La normazione a supporto dell'ICT e delle imprese: la serie UNI EN ISO/IEC 27000

6 aprile 2023

UNI
UN MONDO FATTO BENE

UNINFO

Relatore

Fabio GUASCONI

- ✓ Presidente del CT 510 di **UNI/UNINFO** "Sicurezza"
- ✓ Direttivo **CLUSIT**
- ✓ Esperto **SBS**
- ✓ Esaminatore UNI 11697
- ✓ Certificazioni CISA, CISM, PCI-QSA/3DS/QPA/P2PE/CPSA, ITIL, PRINCE2, ISFS, LA 27001/22301/27701/9001, LI 27001, DPO UNI 11697
- ✓ Co-fondatore di **Bl4ckswan** S.r.l.

Sicurezza Informatica? Cybersecurity?

Information security (sicurezza delle informazioni)
Tutela della riservatezza, integrità e disponibilità dell'informazione

- **Riservatezza:** Proprietà di non essere accessibile o nota a entità non autorizzate
- **Integrità:** Proprietà relativa all'accuratezza e alla completezza
- **Disponibilità:** Proprietà di essere accessibile e usabile a richiesta di un'entità autorizzata

Cybersecurity
Tutela di persone, società, organizzazioni e nazioni dai **rischi cyber**

- **Rischi Cyber (Cyber risks)** Il rischio cyber è associato alla possibilità che le minacce sfruttino le vulnerabilità nel cyberspazio e quindi causino danni alle entità nel cyberspazio
- **Cyberspazio (Cyber space)** Ambiente digitale interconnesso di reti, servizi, sistemi, persone, processi, organizzazioni e ciò che risiede nell'ambiente digitale o lo attraversa

ISO/IEC 27001

La norma ISO/IEC 27001 rappresenta il punto di riferimento internazionale, quando si parla di information security, che descrive le best practice per un SGSI (Sistema di Gestione per la Sicurezza delle Informazioni).

- Applicabile a realtà di ogni dimensione
- Circa 20 anni di esistenza sul mercato
- Ambito definibile a piacimento
- Approccio ciclico (**PDCA**)
- High-level structure tipica dei nuovi sistemi di gestione
- E' basata sulla gestione del rischio
- Costituisce un framework completo
- Dice **cosa fare**, non come farlo
- Rivolto al miglioramento continuo
- E' un riferimento universale e **certificabile**

UNINFO

ISO/IEC 27001 Annex A

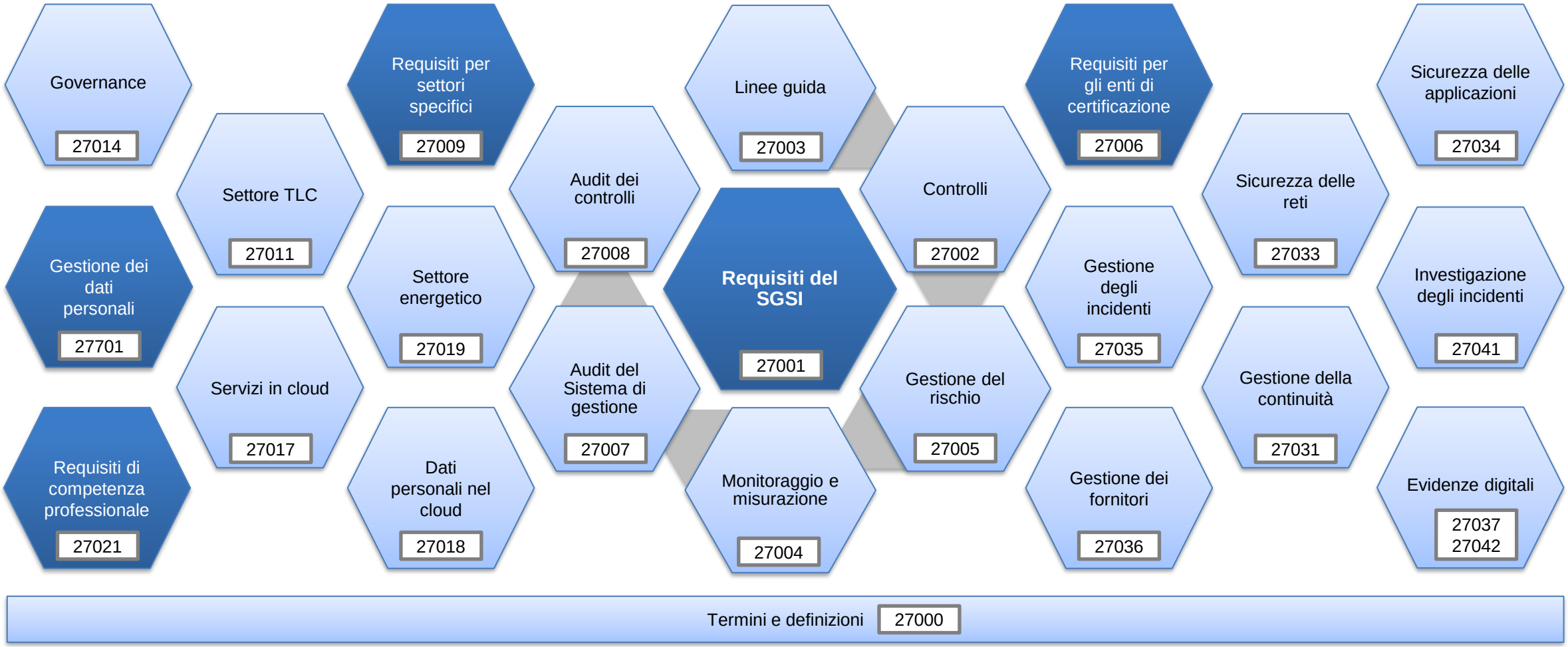
Sintesi della ISO/IEC 27002, l'annex A è un insieme di 93 controlli suddivisi in:

