Q Un aneddoto del 2013

Q Un aneddoto del 2013

The screenshot shows the Cloud Security Alliance (CSA) website's 'Affiliates' page. At the top, there is a navigation bar with links for 'CLOUD 101', 'CIRCLE', 'EVENTS', 'BLOG', and 'SIGN IN OR SIGN UP'. Below the navigation is a search bar. The main content area is titled 'Affiliates' and displays a grid of logos for various organizations. The logos include:
Row 1: AIA (American Institute of CPAs), ASP-aaS (ASP-as-a-Service), ASTRA (Advanced Software Technologies), bdigital (Barcelona Technological Institute),
Row 2: B-HIVE, Cloud Standards Customer Council, Clusit (Cloud Interoperability Laboratory), DMTF (Distributed Management Task Force), DRM INSTITUTE,
Row 3: EDB Singapore, EGA (e-Government Agency), enisa (European Institute for the Protection of Intellectual Property), fei (Fundació ceat innovació),
Row 4: ICSO (International Computer Security Organization), IDRBT (Indira Gandhi Institute of Design & Technology), IPA (Institute of Professional Accountants), ISACA (Information Systems Audit and Control Association), (ISC)² (Information Systems Security Association).

Fin dal 2011 Clusit è affiliato e sostiene Cloud Security Alliance;

Un aneddoto del 2013

The screenshot shows the homepage of the Cloud Security Alliance (CSA). At the top, there's a navigation bar with links for CLOUD 101, CIRCLE, EVENTS, BLOG, SIGN IN OR SIGN UP, and a search icon. Below the navigation is a banner with the text "Explore real-world cloud breaches & actionable insights in the latest Top Threats paper!". Underneath the banner, the "Affiliates" section is displayed, featuring logos for various organizations like AICPA, ASP-aaS, B-HIVE, Cloud Standards Customer Council, EDB Singapore, EGA, enisa, ICSO, IDRBT, and IPA. To the right of the affiliates, there's a sidebar for "Oracle Community For Security". It includes a thumbnail for a report titled "Privacy nel Cloud: Le sfide della tecnologia e la tutela dei dati personali per un'azienda italiana" with the URL <http://c4s.clusit.it/>. Below this, there's another thumbnail for the "Rapporto Clusit 2013 sulla sicurezza ICT in Italia" with the URL <http://www.clusit.it/rapportoclusit/>. The Oracle logo is at the bottom of the sidebar.

Nel 2012 la Clusit Community for Security scriveva un libro sulla Privacy nel Cloud e volendo usare la storica figura ho chiesto al NIST il permesso. Il NIST mi ha detto che la proprietà era di CSA

Un aneddoto del 2013

The screenshot shows the Cloud Security Alliance (CSA) website. On the left, there's a sidebar titled "Affiliates" featuring logos for various organizations like ACPA, Cloud Standards Customer Council, Clusit, EDB Singapore, ICSO, and IPA. To the right, there's a red-bordered box containing the "Oracle Community For Security" logo and a thumbnail for a document titled "Privacy nel Cloud". The document thumbnail shows a wire mesh fence against a blue sky with clouds.

Re: Permission to use a CSA image protected by copyright - Mozilla Thunderbird

File Edit View Go Message Tools Help
Get Messages Write Tag

From Alessandro Vallega <alessandro.vallega@oracle.com>
To Jim Reavis <jreavis@cloudsecurityalliance.org>
Subject Re: Permission to use a CSA image protected by copyright

Ok thank you. In this case I have both of you! They suggested me to write you
cheers Alessandro

On 20/02/2012 17.01, Jim Reavis wrote:

Hi Allesandro,

The copyright was for the entire guidance document, but the graphic
itself is from NIST, which we acknowledged separately in the document.
If you reference NIST as the source who should be fine.

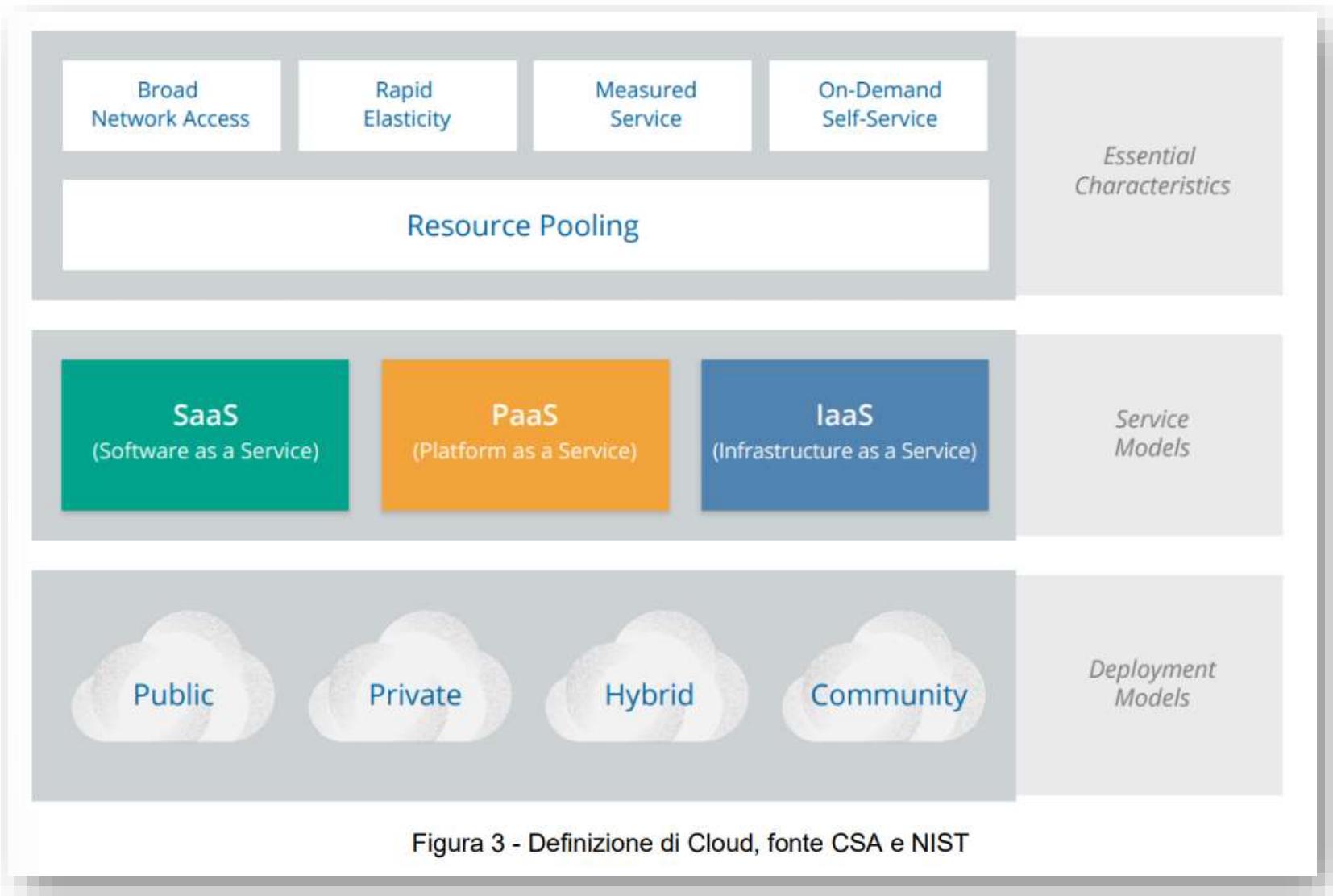
www.nist.gov

Jim Reavis
jreavis@cloudsecurityalliance.org
Executive Director, Cloud Security Alliance
+1.360.820.2545

On Mon, Feb 20, 2012 at 5:15 AM, Alessandro Vallega
alessandro.vallega@oracle.com wrote:

Dear Jim,
we (Oracle Community for Security) are producing a document on the "Italian
Privacy in the Cloud" with the following characteristics:
- the document is in Italian, 50 pages long
- will be distributed to the public with Creative Common BY-SA license

Jim Reavis (CSA) non sapeva di essere il proprietario
dei diritti ©





Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure². The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.³ The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).





- ❑ *Private cloud.* The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- ❑ *Community cloud.* The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- ❑ *Public cloud.* The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- ❑ *Hybrid cloud.* The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).



Essential Characteristics

- ❑ *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- ❑ *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- ❑ *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- ❑ *Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- ❑ *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability¹ at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.



Social
Big data
Internet of Things
Edge computing

Intelligenza artificiale



E consuma energia e data center

Il Sole 24 Ore Giovedì 26 Ottobre 2023 – N. 295

Nòva 24

MOTTO PERPETUO
Se torturi i numeri abbastanza a lungo, confesseranno qualiasi cosa.

GREGG EASTERBROOK

Come crescono le attività digitali

IL TREND
Tendenze globali negli indicatori digitali ed energetici
Dati 2015-2022 a confronto

	2015	2022	VAR. %
Utenti internet in milioni	3	5,3	+78%
Traffico internet in ZB	0,6	4,4	+600%
Data centre workloads in milioni	180	800	+340%
Uso energia dei data center (escluse crypto) in TWh	200	240-340	+20/70%
Uso energia del crypto mining in TWh	4	100-150	+2.300/3.500%
Uso energia per rete di trasmissione dati in TWh	220	260-360	+18/64%

LA DOMANDA GLOBALE DI ENERGIA DEI DATA CENTER
Dati per regione in Twh

Region	2010	2015	2022
Nord America	78	131	161
Europa Occidentale	61	113	138
Asia Pacific	76	101	122

* SDS= scenario di sviluppo sostenibile. Fonte: Iea

Intelligenza artificiale, corsa a costruire nuovi data center

27

GUIDA ONLINE
Ai Gen, come funziona (e a cosa serve) il modello multimodale Llaava? E le illusioni ottiche generate dall'intelligenza artificiale. Le nostre guide sul canale tecnologia.

DOMENICA SU NÒVA
Viaggio nell'Antropocene, da una valle sarda dei Balcani, la riscoperta del valore delle comunità e del rapporto con la natura

Nel 2022 sono stati creati e consumati quasi 100 miliardi di miliardi di gigabyte di dati [...] raddoppiare entro il 2025 [...]

[...] 926 grandi hub, entro sei anni altri 427 datacenter

Fonte Nòva → IDC e Synergy Research Group

🔍 Spending globale sul cloud

Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2021	2022	2023
Cloud Business Process Services (BPaaS)	54,952	60,127	65,145
Cloud Application Infrastructure Services (PaaS)	89,910	110,677	136,408
Cloud Application Services (SaaS)	146,326	167,107	195,208
Cloud Management and Security Services	28,489	34,143	41,675
Cloud System Infrastructure Services (IaaS)	90,894	115,740	150,254
Desktop-as-a-Service (DaaS)	2,059	2,539	3,104
Total Market	412,632	490,333	591,794

PaaS

SaaS

IaaS



[Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \\$600 Billion in 2023](#)

🔍 Spending globale sul cloud

Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2021	2022	2023
Cloud Business Process Services (BPaaS)	54,952	60,127	65,145
Cloud Application Infrastructure Services (PaaS)	89,910	110,677	136,408
Cloud Application Services (SaaS)	146,326	167,107	195,208
Cloud Management and Security Services	28,489	34,143	41,675
Cloud System Infrastructure Services (IaaS)	90,894	115,740	150,254
Desktop-as-a-Service (DaaS)	2,059	2,539	3,104
Total Market	412,632	490,333	591,794

[Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \\$600 Billion in 2023](#)

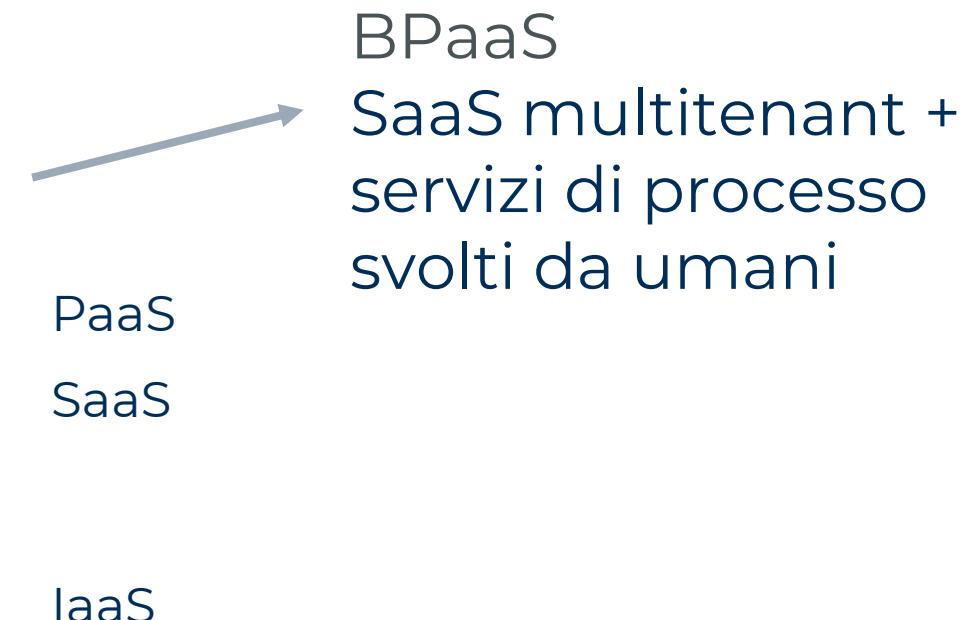


Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2021	2022	2023
Cloud Business Process Services (BPaaS)	54,952	60,127	65,145
Cloud Application Infrastructure Services (PaaS)	89,910	110,677	136,408
Cloud Application Services (SaaS)	146,326	167,107	195,208
Cloud Management and Security Services	28,489	34,143	41,675
Cloud System Infrastructure Services (IaaS)	90,894	115,740	150,254
Desktop-as-a-Service (DaaS)	2,059	2,539	3,104
Total Market	412,632	490,333	591,794

[Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \\$600 Billion in 2023](#)

PaaS
SaaS
IaaS



Cloud mngt & Security
Servizi di gestione e security dello stesso cloud

🔍 Spending globale sul cloud

Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2021	2022	2023
Cloud Business Process Services (BPaaS)	54,952	60,127	65,145
Cloud Application Infrastructure Services (PaaS)	89,910	110,677	136,408
Cloud Application Services (SaaS)	146,326	167,107	195,208
Cloud Management and Security Services	28,489	34,143	41,675
Cloud System Infrastructure Services (IaaS)	90,894	115,740	150,254
Desktop-as-a-Service (DaaS)	2,059	2,539	3,104
Total Market	412,632	490,333	591,794

Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \$600 Billion in 2023

PaaS

SaaS

IaaS



DaaS

Virtualizzazione e
gestione del
desktop

🔍 Shift di paradigma

	Tecnologia	Aspetti economici	Pregi e difetti
Mainframe (1950-1980)	Elaborazione e storage centralizzato	Alti costi di impianto up-front	Stabilità, sicurezza,
Client Server (1980-2000)	Elaborazione e storage distribuiti su PC e Server	Piccoli scalini di investimento	Vicino al business, decentrato, silos, complesso software deployment
Cloud (2000-)	Grandi datacenter scalabili, hardware commodity , virtualizzazione, connettività	Pay as you go, multitenancy	Rapida innovazione



Andare nel cloud

1. Diverso impianto economico
2. Aumentata e scalabile capacità di calcolo
3. Acquisizione di servizi e applicazioni innovative
4. Maggiore sicurezza
5. Migliorata collaborazione della forza lavoro

Q 1. Diverso impianto economico

Si dovrebbe risparmiare ma 

1. Difficile fare confronti a pari qualità, pari sicurezza, pari compliance
2. I costi si classificano fiscalmente in maniera diversa (spese operative vs. conto capitale)
3. Richiede di fare riallocazioni di costi e risorse che hanno una certa inerzia
4. Richiede uno shift di competenze che può essere molto complesso e costare a sua volta (in-out)
5. *Measured service: pay as you go*

Il paradigma di base è quello della specializzazione del lavoro sulla supply chain



Q Il fornitore di cloud (CP) può fare efficienze che il cliente (CC) non può conseguire

1. Economie di fornitura (es. fino al 45% del costo dei server¹)
2. Compensazione dei workload grazie al *resource pooling* (multitenancy)
3. Disponibilità di competenze iperspecializzate
4. Vantaggi geografici e fiscali

Il risparmio ottenuto dal fornitore si ribalta in parte sul cliente

1. Fonte: The Economics Of The Cloud – Rolf Harms; Michael Yamartino

2. Aumentata e scalabile capacità di calcolo

Il cloud «per forma» molto meglio di un'infrastruttura tradizionale

Ciò è dovuto agli elementi «nativi» e plausibilmente scontati del servizio cloud: *rapid elasticity* e *resource pooling* abilitati da potenti tecnologie di virtualizzazione



