SECGOV notes

SAPIENZA
UNIVERSITÀ DI ROMA

Riccardo Versetti

NIST CSF

Ha come obiettivo quello di guidare le attività di cybesecurity di un'organizzazione. E' un framework che permette di valutare il livello di sicurezza e di migliorarlo, permettendo a chi ne fa uso di **considerare il rischio cyber** nella gestione del rischio aziendale.

È composto da 3 parti:

- **Core**: insieme di attività, prassi e linee guida per la gestione del rischio.
- **Implementation Tiers**: aiuta a determinare il livello di maturità dell'organizzazione.
- **Profile**: permette di identificare i requisiti di sicurezza e di privacy.

Core

Si divide a sua volta in:

- **Functions**: categorie di attività di sicurezza.
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- **Categories**
- **Subcategories**: sottoinsiemi di categorie.
- **Informative References**: linee guida e prassi, documenti di riferimento.

Utilizzo

Il CORE fornisce un insieme di attività e raccomandazioni che *possono* essere applicate all'organizzazione. Non è una checklist da seguire per risultare compliant.

Implementation tiers

Sono criteri che permettono di valutare il livello di maturità dell'organizzazione. Sono 4:

- **Partial**: l'organizzazione non ha una strategia di sicurezza.
- **Risk Informed**: l'organizzazione ha una strategia di sicurezza, ma non è formalizzata.
- **Repeatable**: l'organizzazione ha una strategia di sicurezza formalizzata.
- **Adaptive**: l'organizzazione ha una strategia di sicurezza formalizzata e dinamica.

Utilizzo

Risponde alla domanda: *"How rigorous and structured I am in my approach to security?"*.

Attenzione

Gli avanzamenti di livello sono consigliati solo se convenienti dal punto di vista economico.

Profiles

Funzionamento

Gli elementi del core vengono combinati con i requisiti di business, le risorse e la risk tolerance dell'organizzazione per descrivere uno stato.

Questo stato può essere:

- **Current Profile**: rappresenta lo stato attuale dell'organizzazione.
- **Target Profile**: rappresenta lo stato desiderato dell'organizzazione.

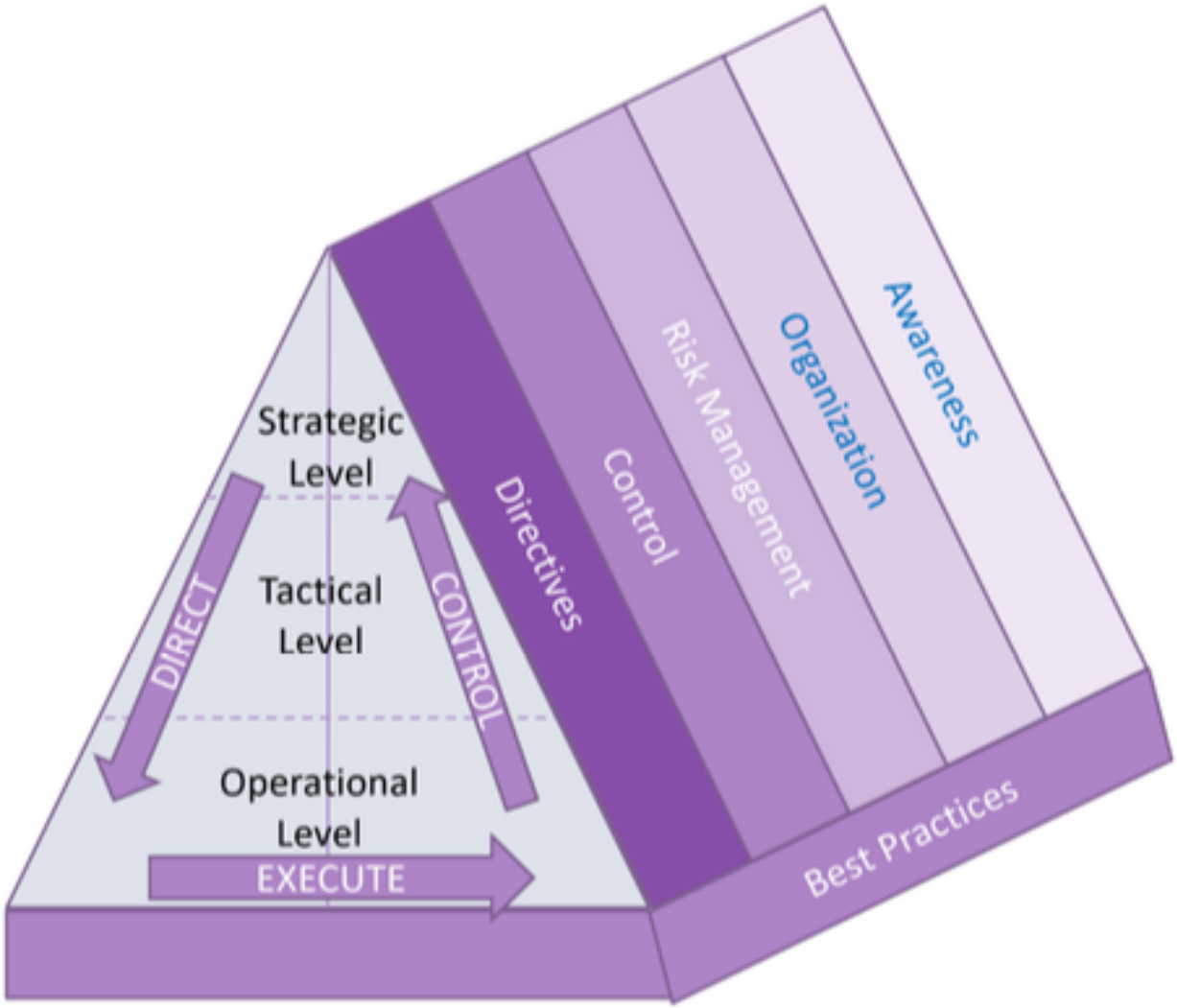
Quello che c'è in mezzo, il GAP, può essere analizzato al fine di stimare gli effort necessari per raggiungere una posizione ideale.

