Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

NOVITÀ E PROSPETTIVE DAL MONDO DELLA NORMAZIONE

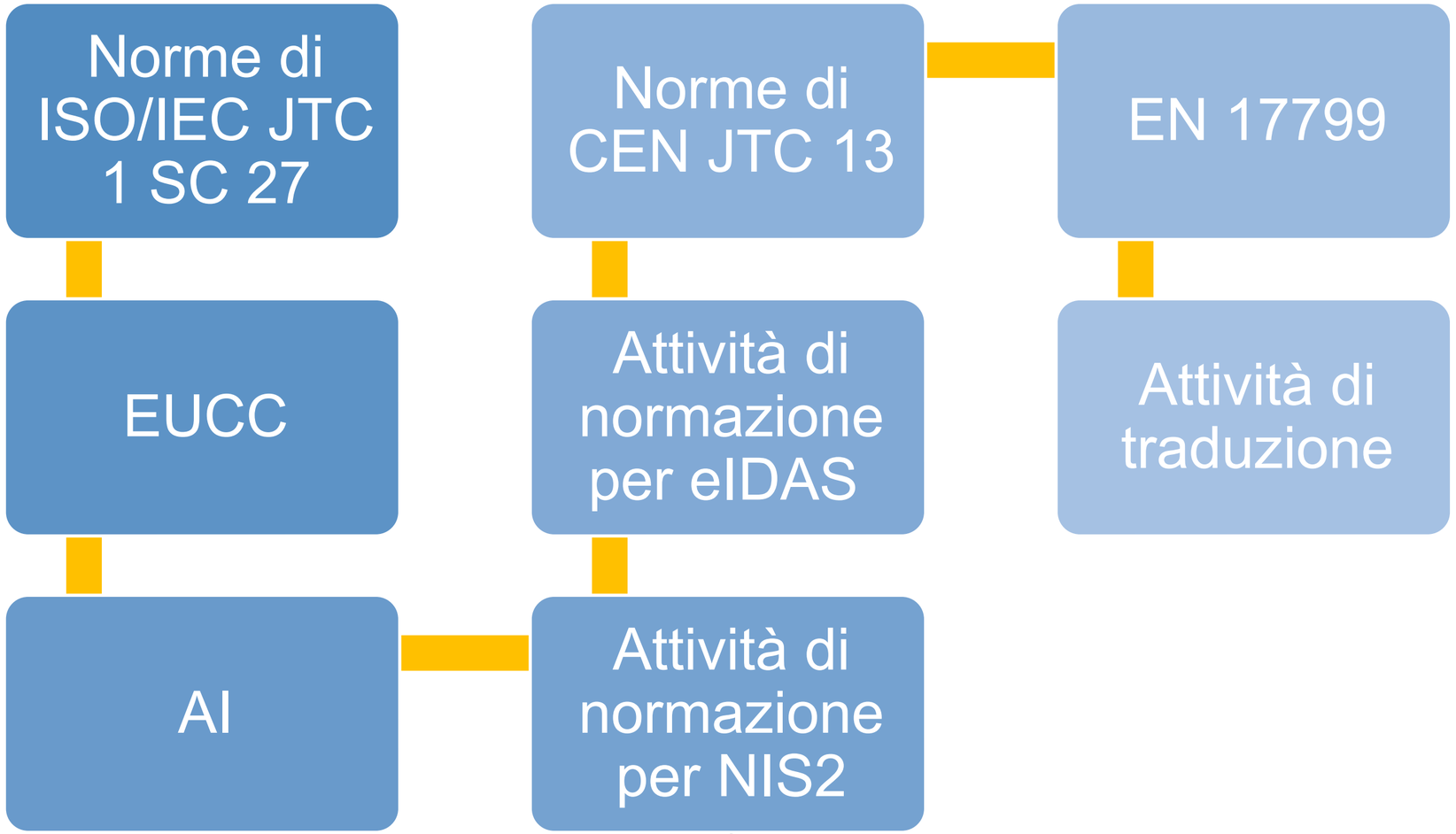
Andrea CACCIA
Cesare GALLOTTI
Fabio GUASCONI