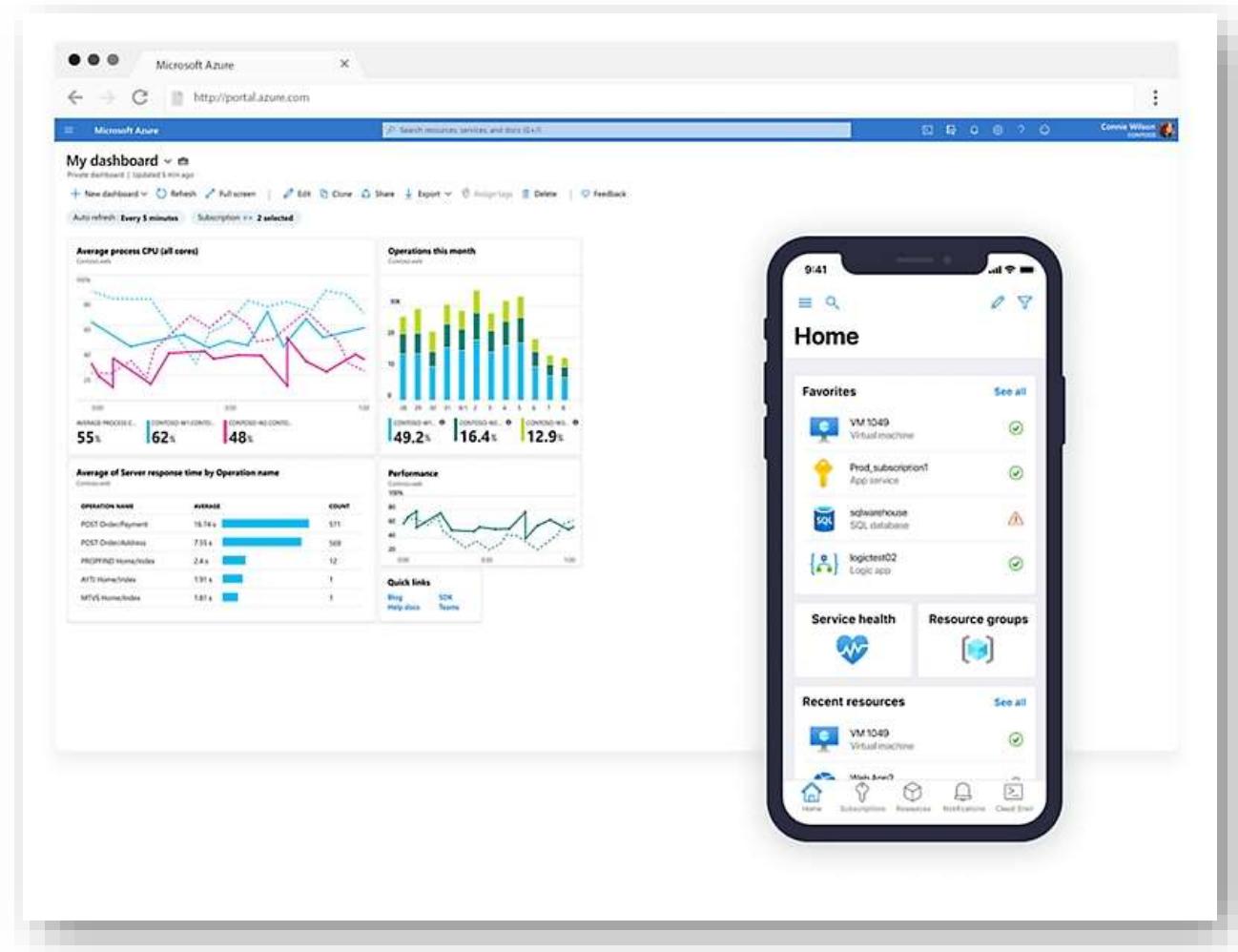
Richiede grande attenzione nella fase di selezione del servizio da parte del cliente e di un'attenta definizione dell'architettura

Il cloud si basa sulla virtualizzazione

Sia la virtualizzazione sia il cloud permettono di astrarre il calcolo, lo storage e la rete dalla componente fisica

Il cloud automatizza e orchestra la gestione delle risorse condivise

La virtualizzazione richiede un amministratore umano. Il cloud offre funzionalità automatiche e self service

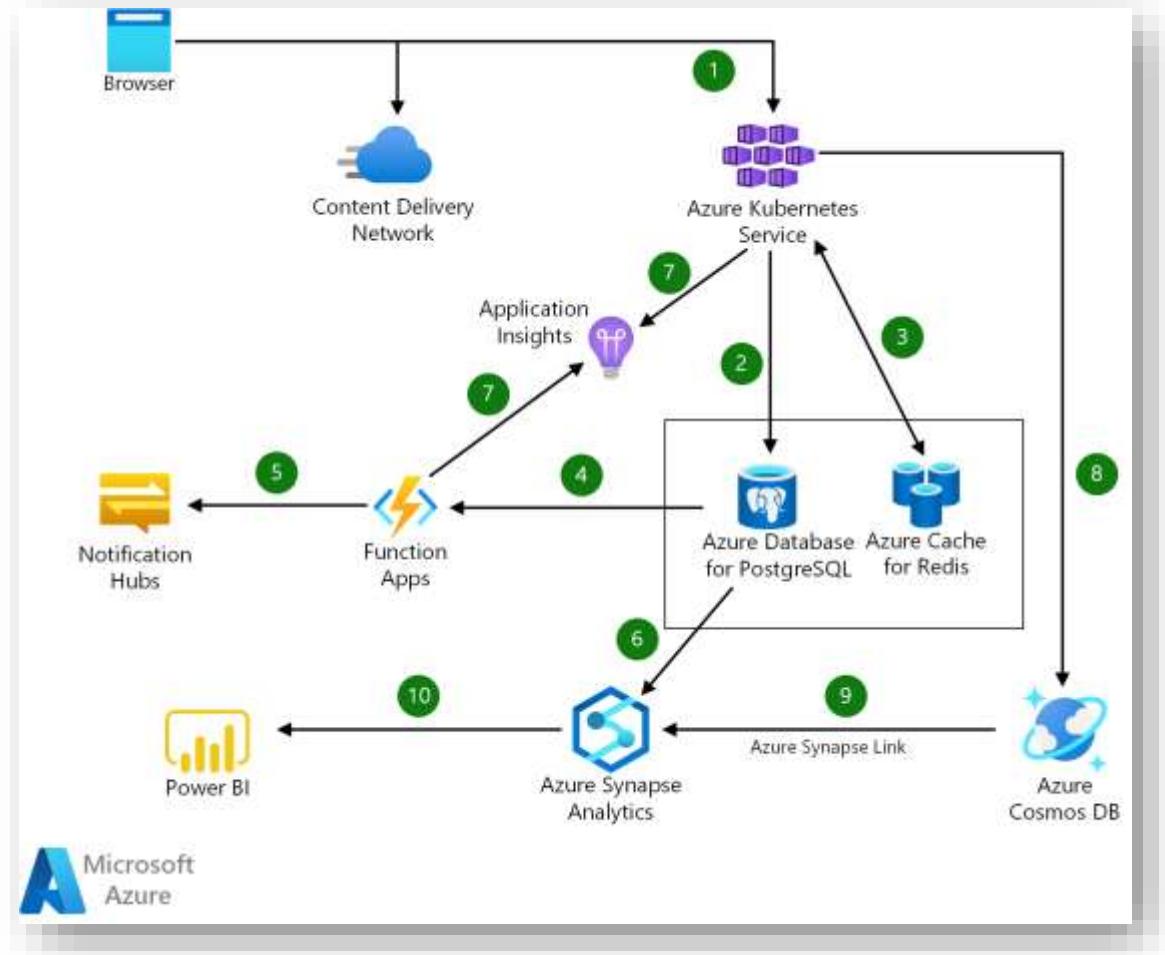


3. Acquisizione di servizi e applicazioni innovative

Lato *PaaS*: importanti trend tecnologici (che Gartner¹ definisce Mesh Apps e architettura a servizi, API platform e Event processing) rendono facilmente disponibili le tecnologie necessarie per comporre il software (vs. make o buy)

Lato *SaaS*: l'offerta di soluzioni è sempre più potente e ampia

PaaS e SaaS abilitano l'innovazione di business

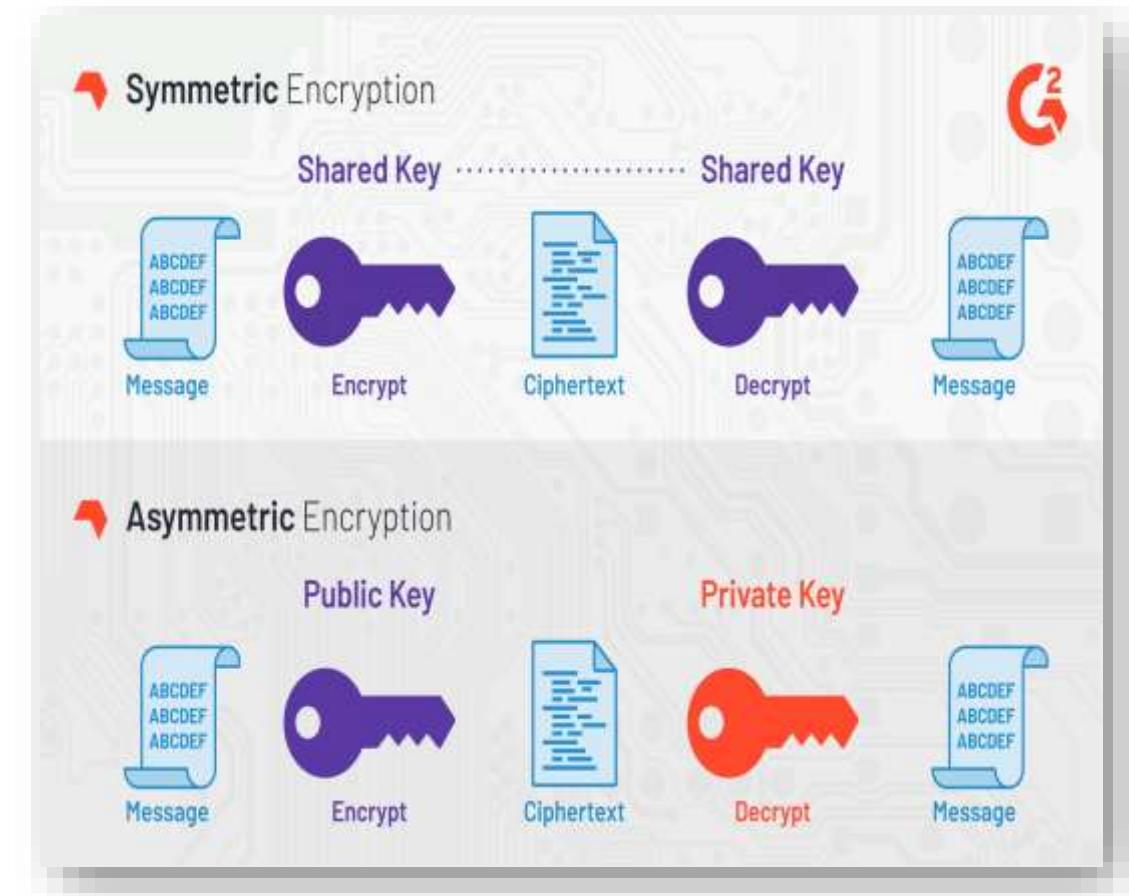


1. Fonte: <https://www.gartner.com/en/documents/3970797>

4. Maggiore sicurezza

L'economia di scala conseguita dal cloud provider gli permette - e l'obiettivo di business gli richiede - di provvedere ad elevati livelli di sicurezza altrimenti non possibili, come:

- Sicurezza fisica del data center
- Alta affidabilità, IT continuity e disaster recovery
- Crittografia, accesso controllato ai dati
- Protezione contro gli attacchi DDOS
- Monitoraggio
- Ecc.



5. Migliorata collaborazione della forza lavoro

Il cloud fornisce grandi benefici anche nel mondo dell'informazione «destrutturata» per il lavoro d'ufficio come documenti e videoconferenze.

La pandemia ha rimosso molti degli ostacoli all'adozione

Ci sono molti possibili percorsi di adozione del cloud che dipendono dalla specifica situazione di partenza. Es:



- Cloud only per le startup (SaaS, PaaS, IaaS)
- Rehosting (**lift and shift**, refactoring) IaaS
- SaaS adoption (collaboration, HR, CRM ...)
- Test & Dev
- Backup services, **Disaster recovery**
- Managed security services



Rischi del cloud

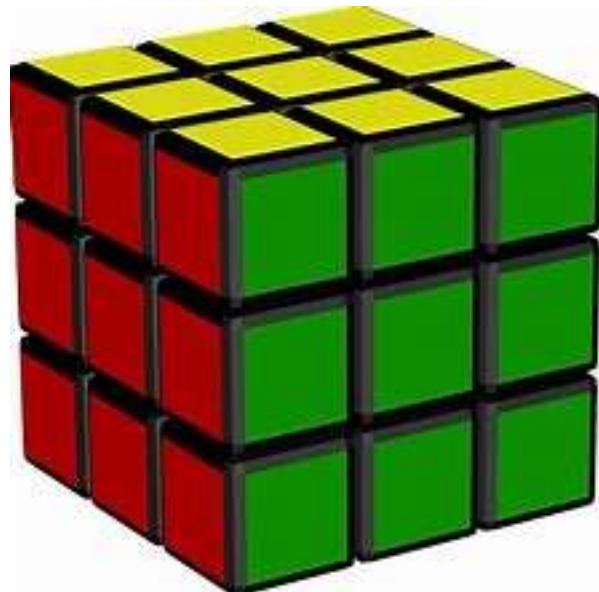
Criteri guida:

1. Il rischio è anche opportunità
2. Essi vanno valutati rispetto al contesto specifico

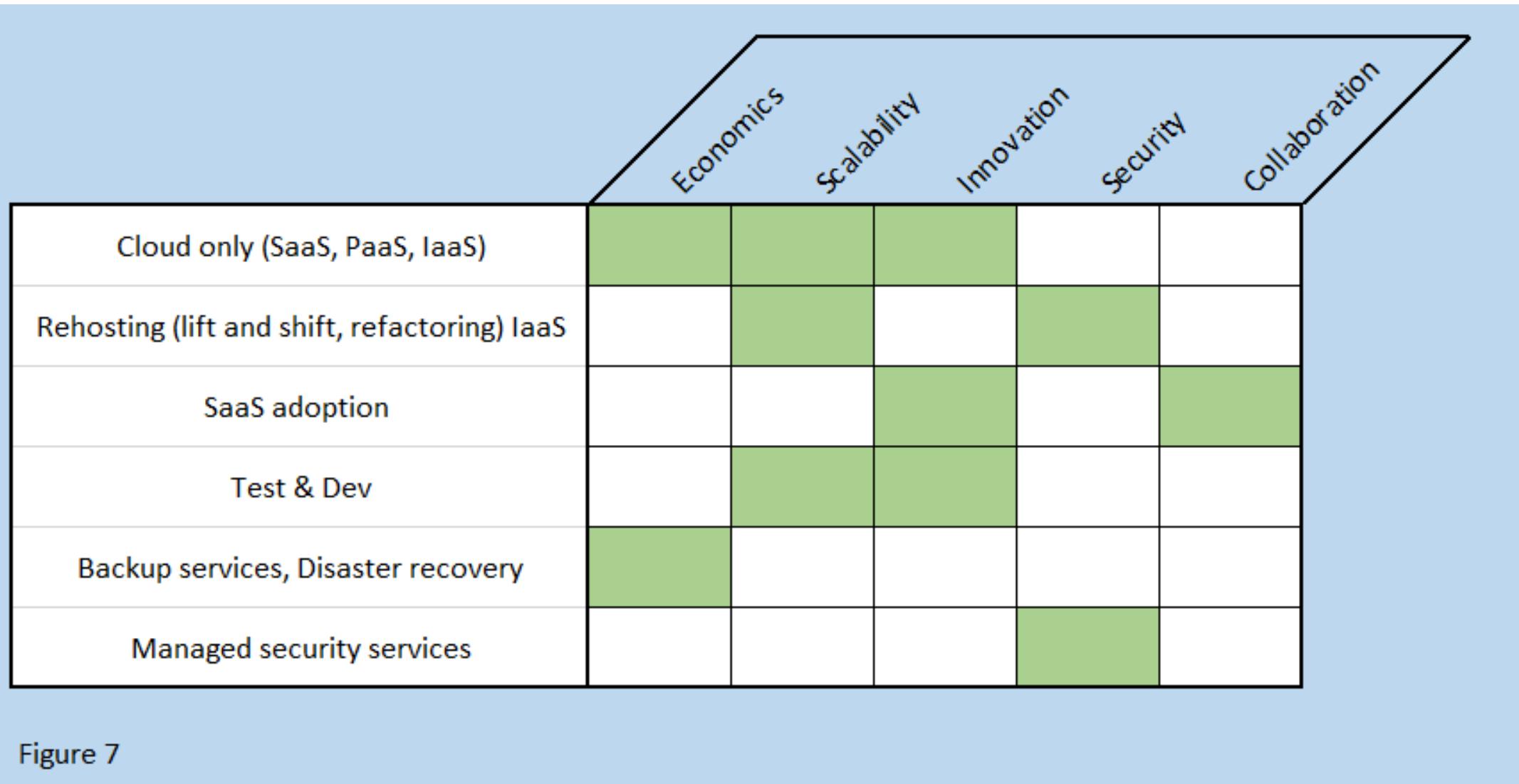
Le prime due dimensioni sono:

1. Rischi / opportunità rispetto all'obiettivo prefissato
2. Rischi / opportunità specifici del percorso seguito

La terza: Rischi / opportunità intrinseci del cloud



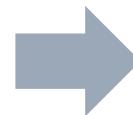
Esempio



La governance è il sistema di direzione e controllo che garantisce che l'organizzazione agisca per conseguire gli obiettivi aziendali stando all'interno dei limiti accettati

E' fatta di regole, controlli e processi che si declinano a diversi livelli: enterprise management, information management, information security, IT

Il cloud aumenta la complessità di governo in funzione del service e del deployment model



- Perdita di controllo diretto nonostante permanga la responsabilità verso terzi e autorità
- Perdita delle competenze e lock-in
- Molteplici giurisdizioni con sistemi legali differenti
- Supply chain estesa e opaca
- Rapidi cambiamenti dei servizi
- Shadow IT 

Gli elementi importanti del contratto cloud includono:

- Ruoli e responsabilità delle parti
- Livelli di servizio e penalizzazioni
- Misure tecniche e organizzative a tutela della sicurezza dei dati
- Informazioni, obblighi e capacità di gestione dei disastri (DR)
- Localizzazione del data center e regole per la filiera di fornitura
- Ruoli privacy obblighi e responsabilità
- Possibilità e meccanismi di audit
- Norme e tutele per la risoluzione e chiusura del contratto (way out; exit strategy; portabilità dei dati)



- Tutto molto bello e molto necessario ma normalmente **impossibile da negoziare**
- Il cloud provider ti rimanda al suo contratto standard, sul suo sito, nella sua lingua, con i suoi allegati, con il suo foro competente per la risoluzione delle controversie ...
- Di conseguenza non rimane che verificare i contratti e decidere se correre il rischio

L'audit è l'esame della capacità di una parte di soddisfare, o continuare a soddisfare, gli accordi come fornitore di servizi

Può essere di seconda parte (cliente / fornitore) e deve essere previsto nel contratto a meno che non debba essere permesso per legge

Es. Art. 28 del GDPR stabilisce – legislativamente – un vero e proprio diritto da parte del titolare di effettuare audit nei confronti dei responsabili, allo scopo di verificare e garantirsi il rispetto dei principi di protezione dei dati.