NIST CSF: investimenti

Obiettivo

Grazie alla possibilità di fare assessment interni, l'organizzazione può valutare la propria postura di sicurezza, valutando l'eventuale distanza dal profilo desiderato e avere una chiara visione di come pianificare gli investimenti (in termini finanziari, di tecnologie, di persone, ...) al fine di raggiungerlo.

Il modello ISG di Von Solms



Core del modello ISG

Nella parte centrale del modello ISG troviamo:

- 3 levels of management: Strategic, Tactical, Operational.
- 3 different actions (DCE loop): Direct, Control, Execute.

Ogni azione avviene in ogni livello di management.

Direct/control loop

Direct

- Strategic: definisce la strategia di sicurezza basandosi sulla vision al "c-level".
- Tactical: definisce le policy di sicurezza, procedure e standard a livello aziendale.
- Operational: implementa le policy di sicurezza, procedure e standard.

Control

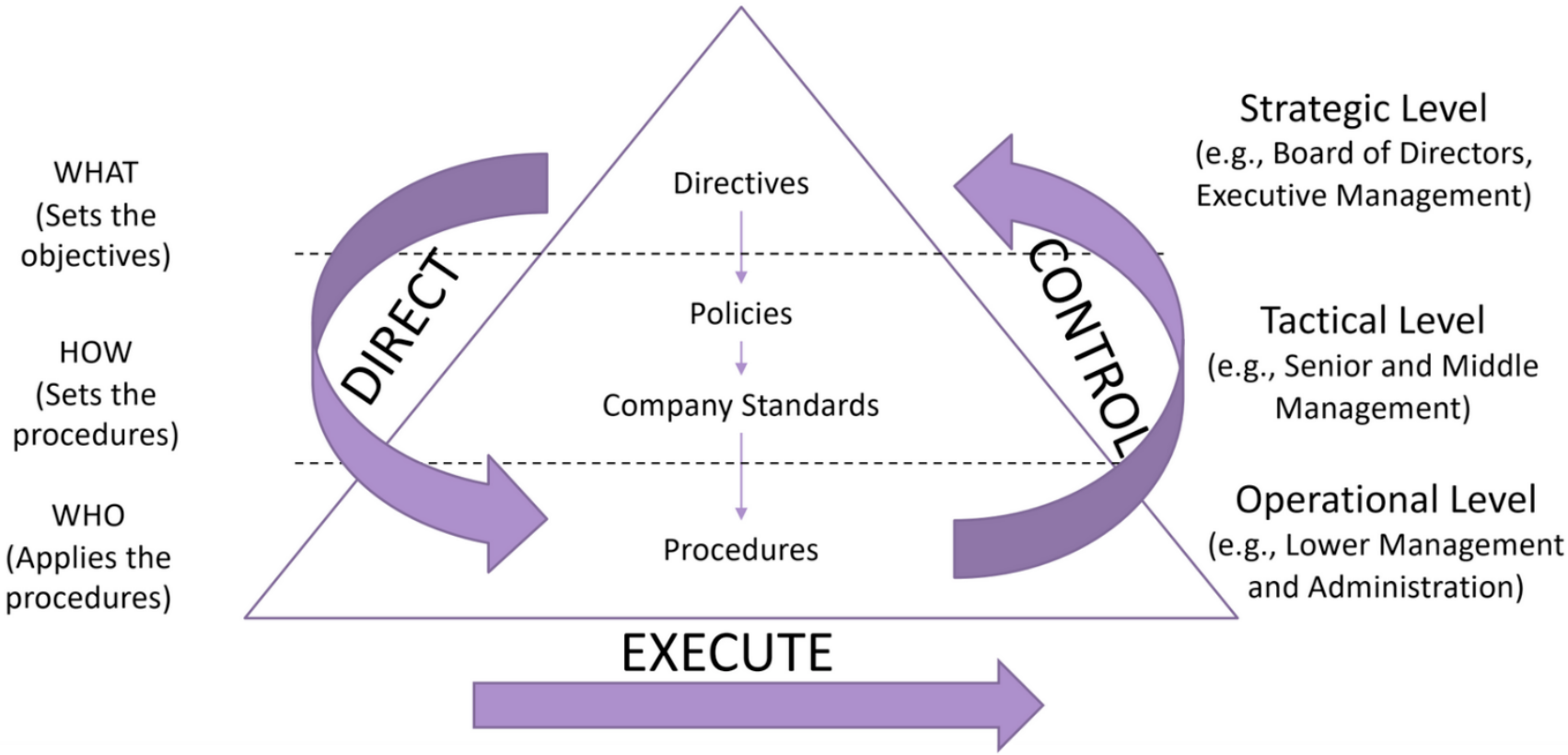
- Strategic: monitora l'efficacia della strategia di sicurezza.
- Tactical: monitora l'efficacia delle policy di sicurezza.
- Operational: dati vengono estratti manualmente o automaticamente, usando sensori, IDS, IPS, etc.

Depth del modello ISG

1. **Directives**
2. **Control**
3. **Risk management**
4. **Organization**
5. **Awareness**
6. **Best practices**

Integrare il CORE, la front dimension, in tutti gli aspetti dell'organizzazione.

Enterpise governance



SISG: standard & BPs

Le best practices e gli standard svolgono un ruolo cruciale nella progettazione e realizzazione di un sistema di Information Security Governance. La loro applicazione consente di definire un quadro strutturato e coerente per la gestione della sicurezza delle informazioni, garantendo l'allineamento con gli obiettivi aziendali e la conformità alle normative vigenti.

- Le **best practices** rappresentano un insieme di linee guida e approcci operativi consolidati, derivati dall'esperienza pratica e riconosciuti a livello internazionale.
- Gli **standard** forniscono una base formale e riconosciuta per progettare e implementare un sistema di ISG. Sono sviluppati da organismi internazionali e regolatori

Awareness nella depth ISG e il programma SETA

Il concetto di awareness rappresenta un elemento fondamentale per garantire che tutti i livelli dell'organizzazione partecipino attivamente alla protezione delle informazioni. Si concentra sull'educazione e la responsabilizzazione di dipendenti e stakeholder per adottare comportamenti sicuri.

