

La Governance dei rischi nella banca digital: metodi e strumenti per migliorare la resilienza e la robustezza del sistema dei controlli aziendali

SUPERVISION, RISKS & PROFITABILITY 2021

Andrea Violato
23 giugno 2021



LA FINANZA. INTERPRETATA A REGOLA D'ARTE.

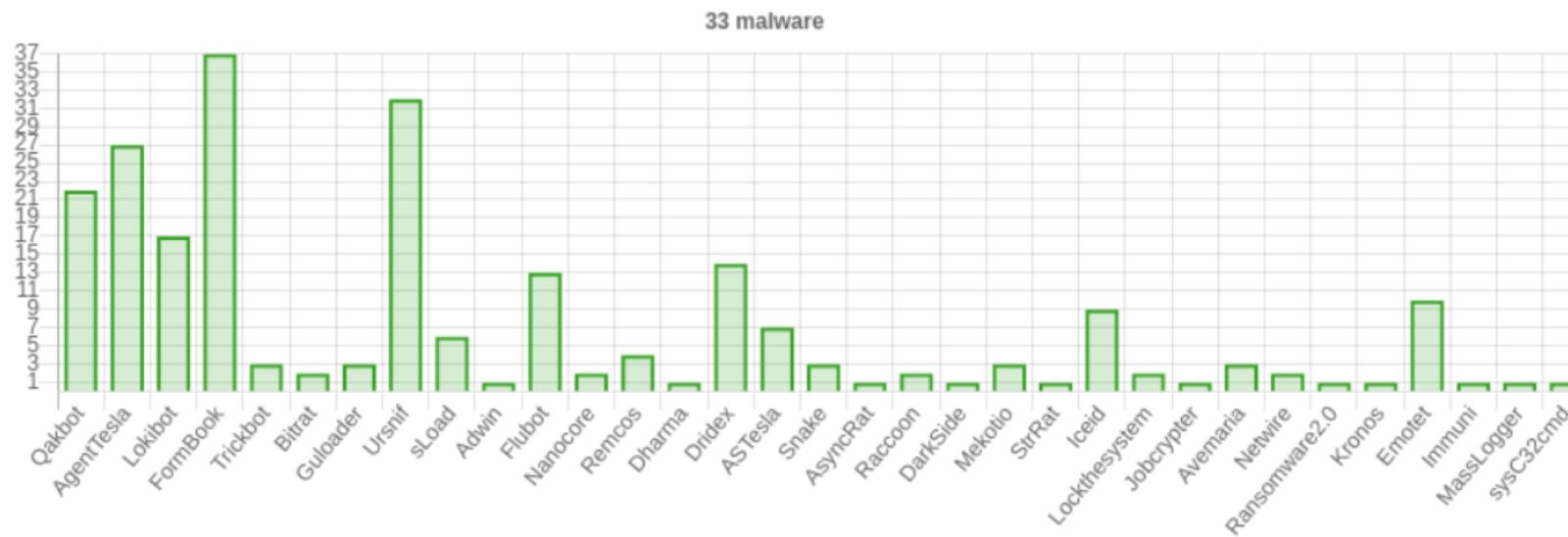
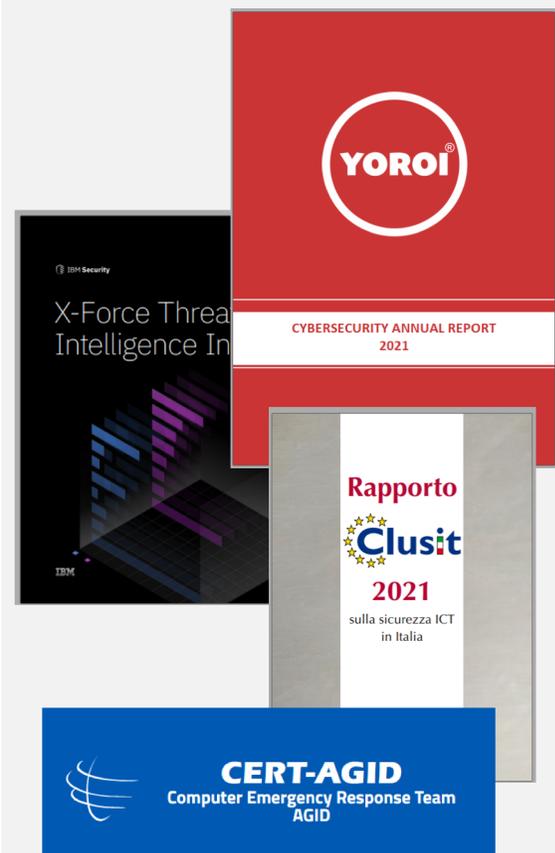
Augeos