Es. Art. 28 del DORA prescrive che [...] le entità finanziarie predeterminano, sulla base di un approccio basato sul rischio, la frequenza delle verifiche di audit e delle ispezioni nonché i settori da sottoporre ad audit [...]

L'attività è onerosa e molto complessa, quindi, all'atto pratico, ci si affida a audit di terze parti, certificazioni, attestazioni e autorizzazioni fornite dal cloud provider

Certification

- ISO/IEC 27001 (27002; 27017, 27018)
- CSA STAR certification

Attestation: AICPA

Autorizzazioni: FedRAMP

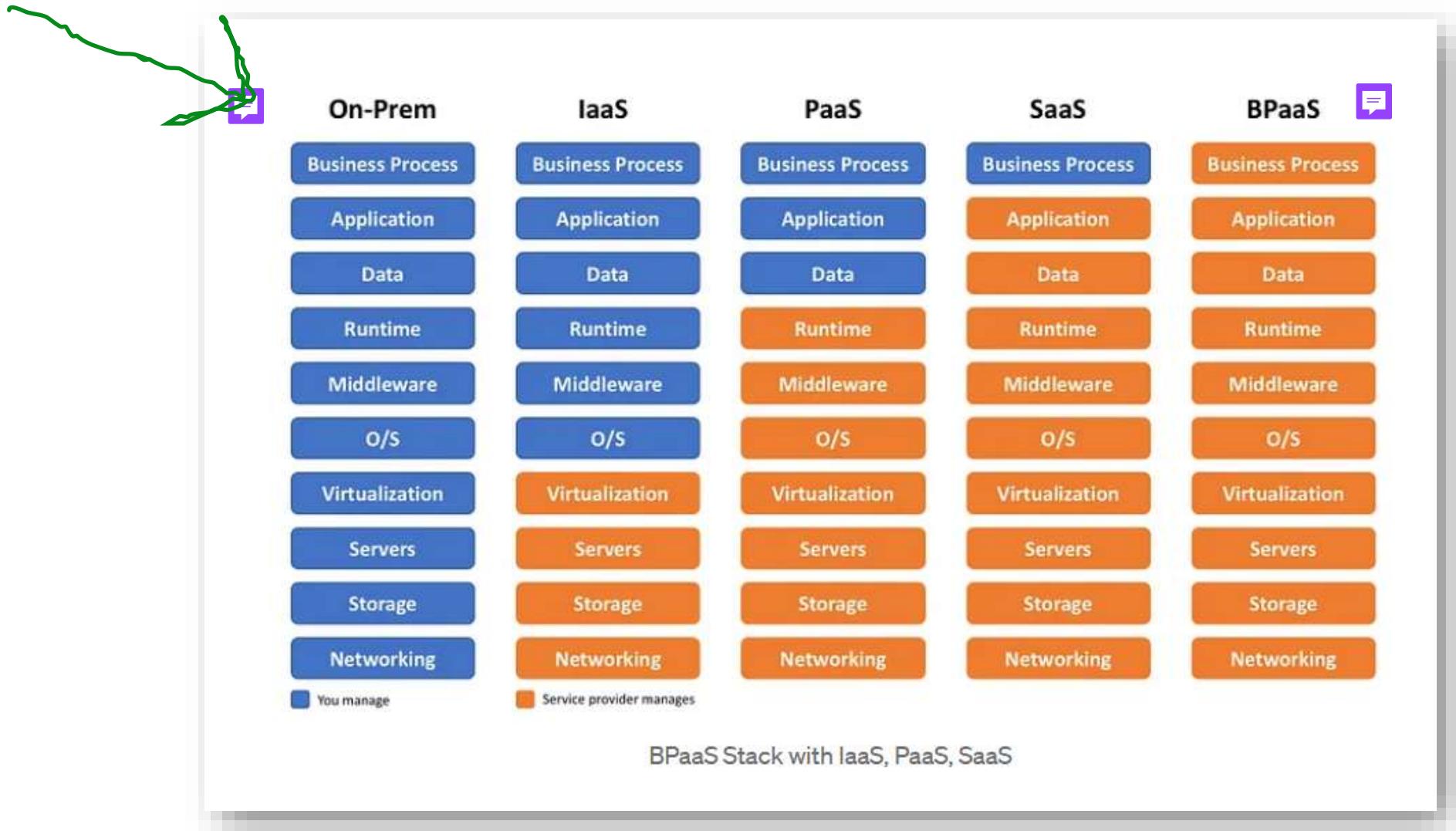
L'incomprensione del modello di responsabilità condivisa è la principale causa degli incidenti di cybersecurity

"Through 2020, 95% of cloud security failures will be the customer's fault"¹

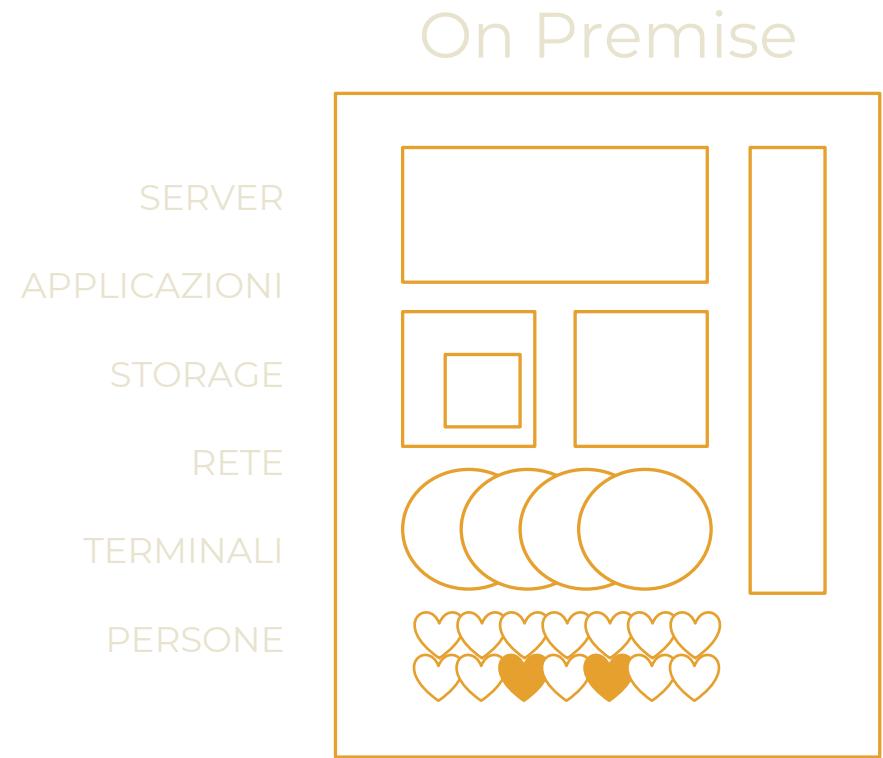
Sources: "Market Guide for Cloud Access Security Brokers," 24 October 2016, Craig Lawson, Neil MacDonald, Brian Lowans, Brian Reed;

Gartner

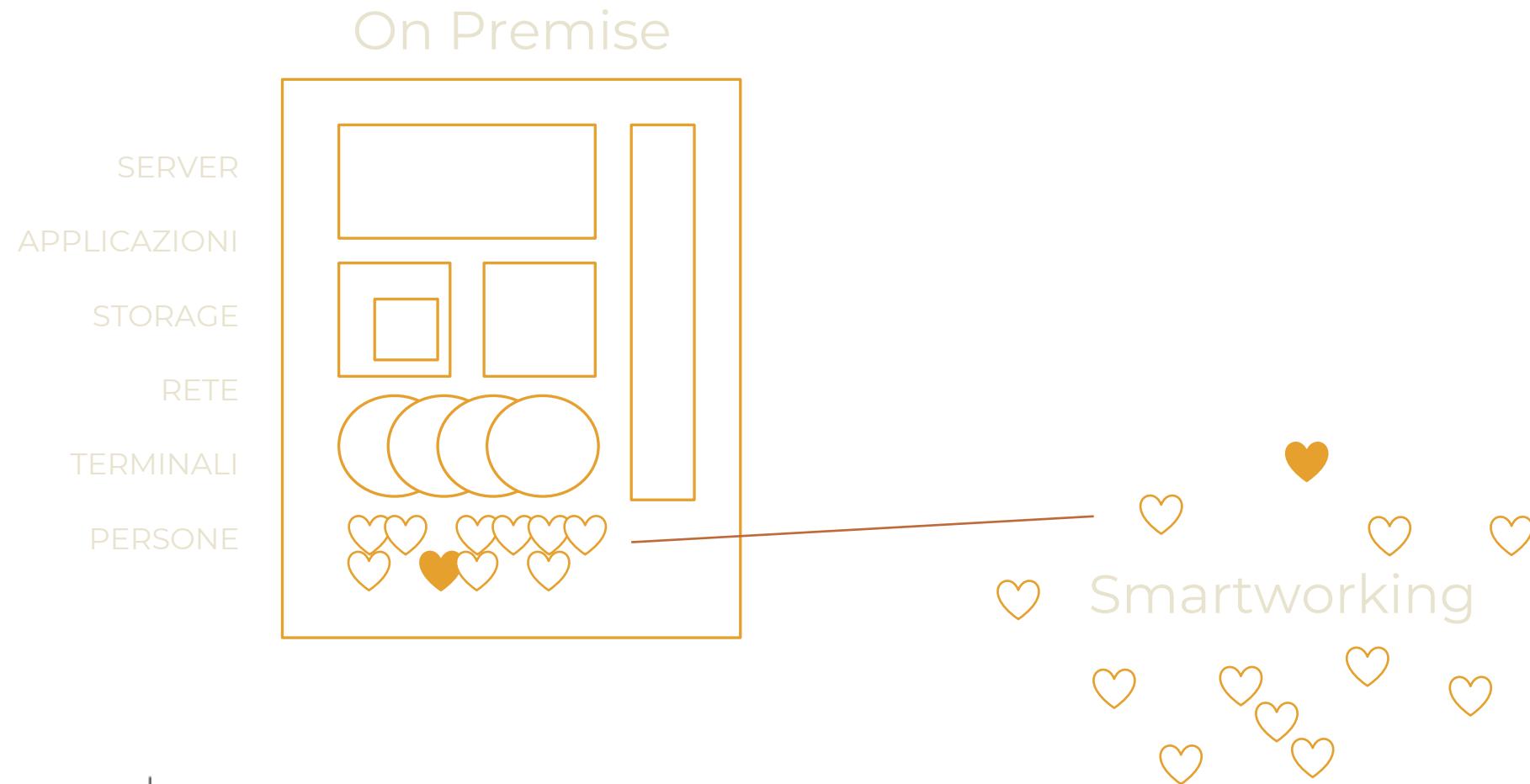
🔍 Shared responsibility



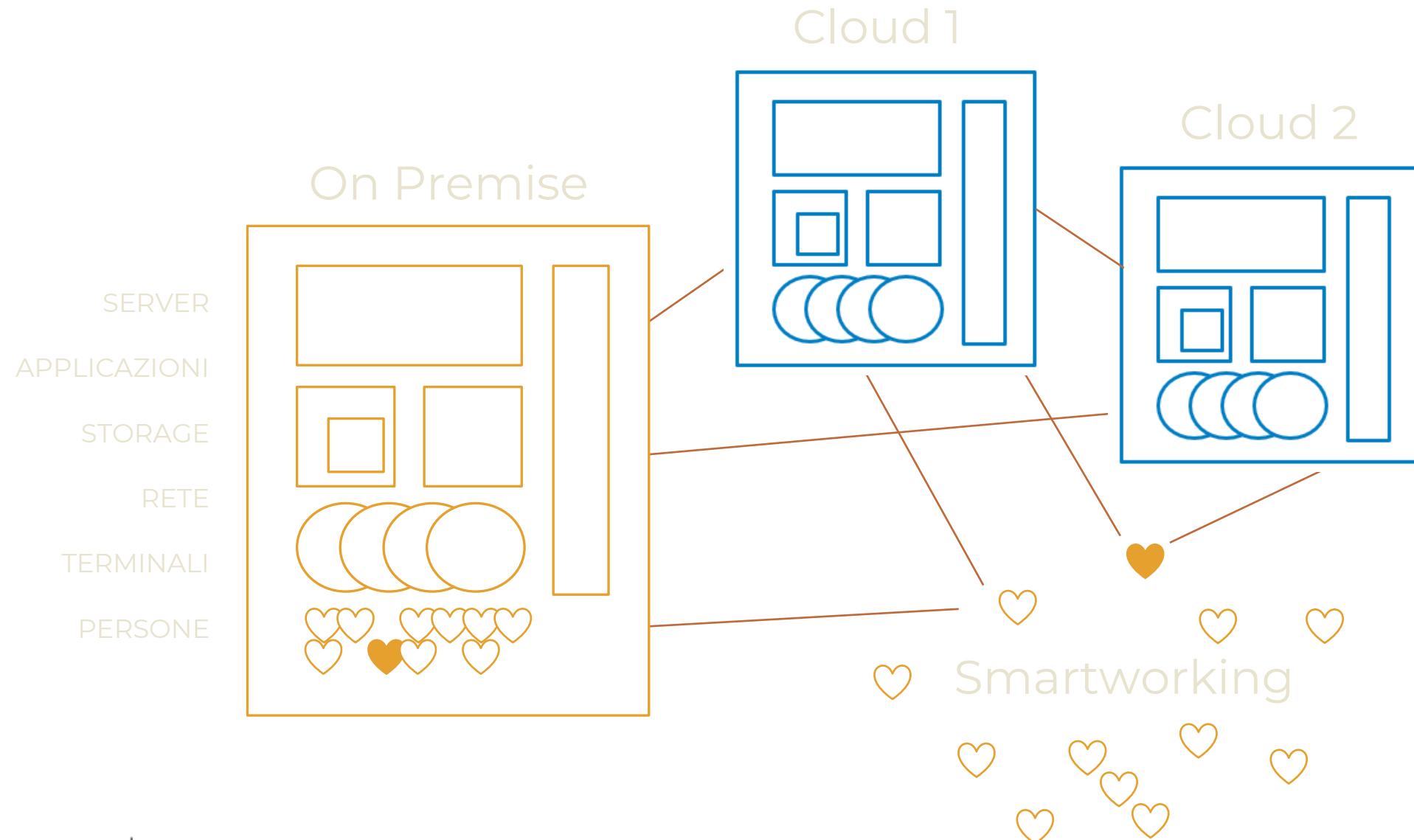
🔍 Vanishing perimeter: 1. On premise



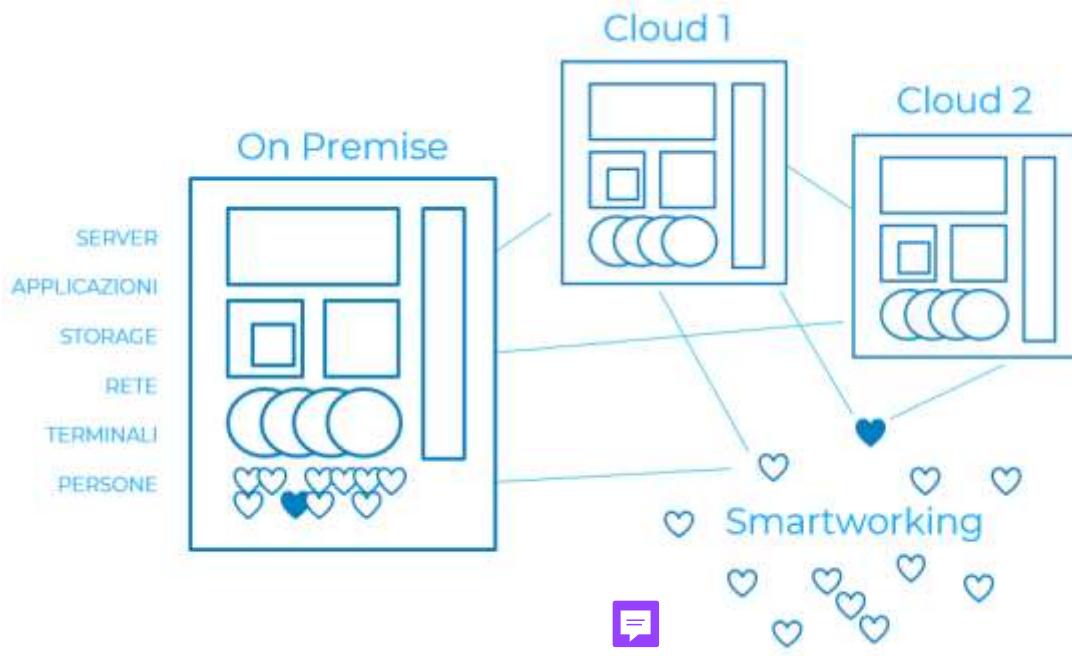
🔍 Vanishing perimeter: 2. Smart working



🔍 Vanishing perimeter: 3. Clouds



🔍 Alcune delle priorità



Network security
Identity management

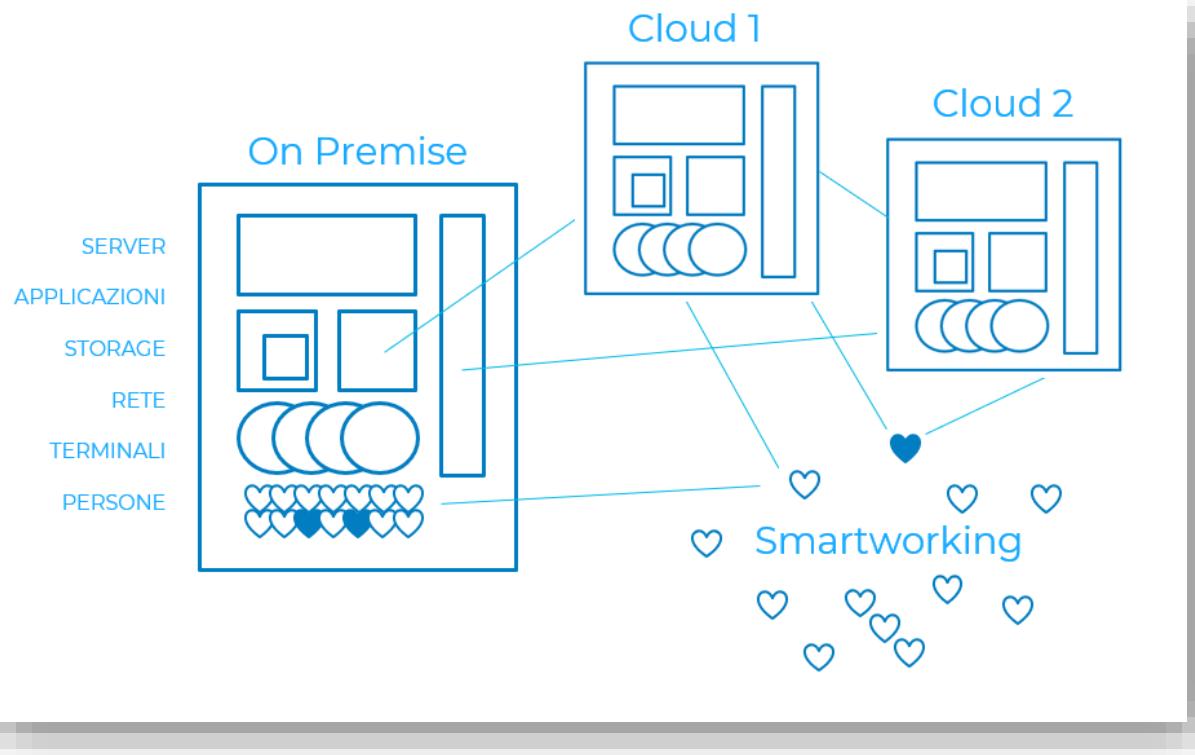
Penetration testing
Hardening 
Continuous monitoring 

