ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Dipartimento di Informatica
Facoltà di Scienze M.F.N.
Università di Roma "La Sapienza"

COBIT

CASE STUDY

NOTE SUL RELATORE :

Ing. Marcello Mistre (marcello.mistre@sistinf.it)

Membro del comitato direttivo di Isaca Roma, è certificato CISA, CISM, Lead auditor BS7799/ISO27001

E' responsabile dell'offering "audit e sicurezza informatica" di Sistemi Informativi S.p.A., società di IBM.

PROBLEMA :

Dato un certo numero di organizzazioni eterogenee che hanno in comune solo il fatto di essere connesse ad una stessa rete trovare:

1. Un valore dello stato della sicurezza per ognuna delle organizzazioni
2. Un valore dello stato complessivo della sicurezza dell'insieme delle organizzazioni

VINCOLI :

Impossibilità di svolgere attività presso le singole organizzazioni

Impossibilità di conoscere la documentazione di sicurezza delle organizzazioni

SOLUZIONE

COBIT!!!

SCELTA DEGLI OBIETTIVI DI CONTROLLO

Gli obiettivi di controllo previsti in COBIT non erano in linea con quanto si intendeva misurare

Sono stati definiti nuovi obiettivi di controllo

Sicurezza organizzativa: rappresenta il processo tramite il quale si esplica la capacità da parte di una organizzazione di dotarsi di strumenti di tipo organizzativo per gestire la sicurezza nel proprio ambito

Sicurezza logica: rappresenta il processo tramite il quale si esplica la capacità di una organizzazione di mettere in campo delle contromisure di sicurezza logica che contrastino efficacemente i rischi

Sicurezza fisica e di ambiente: rappresenta il processo tramite il quale si esplica la capacità di una organizzazione di attuare le opportune misure in grado di preservare la sicurezza degli ambienti fisici, delle macchine e degli apparati di comunicazione.

Pur se tali obiettivi di controllo sono diversi da quelli definiti dal COBIT®, una serie di controlli di dettaglio sono derivati dai seguenti obiettivi di controllo standard:

- PO9: Assess and manage IT risks;
- DS5: Ensure systems security,

I controlli sono dedotti dalle Audit Guidelines del COBIT®

Ad ogni obiettivo di controllo viene associato un set di domande con risposta di tipo SI/NO

I tre set di domande costituiscono una checklist da inviare periodicamente al responsabile della sicurezza di ogni organizzazione

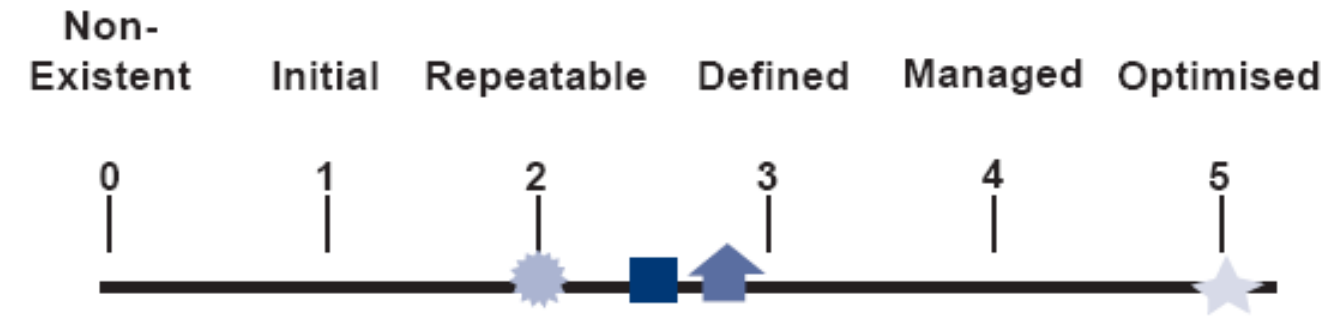
Ad ogni risposta positiva viene assegnato un punto

APPLICAZIONE DEL MATURITY MODEL

Il modello di Maturità dei processi del COBIT® è uno strumento dell'IT Governance che consente di misurare il livello di evoluzione dei processi dell'IT rispetto al controllo interno.

