ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Come rappresentare l'azienda ai fini della gestione della sicurezza delle informazioni

(a cura di **M Cecioni** – CISA - Securteam)

INDICE DELLA PRESENTAZIONE :

1. L'esigenza
2. Perchè occuparsi del modello
3. I tre modelli
4. Requisiti della rappresentazione
5. Modello per componenti
6. Modello per informazioni e componenti
7. Modello per servizi, informazioni e componenti
8. Discussione ed osservazioni

Come rappresentare l'azienda ai fini della gestione della sicurezza delle informazioni

- Per rispondere alle esigenze di sicurezza delle informazioni per il proprio business molte aziende o amministrazioni stanno impostando e realizzando il sistema di gestione (SGSI)
- Nella definizione del SGSI si utilizzano standard (ISO 27001, ISO TR 18004, COBIT, GMITS, metodologie di RA,..) linee guida e normative (ISO 17799, Privacy, SOX, Basilea II, SOLVENCY, HIPAA,…)
- L'applicazione degli standard e normative richiede una loro mappatura sull'organizzazione
- Tale mappatura richiede una rappresentazione (modello) dell'organizzazione specifica ai fini della definizione SGSI perché i modelli tradizionali (organigramma, schemi architetturali, diagramma di dati e processi, …) non coprono tutti gli aspetti di sicurezza

Perchè occuparsi del modello?

- Perché il modello costituisce la cerniera fra standard e normative e la loro pratica applicazione nel contesto aziendale
- Perché il modello utilizzato in azienda è strettamente legato a come viene percepita ed affrontata la sicurezza.
- Perche il modello utilizzato costituisce anche un vincolo alla crescita di maturità ed al legame del processo di sicurezza alla missione e business dell'azienda
- Perché analizzare la rappresentazione utilizzata è una maniera pragmatica e semplice di effettuare un'assessment ad alto livello.
- Perché cambiare modello, ovvero la vista dell'azienda per i particolari fini, costituisce sempre il primo passo di un efficace cambiamento.

Requisiti dei modelli

- I modelli soddisfano i seguenti requisiti
  - collegamento SGSI con missione/business
  - auditability: presenza di riferimenti
  - accountabilty: articolazione delle responsabilità per la sicurezza delle informazioni
    - di adeguato dettaglio
    - formalizzata e chiara
    - in linea con la struttura organizzativa.

I tre modelli

- La presentazione illustra tre modalità di rappresentare l'azienda

- I tre modelli hanno una complessità e costo di realizzazione crescente

- I modelli sono:
  - Modello per componenti
  - Modello per informazioni e componenti
  - Modello per servizi, informazioni e componenti

Modello per Componenti

- Questo tipo di modello si focalizza solo sulle risorse aziendali utilizzate per trattare le informazioni.
- Ogni risorsa a cui si riconducono delle contromisure per specifiche minacce alla sicurezza delle informazioni si candida ad essere presa in considerazione
- Tali risorse nel seguito le chiamiamo Componenti.