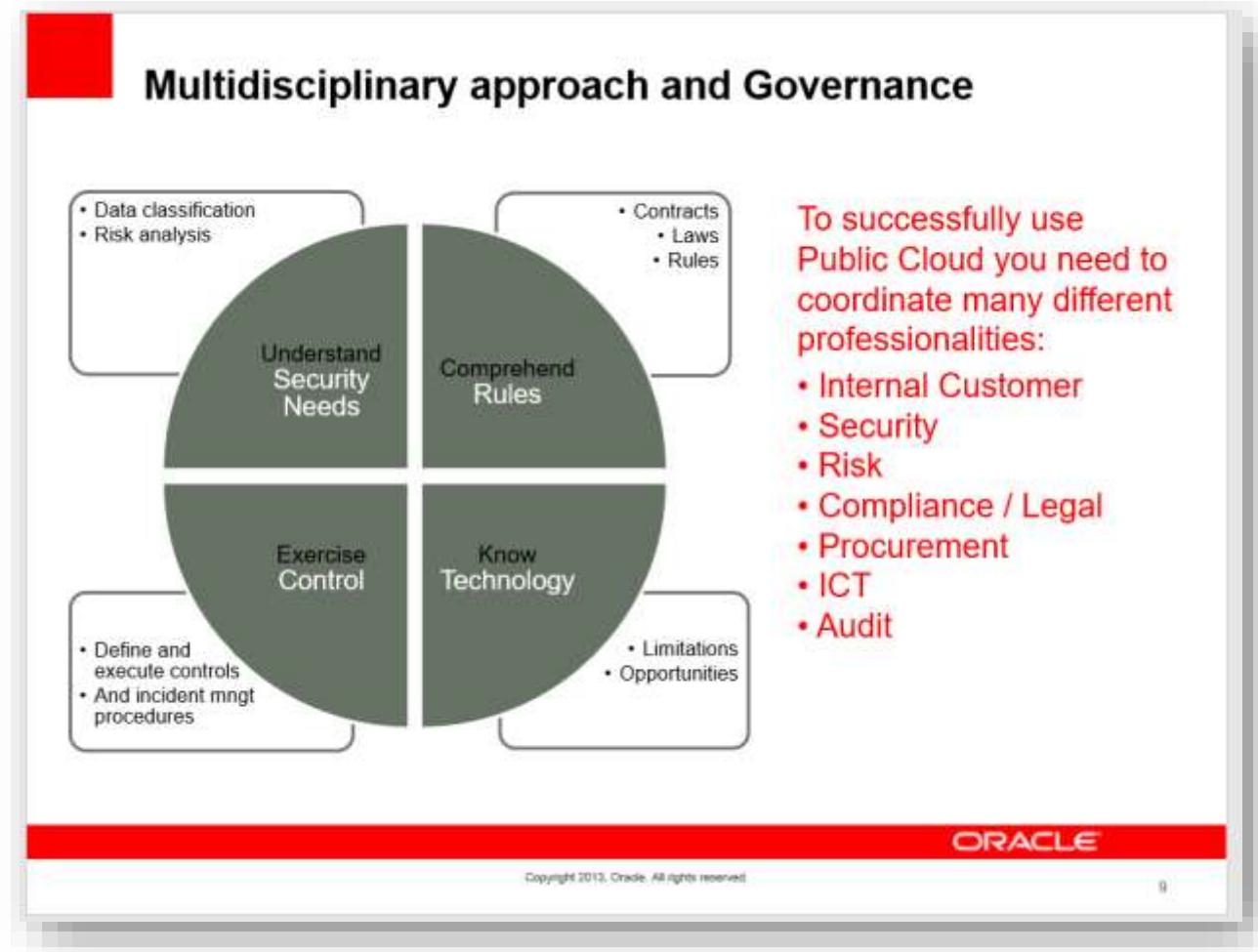
Data security
Key management

Zero trust – need to know
Privileged account management
API Security

Secure software development 

🔍 Priorità e shared responsibility model





Il cloud per la PMI: rischi e opportunità



Incomprensione dello shared responsibility model (soprattutto per lo IaaS)

Disparità negoziale nei contratti con (large) cloud provider

(Small) cloud provider failure ∩ Lock-in

Sicurezza molto maggiore

State of the art technology && nuovi modelli di business

Velocità di implementazione e CAPEX → OPEX



Come approfondire

Il trend di sviluppo del mercato dei servizi cloud è inarrestabile.

Le principali motivazioni sono individuabili nel risparmio sui costi e nei benefici gestionali realizzabili con questi servizi nelle organizzazioni di tutti settori e di tutte le dimensioni, del settore privato e della PA.

Conseguire tali vantaggi non è tuttavia una facile passeggiata, ma richiede, come in tutte le iniziative aziendali che presentano significativi impatti sull'organizzazione e sulle tecnologie, una focalizzazione particolare dei decision makers aziendali sugli aspetti "potenzialmente critici" dei Servizi Cloud: sicurezza, conformità e contratti.

In questo libro li trattiamo estensivamente.



Alessandro Vallega

Founding Partner Rexilience S.r.l.

Fondatore e Chairman Clusit Community for
Security

Comitato Scientifico Clusit

Professore a contratto @UNIMI - corso di Analisi e
gestione del rischio, laurea magistrale di sicurezza
informatica

alessandro.vallega@rexilience.eu

Argomenti

Verticale su Supply Chain
Security



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Argomenti

Verticale su Supply Chain
Security



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



10.05.2023
Webinar

Come affrontare praticamente la sicurezza della fornitura



Alessandro Vallega

Founding Partner Rexilience S.r.l.

Fondatore e Chairman Clusit Community for
Security

Comitato Scientifico Clusit

Professore a contratto @UNIMI - corso di Analisi e
gestione del rischio, laurea magistrale di sicurezza
informatica

alessandro.vallega@rexilience.eu



Cybersecurity & Data Protection (2023)

- | | | |
|-------------------|----------|---|
| 17/03/2023 | ■ | ▶ Il mercato della Cybersecurity e lo scenario in Italia e a livello internazionale |
| 21/03/2023 | ■ | ▶ Dall'incidente alla gestione della crisi |
| 30/03/2023 | ■ | ▶ Lo scenario dei cyber attacchi: evoluzione delle minacce e principali trend |
| 26/04/2023 | ■ | ▶ Il contesto generale della cybersecurity: cyber war e cambiamento della situazione a livello geopolitico |
| 28/04/2023 | ■ | ▶ Vulnerabilità, Vulnerability Assessment e Penetration Test: cosa sono e come gestirli |
| 10/05/2023 | ■ | ▶ Come affrontare praticamente la sicurezza della fornitura |
| 05/06/2023 | ■ | ▶ Trend digitali e nuove tendenze per la cybersecurity |
| 14/06/2023 | ■ | ▶ Rafforzare la "Security culture" per ridurre il rischio legato al fattore umano |
| 07/07/2023 | ■ | ▶ La gestione del rischio cyber e dei rischi connessi alla filiera aziendale |
| 12/07/2023 | ■ | ▶ Digital Operational resilience Act (DORA): struttura, principali novità introdotte e raccordo con le principali normative nazionali ed europee in ambito bancario e finanziario |
| 15/09/2023 | ■ | ▶ Mutua autenticazione e affidabilità informativa in ambito smart mobility |
| 09/10/2023 | ■ | ▶ Internet of Military Things tra Cybersecurity e AI |
| 10/10/2023 | ■ | ▶ Principali cyber minacce e contromisure adeguate |
| 07/11/2023 | ■ | ▶ Le competenze per la cybersecurity e la gestione del fattore umano |
| 10/11/2023 | ■ | ▶ Introduzione al Cloud e rischi da considerare nell'adozione |
| 13/11/2023 | ■ | ▶ Il Cyber Resilience Act: una normativa trasversale per la sicurezza dei prodotti digitali |
| 21/12/2023 | ■ | ▶ La certificazione di prodotto e la cyber security |

Oggi parliamo trattiamo il tema della supply chain security perché è molto importante per le nostre aziende, organizzazioni e per l'intera società

Entro quest'ora vi avrò spiegato il perché e vi avrò dato qualche elemento utilizzabile operativamente

Come indicato nel programma, risponderemo a queste domande:

- Mi dovrei preoccupare della sicurezza dei miei fornitori?
- Cosa è obbligatorio fare al riguardo?
- Come faccio a verificare la sicurezza dei fornitori?
- Come posso organizzare il lavoro?
- Dove trovo altre informazioni per approfondire il tema?

1. Mi dovrei preoccupare della sicurezza dei miei fornitori?



La risposta è sì.
Vediamo perché

The screenshot shows a news article from the Red Hot Cyber website. The headline reads "Blocco immediato del ransomware". The main image features the Toyota logo engulfed in flames. Below the image, there's a sidebar with a "gofundme" button and links to newsletters. The footer contains social media icons and a link to a course on ethical hacking.

La produzione Toyota è bloccata in Giappone a causa di un attacco alla supply-chain di un fornitore di porta bicchieri

Si, avete letto bene. Un fornitore di Portabicchieri e connettori USB della Toyota sta fermando l'assemblaggio delle linee di produzione in Giappone. L'attacco informatico ha bloccato **14 stabilimenti Toyota e ha causato una perdita di 375 milioni di dollari**.

Il produttore giapponese di componenti per interni per auto **Kojima** è stato recentemente colpito da un attacco informatico che ha bloccato la sua produzione, generando un problema di approvvigionamento alla Toyota Motor.

Kojima è un fornitore chiave per i portabicchieri e per i connettori USB dei veicoli Toyota.

Si stima che l'arresto delle linee di assemblaggio per un giorno porterà a una riduzione della produzione di veicoli di **10.000 unità, pari al 5% del volume totale dei veicoli Toyota in un mese in Giappone**.

<https://www.redhotcyber.com/post/la-produzione-toyota-e-bloccata-in-giappone-a-causa-di-un-attacco-alla-supply-chain-di-un-fornitore-di-porta-bicchieri/>

Year	Cyber Attacks #
2019	52
2020	74
2021	134
Total	260

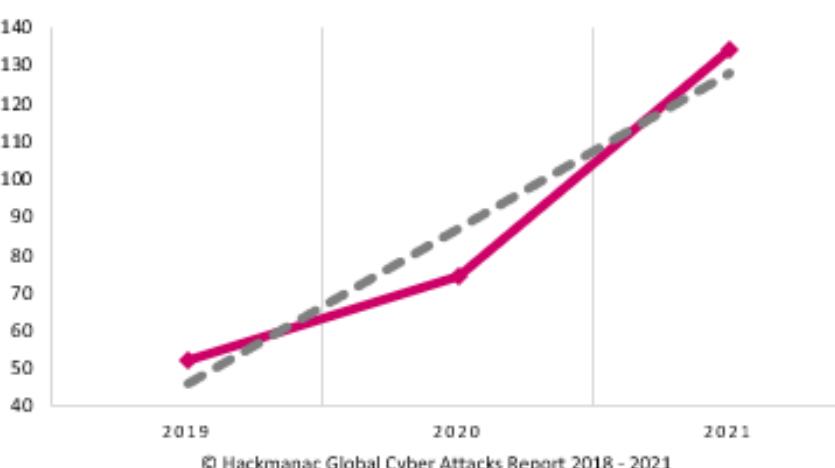
Attackers	Cyber Attacks #
Cybercrime	214
Espionage / Sabotage	43
Information Warfare	2
Hacktivism	1
Total	260

Targets	Cyber Attacks #
Healthcare	66
Government / Military / LE	57
ICT	42
Financial / Insurance	16
Transportation / Storage	16
Education	10
Wholesale / Retail	9
Multiple Targets	8
Professional / Scientific / Technic	8
Organizations	7
Arts / Entertainment	4
Hospitality	4
News / Multimedia	4
Manufacturing	3
Telecommunications	3
Energy / Utilities	2
Other Services	1
Total	260

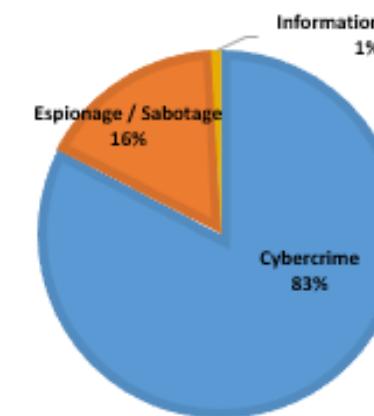
Geography	Cyber Attacks #
America	187
Europe	28
Asia	18
Multiple	17
Oceania	7
Africa	3
Total	260

Severity	Cyber Attacks #
Critical	85
High	121
Medium	54
Total	260

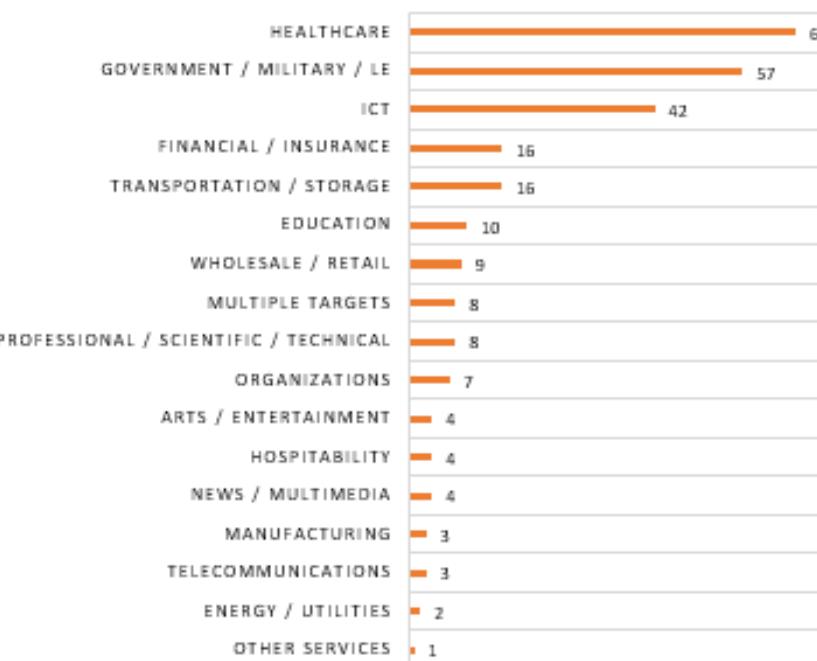
CYBER ATTACCHI VS SUPPLY CHAIN 2019-21



ATTACCANTI VS SUPPLY CHAIN 2019-21

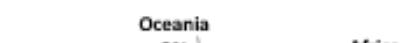


VITTIME VS SUPPLY CHAIN 2019-21



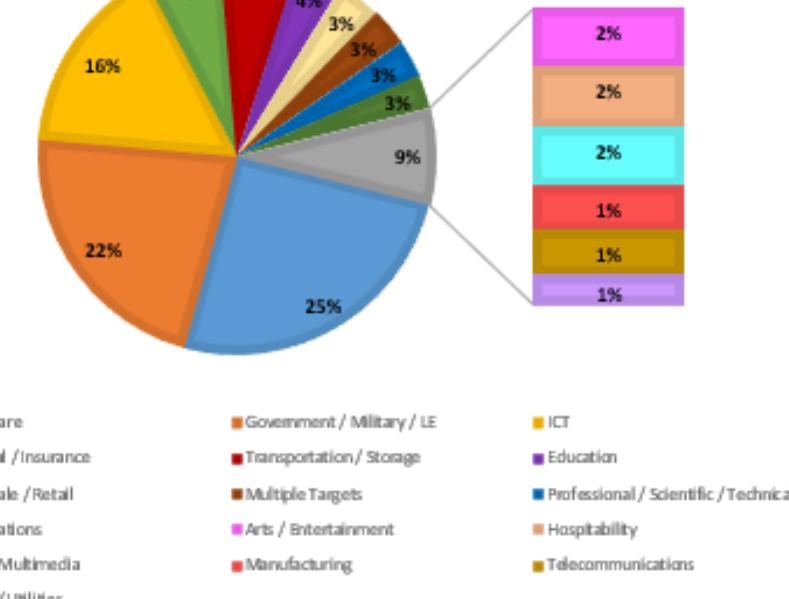
© Hackmanac Global Cyber Attacks Report 2018 - 2021