UNINFO

21 marzo 2024 orario 15.00-15.40

Relatori

Agenda


Norme di ISO/IEC JTC 1 SC 27
EUCC
AI
Attività di normazione per NIS2
Attività di normazione per eIDAS
Norme di CEN JTC 13
EN 17799
Attività di traduzione

Aggiornamenti ISO/IEC

Sono stati pubblicati gli Amendment di tutti gli standard ISO e ISO/IEC per i sistemi di gestione.

In tutti sono state aggiunte due frasi:

- nell'ambito della comprensione del contesto (4.1), è richiesto di determinare se il cambiamento climatico è una questione pertinente;
- nell'ambito della comprensione dei requisiti delle parti interessate (4.2), è stata inserita una nota per segnalare che le parti interessate possono avere requisiti relativi al cambiamento climatico.

IAF ha pubblicato il "IAF-ISO Joint Communiqué on the addition of Climate Change considerations to Management Systems Standards" con una breve descrizione dei cambiamenti.

Attività ISO/IEC JTC 1 SC 27 – WG 1

ISO/IEC 27000: partiti i lavori di aggiornamento; conclusione prevista a metà 2025;

ISO/IEC 27003: partiti i lavori di aggiornamento;

ISO/IEC 27006-1: pubblicata la nuova versione a febbraio;

ISO/IEC 27008 (valutazione dei controlli): in PWI;

ISO/IEC 27011 (controlli per le TLC): aggiornamento previsto inizio 2024;

ISO/IEC 27013 (relazioni ISO/IEC 20000-1): aggiornamento pubblicato feb. 2023;

ISO/IEC 27017 (controlli per cloud): pubblicazione prevista per fine 2025;

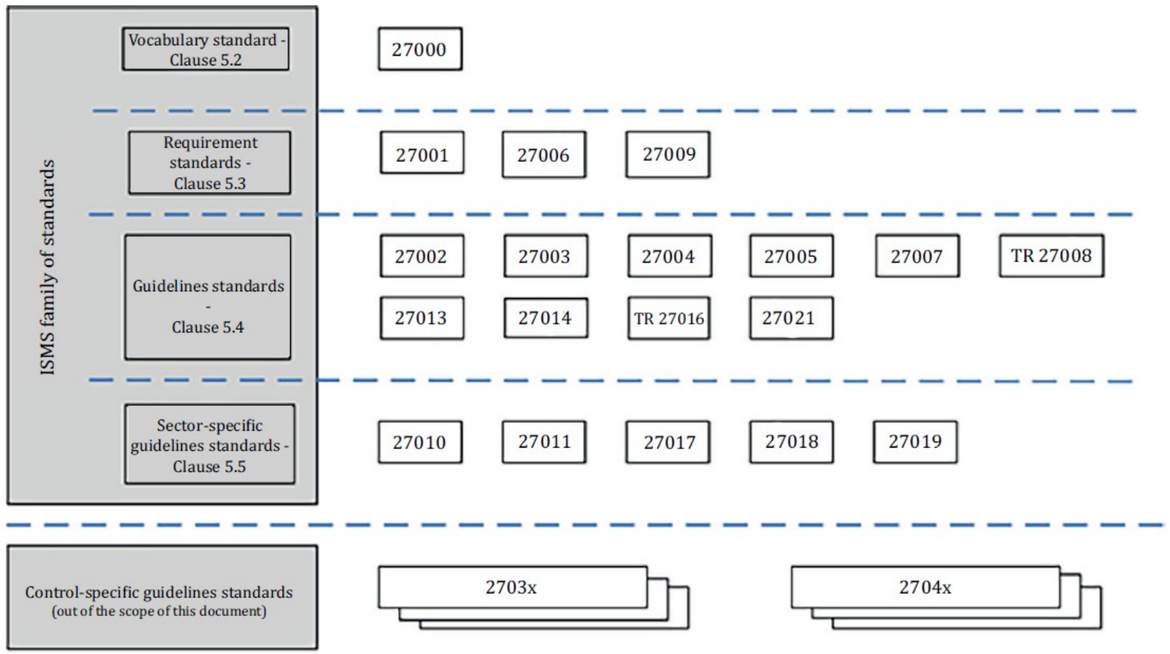
ISO/IEC 27019 (controlli per il settore dell'energia): pubblicazione prevista a fine 2024;

