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

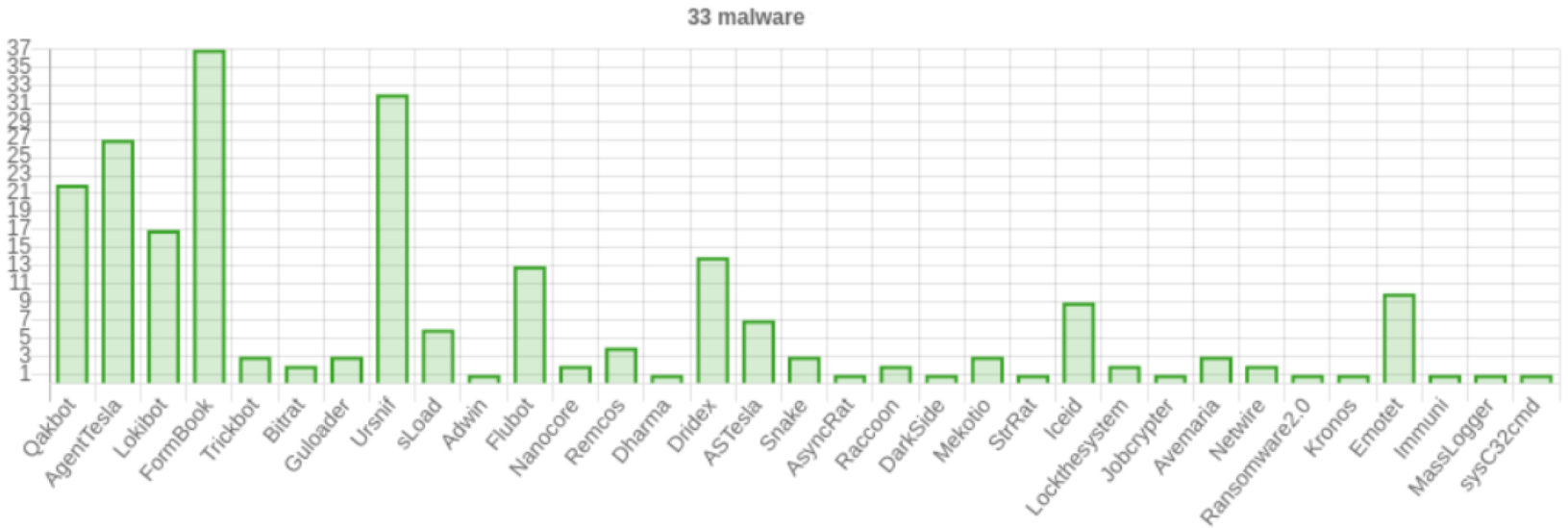
LA FINANZA. INTERPRETATA A REGOLA D'ARTE.