GEOGRAFIA DEGLI ATTACCHI 2019-21



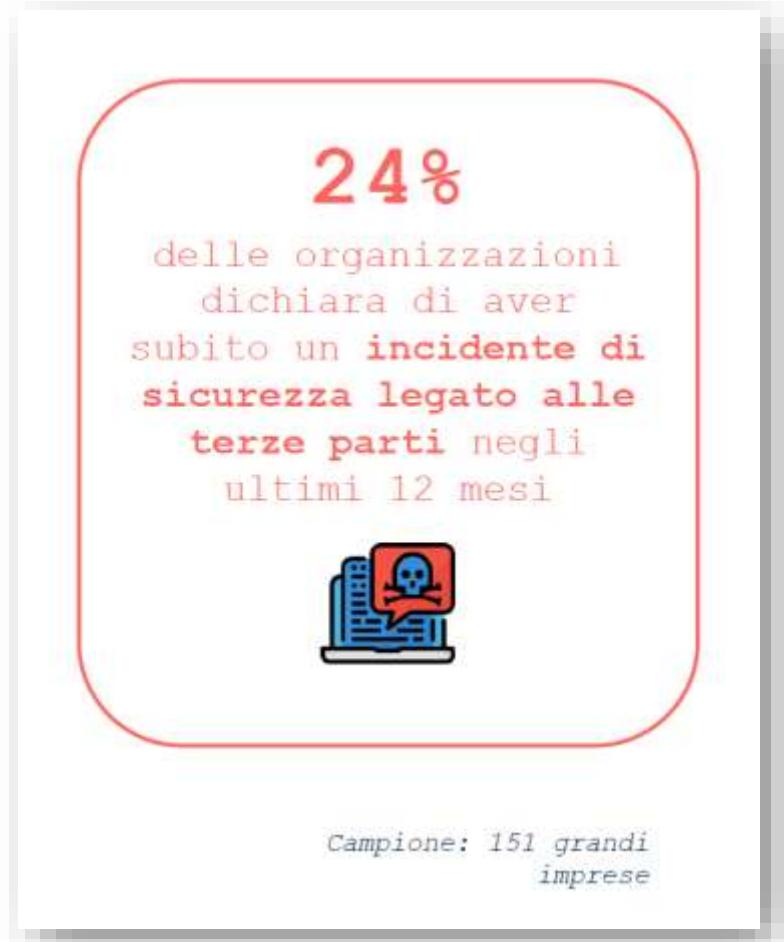
© Hackmanac Global Cyber Attacks Report 2018 - 2021

SEVERITY VS SUPPLY CHAIN 2019-21



© Hackmanac Global Cyber Attacks Report 2018 - 2021

Fonte: <https://hackmanac.com/>



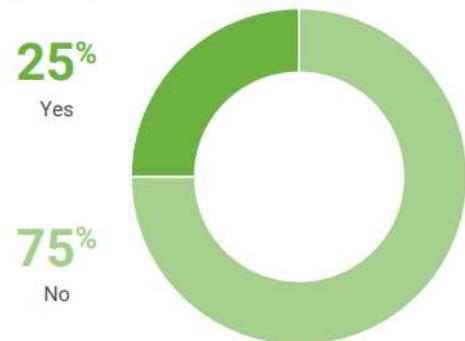
- Le grandi imprese sono meglio protette e più si possono accorgere prima dell'incidente di sicurezza
- Le aziende medie e piccole sono realmente alla mercé dei criminali e a volte non si accorgono nemmeno di essere violate

Fonte: Ricerca "Supply Chain Security" degli Osservatori del Politecnico di Milano

1 in 4 Have Experienced a Supply Chain Attack— And Near-term Improvement Is Unlikely for Many

Twenty-five percent of organizations report experiencing a supply chain attack in the last 12 months, according to the survey.

Has your organization experienced attacks on its digital supply chain in the past 12 months?



Supply chain issues are expected to persist for many organizations, with 53% saying issues will remain the same or worsen over the next six months.

Over the next six months, do you expect your organization's supply chain issues to improve, stay the same, or worsen?





Fonte: <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

Innumerevoli diverse survey confermano che molte organizzazioni hanno sofferto di incidenti originati da terze parti.

Ne hanno scritto:

- Clusit (in vari Rapporti) e Clusit Community for Security (libro)
- World Economic Forum
- Tutte le consulting company e i security vendor
- Molti analisti, blogger e altri ...

Tutti risuonano nello stesso modo (anche se c'è il solito marasma di numeri e, a volte, le fonti si citano le une con le altre)



Quindi la risposta è senz'altro sì!
Ma cosa mi può capitare?

A causa di un prodotto / servizio di un fornitore posso subire un incidente / avere un danno relativo alla:

- Sicurezza (riservatezza, integrità dei dati)
- Continuità operativa (disponibilità dei sistemi / dei prodotti)
- Conformità (norme e leggi, multe, ispezioni)
- Reputazione (verso i clienti, il pubblico)

2. Cosa è obbligatorio fare al riguardo?



Ci sono dei **tratti comuni** a diverse norme italiane e europee (GDPR, NIS e **NIS2**, PSNC, PCI-DSS, PSD2, **DORA**, Circolare 285 di Bdl, Regolamenti IVASS, MDR, circolari e linee guida di diverse autorità come EIOPA, EBA e ESMA ...) come:

- Il rischio cyber non si può più ignorare
- Deve aumentare la resilienza delle organizzazioni
- La responsabilità non si può esternalizzare e rimane in capo all'organizzazione
- I fornitori devono essere valutati / auditati
- I contratti devono avere certe caratteristiche
- Devono essere previsti dei piani di sostituzione (exit plan)
- Bisogna avere i «registri» e censire ogni rapporto significativo
- Bisogna valutare i rischi per definire le misure da implementare
- Bisogna segnalare gli incidenti alle autorità
- Bisogna fare test di resilienza e formazione del personale
- Bisogna condividere le informazioni



Ogni norma ha un obiettivo, un ambito di applicabilità e delle sanzioni specifiche che devono essere considerate. Alcune sono state approvate recentemente ed entreranno in vigore tra qualche mese.

E' evidente che serve un approccio multidisciplinare per affrontare efficacemente e efficientemente questo ambito; servono esperti di molte discipline

- Cybersecurity
- Privacy
- Risk management
- Legal e contratti
- Audit
- Procurement
- Organizzazione e project management

3. Come faccio a verificare la sicurezza dei fornitori?



Chiedo loro di rispondere a dei questionari

B	C	D	E	F	G
51	Audit Logging / Intrusion Detection	IVS-01.1 Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation and response to incidents?		lavoro da remoto?	
52		IVS-01.2 Is physical and logical user access to audit logs controlled by audit personnel?		Q.16	Per le attivazioni su device aziendali, sono state implementate le seguenti misure di sicurezza:
53		IVS-01.5 Are audit logs reviewed on a regular basis for analysis using automated tools?			<input type="checkbox"/> disk Encryption <input type="checkbox"/> DLP <input type="checkbox"/> MDM (Mobile device Management) <input type="checkbox"/> AV con firewall <input type="checkbox"/> Connessione con VPN con 2FA (OTP/authenticator) ovvero altra modalità di connessione attivata (es.accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)
54	Clock Synchronization	IVS-03.1 Do you use a synchronized time-service provider to have a common time reference?		Q.17	Per le attivazioni in BYOD, sono state implementate le seguenti misure di sicurezza:
55	OS Hardening and Base Controls	IVS-07.1 Are operating systems hardened to provide security and services to meet business needs using techniques such as integrity monitoring, and logging) as part of the security architecture?			<input type="checkbox"/> rilascio di agent sulle macchine degli users <input type="checkbox"/> revoca privilegi amministratore <input type="checkbox"/> Verifica presenza AV con firewall con preventiva scansione <input type="checkbox"/> Rilascio di soluzione di connessione con VPN con 2FA (OTP/authenticator) ovvero altra modalità di connessione attivata (es.accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)
56	Production / Non-Production Environments	IVS-08.1 For your SaaS or PaaS offering, do you provide environments for production and test processes?			
57		IVS-08.3			
58	Segmentation	IVS-09.1			
59	VMM Security - Hypervisor Hardening	IVS-11.1 Does the organization use encapsulated communications to the administrator to protect the hypervisor?			
	Wireless Security	IVS-12.1 Are policies and procedures established and implemented to protect the wireless network?		Q.22	L'organizzazione ha implementato e diffuso una password policy che garantisca e applichi un adeguato livello di protezione per i dati sensibili?
					<input type="checkbox"/> si <input type="checkbox"/> no

Risposte: chiuse o aperte
Evidenze indicate: possibili / obbligatorie

I questionari sono derivati liberamente dalle aziende da innumerevoli fonti; es.:

- ISO/IEC 27001 e ISO/IEC 27002, ecc.
- NIST Special Publication 800-53, ecc.
- Framework Nazionale per la Cybersecurity e la Data Protection
- CSA CAIQ
- Center for Internet Security (CIS) Controls
- CMMC (Cybersecurity Maturity Model Certification)
- Health Insurance Portability and Accountability Act (HIPAA)
- OWASP Top 10
- PCI-DSS
- Shared Assessment SIG
- AICPA SOC (American Institute Certified Public Accounts - System and Organization Controls)
- ecc.

I pregi di questo approccio sono:

1. Facile punto di partenza nel percorso di miglioramento continuo
2. Incremento della consapevolezza reciproca
3. Possibile introduzione di clausole di tutela nei contratti
4. Possibilità di dimostrare la propria responsabilizzazione

I difetti di questo approccio sono:

1. Domande non chiare o non contestualizzate e non applicabili
2. Risposte soggettive, parziali, pretestuose
3. Per il fornitore è oneroso compilarli; per il cliente è oneroso controllarli
4. Arbitrarietà rispetto a come trattare i gap; «sei il mio nemico»
5. Mancanza di standardizzazione; impossibile interoperabilità
6. Processo manuale / tool di office automation

SEZIONE	CODICE	DOMANDA	RIFERIMENTI		RISPOSTE (A SCELTA MULTIPLA)
			ISO/IEC 27001	FNCS	
	GSI.01	La politica di alto livello che tratta la cybersecurity / sicurezza delle informazioni / sicurezza informatica è:	5.2	ID.GV-1	Inclusiva di obiettivi e principi Approvata dall'alta direzione Resa disponibile a tutti i soggetti interni ed esterni rilevanti Aggiornata almeno annualmente Non formalizzata in un documento
	GSI.02	Esistono politiche e procedure verticali collegate alla politica di alto livello, che normano i seguenti processi principali:	A.5.1	PR.AC-2 PR.AC-1 Uso accettabile delle risorse IT Gestione degli aggiornamenti PR.IP-1 Gestione dei cambiamenti Sviluppo sicuro del software PR.IP-2 ID.AM-5 ID.PT-1 DP-ID.DM-1 ID.SC-1	Gestione degli incidenti Controllo degli accessi fisici Controllo degli accessi logici Gestione degli aggiornamenti Gestione dei cambiamenti Sviluppo sicuro del software Gestione del ciclo di vita dei sistemi Classificazione delle informazioni Gestione dei log Ciclo di vita dei dati Gestione dei fornitori
REZZA	GSI.03	Esiste un piano per la gestione della continuità operativa?	A.5.30	PR.IP-9 PR.IP-10 RC.RP-1 RC.IM-1 RC.IM-2 PR.IP-4 PR.DS-4 PR.PT-5 PR.IP-9	Si e viene testato con periodicità almeno annuale Si e include la parte IT con una Business Impact Analysis ad esso relativa Si e prevede un piano di disaster recovery per i servizi critici Si ed è mantenuto aggiornato almeno annualmente No Mantenimento di una terza copia di backup dei dati in un sito remoto Allocazione di risorse dimensionate in modo da garantire sempre la disponibilità dei servizi critici Ridondanza locale di tutti i sistemi critici adottando soluzioni ad alta disponibilità Ridondanza geografica di tutti i sistemi critici in un sito remoto situato a più di 100 km dal sito principale
	GSI.04	La continuità operativa dei sistemi ICT è assicurata tramite:	A.5.30	ID.AM-6 ID.GV-2 RS.CO-1	Sono assegnate ad un Responsabile della Sicurezza delle Informazioni / Sono assegnate a chi gestisce dei sistemi informativi per garantirne la disponibilità e la qualità dei dati / Sono assegnate a tutto il personale affinché le informazioni e i sistemi siano protetti / Sono assegnate alle terze parti che hanno un ruolo nella protezione delle informazioni / Sono assegnate a chi deve intraprendere azioni specifiche in caso di emergenza / Sono documentate e mantenute aggiornate / Non sono formalmente assegnate o documentate
	GSI.05	Le responsabilità in merito alla cybersecurity / sicurezza delle informazioni / sicurezza informatica:	A.5.2	DP-ID.AM-7	Sono assegnate ad un Privacy Officer/Manager o equivalente / Sono supportate dalla presenza di un Data Protection Officer / Sono assegnate ai Dirigenti delle aree in cui sono trattati dati personali / Sono assegnate alle terze parti che agiscono in qualità di Responsabili / Sono documentate e mantenute aggiornate / Non sono formalmente assegnate o documentate / Con cadenza almeno annuale
	GSI.06	Le responsabilità in merito alla protezione dei dati personali:	-	PR.AT-1	Sono assegnate ad un Privacy Officer/Manager o equivalente / Sono supportate dalla presenza di un Data Protection Officer / Sono assegnate ai Dirigenti delle aree in cui sono trattati dati personali / Sono assegnate alle terze parti che agiscono in qualità di Responsabili / Sono documentate e mantenute aggiornate / Non sono formalmente assegnate o documentate / Con cadenza almeno annuale

CLUSIT, associazione Italiana per la Sicurezza Informatica, considerando le notevoli problematiche ed inefficienze che interessano questo ambito, ha attivato un gruppo di lavoro per redigere un questionario di riferimento, a supporto universale delle organizzazioni di ogni tipo, per la selezione di fornitori ICT in generale e di prodotti e servizi in particolare, al fine di permettere di verificare agevolmente il loro grado di sicurezza delle informazioni/sicurezza ICT/cybersecurity e, attraverso le risposte, dare dimostrazione dei requisiti applicabili in conformità alle best practice di settore e in linea con la strategia dell'organizzazione.

Il questionario riportato nel foglio successivo si articola in 47 domande, a risposta chiusa e multipla, che mirano a verificare i principali requisiti previsti da ISO/IEC 27001 (Sistema di Gestione per la Sicurezza delle Informazioni) e FNCS (Framework Nazionale di Cyber Security) in termini di Servizi ICT e prodotti ICT (i.e. software e hardware).

L'organizzazione, una volta deciso quale domande e quali risposte proporre ai fornitori (idealmente tutte ma può essere scelto di utilizzarne solo un sottoinsieme) al completamento del questionario da parte del fornitore, sarà in grado di individuare i punti di debolezza/non conformità e, conseguentemente, richiedere le necessarie azioni sul fornitore in modo tale da garantire la propria cybersecurity.



Cerco su di loro delle informazioni con dei tool automatici che operano dall'esterno

Rating Overview

Rating Overview Panel shows how well this company is managing each risk vector. Click on a risk vector to see more details about the risk.