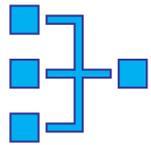
Il contesto di riferimento

Il 2020 è stato il «peggior anno di sempre»:

- In aumento gli attacchi in tema «*Banking*» (+8%, fonte: CLUSIT; CERT-Agid)
- In aumento i «*Data Breach*» (+20%, fonte: CLUSIT)
- In aumento gli attacchi *phishing* e *spearphishing* a mezzo di posta elettronica (fonte: Yoroi)
- I *malware* informatici sono divenuti la principale minaccia (fonte: IBM X-Force; CERT-Agid)
- ...



L'importanza dei controlli aziendali



Predisporre adeguate misure in grado di **mitigare** o **contrastare** l'insorgere di rischi permette di **preservare l'operatività aziendale**, nonché i suoi principali asset.



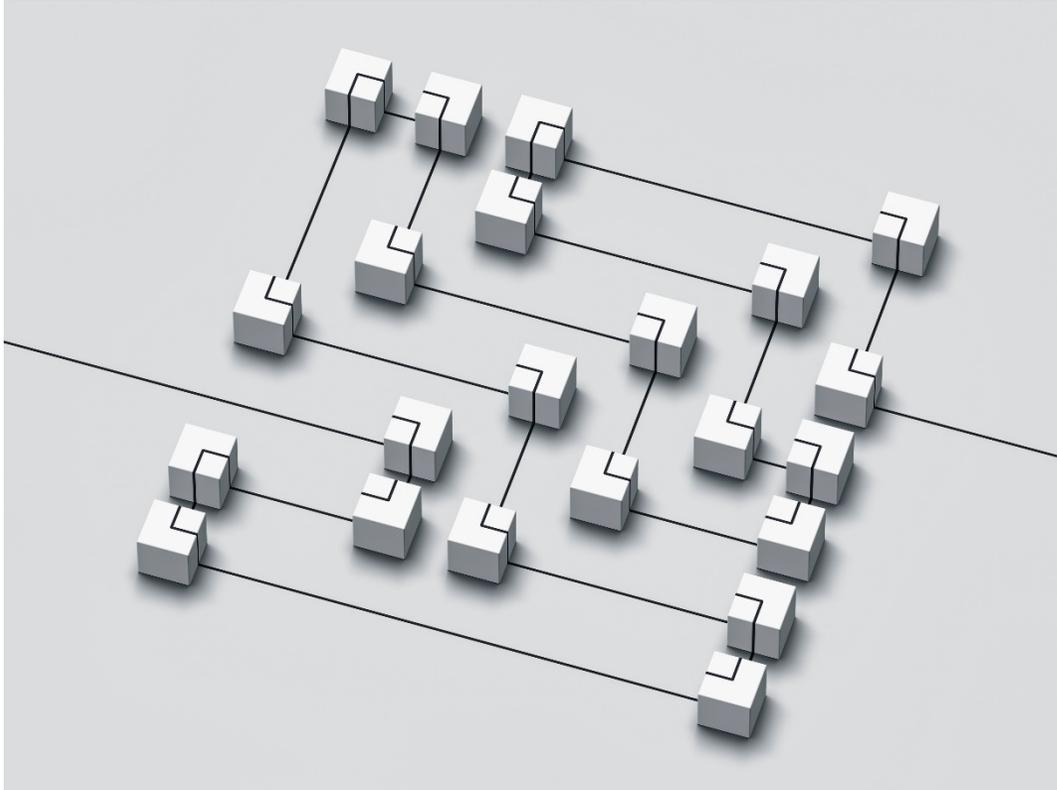
È richiesta una profonda **comprensione** del contesto aziendale, del **mercato** in cui si opera, dell'evoluzione quotidiana degli **scenari di rischio** a cui si è sottoposti.



È necessario un **costante adattamento** basato sull'esperienza e sulla continua ricerca al miglioramento in termini di **robustezza, conformità, maturità** e resilienza dell'intero sistema.



