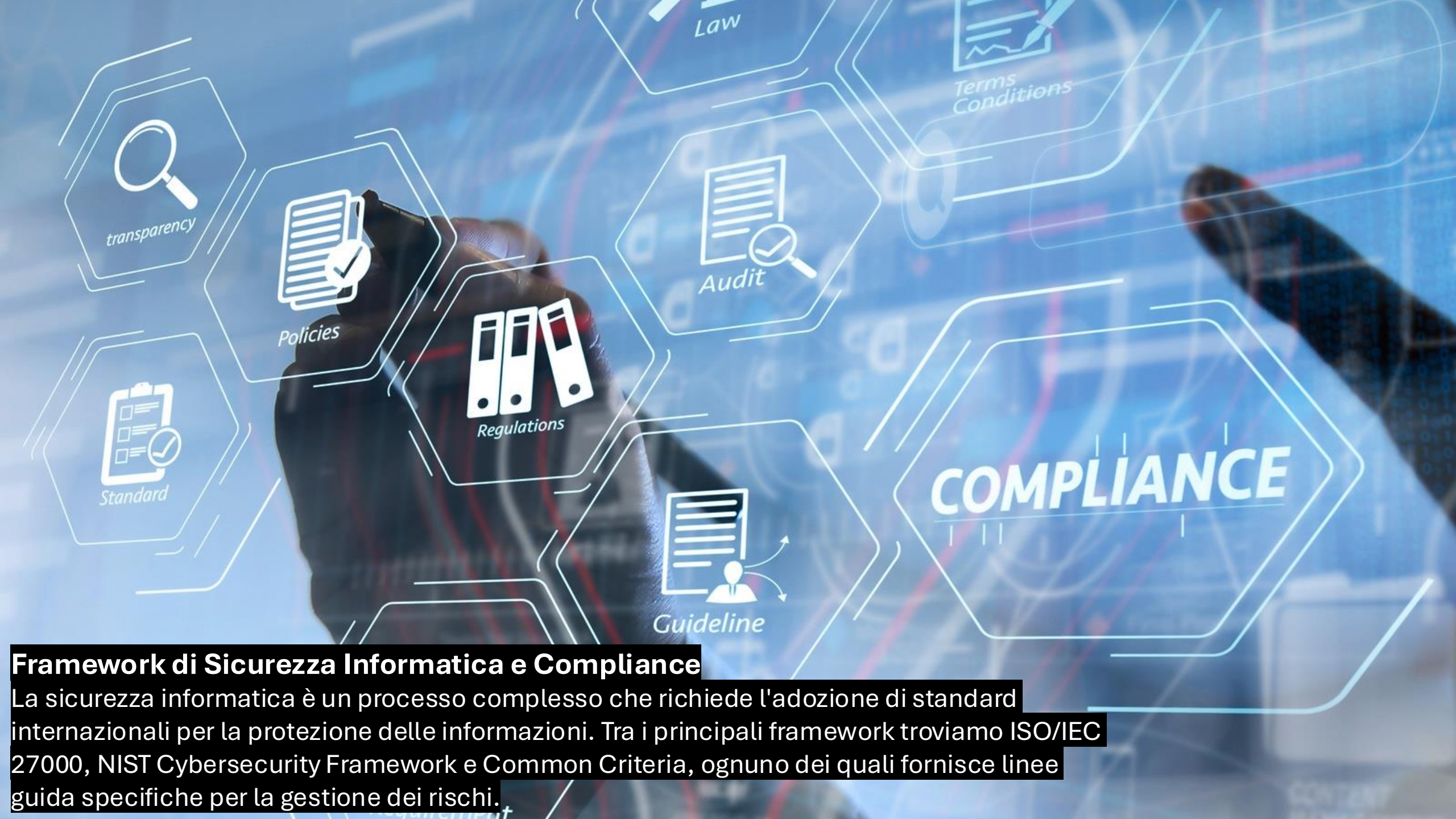


Framework di Sicurezza Informatica e Compliance

La sicurezza informatica è un processo complesso che richiede l'adozione di standard internazionali per la protezione delle informazioni. Tra i principali framework troviamo ISO/IEC 27000, NIST Cybersecurity Framework e Common Criteria, ognuno dei quali fornisce linee guida specifiche per la gestione dei rischi.