- **34 controlli tecnologici**
- **14 controlli fisici**
- **37 controlli organizzativi**
- **8 controlli sul personale**

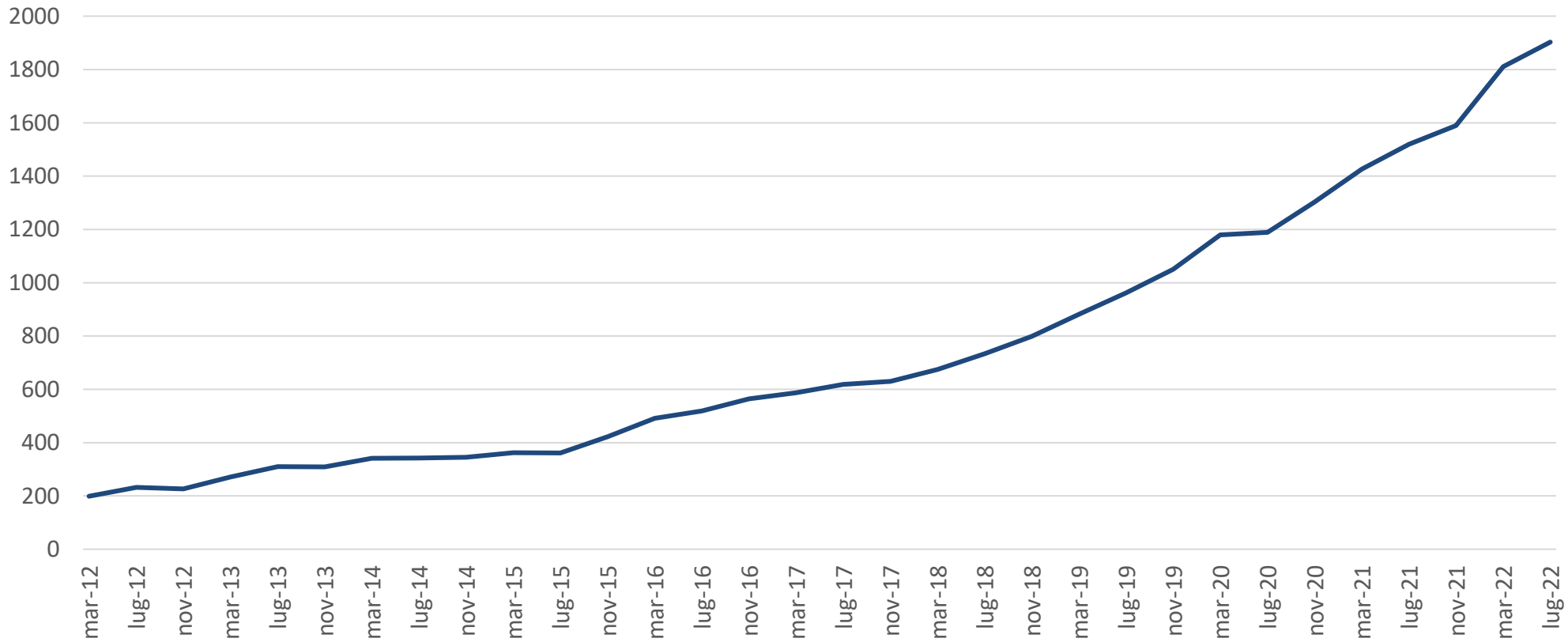
Tutti questi controlli possono essere **ritenuti necessari o meno** sulla base dell'esposizione al rischio (o risk appetite) che l'organizzazione vuole avere.