Metodi e Strumenti

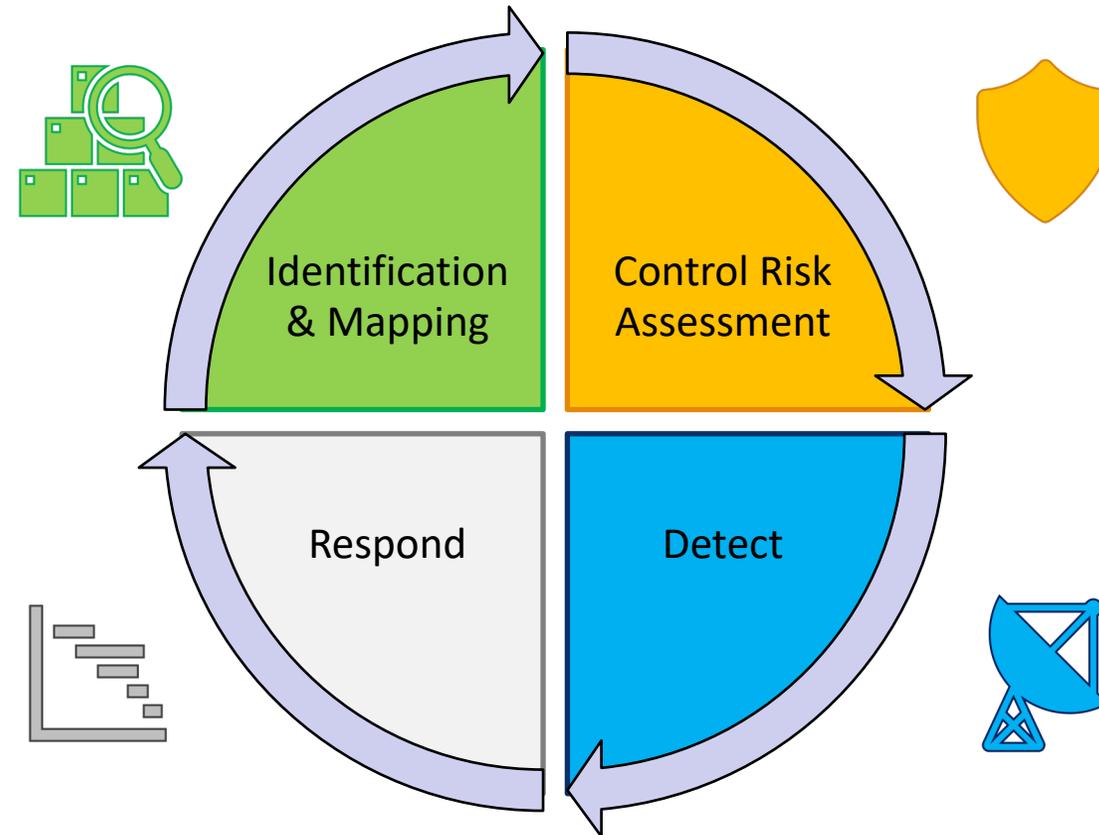


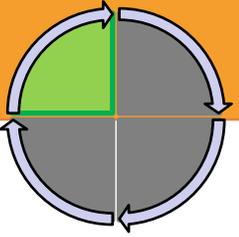
Dotarsi di un **metodo** senza tuttavia interessarsi adeguatamente delle sue modalità operative equivale in molti casi a non avere alcun metodo.

Viceversa, basare le proprie scelte operative sulla base dei vincoli e dei limiti dettati da **strumenti** privi di alcun legame con il proprio *modus operandi*, spesso implica una totale inefficacia dei risultati attesi.



Una possibile Soluzione





Dal punto di vista del *metodo*

Per identificare un sistema dei controlli efficace, ci si deve incentrare sui concetti di «conformità» e di «maturità» delle misure implementate.

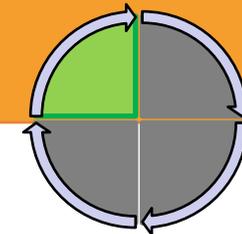
In un contesto come quello moderno, l'attività di identificazione è costante e mai scontata.

La fase di **identificazione** permette di costruire con precisione un quadro di riferimento del sistema dei controlli aziendali basato su:

- Normative
- Regolamenti tecnici
- Best practices
- Policy interne
- Standard internazionali
- ...



Identification & Mapping



Dal punto di vista del *metodo*

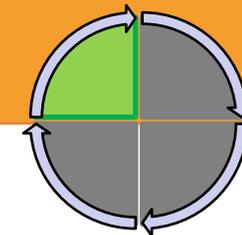
Un sistema dei controlli efficace deve necessariamente relazionarsi con gli scenari di rischio sui quali agisce, nonché sulle relative valutazioni.

La fase di **mapping** permette di relazionare il sistema dei controlli con altre tipologie di informazioni presenti all'interno del contesto aziendale e utili per delineare meglio la baseline di riferimento:

- Asset e risorse informatiche
- Scenari di rischio
- Categorie di minacce, event type
- Processi aziendali
- Strutture organizzative
- ...