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)
- …



Augeos
Servizi e tecnologia per creare valore

L’importanza dei controlli aziendali

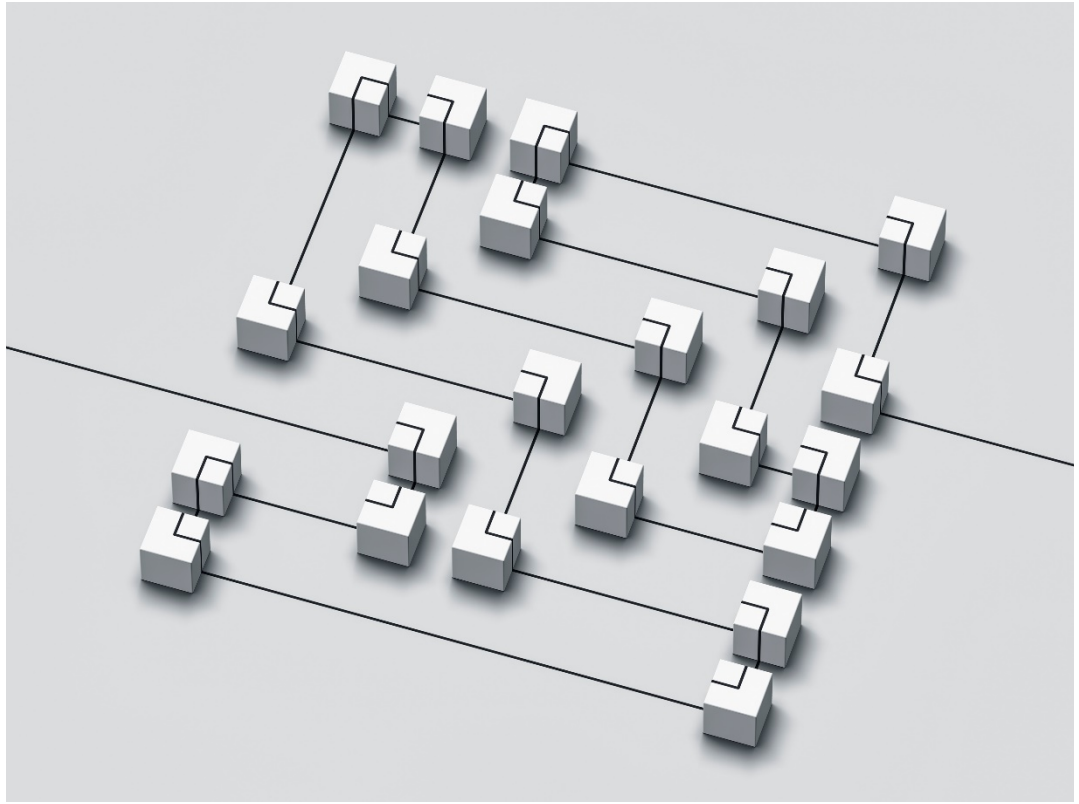
Predisporre adeguate misure in grado di **mitigare** o **contrastare** l’insorgere di rischi permette di **preservare l’operatività aziendale**, nonché i suoi principali asset.

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.

