

Il Continuous Auditing come garanzia di successo dell'IT Governance

Essere consapevoli del proprio livello di sicurezza per agire di conseguenza

A cura di

Alessandro Da Re
CRISC, Partner & CEO
a.dare@logicalsecurity.it

ISACA NEL 2002, POSIZIONAVA IL CONTINUOUS AUDITING A CONFINE TRA FANTASIA E REALTÀ. DI FATTO, NEGLI ATTUALI SCENARI DI IT GOVERNANCE, MONITORARE CONTINUAMENTE E SENZA SOLUZIONE DI CONTINUITÀ I RISCHI GARANTISCE L'OTTIMIZZAZIONE DELLE RISORSE E L'EFFICACIA NELLE CONTROMISURE.

NEI SISTEMI INFORMATIVI MODERNI LA NECESSITÀ DI CONTROLLO E GOVERNO DELLA SICUREZZA DELLE INFORMAZIONI AUMENTA IN MODO DIRETTAMENTE PROPORZIONALE CON LO SVILUPPO DELL'ORGANIZZAZIONE E DELL'INFRASTRUTTURA IT.

MANTENERE AGGIORNATI I SISTEMI IN AMBIENTI DISTRIBUITI ED ETEROGENEI E CONTROLLARNE COSTANTEMENTE LA CONFIGURAZIONE COSTITUISCE UN PROBLEMA SIGNIFICATIVO, DA CUI DERIVA UN INCREMENTO ESPONENZIALE DI RISCHI E INCIDENTI DI SICUREZZA.

NON È QUINDI RARO RICONTRARE, IN ORGANIZZAZIONI DI QUALSIASI DIMENSIONE, LA PRESENZA DI SISTEMI MAL CONFIGURATI, PRIVI DI MANUTENZIONE O CON EVIDENTI ESPOSIZIONI DI SICUREZZA IN TERMINI DI VULNERABILITÀ; QUESTI SISTEMI, ANCHE SE POCO NUMEROSI IN PERCENTUALE, RAPPRESENTANO UNA GROSSA OPPORTUNITÀ PER UN EVENTUALE ATTACCANTE (INTERNO O ESTERNO) CHE, SFRUTTANDO QUESTI PUNTI DEBOLI, PUÒ COMPROMETTERE L'INTEGRITÀ DEI DATI O LA CONTINUITÀ DI SERVIZIO.

IT Governance, ovviamente

Anche l'organizzazione, se priva di *Governance* e dei relativi indicatori di *performance*, rappresenta un rischio. In particolare processi di Change Management non adeguatamente controllati possono portare involontariamente ad esposizioni al rischio difficilmente valutabili.

E' inutile dire che la mancanza di indicatori di performance (KPI), contrasta con la realizzazione di un modello di *Governance* realmente efficace (*Maturity Model*) rispetto all'obiettivo di controllo.

Gli ambiti della discussione vanno spostati quindi su due fronti:

Cosa significa, per una azienda di medie dimensioni che spesso si trova a fare i conti con delle limitazioni di budget, adottare modelli di *Governance*, piuttosto che di *best practice*?

In che modo posso controllare costantemente e continuamente le esposizioni di sicurezza, siano esse organizzative o tecnologiche, per prendere innanzitutto consapevolezza della loro presenza nonché della loro natura e stabilire un piano per porvi rimedio?