Caratteristiche del modello per Componenti

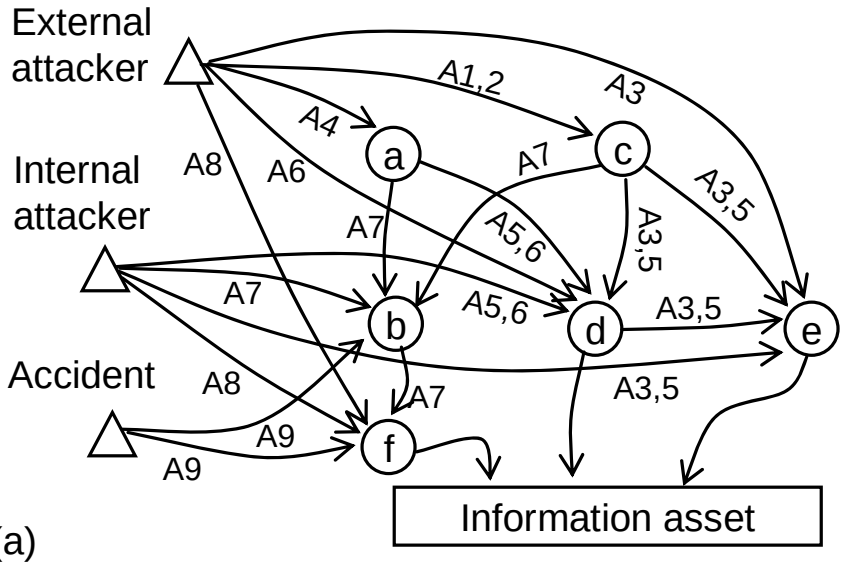
- ad ogni Componente vengono ricondotte delle contromisure di sicurezza
- le contromisure sono realizzate prendendo come riferimento le migliori pratiche del settore in cui l'azienda opera
- permette di eseguire l'assessment di conformità alle migliori pratiche adottate come riferimento
- ha un collegamento debole con la missione ed il business dell'azienda costituito dalla scelta delle migliori pratiche di riferimento
- l'analisi del rischio (se viene effettuata) tiene in conto gli aspetti più delle singole infrastrutture che del business

Due modelli a confronto

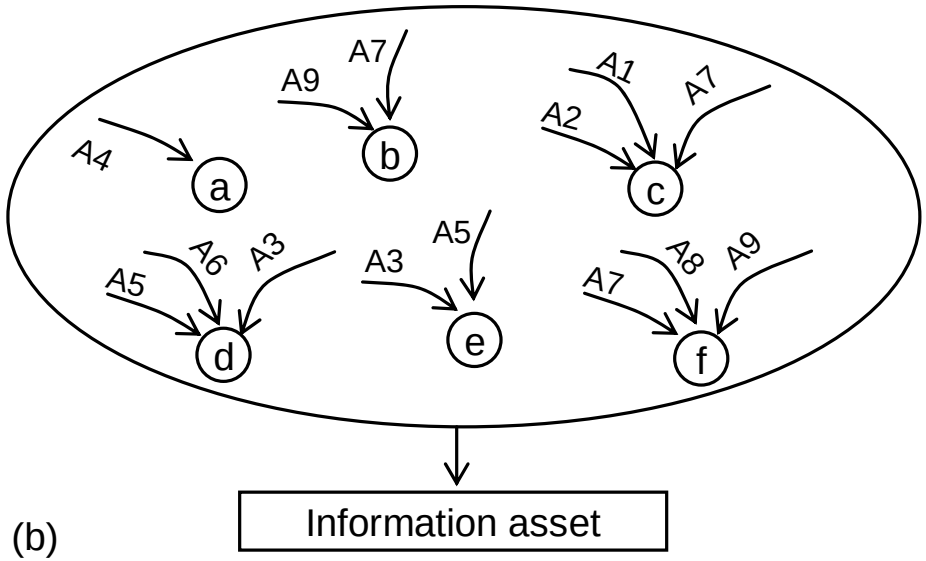
(a) office (b) PC (c) personnel

(d) operating system (e) application sw (f) hard disk

A1 Bribing
A2 Social engineering
A3 Malicious sw injection
A4 Physical intrusion
A5 Theft of identity
A6 Unauthorised access through the network
A7 Theft
A8 Residual information access
A9 Hw failure



(a)



(b)

Il disegno è stato ripreso da SAFE 2005 - First International Conference on Safety and Security Engineering
Key Issues in the Development of Risk Analysis Methodologies and Tools
by Giulio Carducci, Paolo Migliaccio and Emilio Montolivo

Responsabilità per Componente

- Per avere una buona accountability occorre avere cura nell'individuare i Componenti in maniera che la gestione delle contromisure possa essere riferita ad una responsabilità unica e definita in azienda.
- Tale figura di seguito la chiamiamo Gestore del Componente
- Il Gestore viene individuato nell'ambito della struttura aziendale che ha in carico la risorsa caratteristica del Componente.
- Il Gestore ha la responsabilità per la definizione, la realizzazione, la gestione ed il miglioramento delle contromisure di sicurezza attuate dal Componente.

