Information Security Value Proposition

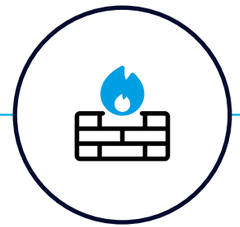
Information Security - I Servizi

SECURITY STRATEGY

Definizione della direzione

SECURITY GOVERNANCE

Creare un modello di governo risk-based

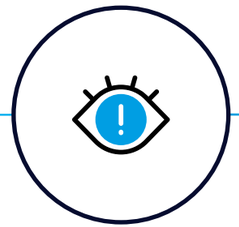


THREAT AND VULNERABILITY MANAGEMENT

Gestire i fattori di esposizione al rischio

ARCHITECTURE, INFRASTRUCTURE AND HI-TECH

Costruire sistemi ed infrastrutture sicure



BUSINESS CONTINUITY MANAGEMENT

Garantire la continuità

Security Strategy

Ad un aumento degli investimenti sulla sicurezza delle informazioni non sempre corrisponde un **reale miglioramento.**

Molte organizzazioni mostrano un approccio reattivo ai temi della sicurezza implementando, in maniera non coordinata e sistematica, specifiche soluzioni in risposta a singole minacce o violazioni.

È necessario **stabilire una strategia** di sicurezza allineata agli obiettivi di business.

Cyber4Growth definisce una strategia di sicurezza, proponendo un **approccio strutturato e stabile** per il miglioramento della sicurezza dell'informazione, aumentando il **livello di maturità** su tutti i domini della sicurezza.

- **Valutazione del livello di maturità in ambito Information Security**
- **Definizione della Roadmad e del Piano Strategico di Information Security**
- **Implementazione della Roadmap e del Piano Strategico di Information Security**
- **Definizione della Strategia di alto livello di Information Security**
- **Definizione di KPI e Dashboard di Information Security**
- **Definizione dell'organizzazione di Information Security**

Livello di Maturità attuale

Rappresentare l'attuale stato di sicurezza dell'informazione, per ogni dominio, in termini di livello di maturità, copertura dei controlli e gravità delle criticità.

Gap Analysis

Rappresentare i Gap identificati fra la situazione attuale e quella desiderata, individuando le azioni da compiere per colmare tali gap.

Piano Strategico

Rappresentare i problemi da implementare a breve, medio e lungo temine per il raggiungimento degli obiettivi strategici di sicurezza.

Comunicazione del Piano

Consultare rapidamente ed in qualsiasi momento tramite web i principali elementi della strategia di sicurezza delle informazioni.

Security Governance

Governare adeguatamente la **sicurezza delle informazioni** è fondamentale per mitigare i rischi aziendali. Attraverso una **gestione basata sul rischio** è possibile ottimizzare l'impiego delle risorse aziendali (tecnologie e persone), rispettando sempre la conformità a normative standard e di settore.

È quindi fondamentale **l'analisi e la gestione del rischio** in modo da definire ed analizzare i requisiti di sicurezza dei sistemi e delle applicazioni.

Metodologia conforme al framework nazionale per la cybersecurity.

- **Definizione e implementazione di una metodologia di Analisi di Rischi IT.**
- **Definizione di una struttura di Information Security Governance**
- **Definizione di un di Information Security Documentation Framework**
- **Definizione di un modello di Data Classification**
- **ISO 27001 Compliance Assessment, Readiness, Certification Preparation and Assistance**
- **ISO 22301 Compliance Assessment, Readiness, Certification Preparation and Assistance**
- **Dlg 65/2018**

Conformità alle leggi

Analizzare la conformità alle normative (i.e. GDPR, 262, 231 etc.) che regolano il trattamento elettronico dei dati.

Aderenza agli standard

Predisporre/assistere alla certificazione e valutare la conformità a standard internazionali sulla sicurezza della informazioni.

RACI

Rappresentare la matrice di assegnamento delle responsabilità: Responsible, Accountable, Cosulted, Informed.