Il modello di maturità consente alle organizzazioni di rilevare il proprio grado di maturità in una scala da "Non esistente" (0) a "Ottimizzato" (5).

Tale classificazione può essere utilizzata per supportare la Direzione nel governo dell'IT, vale a dire nell'esercitare la responsabilità di direzione relativamente all'utilizzo dell'IT rispetto al controllo interno.



LEGEND FOR SYMBOLS USED

- Enterprise Current Status
- International Standard Guidelines
- Industry Best Practice
- Enterprise Strategy

LEGEND FOR RANKINGS USED

0	Non-Existent	— Management processes are not applied at all
1	Initial	— Processes are ad hoc and disorganised
2	Repeatable	— Processes follow a regular pattern
3	Defined	— Processes are documented and communicated
4	Managed	— Processes are monitored and measured
5	Optimised	— Best practices are followed and automated

RANKING

Per ogni obiettivo di controllo viene associato un range di risposte positive a un ranking del maturity model

ESEMPIO

Range di risposte positive	Rank
0 - 0	0
1 - 2	1
3 - 4	2
5 - 6	3
7 - 9	4
10 - 10	5

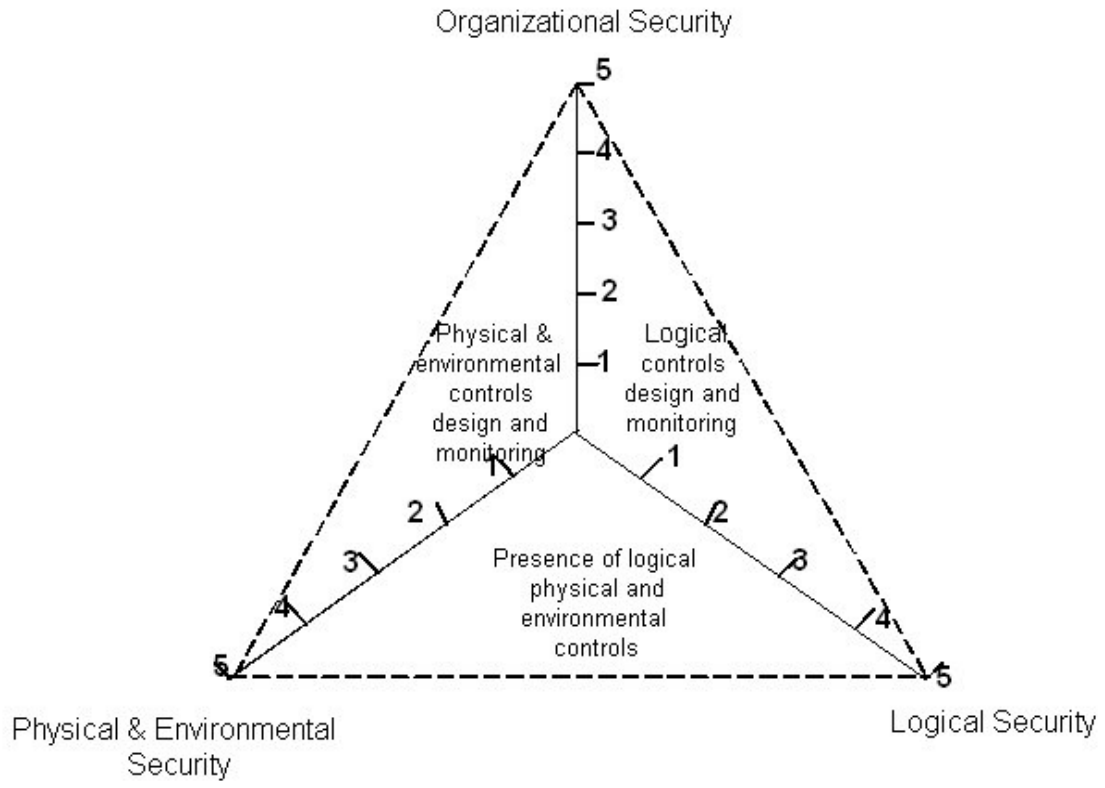
MATRICE DELLA SICUREZZA

In base ai risultati ottenuti verranno dedotti, per ogni organizzazione, i ranking del Maturity Model per ognuno degli obiettivi di sicurezza.