Identification & Mapping



Dal punto di vista dello strumento

Uno strumento ideale alla fase di Identification & Mapping deve offrire funzionalità orientate all'acquisizione e all'aggiornamento anagrafico anche mediante allineamenti da fonti esterne.

Deve inoltre garantire la ricostruibilità storica, pur mantenendo un approccio orientato al risultato, senza comportare un aggravio di processo all'utente.

Nome	Descrizione	Tipologia	Stato di attivazione	Tags
A.10.1.1	Policy per l'uso dei controlli crittografici	ISO	Attivo	
A.10.1.1 test	Policy per l'uso dei controlli crittografici	ISO	Attivo	

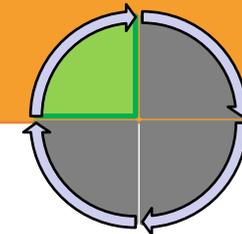


Nome	Descrizione	Tipologia	Stato di attivazione	Tags
a.11				
A.11.1.1	Perimetro di sicurezza fisica	ISO	Attivo	
A.11.1.2	Controllo degli accessi fisici	ISO	Attivo	
A.11.1.3	Sicurezza degli uffici, delle stanze e delle strutture	ISO	Attivo	
A.11.1.4	Protezione da minacce esterne e ambientali	ISO	Attivo	
A.11.1.5	Lavoro in area di sicurezza	ISO	Attivo	
A.11.1.6	Aree di consegna e carico	ISO	Attivo	
A.11.2.1	Localizzazione e protezione delle attrezzature	ISO	Attivo	
A.11.2.2	Servizi di supporto	ISO	Attivo	
A.11.2.3	Sicurezza per il cablaggio	ISO	Attivo	
A.11.2.4	Manutenzione delle attrezzature	ISO	Attivo	
A.11.2.5	Rimozione degli accessi	ISO	Attivo	
A.11.2.6	Sicurezza delle attrezzature e degli asset fuori sede	ISO	Attivo	
A.11.2.7	Disposizione e ri-utilizzo delle attrezzature	ISO	Attivo	
A.11.2.8	Attrezzature non custodite	ISO	Attivo	
A.11.2.9	Trasparenza delle desk e screen policy	ISO	Attivo	

Dettaglio controllo	
Tipologia	ISO
Tipologia delle contromisure	Di mitigazione
Classificazione	C1 - Bassa, C3 - Alta
Modalità di esecuzione	Continuativa
Obbligatorietà della contromisura	Non cogente



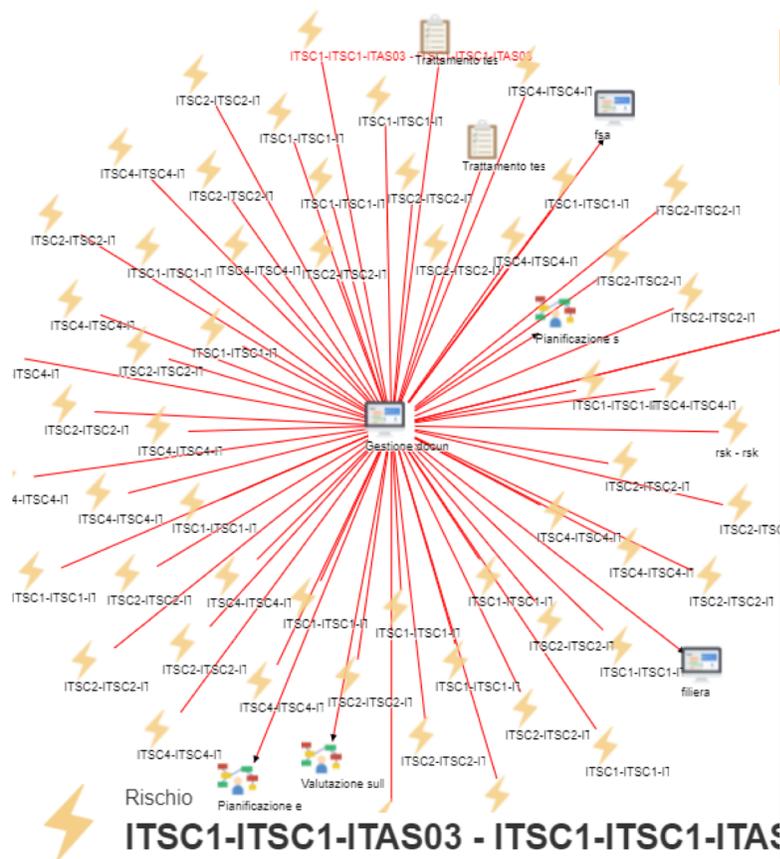
Identification & Mapping



Dal punto di vista dello strumento

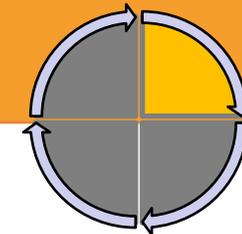
Uno strumento ideale deve inoltre facilitare la **consultazione** delle informazioni tra di loro mappate, garantendo pieno **accesso ai dati** anche mediante modalità di navigazione online.