Risk Analysis Tool

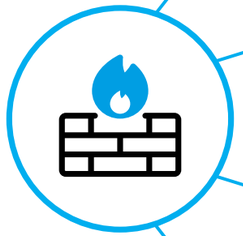
Valutare periodicamente i rischi che incombono sulle informazioni e definire le opportune risposte al fine di mitigare tali rischi.

Threat and Vulnerability Management

Il numero di **minacce informatiche** presenti a livello mondiale è in continuo aumento. Ciò significa che ogni giorno le organizzazioni sono potenzialmente esposte a **nuove forme di attacchi**. È dunque fondamentale rilevare proattivamente e in maniera costante le minacce e le vulnerabilità presenti sui propri sistemi informatici, in modo da adottare le opportune contromisure.

Una metodologia onnicomprensiva è fondamentale per **rilevare minacce e vulnerabilità** tecnologiche a tutti i livelli possibili.

- **Web Application Security Assessment**
- **Infrastructure/Application Vulnerability Assessment**
- **Internal Penetration Test (black box o white box)**
- **Social Engineering Test**
- **Physical Security Test**
- **Source Code Analysis**
- **Wi-Fi Security Assessment**
- **Cyber Intelligence**



Vulnerability Assessment/Penetration Test Report

Descrivono le vulnerabilità rilevate a livello infrastrutturale sui sistemi analizzati, suggerendone i possibili rimedi.

Technical Control Report

Riassumono l'esito delle verifiche manuali condotte sulle configurazioni dei sistemi analizzati.

Source Code Scanning Report

Presentano le vulnerabilità rilevate all'interno del codice di sorgente delle applicazioni analizzate.

Application Scanning Report

Evidenziano le vulnerabilità rilevate a livello applicativo e gli esiti dei test di validazione manuale, suggerendo i possibili rimedi delle vulnerabilità.

Architecture, Infrastructure and HI-TECH

L'evoluzione delle tecnologie degli ultimi anni pone maggiore attenzione sulle **nuove tecnologie IT** e sulla sic**urezza delle informazioni** gestite dalle medesime tecnologie.

È necessario valutare, in termini di sicurezza delle informazioni, infrastruttura tecnologica (sistemi ed applicazioni) per capire se sia il caso di introdurre nuove tecnologie.

È opportuno quindi **valutare l'attuale infrastruttura tecnologica**, le reali esigenze dell'azienda e le configurazioni esistenti. Per rendere questo possibile, Cyber4Growth si avvale di una knowledge base costituita da best practice di controlli tecnici per **verificare la corretta configurazione dei sistemi**.

- **Definizione dei profili di accesso ai sistemi/ applicazioni ed analisi delle utenze presenti sui sistemi aziendali, sulla base dei ruoli aziendali**
- **Valutazione della configurazione di alcuni sistemi aziendali**
- **Valutazione di una piattaforma aziendale applicativa**
- **Valutazione dell'infrastruttura di rete**
- **Valutazione della sicurezza del cloud**

Analisi del contesto tecnologico

Capire il contesto tecnologico, organizzativo e di processi IT rappresenta un elemento indispensabile per la valutazione delle tecnologie nuove ed esistenti.

Valutazione della configurazione dei sistemi

Analizzare la configurazione degli asset rispetto a best practice internazionali al fine di individuare eventuali punti di miglioramento.

Role Base Access Control Methodology

Definire i privilegi di accesso ai sistemi/applicazione aziendali sulla base della definizione di ruoli aziendali.

Rely and Cloud

Valutare i servizi cloud erogati utilizzando un framework cross-referenziato con i principali standard (p.e. Cloud Security Alliance, ISO 27100, ENISA, etc.).

Business Continuity Management

Molte organizzazioni manifestano l'esigenza di **garantire la continuità dei principali processi di business** assicurando l'erogazione dei servizi anche al verificarsi di eventi inattesi (p.e. un disastro).

È quindi necessario strutturare un processo di **Business Continuity Management** (BCM), ossia un processo di management che identifica i potenziali impatti che minacciano un'organizzazione e realizza una struttura capace di dare una risposta efficace in caso di sinistro e/o crisi, per garantire il ripristino del servizio a seguito dell'accadimento del disastro.