ISO/IEC 27028 (linee guida sugli attributi della 27002): in CD

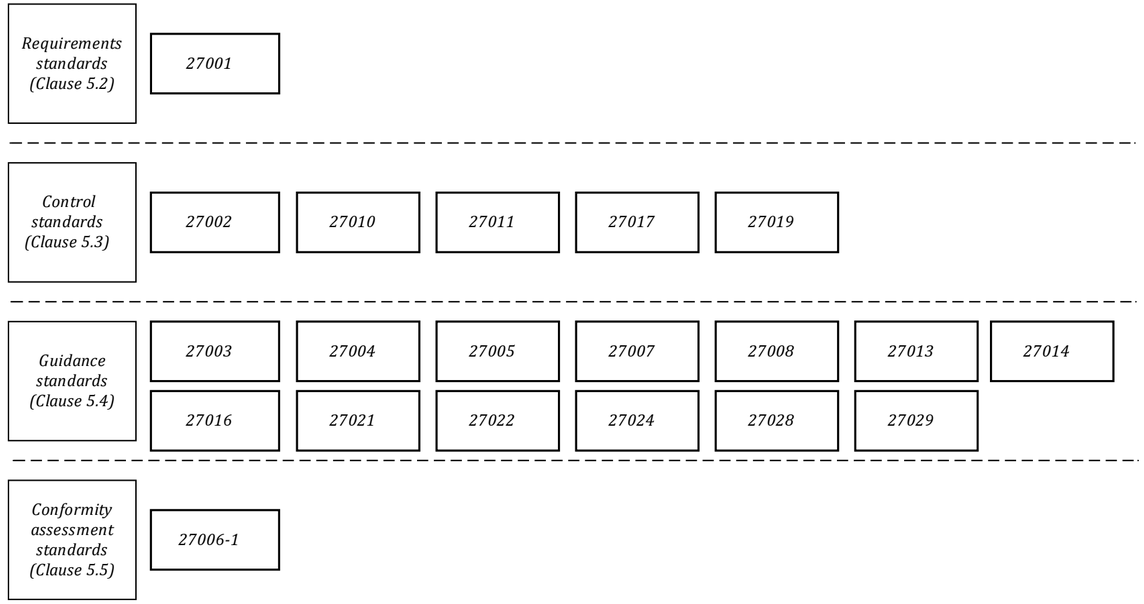
ISO/IEC 27109 sull'istruzione e la formazione sulla cibersicurezza: partiti i lavori di redazione; pubblicazione prevista a metà 2024.

Focus su ISO/IEC 27000

2018 – Overview and vocabulary



Oggi - Overview



Attività ISO/IEC JTC 1 SC 27 – WG 5

ISO/IEC 27701: diventerà una norma scollegata dalla ISO/IEC 27001. Sarà molto simile all'attuale ISO/IEC 27001, ma con riferimento a tre gruppi di controlli: quelli per i titolari, quelli per i responsabili e quelli di sicurezza delle informazioni (dalla ISO/IEC 27001).

ISO/IEC TS 27006 – 2: ne sarà pubblicata una nuova versione a breve per supportare la ISO/IEC 27701:2019 e ripartiranno subito i lavori per supportare la futura ISO/IEC 27701.

ISO/IEC 29151:2017 con controlli per i titolari. Lavori di revisione partiti. Pubblicazione prevista per fine 2025.