Il programma SETA (Security Education, Training, and Awareness) è uno strumento essenziale per implementare l'awareness all'interno della dimensione di profondità del modello ISG. Ogni componente rafforza la sicurezza aziendale in modo complementare:

- **Security Education**: fornisce una formazione specialistica e approfondita sulle tematiche di sicurezza informatica.
- **Security Training**: offre un'istruzione pratica e operativa per acquisire competenze specifiche e abilità tecniche.
- **Security Awareness**: promuove la consapevolezza e la cultura della sicurezza informatica attraverso campagne di comunicazione e sensibilizzazione.

Incident management

Il processo di gestione degli incidenti è una componente essenziale della sicurezza informatica e si articola in diverse fasi che coinvolgono strutture organizzative e figure professionali specifiche. Ogni fase ha l'obiettivo di garantire che l'organizzazione sia in grado di individuare, gestire e mitigare efficacemente gli incidenti di sicurezza, oltre a imparare dall'esperienza per migliorare le difese future.

Il processo di gestione degli incidenti è un lavoro di squadra che richiede la collaborazione di molteplici figure professionali e l'uso di tecnologie avanzate. Ogni fase è essenziale per garantire che l'organizzazione possa non solo reagire agli incidenti, ma anche prevenire quelli futuri. Strutture come il SOC e programmi come il training per la consapevolezza giocano un ruolo fondamentale, integrando la tecnologia con una gestione umana competente e responsabile.

Incident management - 2

Le fasi della gestione degli incidenti

- Identificazione e classificazione dell'incidente
- Risposta e contenimento
- Investigazione e analisi
- Ripristino e recupero
- Monitoraggio e reportistica
- Apprendimento e miglioramento

ISO 27001 vs SP 800-53

ISO 27001

- **Focus**: Information Security Management System (ISMS)
- **Obiettivo**: proteggere le informazioni dell'organizzazione
- **Approccio**: basato sul risk management
- **Priorità**: non fornita

SP 800-53

- **Focus**: Information Security and Privacy Controls
- **Obiettivo**: proteggere le informazioni sensibili del governo federale
- **Approccio**: basato su controlli di sicurezza
- **Priorità**: fornita, in quanto istruzioni passo-passo

ISO 27001 vs SP 800-53 - 2

Like every FISMA standard, it is system-oriented: **viene detto come dovrebbe essere fatto**. Questo non accade con famiglia ISO.

- NIST SP ha un forte riferimento alla struttura federale US. Documento complesso ma un manager non può decidere solo con quello.
- Quasi inutile da avere al di fuori di US

ISO 27001: certificazione rilasciata da auditor (non come 27002).

- È costosa, come molte certificazioni.
- Non esiste una vera e propria *priority list*.
- Volontaria (NIST è obbligatoria in US).
- Non destinata al C-level.

Certificazioni e conformità: facciamo chiarezza

- È possibile essere certificati ISO 27001
- È possibile essere conformi a NIST SP 800-53 (**obbligatoria in US**)
- **Non** è possibile essere certificati ISO 27002: solo guidelines
- ISO 27001 è molto meno flessibile di ISO 27002
- Non è possibile essere certificati NIST CSF: consigli e auto assessment
- È possibile utilizzare NIST CSF per assessment interni

Passi per RIMA e cyber risk

1. **Scope and criteria**
   - 1.1 Internal context (struttura, processi, dipendenze)
   - 1.2 External context
2. **Risk assessment**
   - 2.1 Identification (asset, threat, vulnerability)
   - 2.2 Analysis (likelihood, impact)
   - 2.3 Evaluation (level of risk)
   - 2.4 Treatment (accept, avoid, mitigate, transfer)
3. **Risk management**
   - 3.1 Monitoring
   - 3.2 Communication
   - 3.3 Review
4. **Risk assessment**
5. **Risk treatment**

OWASP metodologia di RISK RATING

Approccio basato sul modello rischio a 2 fattori:
$Risk = Likelihood \cdot Impact$

In tutto ha 6 fasi:

1. **Identificazione dei rischi**
2. **Stima della probabilità di occorrenza**
3. **Stima dell'impatto**
4. **Calcolo della severity rischio**
5. **Decisione di cosa aggiustare**
6. **Customizzazione del modello**

Threat modeling