Augeos
Servizi e tecnologia per creare valore

Metodi e Strumenti

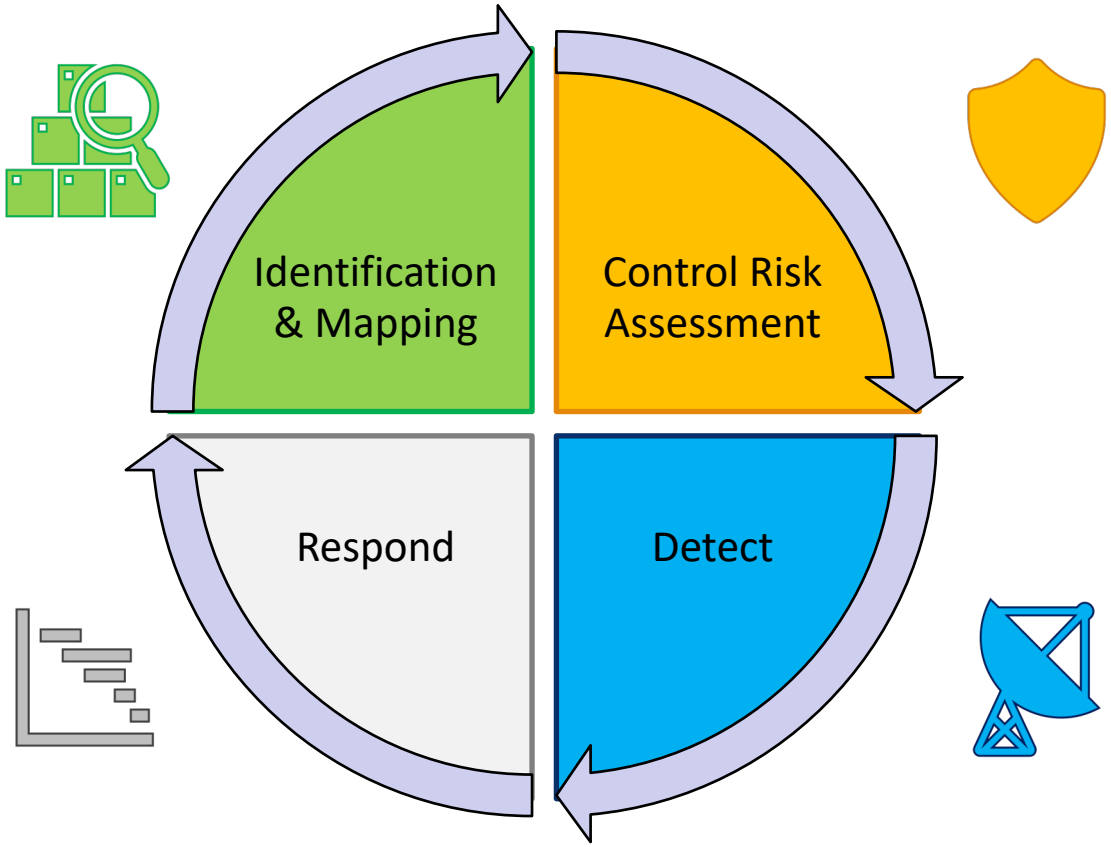


Dotarsi di un **metodo** senza tuttavia interessarsi adeguatamente delle sue modalità operative equivale in molti casi a non avere alcun metodo.

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.

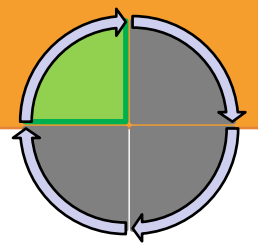
Augeos
Servizi e tecnologia per creare valore

Una possibile Soluzione



Augeos
Servizi e tecnologia per creare valore

Identification & Mapping



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.

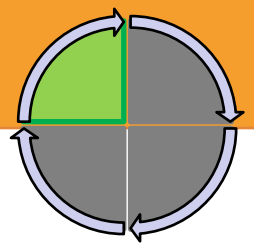
In un contesto come quello moderno, l'attività di identificazione è costante e mai scontata.

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
- …

Augeos
Servizi e tecnologia per creare valore

Identification & Mapping



Dal punto di vista del *metodo*

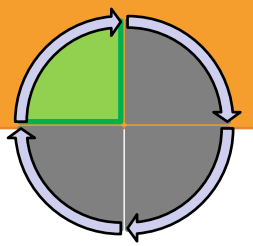
Un sistema dei controlli efficace deve necessariamente relazionarsi con gli scenari di rischio sui quali agisce, nonché sulle relative valutazioni.