Compromised Systems

Botnet Infections	A
Spam Propagation	A
Malware Servers	A
Unsolicited Communications	A
Potentially Exploited	A

User Behavior

File Sharing	A
Exposed Credentials **	N/A

Public Disclosures

Security Incidents/Breaches	A
Other Disclosures *	N/A

Diligence

SPF Domains	A
DKIM Records	A
TLS/SSL Certificates	A
TLS/SSL Configurations	A
Open Ports	A
Web Application Headers	B

Patching Cadence

Insecure Systems	A
Server Software	A

Desktop Software

Mobile Software	N/A
DNSSEC *	C
Mobile Application Security *	N/A
Domain Squatting **	N/A



Total Potential Vulnerabilities

464

Low Severity

33

Medium Severity

346

High Severity

85

Subdomains found

267

IP found

91

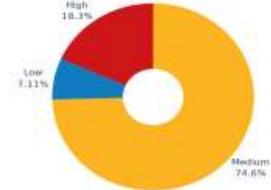
Compromised emails

2430

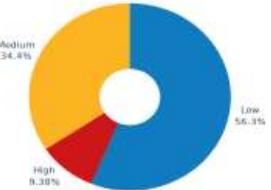
Compromised Emails Sources

32

Technology Risk (potential vulnerability by risk)



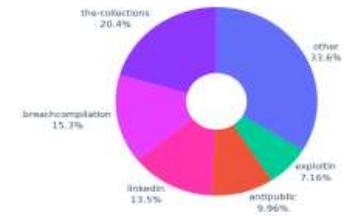
Social Risk (breaches by risk)



GDPR Risk (confidentiality, availability and integrity impact)



Breach Source (breaches chart)



I pregi di questo approccio sono:

1. Completamente automatico
2. Incremento della consapevolezza reciproca
3. Possibilità di dimostrare la propria responsabilizzazione

I difetti di questo approccio sono:

1. Output non contestualizzato, a volte irrilevante
2. Analisi esclusivamente tecnologica
3. Condotta senza la collaborazione del fornitore
4. Alto numero di falsi positivi
5. Arbitrarietà rispetto a come trattare i gap; «sei il mio nemico»



Integro i due approcci e aumento il valore

Integro i due approcci e aumento il valore

Webinar
13.12.22

SCORE
Security and Compliance
Overall Risk Evaluation

HOME / REPORT

Fornitore 17 di Acme 01234567899 (it)

Valutazione svolta il 8/9/2022 11:47:39

Punteggio totale 51%

Utente che ha materialmente fornito i dati:
Jeff Bezos (admin@acme.net)

Persona che ha fornito i dati per la valutazione:
Paolo Rossi

I dati sono stati forniti per fare una prova

Scarica il report di dettaglio

Inserisci un indirizzo e-mail per inviare il report
example@example.com

Domanda	Risposta	Suggerimenti
Inserisci il nome dell'azienda	Acme s.r.l.	
Seleziona la tua nazione	it	
Inserisci la partita IVA	01234567899	
L'azienda ha il sito web?	Si	
Per favore inserisci l'indirizzo	https://acme.net	
L'azienda fornisce la connessione Wi-Fi alla rete?	Si	
Hai il Wi-Fi per gli ospiti?	Si limitato a Internet	
Viene eseguito il backup dei sistemi aziendali?	No	<input type="button" value="Suggerisci"/>
Il backup è automatico?		
Il backup è remoto?		
È presente un documento che descrive come vengono eseguiti i backup?		
Per favore, se puoi, caricalo		
I collaboratori usano device personali collegati alla rete aziendale?	Si; solo un numero ristretto di dipendenti	<input type="button" value="Suggerisci"/>
I computer aziendali hanno l'hard disk cifrato?	Si; assolutamente tutti i PC portatili e anche i PC fissi	<input type="button" value="Suggerisci"/>

I pregi di questo approccio sono:

1. Facile punto di partenza nel percorso di miglioramento continuo
2. Completamente automatico
3. Valutazione tecnica e anche organizzativa
4. Incremento della consapevolezza reciproca e suggerimenti per migliorare
5. Possibilità di dimostrare la propria responsabilizzazione

I difetti di questo approccio includono:

1. Output non contestualizzato, a volte non applicabile
2. Analisi superficiale

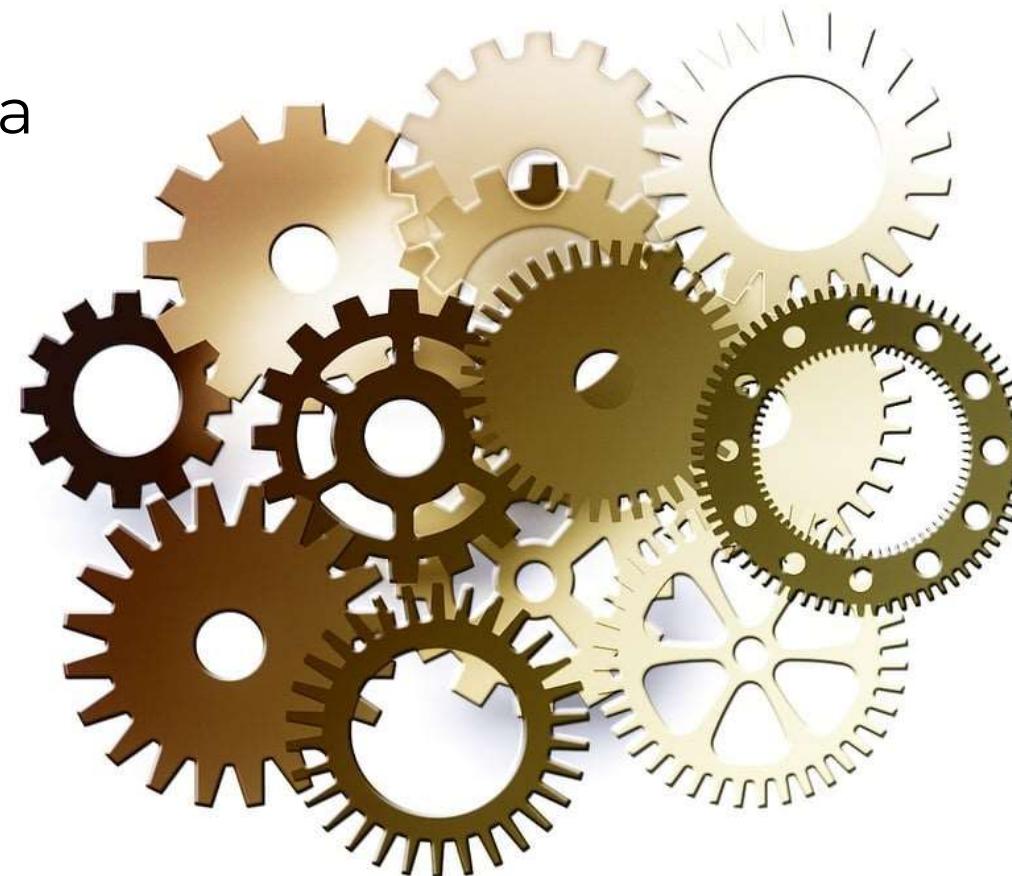
4. Come posso organizzare il lavoro?

E' utile comprendere lo specifico contesto interno ed esterno della mia organizzazione

- Il ruolo multiplo nella relazione cliente – fornitore – subfornitore
- L'esposizione al rischio, inteso come motivazione delle possibili minacce (cybercrime; state-sponsored actor; hacktivist; hacker-for-hire)
- Il valore delle informazioni (RID)
- Lo stato attuale della cybersecurity e della supply chain (vulnerabilità e misure di sicurezza)
- Gli obblighi di conformità



La mia sicurezza
dipende da me



E dipende dalla
sicurezza dei miei
fornitori

E condiziona la sicurezza dei miei clienti

La sicurezza dei miei fornitori è da me percepita

LIVELLO DELLA MIA SICUREZZA \ DEL FORNITORE	Fornitore ha scarsa sicurezza	Fornitore ha buona sicurezza
La mia sicurezza è effettivamente		
La mia è scarsa	Lavoro urgentemente su di me; sollecito i fornitori di fare altrettanto	Lavoro urgentemente su di me; mi faccio aiutare dai fornitori, faccio squadra
La mia è buona	Creo un programma di verifica dei Continuo a migliorare i processi e le tecnologie	

Lavoro su di me? Lavoro su di loro?

Il danno che potrei provocare ai miei clienti è da loro percepito

La mia sicurezza è percepita	PERCEZIONE DEL CLIENTE RISPETTO ALLA MIA SICUREZZA E AL DANNO ARRECABILE	Posso procurare un danno alto	Posso procurare un danno basso
	Sono percepito insicuro	Mi devo aspettare controlli e verifiche severe; rischio di perdere il cliente	Mi devo aspettare controlli e verifiche severe; mi chiederanno di migliorare
Sono percepito sicuro	Mi devo aspettare controlli e verifiche severe dai clienti	Si concentreranno in primis su altri	

Rischio anche di perdere i clienti?

Il livello di sicurezza del mio fornitore		
RISCHIO DEL PRODOTTO SERVIZIO ACQUISTATO \ CARATTERISTICHE DEL FORNITORE	Fornitore è grande, affidabile, strutturato, certificato	Fornitore piccolo o impreparato
Il rischio della fornitura nel mio contesto	Priorità media	PRIORITÀ ALTA
Il rischio della fornitura è basso	Priorità bassa	Priorità media

Per prioritizzare gli interventi ...



Alcune considerazioni specifiche

Il rischio è alto quando, a causa di un prodotto / servizio di un fornitore posso subire un incidente / avere un danno relativo alla:

- Sicurezza (riservatezza, integrità dei dati)
- Continuità operativa (disponibilità dei sistemi e dei prodotti)
- Conformità (norme e leggi, multe, ispezioni)
- Reputazione (verso i clienti, il pubblico)

che è reputato eccedere il risk appetite ...

... servirebbe un approccio risk based

+ Data protection

Nelle situazioni di monopolio di fatto / di legge il fornitore non è normalmente disposto a collaborare

- ma spesso espone delle certificazioni di cybersecurity e della documentazione di security sui loro siti
- Inoltre, le autorità di controllo tendono a verificare / controllare i requisiti di security

E' quindi solo necessario / possibile avere consapevolezza dei loro limiti, controllare la documentazione disponibile, avere cognizione delle clausole contrattuali

I (grandi) cloud provider sono spesso non collaborativi

Oltre a quanto appena detto è necessario:

- Comprendere la shared responsibility
- Disporre di un exit plan (+semplice IaaS; molto complesso per il SaaS)

Normalmente durante la qualificazione del fornitore vengono chiesti numerosi documenti come

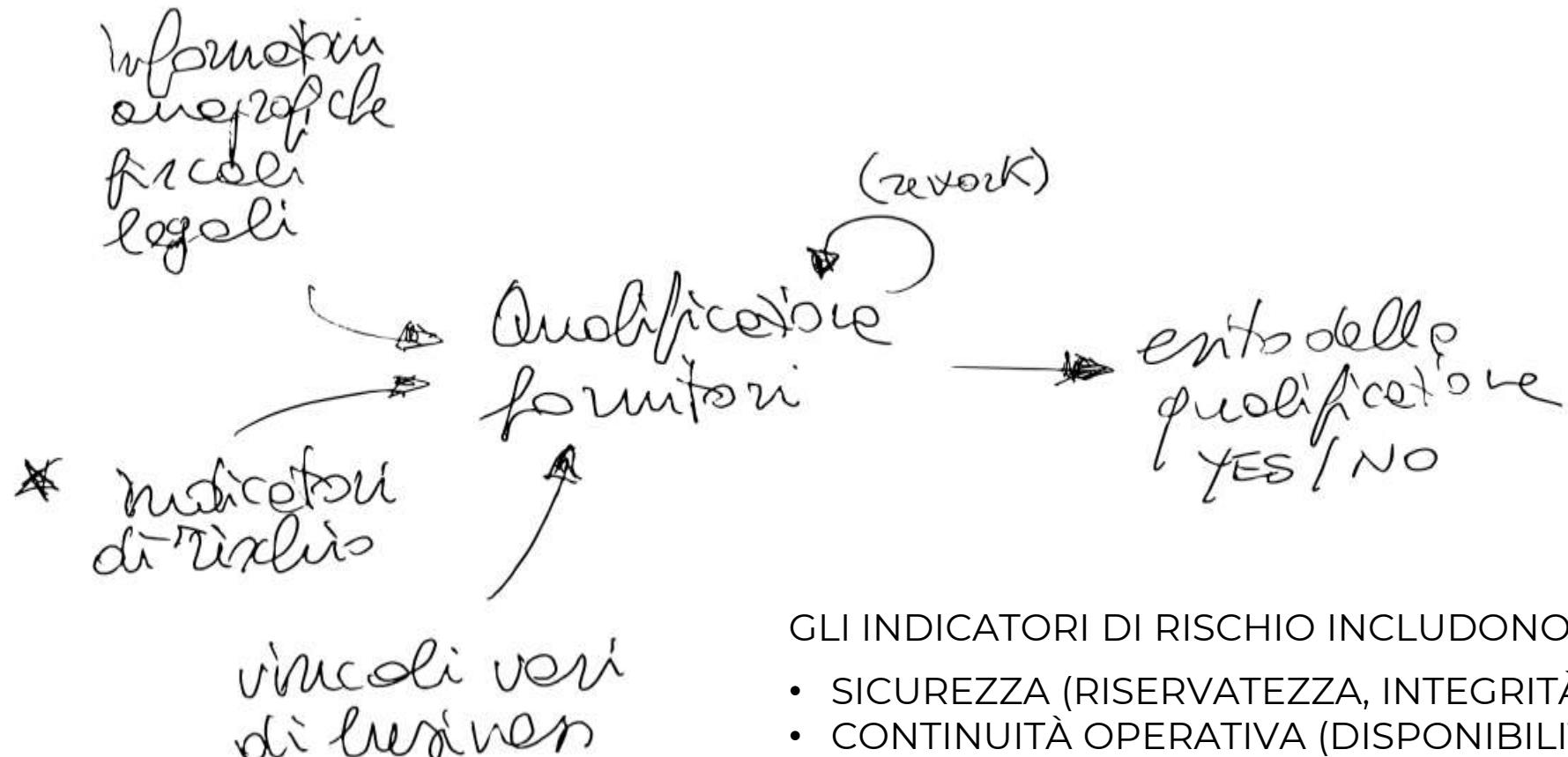
- Visura camerale, ultimi bilanci, dati bancari
- Dichiarazione antiriciclaggio, dichiarazione unica regolarità contributiva
- Composizione aziendale, brochure aziendale, mail e telefono del responsabile, documento del rappresentante legale

allo scopo di verificare l'affidabilità economica e prevenire i rischi di frode e di conformità.

Nessun controllo sulla resilienza cyber!!

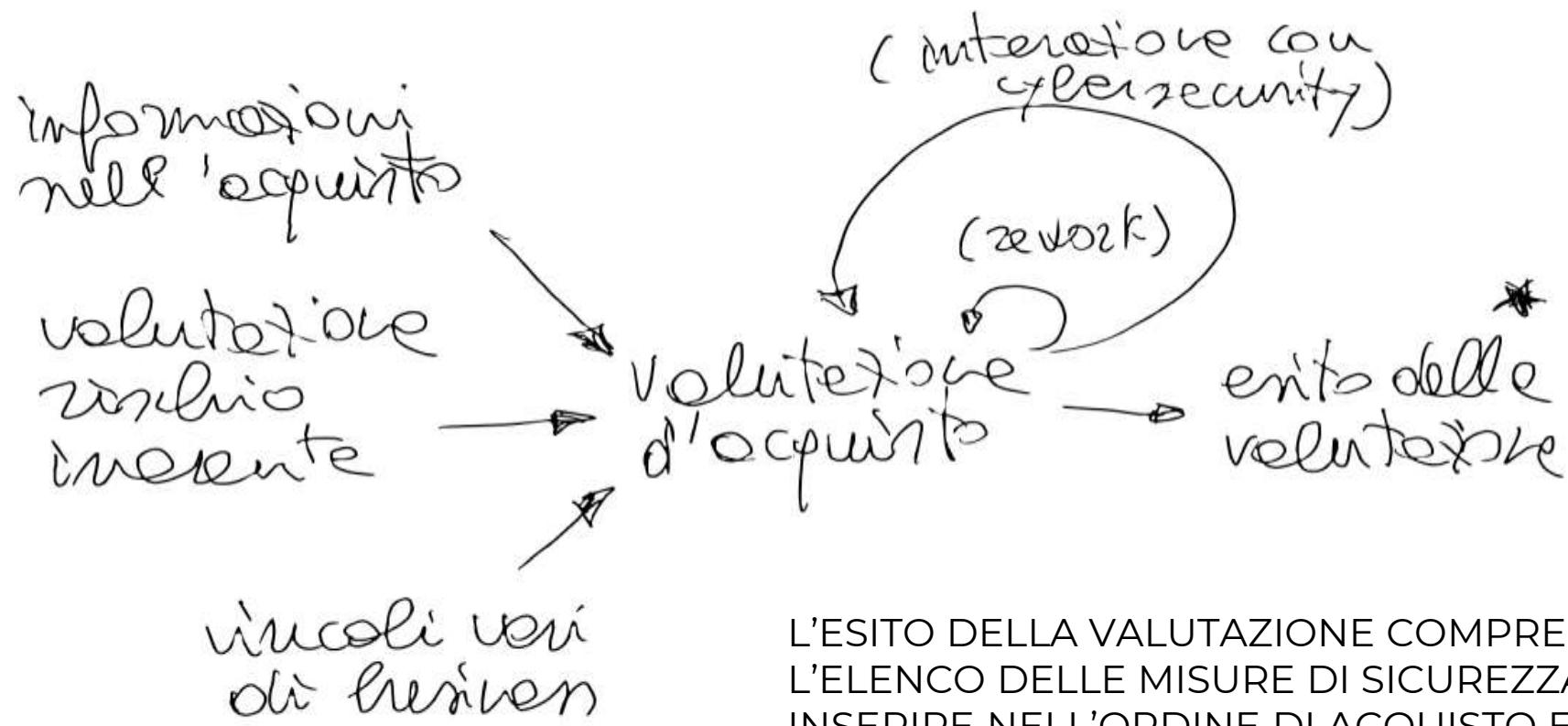


Modificare i processi



GLI INDICATORI DI RISCHIO INCLUDONO:

- SICUREZZA (RISERVATEZZA, INTEGRITÀ DEI DATI)
- CONTINUITÀ OPERATIVA (DISPONIBILITÀ DEI SISTEMI)
- CONFORMITÀ (NORME E LEGGI, MULTE, ISPEZIONI)
- REPUTAZIONE (VERSO I CLIENTI, IL PUBBLICO)



L'ESITO DELLA VALUTAZIONE COMPRENDE
L'ELENCO DELLE MISURE DI SICUREZZA DA
INSERIRE NELL'ORDINE DI ACQUISTO E,
EVENTUALMENTE, LA DATA ULTIMA
ACCETTABILE DI RIMEDIO



volete? sì
(piano di
audit)



notizie ed
eventi

SE LA VERIFICA DA' ESITO NEGATIVO SI
ATTIVA IL PROCESSO DI ESCALATION E DI
CONTENZIOSO



Serve coinvolgere

- Cybersecurity
- Privacy
- Risk management
- Legal e contratti
- Audit
- **Procurement**
- Organizzazione e project management

Serve integrare i sistemi informativi

- A supporto **degli acquisti** (IT)
- Per il governo del rischio, della compliance e della security

5. Dove trovo altre informazioni per approfondire il tema?

Clusit Community For Security

Documentazione per la sicurezza informatica delle aziende

Il nostro impegno è produrre documentazione di qualità e renderla disponibile gratuitamente per aiutare le aziende ad affrontare temi importanti: come fare e cosa fare per aumentare la sicurezza e la compliance e comprendere il rischio e le best practice.