ISO/IEC 27018:2019. Lavori di revisione partiti. Pubblicazione prevista per fine 2025.

Focus su ISO/IEC 27701

- La struttura sarà quella dell'HS (ex HLS) con un numero variabile di annex con i controlli
- Il collegamento con ISO/IEC 27001 ma soprattutto 27002 è ancora da definire
- La ISO/IEC 27006-2 dovrà essere aggiornata anch'essa
- Questo "stop" sta provocando ritardi nella versione CEN della norma, con accreditamento 17065
- Difficilmente si avrà una nuova edizione della norma entro il 2024
- Le attuali certificazioni non sono minimamente influenzate, continuano ad essere valide

EUCC

L'Unione Europea, secondo quanto previsto dal Cybersecurity Act nel 2019, ha adottato il primo schema di certificazione sulla cybersecurity: https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme. Ringrazio Riccardo Lora per averlo segnalato agli Idraulici della privacy.

Questo schema è basato sui Common Criteria.

Accredia ha pubblicato le prime indicazioni che confermano che le attività di certificazione richiedono, in molti casi, la partecipazione di ACN.

ISO/IEC 42001:2023 sull'IA

Riporta i requisiti per un sistema di gestione per l'intelligenza artificiale.

La norma richiede di valutare il rischio relativo all'efficacia del sistema di gestione e all'intelligenza artificiale. Richiede anche una valutazione d'impatto dell'IA (ossia una valutazione relativa agli impatti sugli individui e sulla società).

I requisiti di valutazione del rischio sono organizzati come nella ISO/IEC 27001.

Importanti gli Annex:

- Annex A con i controlli da considerare per il trattamento del rischio;
- Annex B con la guida per l'implementazione dei controlli
- Annex C con alcuni obiettivi organizzativi relativi all'IA e alcune sorgenti di rischio;
- Annex D sull'uso dei sistemi di gestione per l'intelligenza artificiale in diversi domini e settori e sulla loro integrazione con altri sistemi di gestione.

Attività di normazione per NIS2

La direttiva NIS2 deve essere adottata entro il 18 ottobre 2024

Essendo la NIS2 una Direttiva, deve essere adottata con leggi nazionali, questo è potenzialmente un problema.

Devono ancora essere discussi e pubblicati i decreti attuativi che riporteranno, tra l'altro, i controlli di sicurezza da adottare. Per il momento non ci sono indicazioni in merito (auspichiamo siano basati sulla ISO/IEC 27001, alla cui redazione possono partecipare delegati italiani).

Attività di normazione per eIDAS

I prestatori di servizi fiduciari eIDAS e i relativi servizi rientrano nella NIS2 che ne specifica i requisiti sostituendo l'articolo 19 di eIDAS, che viene abrogato a partire dalla data di recepimento della direttiva.

ETSI ha modificato lo standard base dei servizi fiduciari EN 319 401, ora in inchiesta pubblica, per tener conto dei requisiti della NIS2.

Il recepimento della NIS2 e la definizione dei reciproci ruoli di ACN ed AGID per il Regolamento eIDAS sarà attuato dal Governo in base alla legge di delegazione europea 2022-2023, (legge 21 febbraio 2024, n. 15).

Revisione del Regolamento eIDAS

Il Regolamento UE di modifica del Regolamento eIDAS «eIDAS2» è nelle fasi finali dell'adozione e introduce molte modifiche significative, tra cui:

- un wallet europeo di identità digitale, basato su un mezzo di identificazione nazionale, obbligatorio per ogni Stato membro (30 mesi dall'entrata in vigore)
- nuovi servizi fiduciari (archiviazione, attestazioni, registri elettronici)
- l'obbligo per la Commissione di pubblicare riferimenti a standard per i servizi fiduciari entro 12 mesi dall'entrata in vigore

Pubblicazione ed entrata in vigore prevista ad aprile 2024.