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
- …

Augeos
Servizi e tecnologia per creare valore

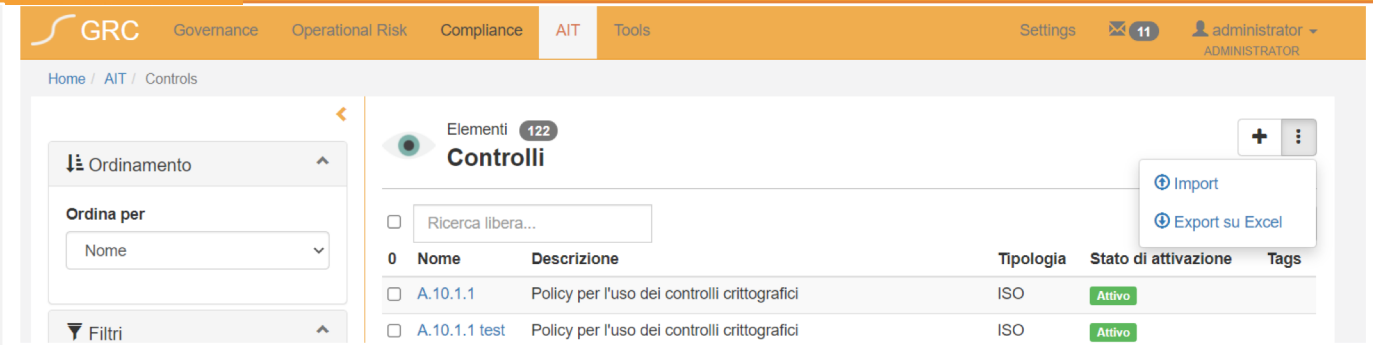
Identification & Mapping

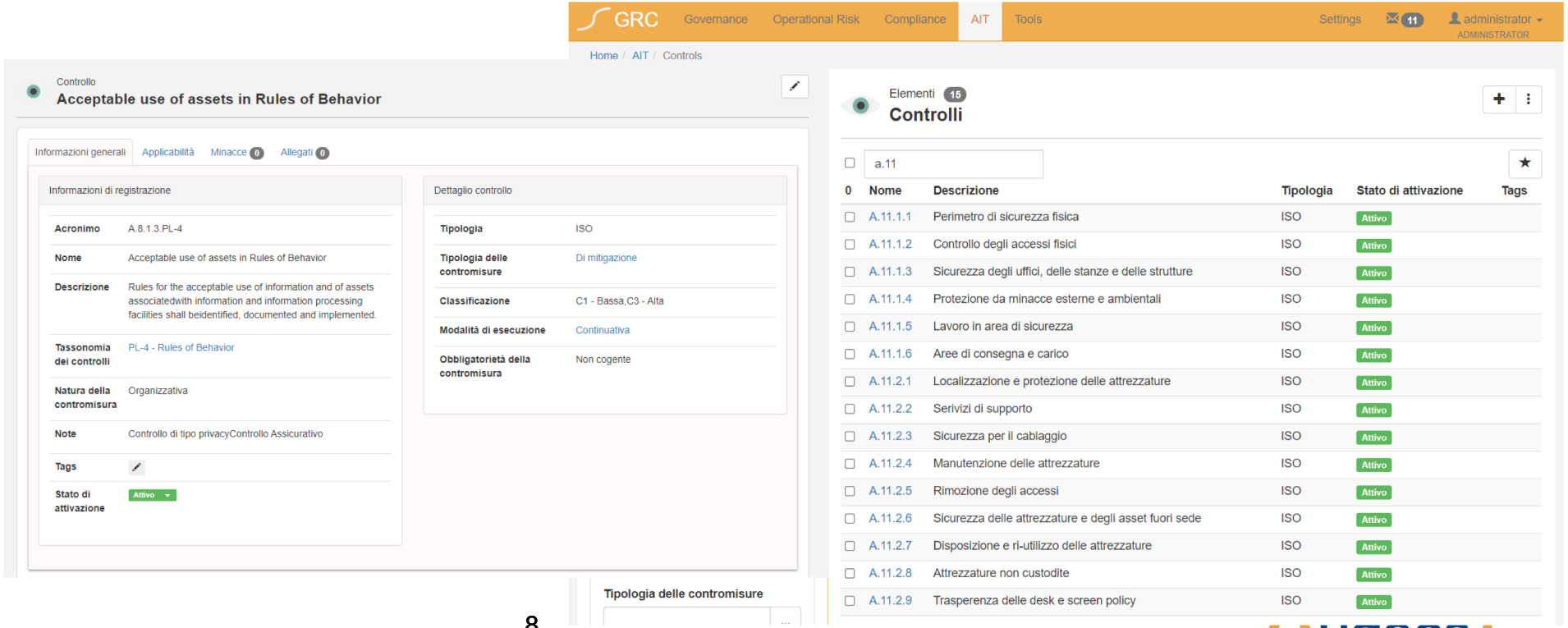


Dal punto di vista dello *strumento*

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

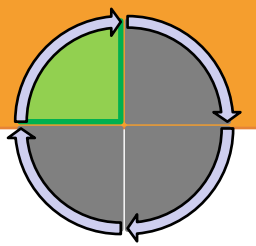
Deve inoltre garantire la **ricostruibilità storica**, pur mantenendo un approccio **orientato al risultato**, senza comportare un aggravio di processo all'utente.