Componenti: approfondimento

- I Componenti sono caratterizzati:
  - dalle minacce a loro riferibili
  - dalle vulnerabilità che eventualmente offrono e che possono essere sfruttate dalle minacce
  - dalle contromisure riferibili al componente che possono essere attuate per contrastare le minacce
- L'insieme delle contromisure con le minacce che contrastano rappresentano il Profilo di Protezione del Componente.
- L'analisi del rischio viene condotta per Componenti

Esempi di Componenti e Profili di Protezione

- Personale - Dipendenti

		Abuso di privilegi	Accesso non autorizzato	Errore umano	Furto e sabotaggio	Carenze organizzative
		M01	M03	M06	M07	M15
6.1.5	Accordi di riservatezza	X				
8.1.1	Ruoli e responsabilità					X
8.1.2	Selezione	X			X	
8.1.3	Termini e condizioni di impiego	X				X
8.2.2	Consapevolezza, formazione e istruzione sulla sic. dell'inf.			X		
8.2.3	Processo disciplinare	X			X	
8.3.1	Responsabilità nella fine dell'impiego					X
8.3.2	Restituzione dei beni					X
8.3.3	Rimozione dei diritti di accesso		X			

Esempi di Componenti e Profili di Protezione

- Processo – Gestione utenti e autorizzazioni

		Abuso di privilegi M01	Accesso non autorizzato M03	Carenze organizzative M15
8.03.03	Rimozione dei diritti di accesso		X	
10.01.01	Documentazione delle procedure operative			X
10.01.03	Separazione delle funzioni	X		
10.10.01	Log di audit	X		
10.10.02	Monitoraggio sull'uso del sistema	X		
11.02.01	Registrazione degli utenti			X
11.02.02	Gestione dei privilegi		X	
11.02.03	Gestione delle password degli utenti		X	
11.02.04	Verifica dei diritti di accesso degli utenti		X	

Categorie ISO 17799

05	Politica di sicurezza
06	Organizzazione della sicurezza delle informazioni
07	Gestione dei beni
08	Sicurezza delle risorse umane
09	Sicurezza fisica e ambientale
10	Gestione delle comunicazioni e delle operazioni
11	Controllo accessi
12	Acquisizione, sviluppo e manutenzione dei sistemi informativi
13	Gestione degli incidenti di sicurezza delle informazioni
14	Gestione della continuità del business
15	Conformità

Tipi di Componenti

- Si possono avere varie tipologie di Componenti quali hardware, software, logistiche, di processo e di persone.

- Lo schema dei Componenti e l'assegnazione delle minacce e delle contromisure ha un certo grado di variabilità che dipende dalle specificità dell'azienda e dal grado di approfondimento che si vuole ottenere.

Esempio schema di Componenti

Hardware	Server
	Postazioni di lavoro
	Apparati di rete
Software	Software di sistema
	Software applicativo
	DBMS
Logistica	Edificio
	Sala Server Farm
Personale	Dipendenti
Processo	Acquisto di beni/servizi e prestazioni
	Gestione operativa rete
	Gestione operativa delle elaborazioni
	Supporto sistemistico
	Continuità del business
	Gestione Accessi
	Gestione AntiVirus
	Gestione della sicurezza perimetrale
	Gestione Incidenti
	Sviluppo e manutenzione applicazioni
	Servizi Tecnici
	Gestione della Sicurezza delle Informazioni

Componenti Hardware

- Esempi: i server, apparati di rete, dispositivi di memorizzazione, ecc.
- Possono essere soggetti a guasti e danneggiamenti.
- Per contrastare tali minacce il reparto che si occupa di physical planning e manutenzione hardware può prevedere delle contromisure quali il piano di manutenzione preventiva, la ridondanza delle risorse critiche, il loro posizionamento fisico corretto, ecc.

Componenti Software

- Esempi: i sistemi operativi, il software applicativo, il DBMS, il sistema operativo, ecc.
- Attuano delle contromisure per contribuire a contrastare varie minacce alle informazioni.
- Fra le contromisure realizzate tramite meccanismi software vi sono il logging per l'accountability, la crittografia per la riservatezza, il controllo accesso con ACL, la firma elettronica per il non ripudio, i checksum, digest per l'integrità, ecc.