Le nostre pubblicazioni

Supply Chain SECURITY
L'importanza di conoscere e gestire i rischi della catena di forniture
data pubblicazione: marzo 2023
Rischio digitale
Innovazione e Resilienza
Conoscere, ottimizzare e mitigare i rischi digitali
data pubblicazione: marzo 2022
INTELLIGENZA ARTIFICIALE E SICUREZZA
OPPORTUNITÀ, RISCHI E RACCOMANDAZIONI
data pubblicazione: marzo 2021
IoT Security e Compliance
Gestire la complessità e i rischi
data pubblicazione: marzo 2020
CONSAPEVOLMENTE CLOUD
Guida per l'azienda che deve affrontare l'introduzione con le nuove cloud
data pubblicazione: marzo 2019
SOC E CONTINUOUS MONITORING
FACCIA A FACCIA CON LA CYBERSECURITY
Il continuo monitoring è necessario perché i business non dormono mai
data pubblicazione: marzo 2018

Cloud security
data pubblicazione: marzo 2023
PIN PROTECTED
Enter Your PIN
Press BACK
data pubblicazione: marzo 2022
La Sicurezza nei
nuovi servizi cloud
data pubblicazione: marzo 2021
SECURITY PROTECTION
data pubblicazione: marzo 2020
data pubblicazione: marzo 2019

Componente: 8200 - Che fare - Prodotti per l'analisi del rischio di fornitura

Versione: 1

Autori: Giuseppe Cusello, Franco Marconcini, Angelo Bosis, Luca Zam-marchi

TLR: Alessandro Vallega

ProcessUnity	https://www.processunity.com/	Leaders	Customer's Choice
Red Piranha	https://redpiranha.net/	Not rated	Strong Performer
RiskRecon	https://www.riskrecon.com/	Not rated	Aspiring
SCORE (Rexilience)	https://score.rexilience.eu/	Not rated	Not rated
SecurityScorecard	https://securityscorecard.com/	Not rated	Customer's Choice
ServiceNow	https://www.servicenow.com/	Leaders	Established
Swascan	https://www.swascan.com/	Not rated	Not rated
UpGuard	https://www.upguard.com/	Not present	Established

Prodotto	URL	Forrester	Gartner
Allgress	https://allgress.com/	Not rated	Aspiring
Aravo	https://aravo.com/	Strong Performers	Strong Performer
Archer	https://www.archerirm.com/	Strong Performers	Aspiring
BitSight	https://www.bitsight.com/	Not rated	Customer's Choice
Black Kite	https://blackkite.com/	Not rated	Customer's Choice
Coupa	https://www.coupa.com/	Contenders	Not rated
CyberGRX	https://www.cybergrx.com/	Not rated	Strong Performer
	https://www.mastercard.ca/en-ca/business/large-enterprise/safety-security/cyber-solutions/cyber-quant.html		
Cyber Quant (MasterCard)		Not rated	Not rated
Diligent (Galvanize)	https://www.diligent.com/	Strong Performers	Strong Performer
LogicManager	https://www.logicmanager.com/	Contenders	Not rated
LogicGate	https://www.logicgate.com/	Strong Performers	Not rated
MetricStream	https://www.metricstream.com/	Strong Performers	Not rated
NAVEX	https://www.navex.com/	Strong Performers	Not rated
OneTrust	https://www.onetrust.com/	Leaders	Customer's Choice
Panorays	https://panorays.com/	Not rated	Strong Performer
Prevalent	https://www.prevalent.net/	Strong Performers	Customer's Choice

La tabella sintetizza quanto indicato nei report 2022 sul Third-Party Risk Management di Forrester Research (1) e di Gartner (2).

Il report di Forrester Research valuta i top vendor presenti sul mercato usando le quattro classificazioni decrescenti: **Leaders, Strong Performers, Contenders e Challengers**. L'analisi è svolta utilizzando 21 indicatori che valutano Offerta Corrente, Strategia e Presenza di Mercato.

Il report "Voice of the Customer" di Gartner aggrega le recensioni dei decisori IT sui vari prodotti. Le recensioni sono riclassificate come:

- **Customer's Choice:** soddisfa o supera sia la valutazione complessiva media del mercato sia l'interesse e l'adozione medi degli utenti del mercato.
- **Established:** soddisfa o supera la media di mercato dell'interesse e dell'adozione degli utenti, ma non soddisfa la media di mercato della valutazione complessiva.

(1) "The Forrester Wave™: Third-Party Risk Management Platforms, Q2 2022. The 12 Providers That Matter Most and How They Stack Up", May 16, 2022.

(2) "Gartner Peer Insights 'Voice of the Customer': IT Vendor Risk Management Tools", March 2, 2022 - ID G00763741

Bisogna

1. gestire il rischio delle terze parti per obbligo normativo e **per ovvio interesse aziendale**
2. Bisogna distinguere e integrare diversi approcci a seconda dei casi
3. Bisogna coinvolgere diverse strutture aziendali per rendere efficace ed efficiente la nuova gestione



Cybersecurity & Data Protection (2023)

- | | | |
|-------------------|----------|---|
| 17/03/2023 | ■ | ▶ Il mercato della Cybersecurity e lo scenario in Italia e a livello internazionale |
| 21/03/2023 | ■ | ▶ Dall'incidente alla gestione della crisi |
| 30/03/2023 | ■ | ▶ Lo scenario dei cyber attacchi: evoluzione delle minacce e principali trend |
| 26/04/2023 | ■ | ▶ Il contesto generale della cybersecurity: cyber war e cambiamento della situazione a livello geopolitico |
| 28/04/2023 | ■ | ▶ Vulnerabilità, Vulnerability Assessment e Penetration Test: cosa sono e come gestirli |
| 10/05/2023 | ■ | ▶ Come affrontare praticamente la sicurezza della fornitura |
| 05/06/2023 | ■ | ▶ Trend digitali e nuove tendenze per la cybersecurity |
| 14/06/2023 | ■ | ▶ Rafforzare la "Security culture" per ridurre il rischio legato al fattore umano |
| 07/07/2023 | ■ | ▶ La gestione del rischio cyber e dei rischi connessi alla filiera aziendale |
| 12/07/2023 | ■ | ▶ Digital Operational resilience Act (DORA): struttura, principali novità introdotte e raccordo con le principali normative nazionali ed europee in ambito bancario e finanziario |
| 15/09/2023 | ■ | ▶ Mutua autenticazione e affidabilità informativa in ambito smart mobility |
| 09/10/2023 | ■ | ▶ Internet of Military Things tra Cybersecurity e AI |
| 10/10/2023 | ■ | ▶ Principali cyber minacce e contromisure adeguate |
| 07/11/2023 | ■ | ▶ Le competenze per la cybersecurity e la gestione del fattore umano |
| 10/11/2023 | ■ | ▶ Introduzione al Cloud e rischi da considerare nell'adozione |
| 13/11/2023 | ■ | ▶ Il Cyber Resilience Act: una normativa trasversale per la sicurezza dei prodotti digitali |
| 21/12/2023 | ■ | ▶ La certificazione di prodotto e la cyber security |



Alessandro Vallega

Founding Partner Rexilience S.r.l.

Fondatore e Chairman Clusit Community for
Security

Comitato Direttivo Clusit

Professore a contratto corso di Analisi e Gestione
del Rischio (Università degli studi di Milano / Laurea magistrale
di sicurezza informatica)

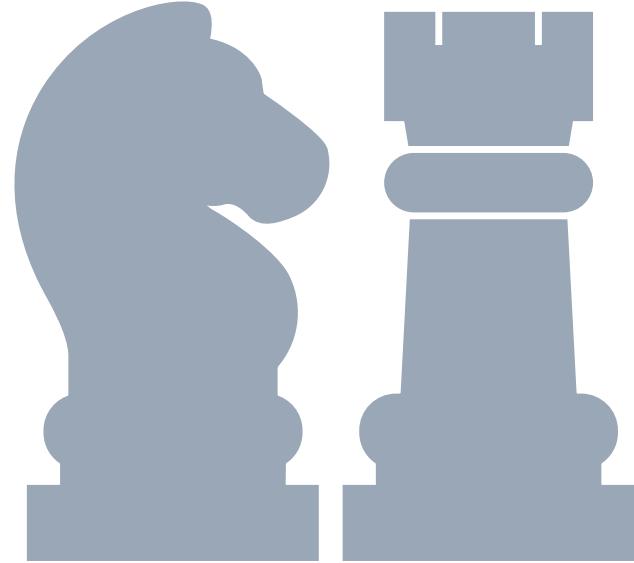
alessandro.vallega@rexilience.eu



10.05.2023
Webinar

Come affrontare praticamente la sicurezza della fornitura

PARTE 4 - IL CISO (CHIEF INFORMATION SECURITY OFFICER)



Chief information security officer (CISO)

Security director (CSO)

Security manager

Security architect

Security analyst

Security administrator

Security specialist

Secure code auditor

Security consultant

Computer Security Incident Responder

Forensics expert

Intrusion Detection Specialist

Security engineer

Security auditor

Vulnerability assessor

Penetration tester

Argomenti

Riepilogo di quanto visto finora

Chi è il CISO e cosa ha di fronte



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



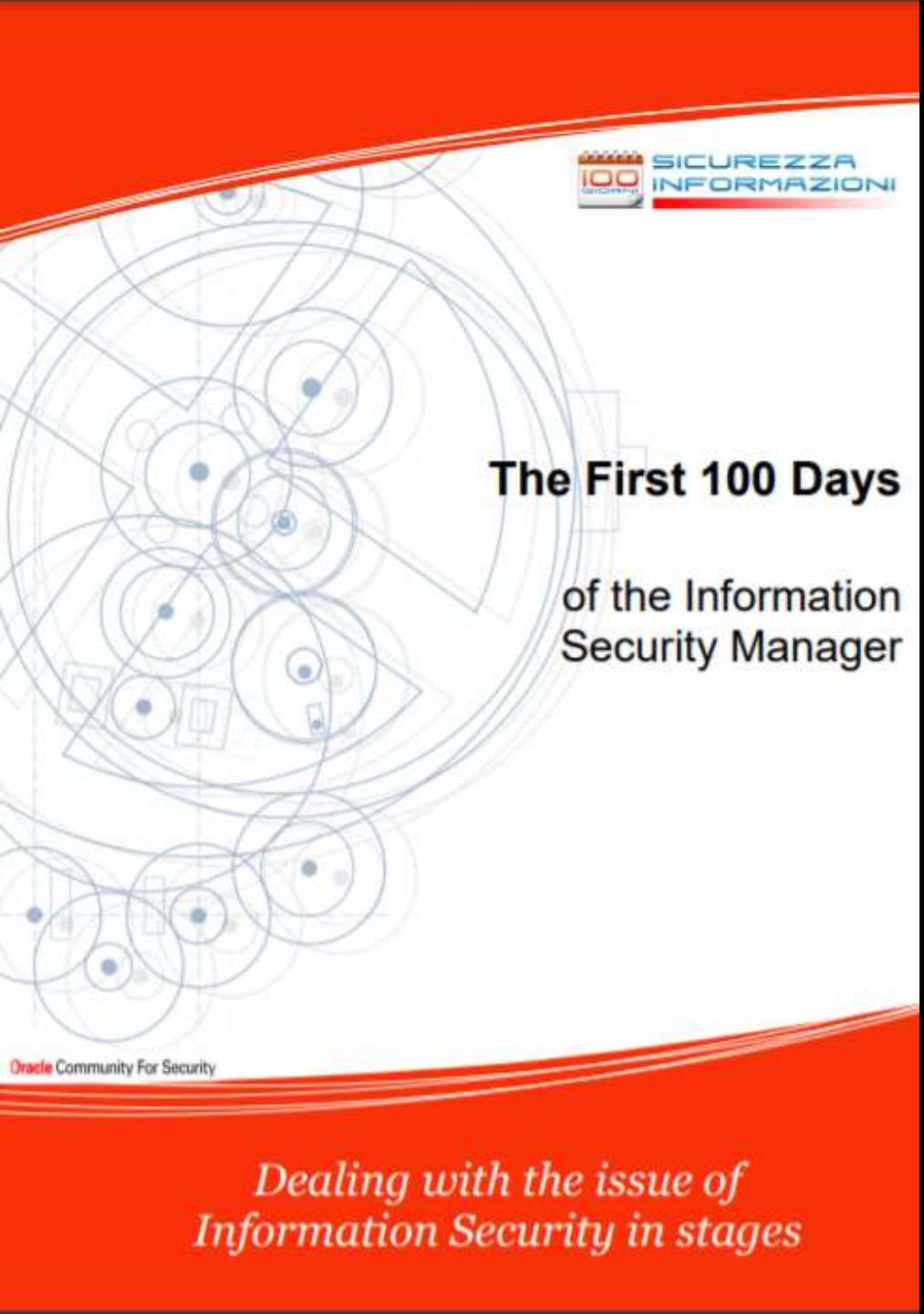
Riepilogo di quanto visto finora

1. Il cybercrime è un problema serio e concreto
2. Il nostro operato avviene all'interno delle organizzazioni. Abbiamo bisogno di capire come sono fatte le aziende
3. Abbiamo capito cos'è il risk management e come organizzare un processo di risk management
4. Il risk management aumenta la probabilità di successo delle organizzazioni. Introduce un po' di razionalità nella gestione
5. Abbiamo visto cos'è l'information security e cosa sono gli information security management system
6. Ci siamo addentrati in una specifica lista di possibili controlli
7. Per qualche ambito specifico (i verticali), abbiamo visto alcuni degli errori comuni di gestione e i rischi tipici...



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 tempo fruibili.



*Dealing with the issue of
Information Security in stages*

Clusit Community for Security; The first 100 days of the Information Security Manager

[HTTPS://100DAYS.CLUSTIT.IT/#/DOWNLOAD](https://100days.clusit.it/#/DOWNLOAD)

OPTIONAL Free



I Primi 100 giorni
del Responsabile della
Sicurezza delle Informazioni

*Come affrontare il problema della
Sicurezza informatica per gradi*

Clusit Community for Security; I primi 100 giorni del Responsabile della Sicurezza delle Informazioni

[HTTPS://100GIORNI.CCLUSIT.IT/#/](https://100giorni.clusit.it/#/)

OPZIONALE Free

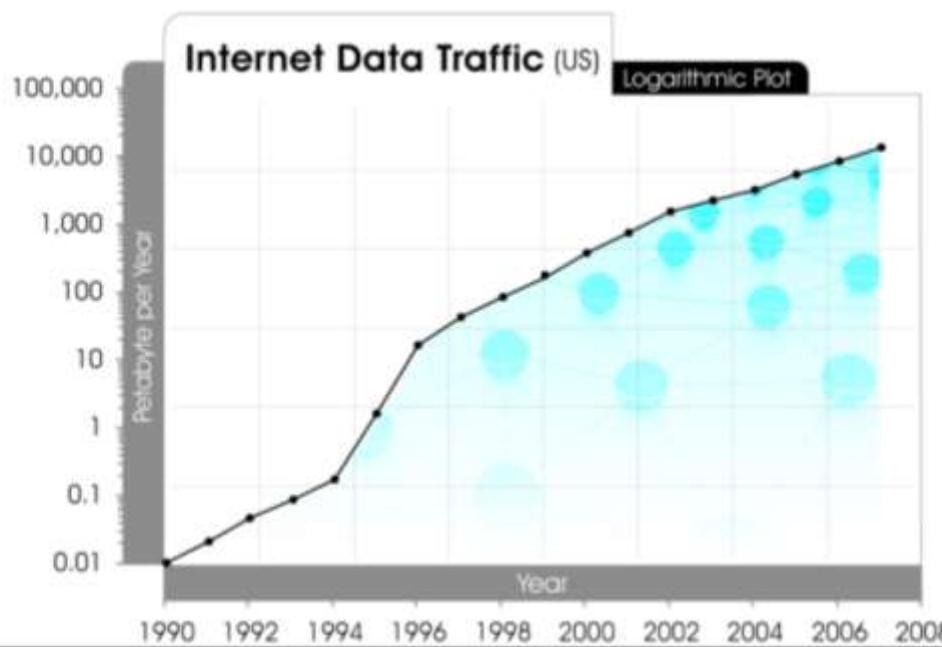
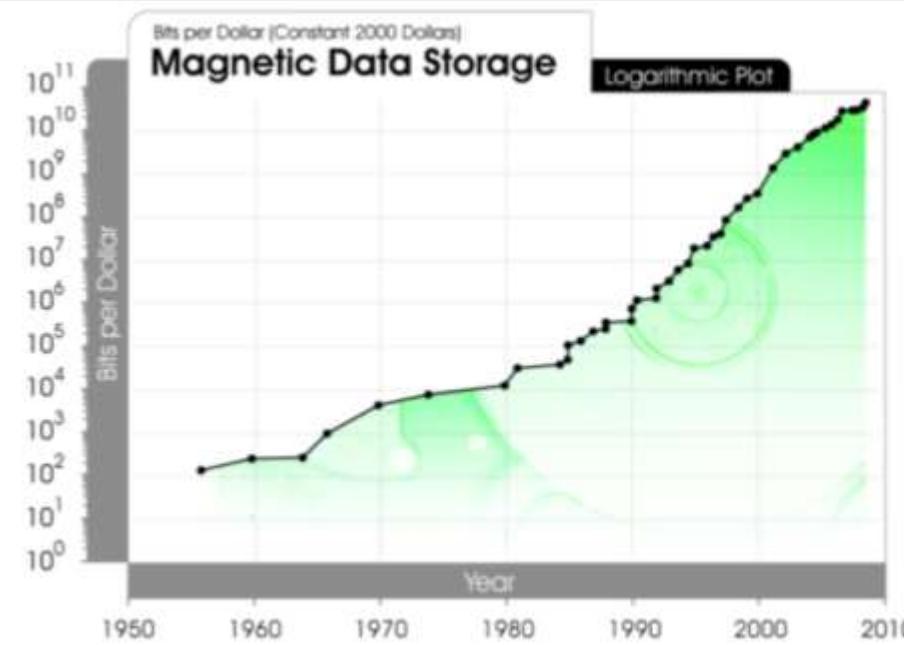


Contesto macroeconomico, tecnologico e sociale

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, sulle innovazioni realizzabili, sulle informazioni da produrre e da proteggere.