Grafo collegamenti Gestione documentale



Acronimo	Nome
ITM26	Inefficienza del disegno dei sistemi
27	Utilizzo improprio di software
ITM19	Errori nei processi di imputazione dei dati
ITM1	Malfunzionamento SW
ITM12	Accesso fisico non autorizzato
ITM14	Furto di apparati hardware
ITM22	Insufficiente processo di comunicazione degli obiettivi progettuali
ITM3	Modifica dei dati in ambiente di produzione
ITM25	Inefficiente identificazione delle business ownership





Dal punto di vista del *metodo*

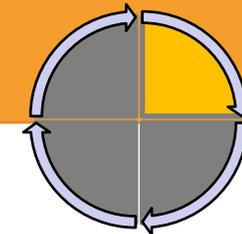
Un Control Risk Assessment deve basarsi su **modelli metodologici consolidati**, che permettono di ottenere con precisione valutazioni di **conformità** e **maturità** del sistema dei controlli utili a giudicarne la **robustezza** e **resilienza** rispetto agli **scenari di rischio** considerati.

Effettuare periodicamente un ***Control Risk Assessment*** permette di «misurare» il livello di adeguatezza del sistema attraverso approcci di varia natura, tra i quali:

- Modelli «**Top-down**» basati su meccanismi che disegnano i livelli di maturità partendo da macro-aggregati o famiglie di controlli applicati via-via fino al livello foglia
- Modelli «**Bottom-up**» incentrati su sessioni di valutazioni puntuali sulle singole misure o sulle singole relazioni di queste con i rispettivi rischi e che mediante logiche di aggregazione permettono di definirne i livelli superiori



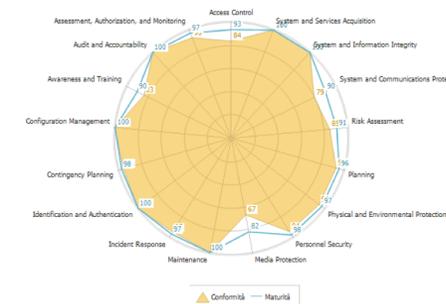
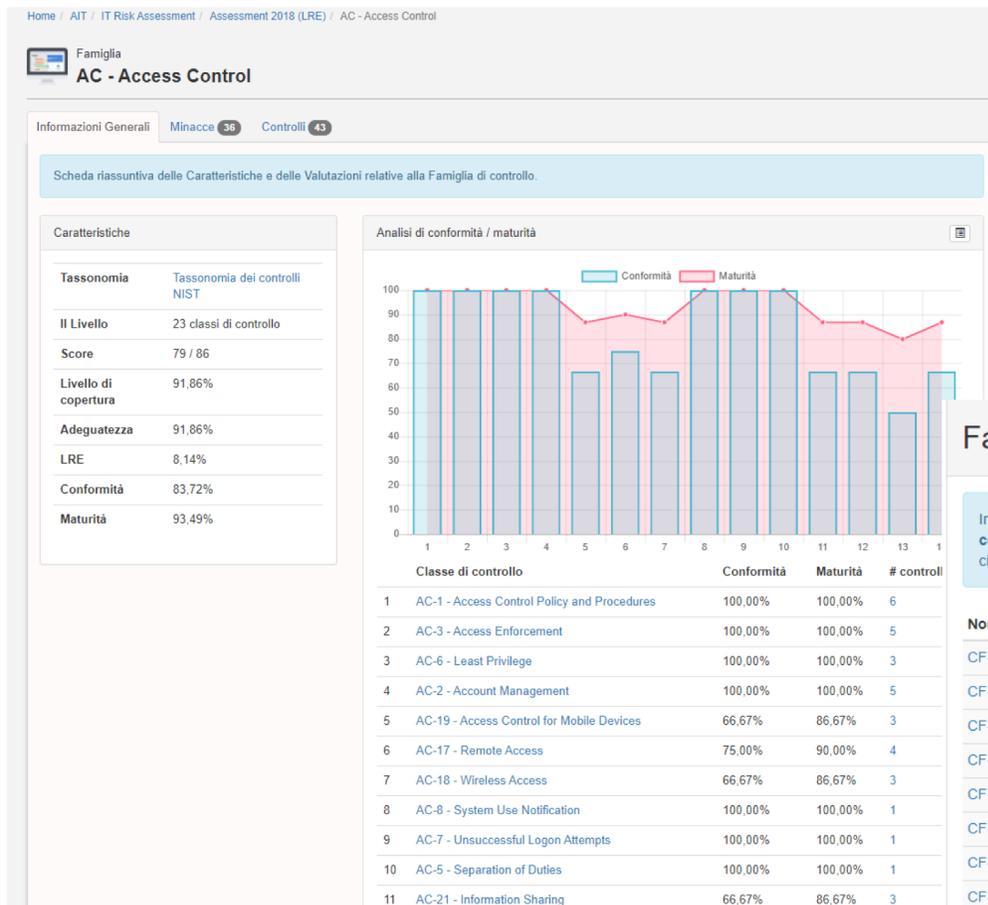
Control Risk Assessment