Componenti Logistici

- Esempi: edifici, sale CED, uffici, cablaggi, impianti ausiliari, ecc.
- Sono soggetti a minacce quali intrusioni, allagamenti, incendi, guasti e danneggiamenti.
- Per contrastare tali minacce il reparto che si occupa di logistica, impianti e sicurezza fisica, può prevedere delle contromisure quali sistemi di antintrusione, controllo accesso fisico, sistemi antincendio ed antiallagamento, ecc.

Componenti Personale

- Esempi: amministratore di sistemi, amministratore dei profili di autorizzazione agli accessi, addetti alle operazioni, ecc.
- Possono essere portatori di minacce quali errori umani, abuso di privilegi, collusioni in frodi, ecc..
- Per contrastare tali minacce si possono prevedere, da parte del reparto dei Gestione delle risorse umane, delle contromisure quali l'accurata selezione anche per aspetti di affidabilità del personale critico per la sicurezza, la formazione tecnica continua, la disciplina sanzionatoria, la separazione di funzioni, ecc.

Componenti Processi

- Esempi: impostazione della sicurezza, autorizzazione agli accessi, passaggio in produzione, gestione elaborazioni, audit di conformità, ecc.
- Il processo può essere soggetto ad errori, disallineamento con le variazioni organizzative (ruoli), ecc.,, ma principalmente contribuisce insieme ad altre Componenti a contrastare varie minacce alle informazioni.
- Per contrastare tali minacce si possono prevedere delle contromisure quali la definizione dei ruoli opportuna e chiara, il monitoraggio, la gestione del cambiamento, degli incidenti, delle autorizzazioni agli accessi, le verifiche ispettive periodiche, ecc.

Componenti		Sez. ISO 17799
Hardware	Server	09
	Postazioni di lavoro	09
	Apparati di rete	09
Software	Software di sistema	10, 11
	Software applicativo	10, 11, 12
	DBMS	10, 11
Logistica	Edificio	09
	Sala Server Farm	09
Personale	Dipendenti	08
Processo	Acquisto di beni/servizi e prestazioni	06, 12
	Gestione operativa rete	10
	Gestione operativa delle elaborazioni	10
	Supporto sistemistico	10, 12
	Continuità del business	14
	Gestione Accessi	10, 11
	Gestione AntiVirus	10
	Gestione della sicurezza perimetrale	10, 11
	Gestione Incidenti	13
	Sviluppo e manutenzione applicazioni	12
	Servizi Tecnici	09
	Gestione della Sicurezza delle Informazioni	05, 06, 07,15

Modello per Informazioni e Componenti

- In tale modello sono previste due dimensioni
  - Informazioni
  - Componenti

- Nel modello occorre indicare in quali componenti sono trattate le singole informazioni

Informazioni

- Le informazioni si caratterizzano in termini di criticità verso Riservatezza, Integrità, Disponibilità (RID)
- La criticità è funzione dell'impatto al business che l'organizzazione avrebbe se perdessero le loro qualità RID
- Per ogni informazione deve essere identificato il Proprietario

Correlazione
Componenti - Informazioni

Componenti		Inf. A	Inf. B
Hardware	Server A	X	
	Server B		X
	Postazioni di lavoro	X	X
	Apparati di rete	X	X
Software	Software di sistema		
	Software applicativo A	X	
	Software applicativo B		X
	DBMS		X
Logistica	Edificio	X	X
	Sala Server Farm	X	X
Personale	Dipendenti	X	X
Processo	Acquisto di beni/servizi e prestazioni	X	X
	Gestione operativa rete	X	X
	Gestione operativa delle elaborazioni	X	X
	Supporto sistemistico	X	X
	Continuità del business	X	X
	Gestione Accessi	X	X
	Gestione AntiVirus	X	X
	Gestione della sicurezza perimetrale	X	X
	Gestione Incidenti	X	X
	Sviluppo e manutenzione applicazioni	X	X
	Servizi Tecnici	X	X
	Gestione della Sicurezza delle Informazioni	X	X