L'approccio di C4G è basato sullo standard BS25999, ISO 22301 e sulle **Business Continuity Management Good Practice Guidelines** del Business Continuity Institute (BCI).

- **Business Impact Analysis**
- **Risk Analysis (IT e Funzionale)**
- **Definizione di un Business Continuity Plan**
- **Definizione di un Disaster Continuity Plan**

Business Impact Analysis (BIA)

Individuare gli impatti in caso di perdita di disponibilità e valutare in maniera oggettiva il livello di criticità di ciascun impatto individuato.

System Profile

Valutare i fattori di esposizione al rischio ed il rischio di perdita di disponibilità associato ai processi e ai sistemi in ambito di analisi.

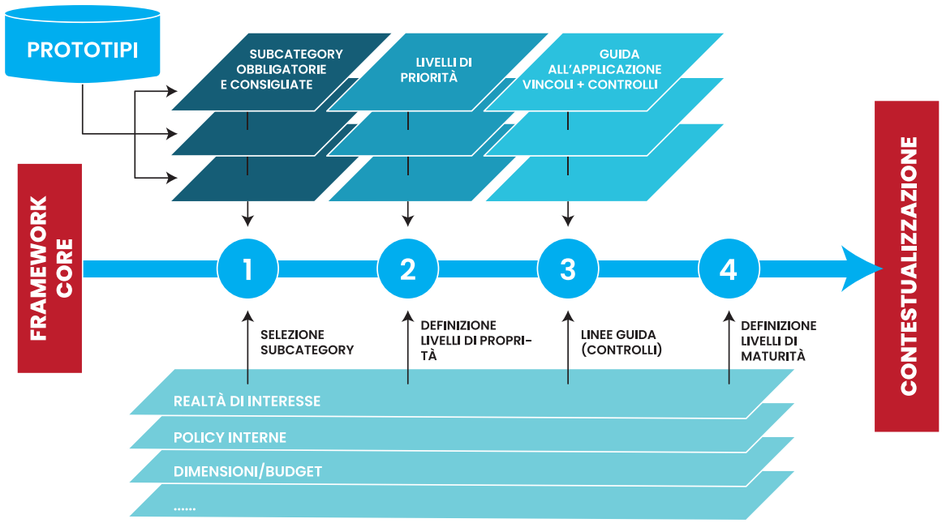
Process Continuity Requirements

Valutare i requisiti di continuità dei processi in termini di People, Premises, Thecnology, Information e Supplies.

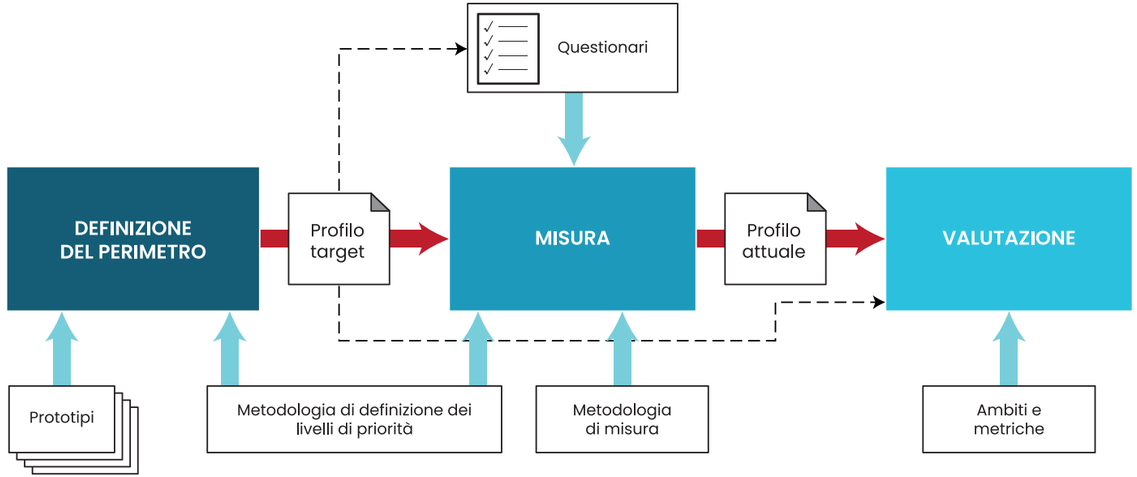
Business Continuity Plan/Disaster Recovery Plan