Il testo più recente di eIDAS2 è disponibile sul sito del Parlamento UE:

https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf

Norme da sviluppare a supporto del wallet

ETSI sta approvando i seguenti deliverable a supporto del Wallet:

D1) Policy and Security requirements for Providers of Electronic Attestation of Attributes Services (TS 119 471)

D2) Profiles for Electronic Attestation of Attributes (TS 119 472-1)

D3) Profiles for Relying party interface to EUDI Wallet (TS 119 472-2)

D4) Wallet interfaces for trust services and signing (TS 119 462)

D5) Update to Trust Lists to support new EUDI framework (revised TS 119 612)

D6) Update to identify proofing of trust service subjects under new EUDI framework (revised TS 119 461)

D7) Coexistance of web browser and EU trust controls for qualified certificates for website authentication (TS 119 411-5)

D8) Relying party authorisations for access to EUDI Wallet (TS 119 475)

D9) Update to existing standard for the management of a remote electronic signature creation device under new EUDI framework (revised TS 119 431-1).

D10) Update to the standards framework for digital signatures and trust services to support new EUDI framework (revised TR 119 000)

Norme da sviluppare a supporto del wallet

CEN TC 224 si occuperà degli standard a supporto della certificazione e collegata coi dispositivi. Gruppi coinvolti:

- WG 17 - protection profiles dispositivi di firma
- WG 20 – specifico per i wallet

In una prima fase le certificazioni sono in parte definite con regole nazionali

Non è più previsto l’obbligo di certificazione GDPR ma la protezione dei dati personali resta un elemento fondamentale di eIDAS2

Norme da sviluppare a supporto dei servizi fiduciari

Ruolo centrale di ETSI/ESI

Coinvolgimento di CEN/CLC JTC 19 per i registri elettronici (electronic ledgers)

CEN/TC 468 sta votando un NWIP per gli aspetti archivistici dei servizi di archiviazione (mirror UNI)

Per i servizi di recapito il testo pare in linea con l'approccio italiano, promuovendo l'interoperabilità con accordo tra le parti e verifica tramite CAB

Attività CEN JTC 13 – WG 5

Norme con requisiti privacy come parte dei requisiti richiesti per le certificazioni in accordo agli articoli 42 e 43 del GDPR:

EN 17799: pubblicata. Non sarà proposto uno schema di certificazione.

EN 17926: pubblicata. Presenta raffinamenti della ISO/IEC 27701, ma dovrà essere aggiornata. I lavori per lo schema di certificazione proseguono, ma dovrà essere avviata una discussione per considerare le scelte fatte per la EN 17799.