Caratteristiche

- le contromisure sono realizzate tenendo conto dei requisiti di sicurezza delle informazioni trattate indicati dai proprietari e delle migliori pratiche
- permette di eseguire l'assessment di conformità ai requisiti indicati per le informazioni e alle migliori pratiche
- ha un collegamento forte con le esigenze, anche di business, delle informazioni
- l'analisi del rischio con tale modello tiene in conto sia gli aspetti delle singole infrastrutture sia quelli di business legati alle informazioni
- due figure: proprietario dei dati e gestori componente: vi è una migliore separazione delle funzioni, ma richiede una gestione super partes

Modello per servizi, informazioni e componenti

- Il servizio, con tutte le risorse coinvolte per la sua erogazione, rappresenta l'ambito dell'analisi di sicurezza e della sua gestione.
- Tale ambito viene denominato nel seguito "Perimetro".
- E' il modello più complesso che prevede più Perimetri in funzione dei servizi erogati dall'organizzazione
- Permette la realizzazione del SGSI per gradi un Perimetro alla volta (combined approach) partendo dai più critici

Perimetri

- Sono orientati alla missione di business
- Sono caratterizzati
  - dalle informazioni che gestiscono
  - dalle risorse che hanno influenza sul trattamento dell'informazione (Componenti)
- L'analisi di sicurezza viene condotta per singoli Perimetri
- Per ogni Perimetro è prevista la figura di Responsabile del Servizio individuata nell'ambito della struttura che gestisce i rapporti con il committente del sevizio (Service Manager, Account Manager)

Profilo di Protezione del Perimetro

- L'assessment delle minacce e delle contromisure viene eseguito per Componente. L'assessment definisce il livello di esposizione per ogni minaccia e la robustezza per ogni contromisura.
- L'assessment e la gestione del rischio, che tengono in conto l'impatto per lo specifico servizio, vengono eseguiti per Perimetro.
- Lo schema permette di analizzare se il Profilo di Protezione del Perimetro (somma dei Profili di Protezione di tutti i Componenti) è adeguato al rischio ovvero alla criticità delle informazioni che sono alla base del servizio erogato ed al livello di esposizione delle minacce.