La risposta a queste domande sta, secondo la nostra esperienza, nel riuscire a ritagliare su misura (*tailoring*) ciò che in questo momento è a tutti gli effetti uno standard *de facto* e principio ispiratore per la *Governance*, ossia CobiT 4.1 dove *Valore*, *Rischio* e *Controllo* diventano il nocciolo della questione, in ambienti di questo tipo:

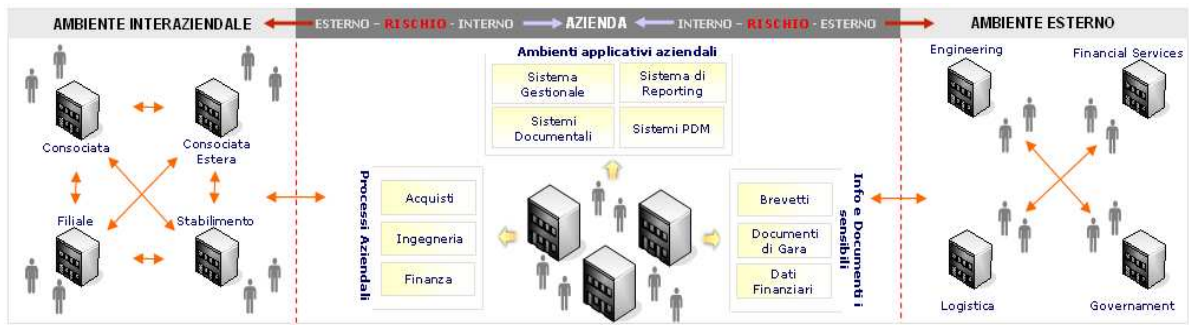


Fig. 1: Esempio flusso informativo

e dove l'ambito di intervento è riassumibile in questo schema:

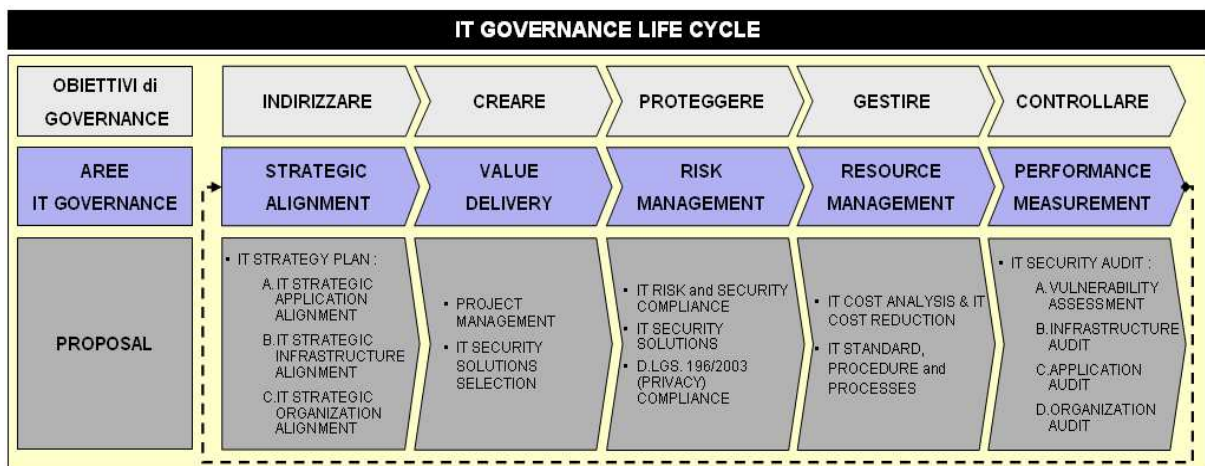


Fig. 2: Approccio strutturato alla Governance

Il Continuous Auditing non è l'acqua calda

La sfida sta nell'applicare quanto dichiarato da ISACA in un articolo del 2002 (cfr. *Information Systems Control Journal, Volume 5, 2002, Continuous Auditing: Is It Fantasy or Reality?*) quando, nella sua esposizione, definisce il *Continuous Auditing* la panacea per la "diagnosi precoce" delle vulnerabilità presenti in un sistema informativo, come evidenziato nei grafici che seguono:

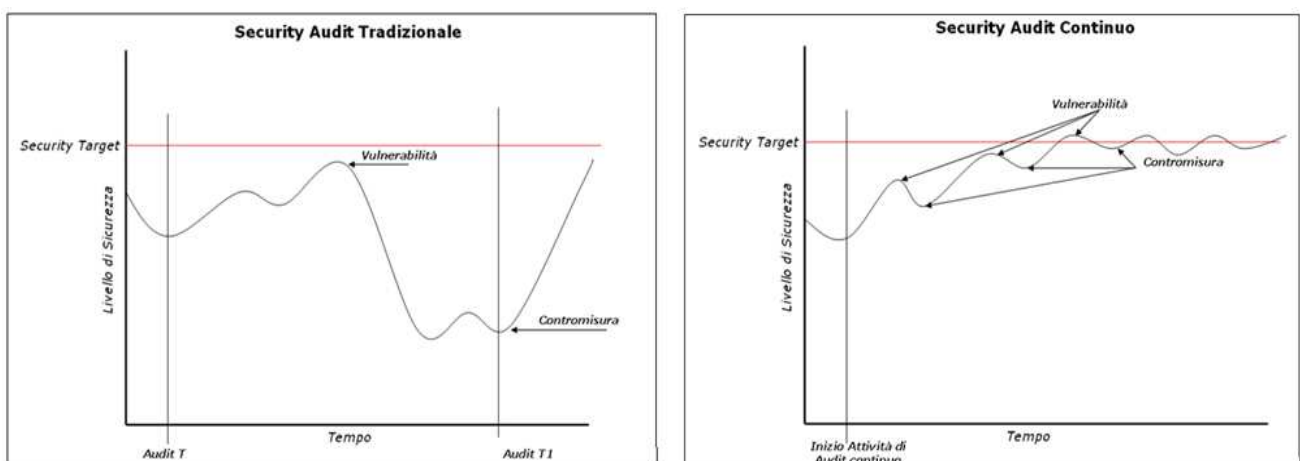


Fig. 3: Modelli di Audit a Confronto

L'esperienza ci porta a dire che in genere le debolezze sono rilevate solo da revisioni periodiche a tappeto, quando sono presenti negli assets da diverso tempo (anche sei mesi o un anno): per tutto questo tempo esse costituiscono fonte di un potenziale rischio.

L'approccio che riteniamo utile e necessario per un'azienda è quello di investire nello sviluppo di alcuni principi di *Governance*, anche per la Sicurezza, con l'obiettivo di dare all'organizzazione, in ogni momento, la piena consapevolezza del livello di sicurezza realmente raggiunto e dei rischi ancora presenti, così da dar modo di agire in tempo per prevenire incidenti.

Questo approccio prevede da un lato un controllo costante, tale da individuare le potenziali debolezze appena si manifestano e quindi ragionevolmente prima che possano essere sfruttate da aggressori, dall'altro un'informativa continua e completa al management per mantenerlo aggiornato sui rischi realmente esistenti e quindi per consentirgli di avviare tempestivamente le azioni correttive.

Il modello deve prevedere un sistema di monitoraggio intelligente, che consideri tutte le componenti con un impatto sulla sicurezza, ne rilevi le debolezze, le misuri e presenti al Manager un semplice "cruscotto" grazie al quale conoscere, con un sol colpo d'occhio, il livello di sicurezza complessivo in cui si trova in quel momento la propria rete aziendale. Come conseguenza della presa visione della situazione generale, il Manager può decidere l'urgenza dell'azione e poi monitorare nel tempo i risultati degli interventi dei tecnici.

Per contro il tecnico deve essere in grado, a fronte di una diminuzione del livello di sicurezza, di scendere in dettaglio sui componenti più deboli e sulle singole vulnerabilità per analizzarle e rimuoverle. Naturalmente occorre uno strumento di supporto: se pensiamo solamente alla gestione dei sistemi in un *environment* IT distribuito con centinaia di calcolatori in rete, dislocati su siti remoti, non sarebbe assolutamente né semplice né immediato individuare il calcolatore che rappresenta una minaccia per l'infrastruttura, né tantomeno individuarne le vulnerabilità.