Dal punto di vista dello strumento

Uno strumento idoneo a supportare la fase di Control Risk Assessment deve offrire strumenti capaci di applicare, senza aggravio di processo e in base all'impostazione desiderata, modelli, prassi, standard internazionali utili per la definizione dei livelli di conformità e maturità delle misure.

A fronte del CRA, è inoltre fondamentale la capacità di rilevarne i punti deboli, offrendo dunque una indicazione puntuale su come e dove intervenire nel sistema dei controlli

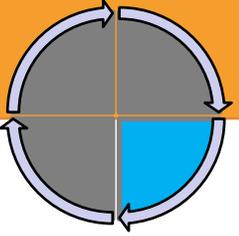


Famiglie di controlli 17

In questa tabella può essere imputata l'adeguatezza di ciascuna Famiglia di controllo sulla base del Livello di copertura calcolato. A partire da tale adeguatezza, il sistema calcola il Livello di Rischio di Esposizione (LRE) di ciascuna Famiglia.

Nome	Adeguatezza	LRE	Livello di copertura
CF-1 - ACCESS CONTROL	85,71%	14,29%	85,71%
CF-3 - AUDIT AND ACCOUNTABILITY	80,00%	20,00%	80,00%
CF-2 - AWARENESS AND TRAINING	83,33%	16,67%	83,33%
CF-5 - CONFIGURATION MANAGEMENT	100,00%	0,00%	100,00%
CF-6 - CONTINGENCY PLANNING	68,75%	31,25%	68,75%
CF-7 - IDENTIFICATION AND AUTHENTICATION	90,00%	10,00%	90,00%
CF-8 - INCIDENT RESPONSE	100,00%	0,00%	100,00%
CF-9 - MAINTENANCE	75,00%	25,00%	75,00%
CF-10 - MEDIA PROTECTION	66,67%	33,33%	66,67%
CF-13 - PERSONNEL SECURITY	90,00%	10,00%	90,00%

Detect



Dal punto di vista del metodo

Rilevare efficacemente un evento implica la definizione di regole di monitoraggio puntuali, che richiedono il necessario coinvolgimento di una pluralità di attori.

In base alla tipologia di eventi monitorati, sono inoltre necessari differenti conoscenze e sensibilità utili a valutarne gli effettivi impatti.

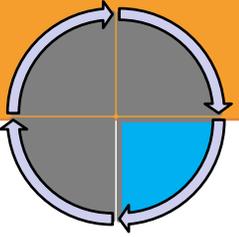
La fase di **Rilevamento** assume più che mai importanza di fronte a una **evoluzione** così **repentina** degli **scenari di rischio** da considerare.

Questa consiste nel **monitoraggio attivo e tempestivo** di tutte le **fattispecie di evento** che possono incidere sul sistema dei controlli:

- Ex post
 - Incidenti informatici
 - Incidenti di sicurezza
 - Data Breach
 - Eventi di perdita operativa
 - Altri tipi di eventi operativi
 - Segnalazioni di non conformità
 - ...
- Ex ante
 - Indicatori di rischio
 - Analisi di Stress Test
 - ...



Detect



Dal punto di vista dello *strumento*

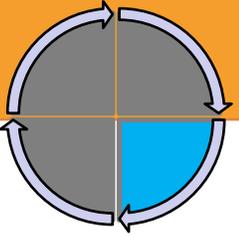
Governare un **processo di raccolta informativa** attraverso un supporto strumentale richiede che questo metta a disposizione funzionalità di gestione e controllo **flessibili**, in linea con le regole interne e facilmente **monitorabili** dai supervisor.