Augeos
Servizi e tecnologia per creare valore

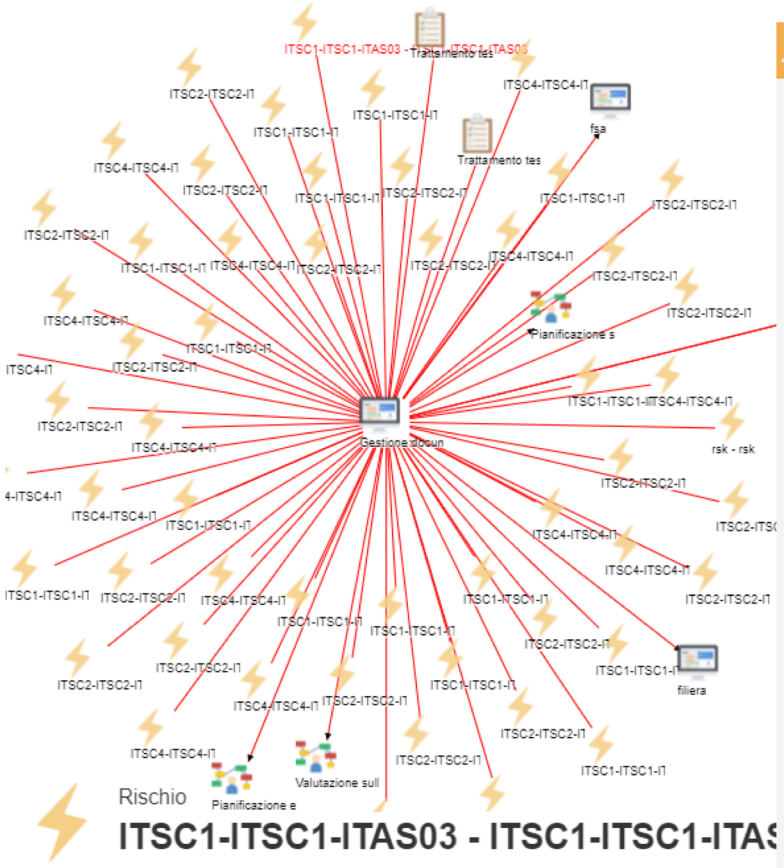
Identification & Mapping



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



GRC | Governance | Operational Risk | Compliance | AIT | Tools

Home / AIT / Controls / A.10.1.1

Controllo
A.10.1.1

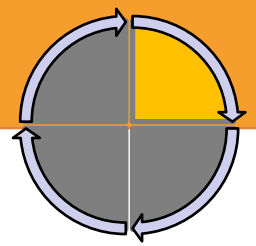
Informazioni generali | Applicabilità | Minacce 9 | Allegati 0

Minacce

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

Augeos
Servizi e tecnologia per creare valore

Control Risk Assessment



Dal punto di vista del *metodo*

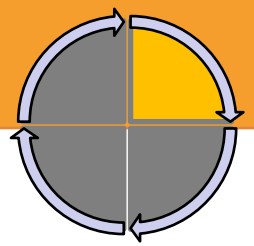
Un Control Risk Assessment deve basarsi su **modelli metodologici consolidati**, che permettono di ottenere con precisione valutazioni di **conformità** e **maturità** del sistema dei controlli utili a giudicarne la **robustezza** e **resilienza** rispetto agli **scenari di rischio** considerati.