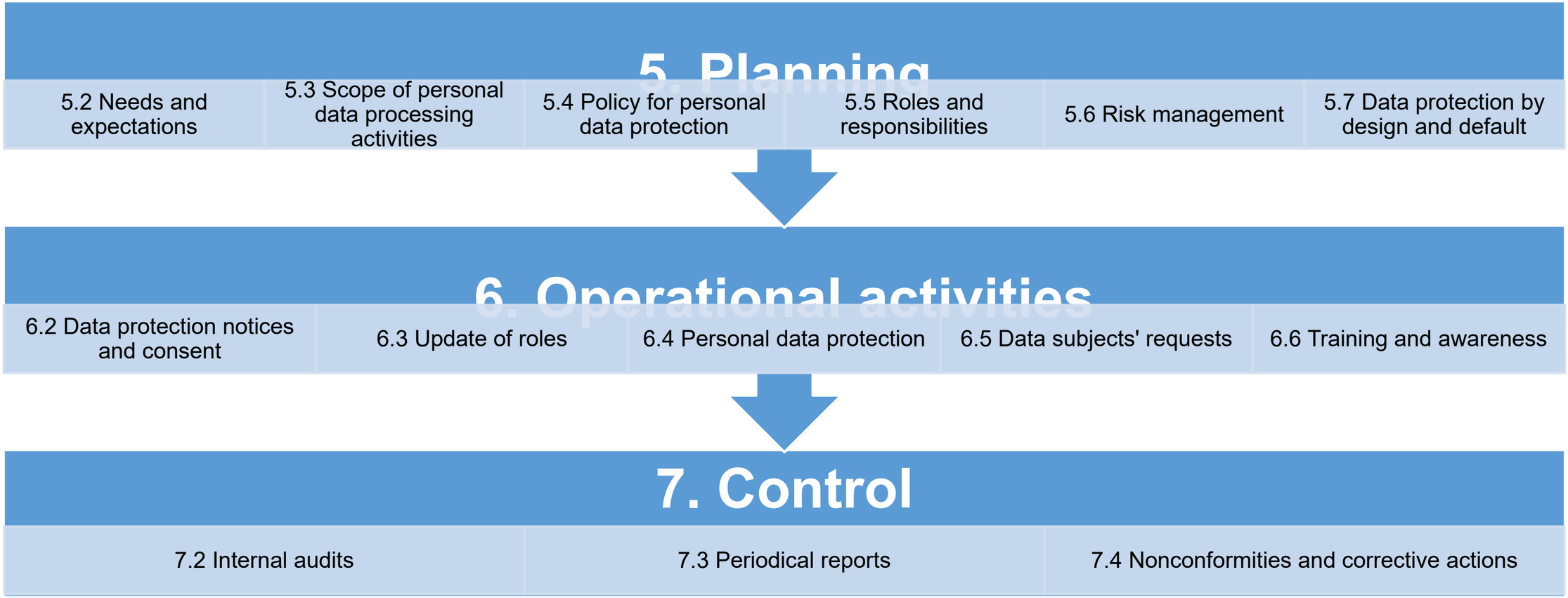
EN 17799

Dopo quasi 5 anni di travagliata gestazione finalmente si sta pubblicando la EN 17799 intitolata: **"Personal data protection requirements for processing operations"**

Rispetto al testo in inglese della PdR 43-2 da cui ha origine (a sua volta basato sulla BS 10012), utilizzato come base di partenza, si è deciso di apportare le seguenti modifiche:

- esplicitazione di quali sono i requisiti in carico a Titolari e Responsabili e le relative necessità di interazione
- aggiunta di un'annex di mappatura tra le sezioni della norma e il ruolo di Titolare o di Responsabile
- rimozione dell'annex per la valutazione della conformità
- ampliamento al di là dell'ambito ICT a cui era formalmente legata la PdR
- revisione dei rimandi diretti al GDPR (ora limitati alle note)
- maggiore coerenza con i contenuti del GDPR

EN 17799


5. Planning
5.2 Needs and expectations
5.3 Scope of personal data processing activities
5.4 Policy for personal data protection
5.5 Roles and responsibilities
5.6 Risk management
5.7 Data protection by design and default
6. Operational activities
6.2 Data protection notices and consent
6.3 Update of roles
6.4 Personal data protection
6.5 Data subjects' requests
6.6 Training and awareness
7. Control
7.2 Internal audits
7.3 Periodical reports
7.4 Nonconformities and corrective actions

EN 17799

La norma, che in alcuni aspetti si avvicina ad un sistema di gestione, riprende tutti i principali requisiti del GDPR fornendo un taglio più pratico e aggiungendo o incrementando l'attenzione su elementi specifici che ne aiutano l'implementazione quali, in primis:

- Privacy policy
- Training & awareness
- Risk management (risk treatment)
- Misure di sicurezza
- Cancellazione / anonimizzazione dei dati personali
- Procedure per l'esercizio dei diritti degli interessati (e dei reclami)
- Audit interni
- Report periodici

Attività di traduzione

Conclusi finalmente i lavori sulle nuove 27001 e 27002 siamo partito con quelli per la ISO/IEC 27005.

Previsione fine lavori: aprile 2024


Q
A