

# Framework di Sicurezza e Compliance Normativa

Presentazione tecnica Sistemi e reti/ed Civica  
Denis Canevarolo – Classe 4D

# Overview

- Analisi di  
standard e  
normative di  
sicurezza IT

- Confronto tra  
ISO/IEC 27001 e  
NIST CSF

- Aspetti tecnici,  
normativi ed etici

# Contesto



- Aumento dei  
cyber-attacchi

- Importanza  
della protezione  
dei dati

- Necessità di  
standard  
comuni

# ISO/IEC 27001

- Standard per la gestione della sicurezza delle informazioni (ISMS)

- Approccio basato sul rischio

- Ciclo PDCA: Plan, Do, Check, Act

# NIST CSF

- Framework volontario sviluppato dal NIST (USA)

- Funzioni: Identify, Protect, Detect, Respond, Recover

- Tiers di implementazione

# Confronto ISO 27001 / NIST CSF

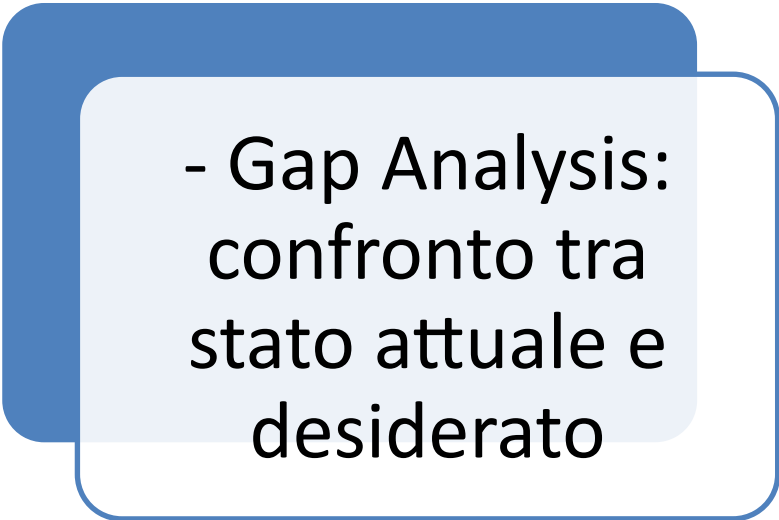
Origine: ISO →  
internazionale |  
NIST → USA

Certificabilità: ISO  
sì | NIST no

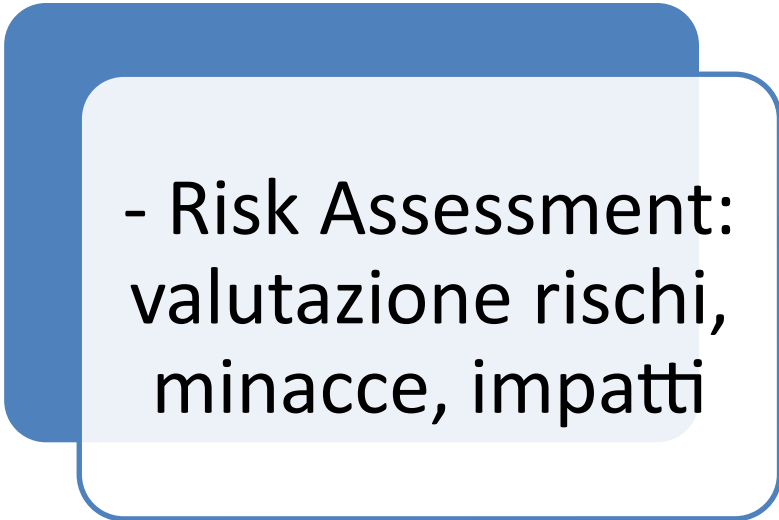
Obiettivo: ISO →  
ISMS | NIST →  
risk management



# Gap Analysis e Risk Assessment



- Gap Analysis:  
confronto tra  
stato attuale e  
desiderato



- Risk Assessment:  
valutazione rischi,  
minacce, impatti

---

# Controlli di Sicurezza

- Tecnici (es.  
firewall,  
crittografia)

- Organizzativi  
(es. formazione,  
politiche)

- Fisici (es.  
accesso ai  
locali)

---



## Caso Studio

- Azienda X implementa ISO 27001

- Introduzione firewall, backup cifrati, gestione accessi

- Audit annuali per mantenere la certificazione

## Matrice Requisiti- Controlli

- Riservatezza →  
Controllo accessi

- Integrità → Audit  
log

- Disponibilità →  
Sistemi ridondanti

## Aspetti Etici e Sociali

- Responsabilità degli operatori IT

- Protezione dei dati personali

- Conflitto tra sicurezza e privacy

# Normativa

- GDPR (UE 2016/679)

- ISO/IEC 27001

- Direttiva NIS

- Codice dell'Amministrazione Digitale (CAD)

## Sfide Attuali

---

- Cyberattacchi avanzati

---

- Equilibrio tra sicurezza e usabilità

---

- Adattamento continuo agli standard

## Opportunità Future

- Adozione AI e automazione

- Aumento fiducia clienti

- Vantaggio competitivo grazie alle certificazioni

## Raccomandazioni

- Applicare framework di sicurezza riconosciuti
- Formare il personale IT
- Monitoraggio continuo dei sistemi

## Conclusione

- Gli standard migliorano la sicurezza e la trasparenza

- La sicurezza è una responsabilità condivisa





## Riferimenti

- - ISO.org
- - NIST.gov
- - GDPR – eur-lex.europa.eu
- - Dispense: "4D - Standard e sicurezza avanzata.pdf"