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

Augeos
Servizi e tecnologia per creare valore

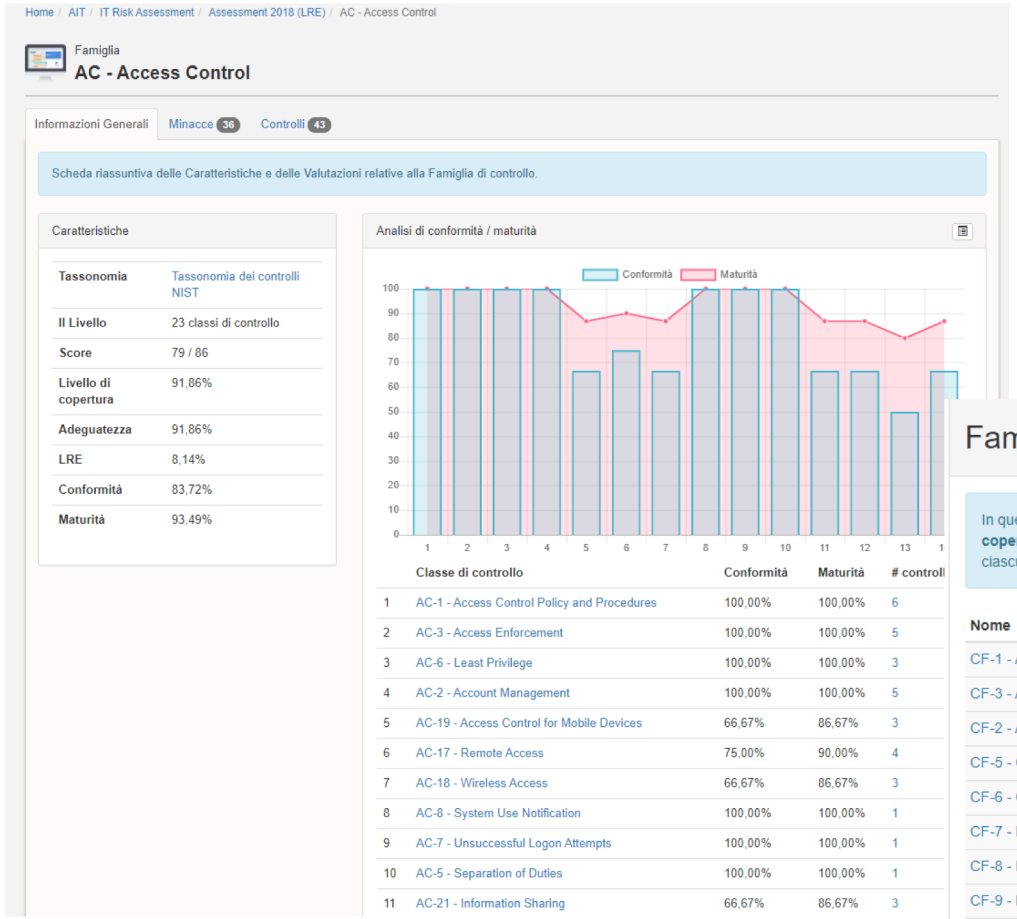
Control Risk Assessment



Dal punto di vista dello *strumento*

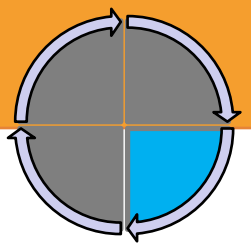
Uno strumento idoneo a supportare la fase di Control Risk Assessment deve offrire strumenti capaci di applicare, senza aggravio di processo e in base all'impostazione desiderata, modelli, prassi, standard internazionali utili per la definizione dei livelli di conformità e maturità delle misure.

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



Augeos
Servizi e tecnologia per creare valore

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.

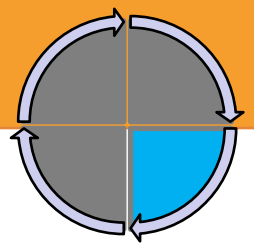
La fase di **Rilevamento** assume più che mai importanza di fronte a una **evoluzione** così **repentina** degli **scenari di rischio** da considerare.