Sono inoltre essenziali funzionalità che permettono la **storicizzazione** e la **ricostruibilità** delle informazioni nel tempo

The screenshot displays the Augeos incident management system interface. It shows two incident cards. The first card, for incident INC000343, is in the 'In registrazione' (In registration) state, with a progress bar starting at 07/01/20. The second card, for incident INC000476, is in the 'Attivo' (Active) state, with a progress bar starting at 20/11/20 and ending at 09/06/21. Below the incident cards, there is a detailed view of incident registration information for INC000343, including fields for Title, Date of detection, Start and End times, Reaction time, Parent Event ID, Description, and Notes. A 'Controlli falliti' (Failed controls) section is also visible, showing a table with columns for Acronym, Name, and Taxonomy of controls.

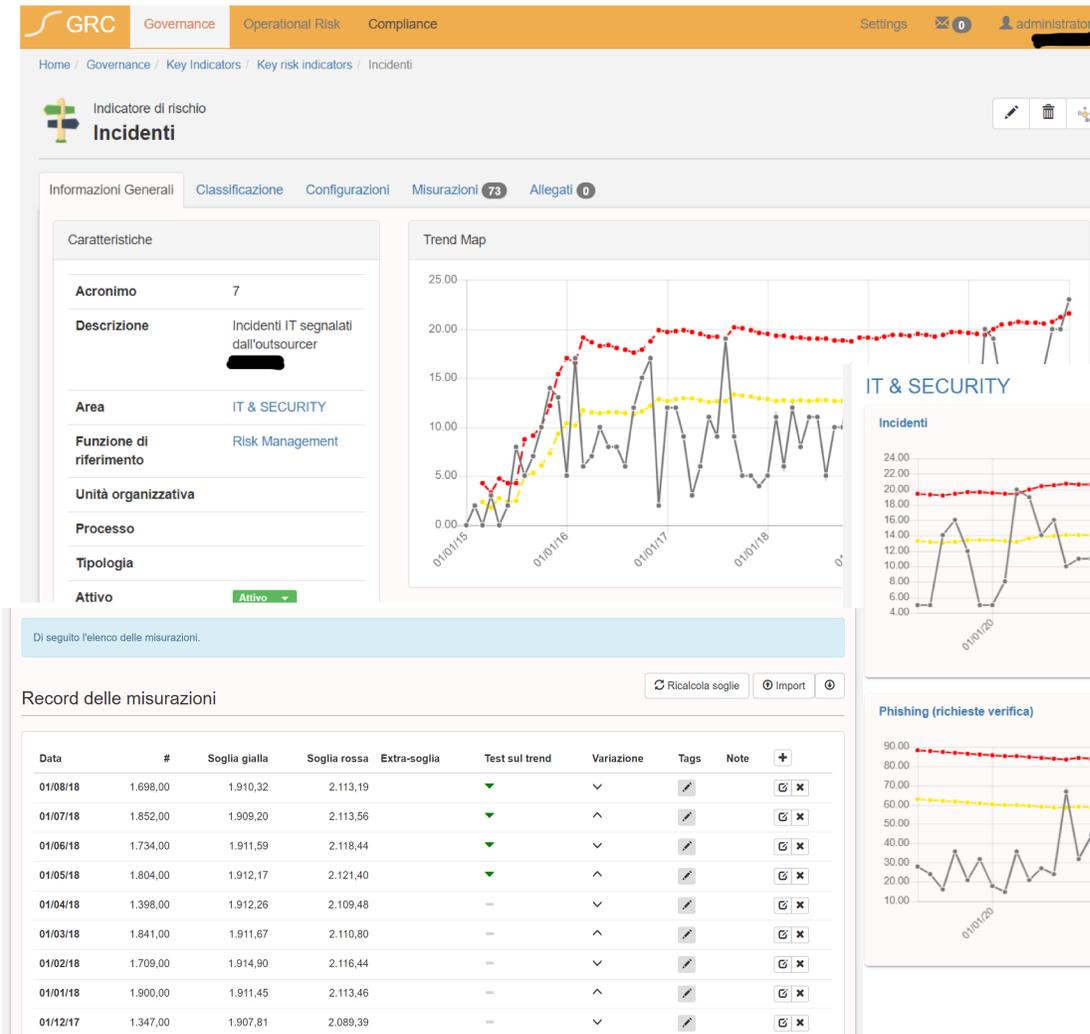
Acronimo	Nome	Tassonomia dei controlli
CTRL2013	Access Control	FC01 - Controllo Ignoto 1

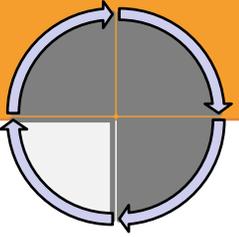
Detect



Dal punto di vista dello strumento

Il Rilevamento a priori è certamente un plus di qualsiasi modello e strumento di governance, in quanto l'individuazione di **trend significativi** può agevolare nell'adattamento in continuo del sistema dei controlli.