Il risultato di tale elaborazione permette di tracciare per ogni organizzazione, una matrice a tre dimensioni dello stato della sicurezza, che consente di determinare il livello raggiunto.

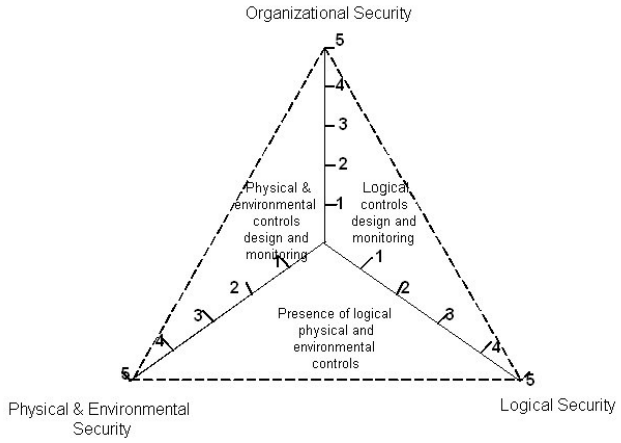
GRAFICO DELLA MATRICE DI SICUREZZA

Il risultato ottenuto può essere anche determinato in forma grafica

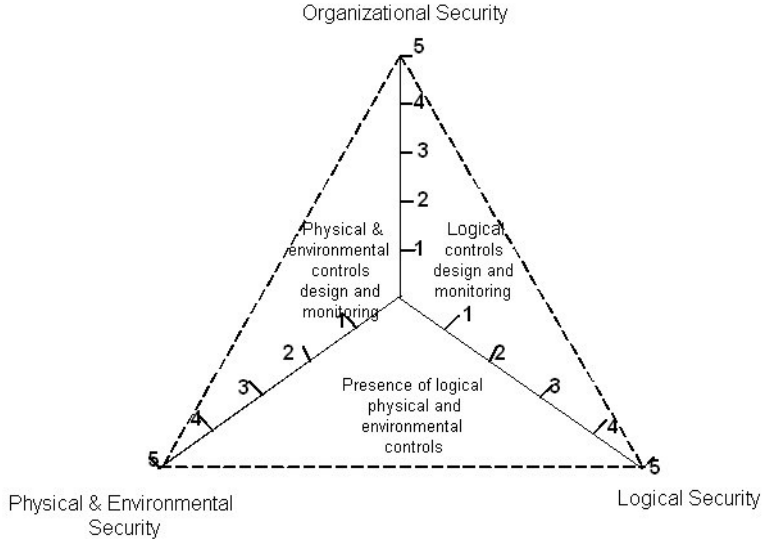


Dalla figura si può notare che le aree determinate dai singoli assi cartesiani, rappresentano la misura di specifiche grandezze