Come si vede, si tratta di concetti semplici da definire ma complessi da realizzare.

Metriche di Sicurezza: bella idea, ma quali?

Occorre in primo luogo selezionare gli indicatori da controllare, scegliendo quelli che impattano più significativamente sulla sicurezza, dare loro un "peso" (quanto cioè contribuiscono al livello di sicurezza) e poi monitorarli continuamente in modo automatico e su tutto il perimetro esistente.

Successivamente occorre definire le "*metriche di sicurezza*", ovvero un metodo *oggettivo* per uniformare il monitoraggio in un ambiente *soggettivo*, dei singoli indicatori e produrre un unico indice globale di sicurezza. Diventa importante riflettere sull'interazione che queste variabili hanno sulla sicurezza in uno specifico ambiente, perché da questo si ricavano i criteri con cui ponderare l'influenza di ciascuna variabile.

Armonizzare successivamente i dati raccolti sta alla base del calcolo di un indice di sicurezza in grado di fornire una prima valutazione sullo stato di salute del sistema di *Governance* e dello stesso sistema informativo; il modello che si applica allo scopo è riassunto nello schema a blocchi che segue:

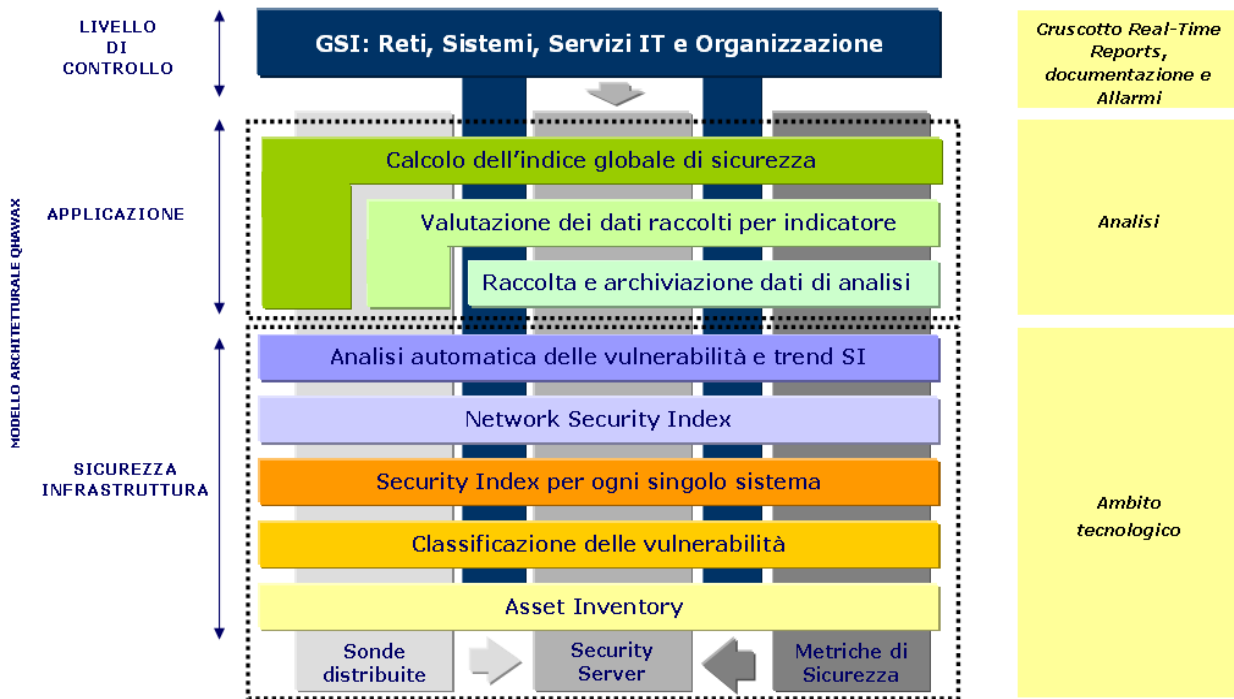


Fig. 4: Modello e approccio di controllo strutturato