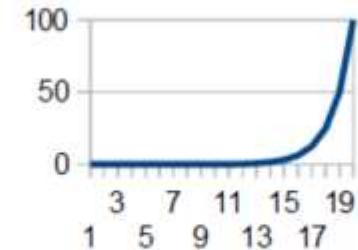
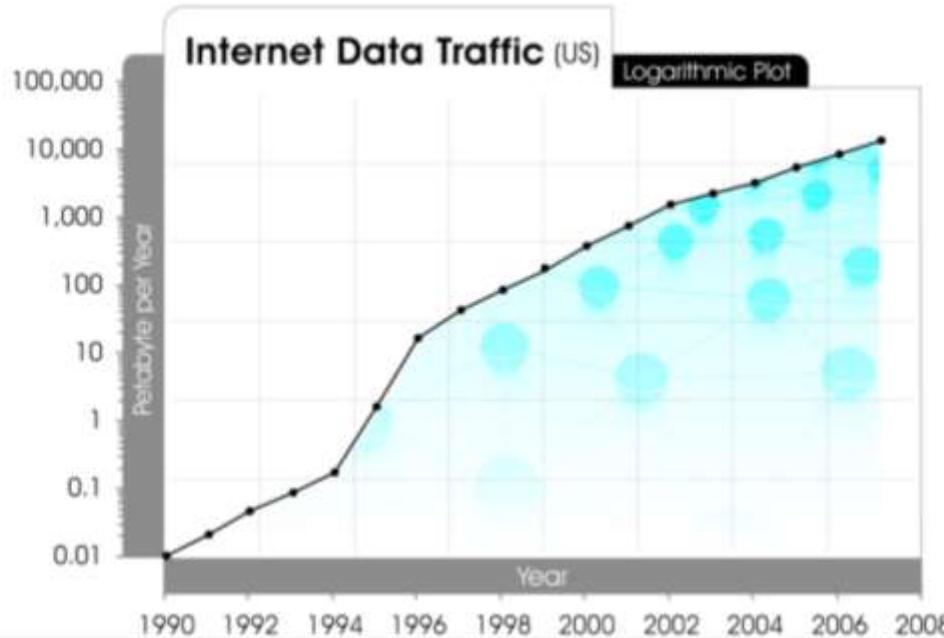
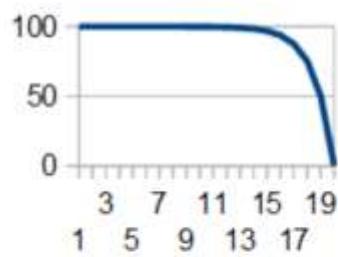
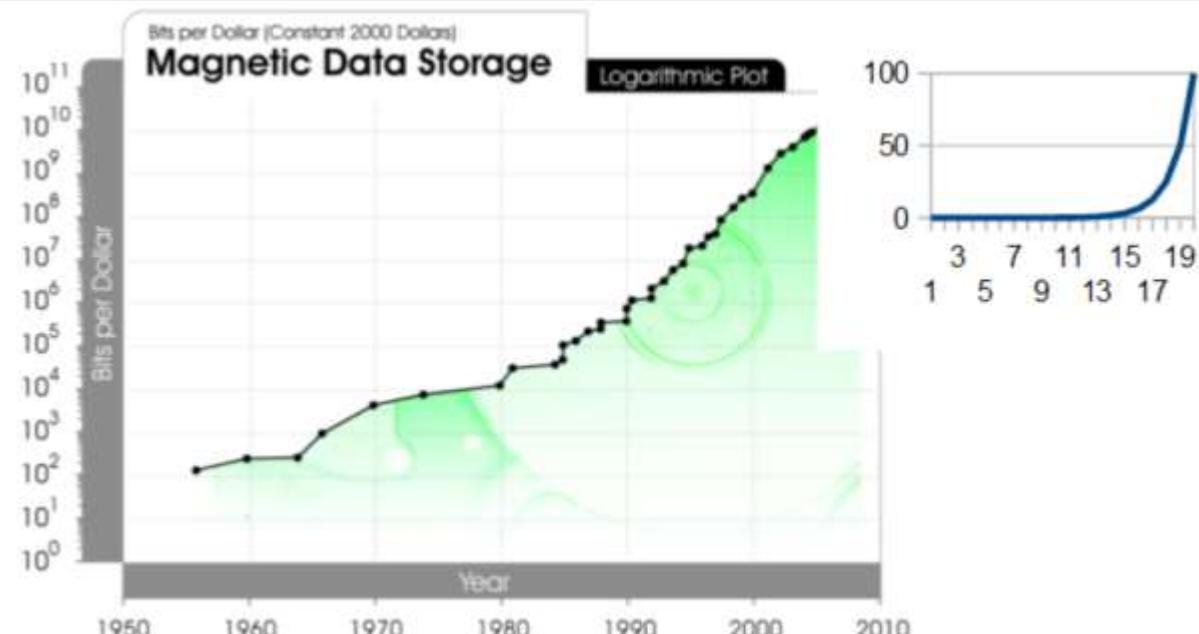
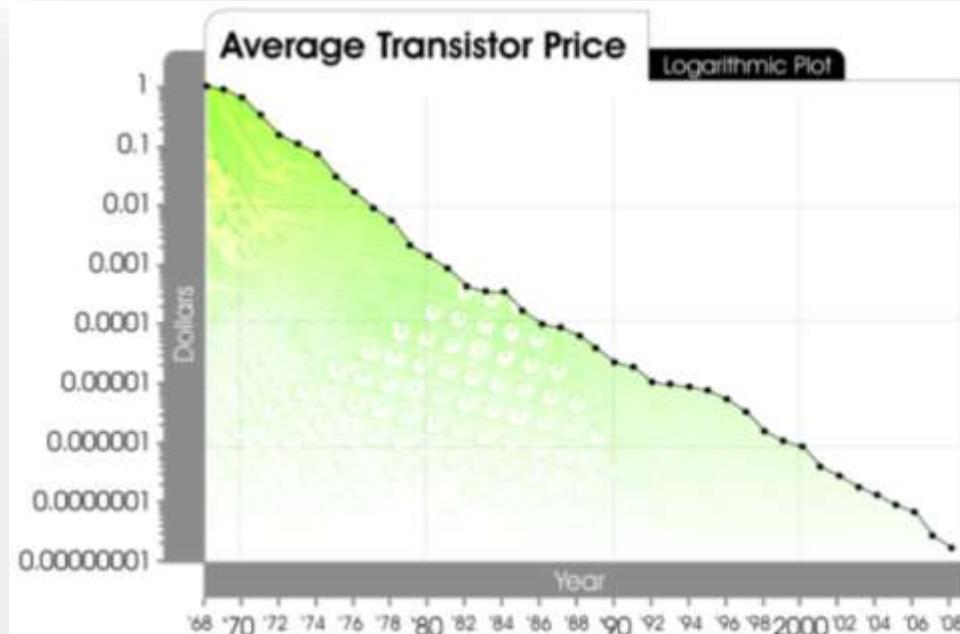
Il CISO arriva ultimo e il suo operato tiene insieme tutti i pezzi.

Il cambiamento è molto rapido.

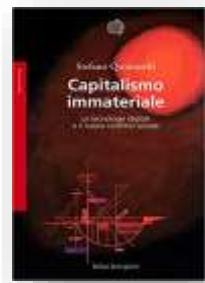
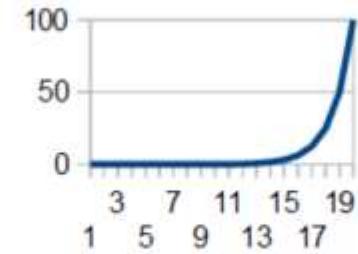
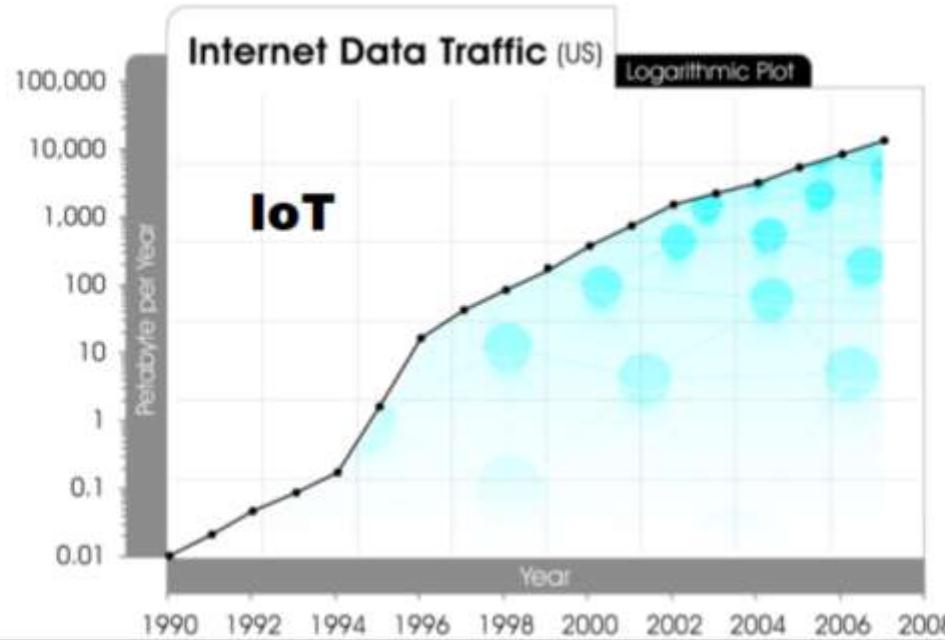
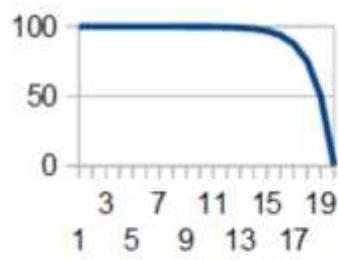
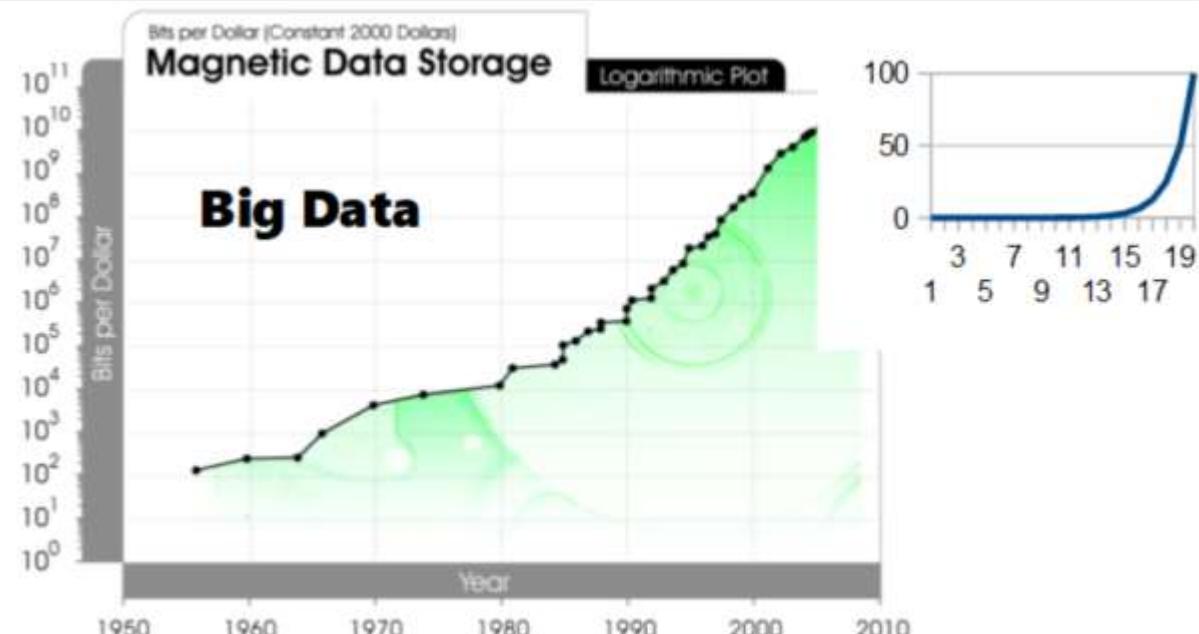


FONTE: Stefano Quintarelli





FONTE: Stefano Quintarelli



FONTE: Stefano Quintarelli



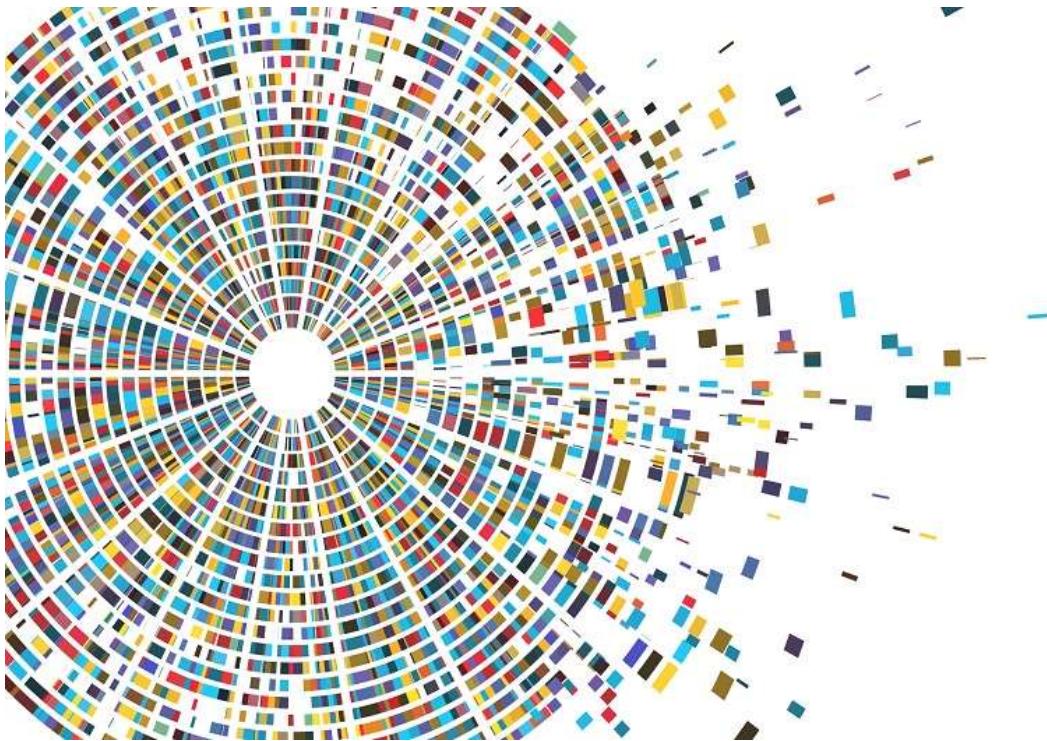
Gli utilizzatori consegnano ai **social** grandi quantità di dati utili alla profilazione



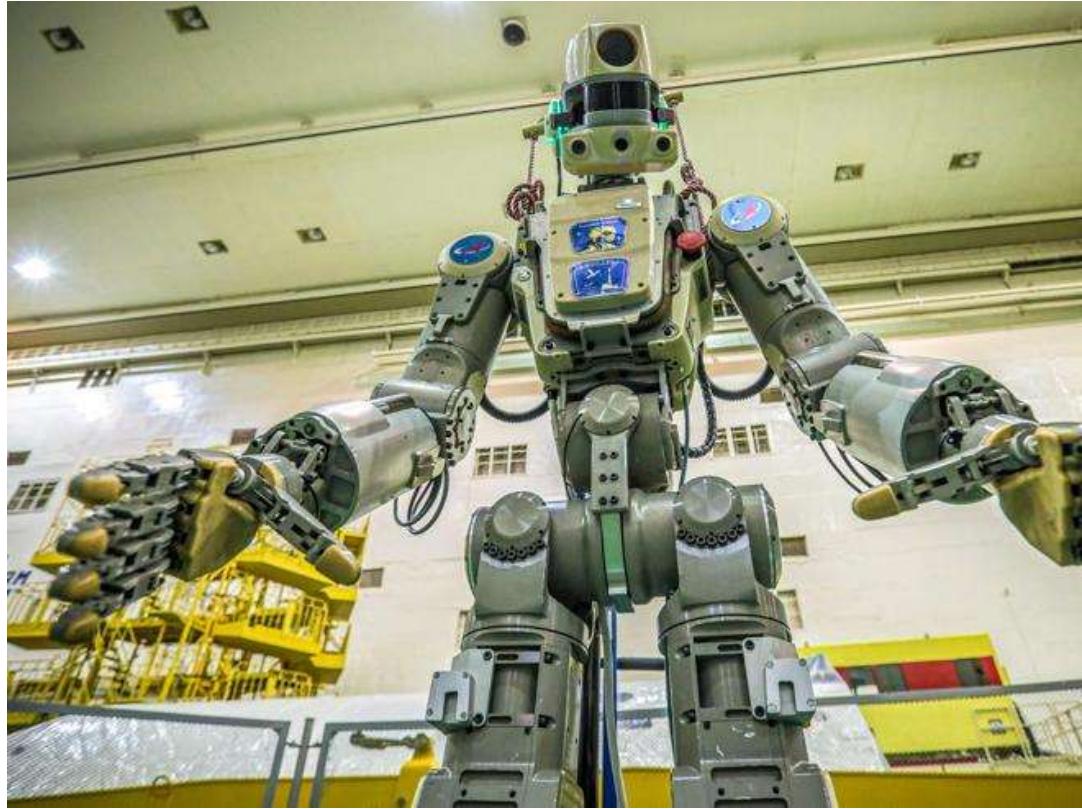
Lo fanno tramite tecnologie
mobile lavorando e in
generale interagendo da
ogni luogo e in ogni orario



L'**IoT** vi aggiunge i dati che arrivano tramite sensori dal mondo delle cose



Tali quantità di dati sono raccolte e rese gestibili tramite tecnologie di **big data**



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



L'**IT** si ibrida con l'**OT**
estendendo il dominio
dell'informatica nel modo
di produrre e gestire



Tutto questo si basa sul **cloud**, che unifica, abilita e garantisce: senza di esso niente sarebbe possibile

La trasformazione digitale per competere

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 aziende che fanno del digitale la loro leva 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