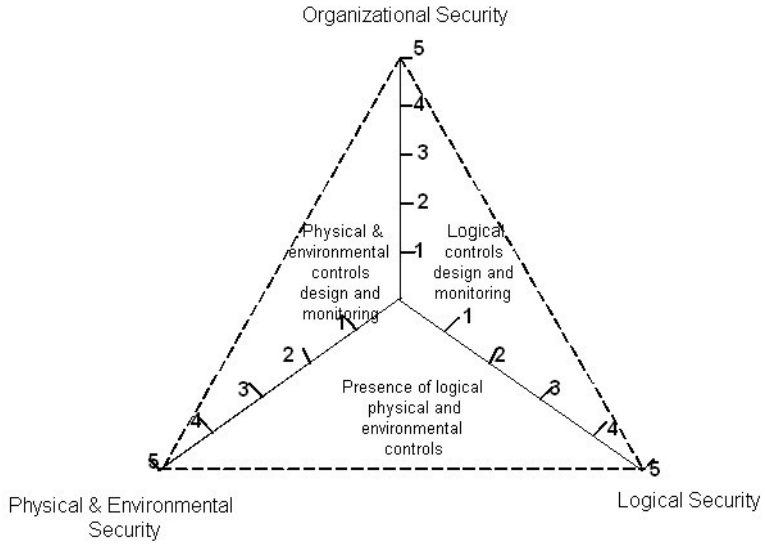
L'area compresa tra l'asse della sicurezza organizzativa e l'asse della sicurezza logica, rappresenta graficamente la misura in cui l'organizzazione attua processi di definizione e monitoraggio delle misure di sicurezza logica



L'area compresa tra l'asse della sicurezza organizzativa e l'asse della sicurezza fisica e ambientale, rappresenta graficamente la misura in cui l'organizzazione attua processi di definizione e monitoraggio delle misure di sicurezza fisica e dell'ambiente tecnologico



L'area compresa tra l'asse della sicurezza logica e l'asse della sicurezza fisica e ambientale, rappresenta graficamente la misura in cui l'organizzazione è dotata di contromisure di sicurezza logica, fisica e dell'ambiente tecnologico



MISURAZIONE DELLA SICUREZZA COMPLESSIVA

Per poter ottenere tale risultato si prenderanno in considerazione, per ogni obiettivo di sicurezza, i valori di ranking rilevati per ogni organizzazione.

Si noti che in questo caso, non è possibile assegnare un certo valore di ranking complessivo se tutte le organizzazioni non l'hanno raggiunto, dato che la sicurezza deve essere sempre essere rapportata alla misura dell'anello più debole della catena

In questo modo però il Maturity Model non darebbe alcuna indicazione su quanto è prossimo il raggiungimento del livello di ranking successivo

MISURAZIONE DELLA SICUREZZA COMPLESSIVA

Pertanto in questo caso il livello raggiunto di ogni obiettivo di sicurezza non verrà fornito con valori interi da zero a cinque, bensì con un valore incrementato di uno o più decimali secondo la formula seguente:

$$RTOT = RMIN + \frac{NSUP}{NTOT}$$

MISURAZIONE DELLA SICUREZZA COMPLESSIVA

$$RTOT = RMIN + \frac{NSUP}{NTOT}$$

In cui:

RTOT è il livello di ranking complessivo raggiunto;
RMIN è il livello di ranking più basso raggiunto dalle organizzazioni
NSUP è il numero di organizzazioni che hanno superato il livello RMIN
NTOT è il numero totale delle organizzazioni monitorate

Il risultato del rapporto verrà arrotondato per difetto al primo decimale.

ESEMPIO DI CALCOLO

Supponiamo che le organizzazioni monitorate siano complessivamente venti e che l'ultima rilevazione, relativamente a un obiettivo di sicurezza abbia dato i seguenti risultati:

- 6 organizzazioni hanno valore 2 di ranking;
- 10 organizzazioni hanno valore 3 di ranking;
- 4 organizzazioni hanno valore 4 di ranking.

Il valore di ranking complessivo per quell'obiettivo di sicurezza sarà

$$RTOT = 2 + \frac{14}{20} = 2{,}7$$

ESEMPIO DI CALCOLO

Se alla successiva rilevazione, tre delle sei organizzazioni che avevano livello 2, avessero raggiunto il livello 3, il nuovo valore di ranking complessivo per quell'obiettivo di sicurezza sarà

$$RTOT = 2 + \frac{16}{20} = 2{,}8$$