UNINFO

Processi (e famiglia) ISO/IEC 27001



Certificazioni ISO/IEC 27001



Fonte: **Accredia**

ISO/IEC 27001, perché utilizzarla?

Offre un' "**ancora**" terminologica e metodologica condivisa nel mondo in un ambito continuamente in evoluzione

Il bacino di **risorse** ad essa collegate sul mercato è estremamente ampio

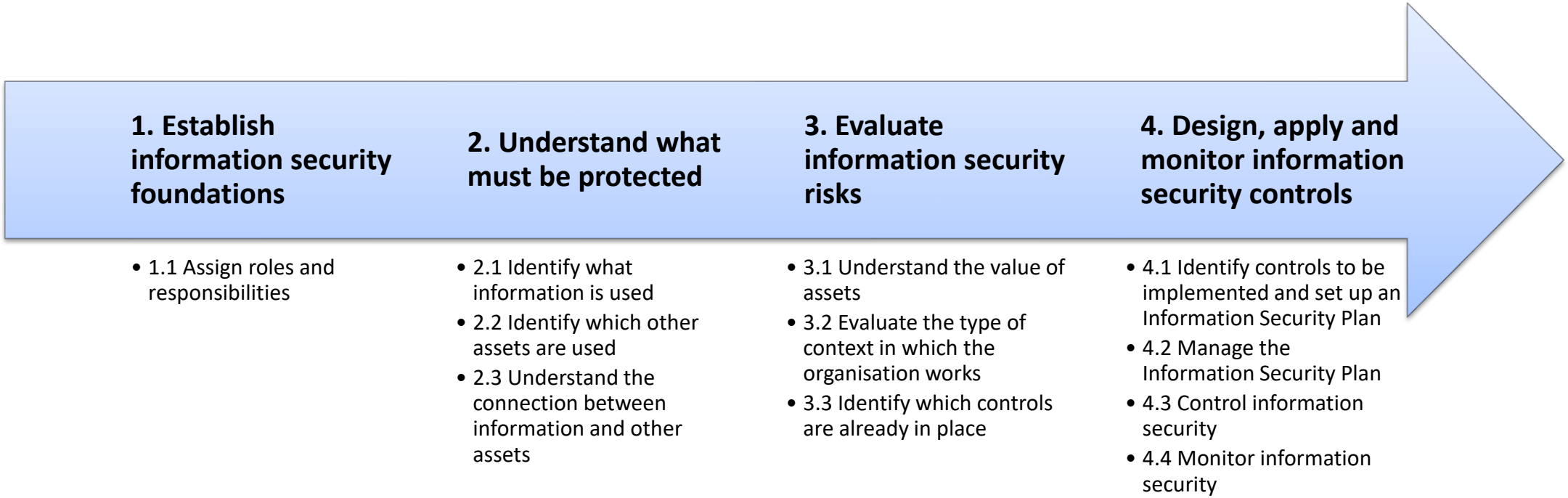
Permette un approccio "**intelligente**" e non solo prescrittivo a questi temi

Si **integra** perfettamente con gli altri sistemi di gestione, con il tema della protezione dei dati personali (27701) e con la gestione del rischio a livello d'impresa

E' una norma adottata a livello **europeo** dal CEN ed ufficialmente tradotta anche in Italiano

SME Guide for the implementation of ISO IEC 27001

Se la ISO/IEC 27001 può sembrare troppo impegnativa, è anche possibile arrivarci per gradi, utilizzando approcci guidati e progressivi come quello suggerito dalla linea guida per l'implementazione di SBS.



https://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management

UNINFO

Conclusioni

1

Esistono norme tecniche importanti sulla sicurezza, non serve reinventare la ruota quando si può viaggiare sulle spalle dei giganti

2

La tecnologia da sola non è la risposta ai problemi di sicurezza informatica / delle informazioni / cyber, la sua governance è indispensabile

3

Tutte le considerazioni relative all'adozione o meno di misure di sicurezza informatica / delle informazioni / cyber dovrebbero essere basati sul rischio

Contatti

fabio.guasconi@bl4ckswan.com