L'approccio di Logical Security

Fin dai primi Documenti programmatici sulla sicurezza e relativa "analisi dei rischi che incombono sui dati", parliamo ormai di quasi 13 anni or sono, notavamo che sistematicamente ad ogni audit di conformità annuale, la presenza ricorsiva di vulnerabilità note o nuove non gestite, che vanificavano regolarmente l'attività di applicazione delle contromisure tecnologiche (leggi *patch management*). E' un problema organizzativo di "Governo" delle infrastrutture, è chiaro, ma anche e soprattutto di "costante controllo".

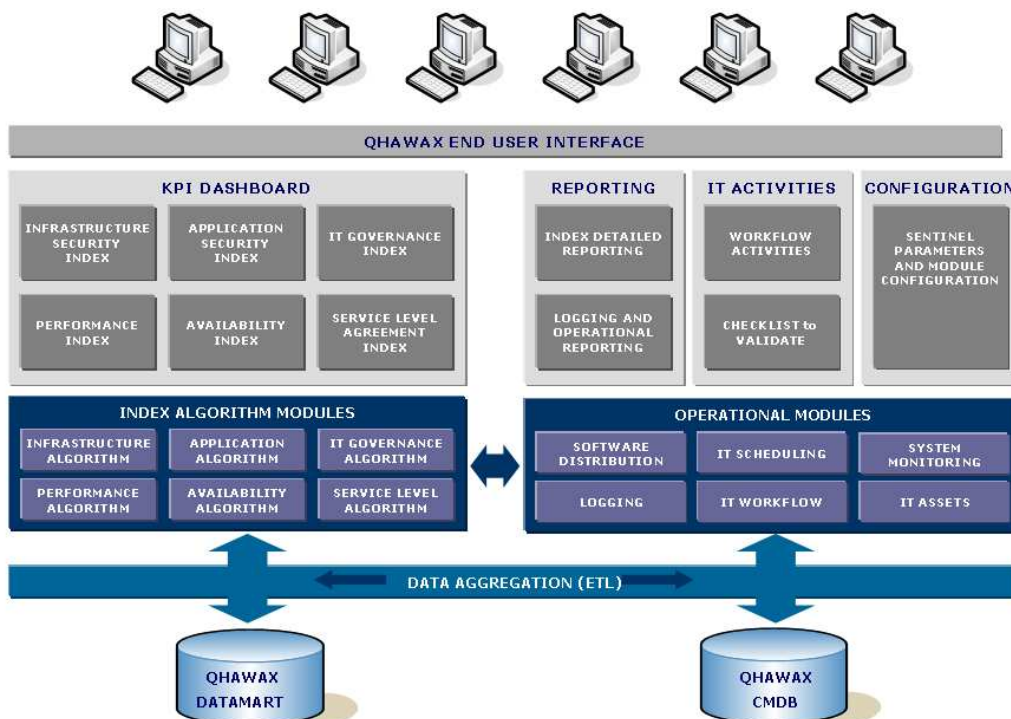


Fig. 5: Qhawax workflow

In questo contesto è nata una soluzione di ausilio al governo dei sistemi che consente di controllare continuamente l'ambiente, di individuare le debolezze e misurare il livello di sicurezza complessivo, utilizzando una interfaccia di gestione e controllo semplice ed intuitiva.

Qhawax, questo il nome del sistema di controllo, facilita lo sviluppo dell'approccio del *Continuous Auditing* che risulta fondamentale per una efficace gestione della Sicurezza.

Questa tecnologia brevettata, è stata presentata in anteprima in occasione del 7° Forum Expo ICT Security.



Fig. 6: Esempio di dashboard di controllo Qhawax