Strutturare un piano composto da 3 principali componenti: Crisis Management, Business Operations Recovery e Disaster Recovery Plan.

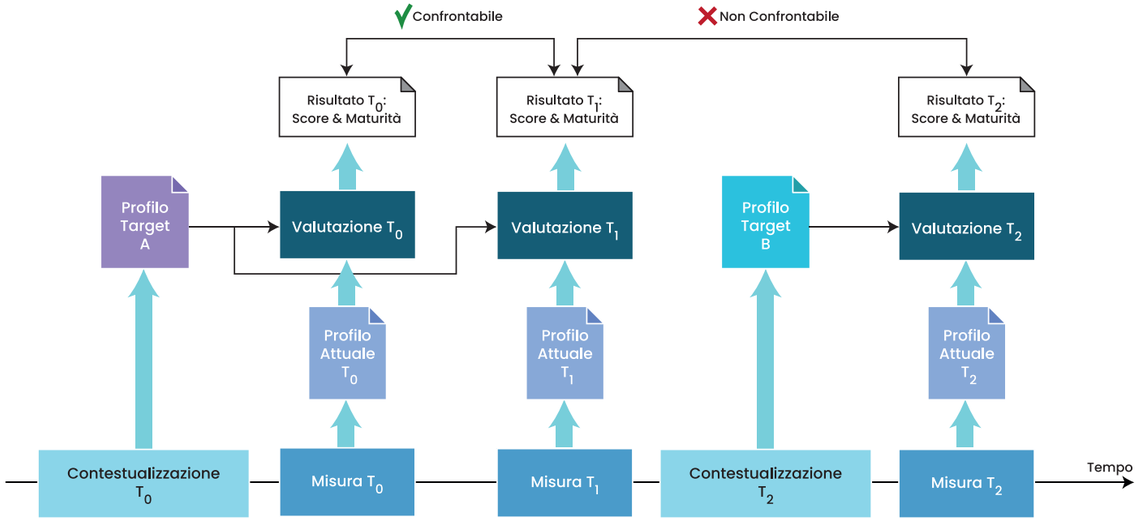
Contestualizzazione



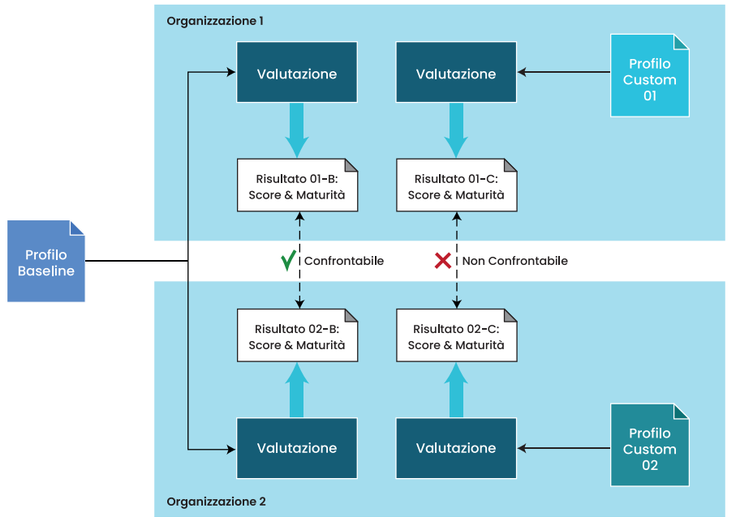
Metodologia



Confronto



Organizzazioni




Cyber4Growth
Grow your business