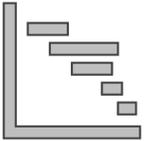
Dal punto di vista del *metodo*

L'obiettivo finale di una Risposta è quella di contenere, per quanto possibile, l'impatto determinato da una fattispecie di rischio quale un incidente informatico, un evento di perdita, un data breach,

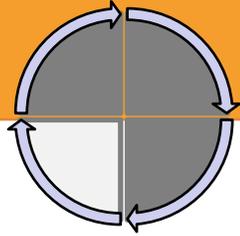
Alla rilevazione di una fattispecie di rischio, corrisponde un'azione di risposta volta a **contrastare** o **mitigare** qualsiasi effetto.

Tale attività è spesso definita a priori secondo requisiti dettati da:

- Policy interne
- Best practices
- Standard internazionali
- Normative e regolamenti di settore



Respond

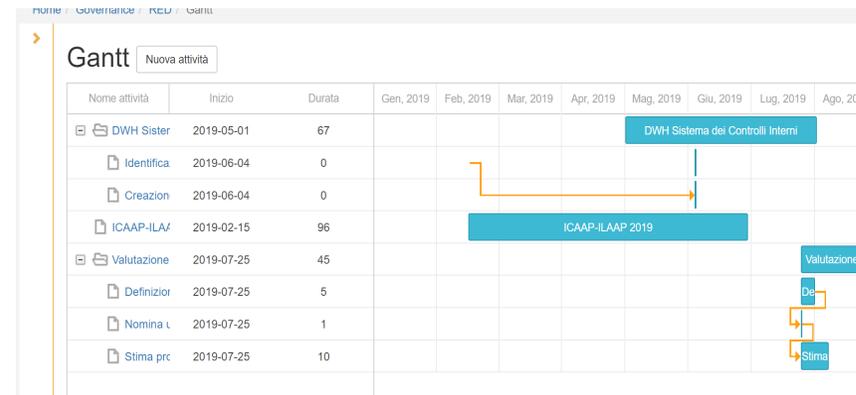


Dal punto di vista dello strumento

Una applicazione a supporto della fase di Risposta deve possedere differenti caratteristiche:

- Scalabilità
- Automazione
- Storizzazione
- Pianificazione
- Reportistica integrata

The screenshot shows the Respond web application interface. The top navigation bar includes 'GRC', 'Governance', 'Operational Risk', 'Compliance', 'AIT', and 'Tools'. The main content area displays a list of activities under the heading 'Elenco Attività'. Two activities are visible: 'DWH Sistema dei Controlli Interni' (August 2019) and 'ICAAP-ILAAP 2019' (June 2019). The 'DWH Sistema dei Controlli Interni' activity is highlighted, showing its status as 'Parzialmente adeguato' and a progress bar indicating it is 'In lavorazione' (in progress) from 14/02/19 to 04/06/19. Below the progress bar, there are tabs for 'Informazioni generali', 'Attività preparatorie', 'Fasi', 'Valutazione', 'Allocazione risorse', 'Oggetti GRC', and 'Allegati'. A table below these tabs lists activities with columns for 'Titolo', 'Data inizio', 'Data fine', 'Durata', 'Responsabile', 'Stato / Valutazione', and 'Dipendenze'.



The summary report for 'DWH Sistema dei Controlli Interni' is titled 'Riepilogo delle attività'. It provides a high-level overview of the activity's status and compliance. The report includes a table with columns for 'Titolo', 'Tipologia', and 'Valutazione'. The 'DWH Sistema dei Controlli Interni' activity is listed with a 'Parzialmente adeguato' status. The report also includes a section for 'Iniziari' (Initiators) and 'Attività normative' (Normative Activities), both showing a 'Completato' (Completed) status.

Grazie

SUPERVISION, RISKS
& PROFITABILITY 2021

Andrea Violato

andrea.violato@augeos.it

<https://www.augeos.it>

<https://it.linkedin.com/pub/dir/Andrea/Violato>



17

2021 © Augeos S.p.A.

Documento riservato ad uso esclusivo dei destinatari autorizzati. Vietata la diffusione