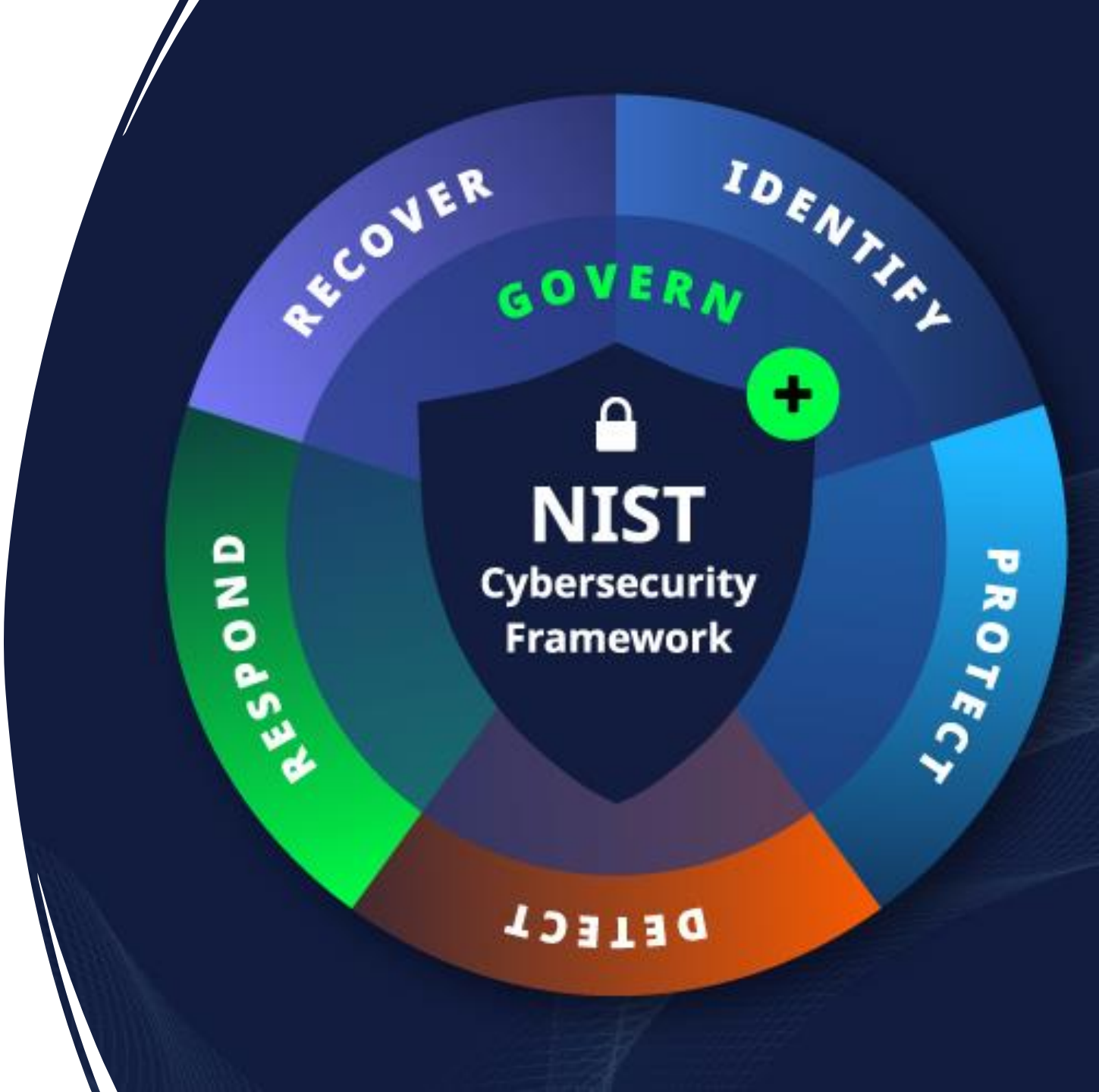
ISO/IEC 27001 e Famiglia 27000

La serie ISO/IEC 27000 stabilisce le best practice per un ISMS (Information Security Management System), che include la gestione della sicurezza delle informazioni attraverso un ciclo strutturato. ISO 27000:Introduzione generale e terminologia. ISO 27001: Requisiti per l'implementazione di un ISMS, tra cui leadership, pianificazione, operatività, valutazione delle prestazioni e miglioramento continuo. ISO 27002:Linee guida per controlli di sicurezza (accessi, crittografia, sicurezza fisica). ISO 27005: Gestione del rischio attraverso analisi e valutazione delle minacce. ISO 27017/27018: Sicurezza nei servizi cloud.

- Ciclo PDCA - ISO 27001 Plan: Definire politiche e obiettivi basati sull'analisi dei rischi.
- Do:Implementare misure di sicurezza.
- Check: Monitorare e valutare l'efficacia dei controlli.
- Act: Migliorare i processi basandosi sui risultati del monitoraggio.

- NIST Cybersecurity Framework

- Il NIST Framework fornisce un approccio volontario per la gestione dei rischi, organizzato in tre componenti:
- Core:Identificare, Proteggere, Rilevare, Rispondere, Ripristinare.
- Implementation Tiers: Livelli di maturità (da processi ad hoc a completamente adattivi). Profile:Allineamento tra obiettivi di sicurezza e strategie aziendali.



- Common Criteria (ISO/IEC 15408)
- Il Common Criteria valuta la sicurezza dei prodotti IT attraverso un sistema di livelli EAL (Evaluation Assurance Levels). Protection Profile (PP): Requisiti generali di sicurezza. Security Target (ST): Requisiti specifici per il prodotto. Target of Evaluation (TOE): Prodotto oggetto di valutazione.

- Struttura dei livelli EAL:
- EAL1:Test funzionale di base.
- EAL2: Test strutturale con documentazione più dettagliata.
- EAL3: Test metodico del design e del codice.
- EAL4: Progettazione metodica con revisione del codice.
- EAL5: Progettazione semi-formale con controlli stringenti.
- EAL6: Verifica semi-formale con analisi dettagliata.
- EAL7: Verifica formale basata su prove matematiche.

NIST Cybersecurity Framework

- Implementazione Pratica della Sicurezza
- L'implementazione pratica richiede la gestione dei rischi e la risposta agli incidenti, organizzata in cinque fasi: Gap Analysis e Risk Assessment:Identificare le vulnerabilità.
- Protect: Implementare misure come firewall e crittografia.
- Detect: Monitorare gli eventi di sicurezza.
- Respond: Definire le azioni post-incidente.
- Recover: Pianificare la ripresa operativa.

- I livelli di maturità della sicurezza sono suddivisi in:
- Tier 1: Processi ad hoc e reattivi.
- Tier 2: Processi approvati ma non integrati.
- Tier 3: Processi formalizzati e integrati.
- Tier 4: Processi adattivi e proattivi.