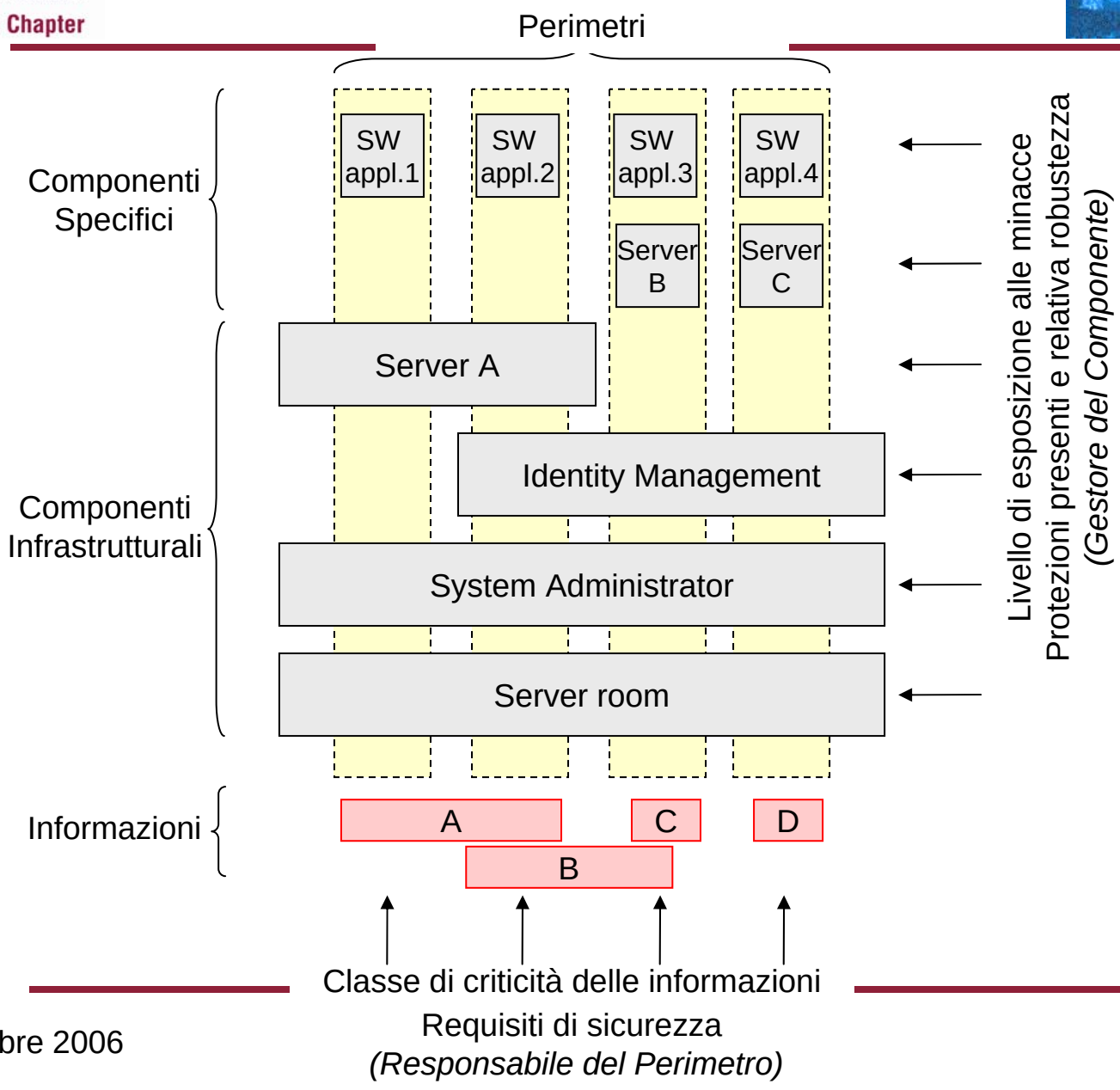
Perimetro e Componenti

- In un Perimetro si possono avere:
  - Componenti specifici: dedicati solo all'erogazione del particolare sevizio quali per esempio server dedicato, software applicativo,
  - Componenti infrastrutturali: che partecipano in più Perimetri ovvero all'erogazione di più servizi quali per esempio server mainframe, sala sever.

Servizi e Componenti

- La rappresentazione è di tipo matriciale a tre dimensioni:
  - La prima dimensione (verticale - Perimetri) considera il servizio informativo erogato
  - La seconda dimensione (orizzontale – Componenti) considera le risorse utilizzate per l'erogazione dei servizi
  - La terza dimensione considera le Informazioni trattate
- Le tre dimensioni sono fra loro correlate in maniera complessa

Esempio


Perimetri
Componenti Specifici
SW appl.1
SW appl.2
SW appl.3
SW appl.4
Server B
Server C
Componenti Infrastrutturali
Server A
Identity Management
System Administrator
Server room
Livello di esposizione alle minacce
Protezioni presenti e relativa robustezza
(Gestore del Componente)
Informazioni
A
C
D
B
Classe di criticità delle informazioni
Requisiti di sicurezza
(Responsabile del Perimetro)

Schema delle responsabilità

Responsabile del Servizio

- Identifica le informazioni gestite nel perimetro ed il relativo proprietario
- Classifica con il proprietario le informazioni in termini di criticità RID
- Definisce i requisiti di sicurezza in linea anche con le politiche aziendali
- Definisce lo scenario del Servizio e identifica i relativi Componenti
- Esegue l'assessment del rischio
- Verifica e monitora i livelli di sicurezza raggiunti

Gestore del Componente

- Recepisce i requisiti di protezione e concorda con i Responsabili di Servizio la loro realizzazione
- Definisce, realizza e gestisce le contromisure
- Esegue l'assessment delle minacce e delle contromisure
- Monitora l'efficacia delle contromisure

Esempio struttura