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
  - …

Augeos
Servizi e tecnologia per creare valore

Detect



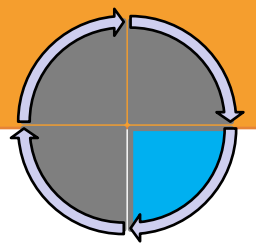
Dal punto di vista dello *strumento*

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 supervisori.

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

Augeos
Servizi e tecnologia per creare valore

Detect

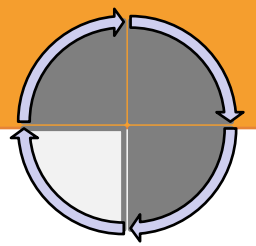


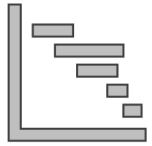
Dal punto di vista dello *strumento*

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.

Augeos
Servizi e tecnologia per creare valore

Respond





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, ….

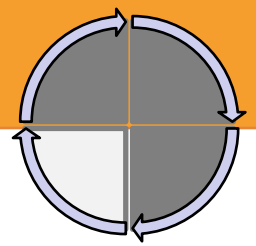
Alla rilevazione di una fattispecie di rischio, corrisponde un'**azione di risposta** volta a **contrastare** o **mitigare** qualsiasi effetto.

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

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

Augeos
Servizi e tecnologia per creare valore

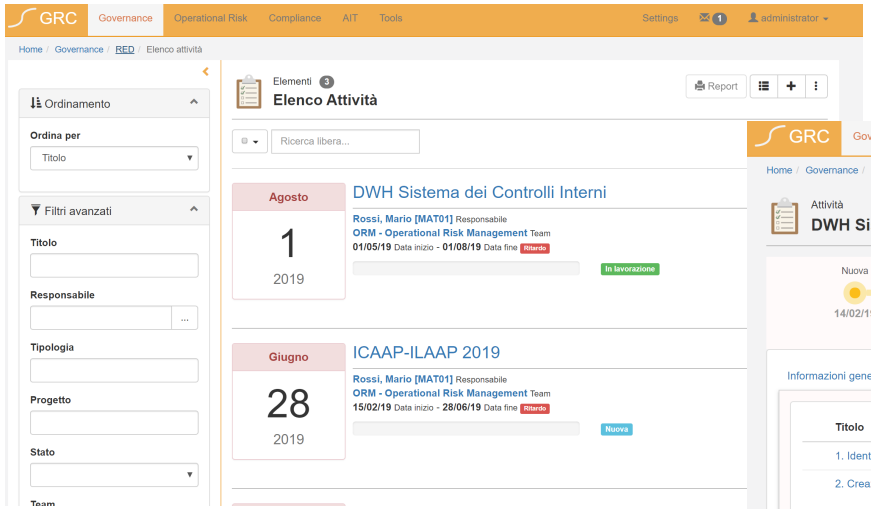
Respond

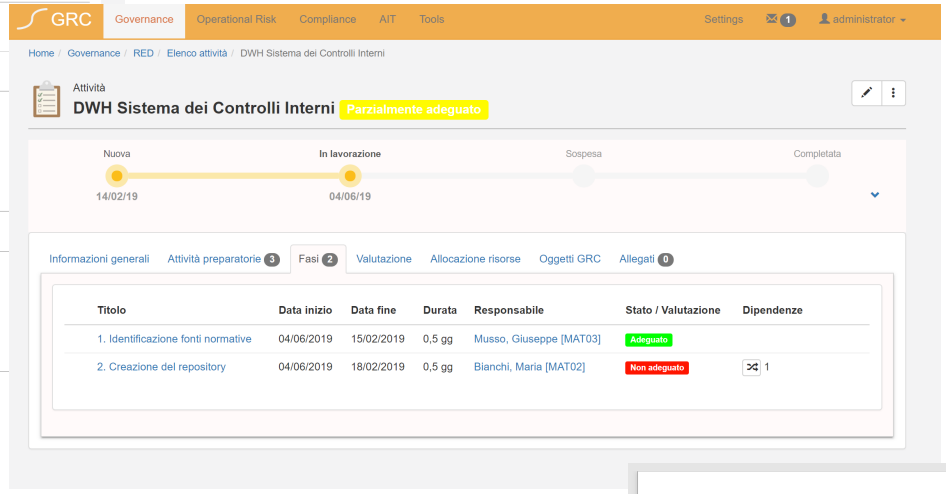


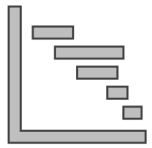
Dal punto di vista dello *strumento*

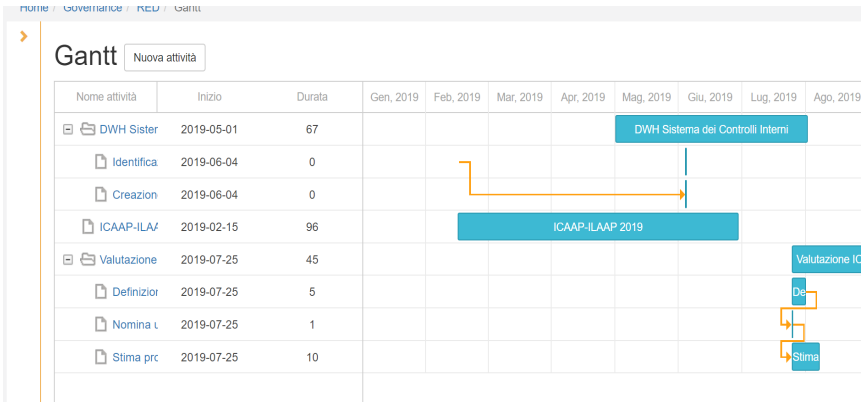
Una applicazione a supporto della fase di Risposta deve possedere differenti caratteristiche:

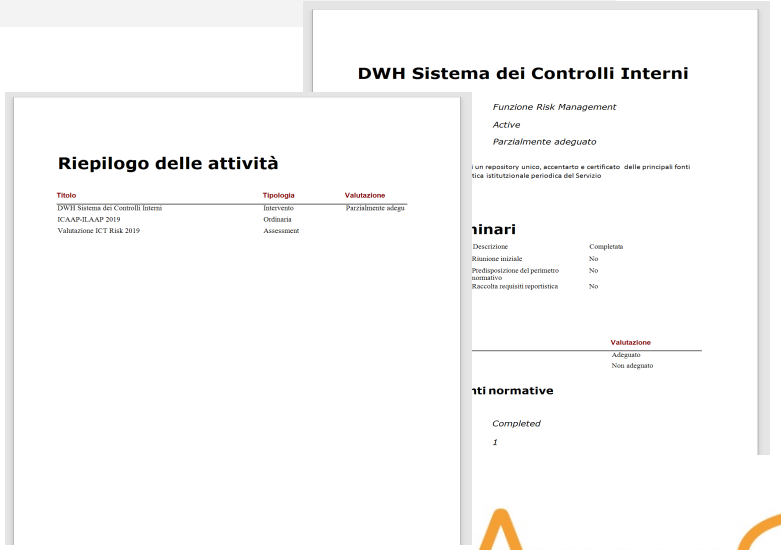
- Scalabilità
- Automazione
- Storicizzazione
- Pianificazione
- Reportistica integrata











Augeos
Servizi e tecnologia per creare valore

Grazie

SUPERVISION, RISKS
& PROFITABILITY 2021

Andrea Violato

andrea.violato@augeos.it
https://www.augeos.it
https://it.linkedin.com/pub/dir/Andrea/Violato

Augeos
Servizi e tecnologia per creare valore