AUTORE: FABRIZIO CIRILLI – SENIOR PARTNER REXILIENCE SRL - MAIL: FABRIZIO.CIRILLI@REXILIENCE.EU

— VER. 1.0 25 NOVEMBRE 2022
— VER. 1.1 5 DICEMBRE 2022

La transizione alla ISO/IEC 27001:2022 – Effetti e impatti sui sistemi di gestione integrati – La soluzione

C'è un grande fermento intorno alla ISO/IEC 27001 e ai Sistemi di Gestione collegati.

L'arrivo della terza edizione della norma sta smuovendo il mercato e generando il tanto atteso effetto: generare interesse e lavoro sui temi della sicurezza delle informazioni.

Gli interventi e le pubblicazioni si moltiplicano giorno dopo giorno.

Vogliamo dare il nostro contributo, come Rexilience, proprio per condividere la nostra esperienza e la nostra visione del tema.

Le dimensioni del fenomeno

Dalla ISO Survey del 2021 apprendiamo che la ISO/IEC 27001 è la quarta norma a livello mondiale come numero di certificati emessi e come numero di siti certificati.

	Total valid certificates	Total number of sites
ISO 9001:2015	1.077.884	1.447.080
ISO 14001:2015	420.433	610.924
ISO 45001:2018	294.420	369.897
ISO IEC 27001:2013	58.687	99.755
ISO 22000:2005&2018	36.124	42.937
ISO 13485:2016	27.229	38.503
ISO 50001:2011&2018	21.907	54.778
ISO 20000-1:2011&2018	11.769	13.998
ISO 37001:2016	2.896	7.982
ISO 22301:2012&2019	2.559	5.969
ISO 39001:2012	1.285	2.357
ISO 28000:2007	584	1.106
ISO 55001:2014	488	1.993
ISO 20121:2012	253	712
ISO 29001:2020	157	795
ISO 44001:2017	136	186

Quindi una grande crescita negli ultimi anni, considerando che le norme che la precedono esistono da un numero maggiore di anni.

Un altro dato rilevante è la posizione dell'Italia in questo scenario[1]:

Country	certificates	sites
China	18446	18569
Japan	6587	17784
United Kingdom of Great Britain and Northern Ireland*	5256	8647
India	2775	6024
Italy	1924	3474
United States of America	1742	4504
Germany	1673	3486
Netherlands	1508	2421
Taiwan, Province of China	1129	3147
Israel	1056	1083

Siamo al quinto posto, considerando il boom della Cina e dell'India, e la supremazia storica del Giappone.

Un posizionamento di tutto rispetto, considerando anche che alcuni di questi paesi hanno una sicurezza delle informazioni finanziata a livello governativo (in gran parte per effetto del terrorismo o per politiche locali).

Interessante anche notare il numero di siti certificati in relazione ai certificati emessi, facendo una rapida analisi è possibile capire anche i criteri adottati nelle varie nazioni, in particolare basti vedere il rapporto in Cina e in Giappone.

In totale abbiamo 58.687 certificati emessi a livello mondiale su 99.755 siti. Da considerare che i dati sono aggiornati al 2021 e che quindi non contengono i dati più recenti (poi vedremo la situazione aggiornata in Italia).

Se poi, gli stessi dati, li riportiamo al settore merceologico di appartenenza appare evidente la posizione dominante del settore ICT (IAF 33):

Code	Sector	Number
	When Sector not known, fill data here	38009
33	Information technology	10644
31	Transport, storage and communication	6909
35	Other Services	1693
32	Financial intermediation, real estate, renting	645
34	Engineering services	630
29	Wholesale & retail trade, repairs of motor vehicles, motorcycles & personal & household goods	562
28	Construction	527
19	Electrical and optical equipment	477
38	Health and social work	393
36	Public administration	338

[1] Lo schema riporta solo le nazioni con un numero di certificati superiori a mille, le nazioni censite nella survey sono 193

37	Education	262
39	Other social services	219
9	Printing companies	172
25	Electricity supply	120
18	Machinery and equipment	113
4	Textiles and textile products	84
17	Basic metal & fabricated metal products	71
27	Water supply	63
24	Recycling	60
3	Food products, beverage and tobacco	47
14	Rubber and plastic products	45
12	Chemicals, chemical products & fibres	31
23	Manufacturing not elsewhere classified	25
8	Publishing companies	21
21	Aerospace	21
7	Pulp, paper and paper products	19
22	Other transport equipment	19
26	Gas supply	19
30	Hotels and restaurants	17
13	Pharmaceuticals	16
10	Manufacture of coke & refined petroleum products	13
2	Mining and quarrying	10
6	Manufacture of wood and wood products	6
16	Concrete, cement, lime, plaster etc.	5
20	Shipbuilding	5
5	Leather and leather products	3
11	Nuclear fuel	2
15	Non-metallic mineral products	2

Vale la pena ricordare che la ISO/IEC 27001 è considerata "settore trasversale" in alcuni paesi; quindi, viene assegnato il codice 33 (Information Technology) "by default".

Il numero di casi per i quali il settore non è "conosciuto" denota un gran numero di certificati (intorno al 50%) la cui collocazione influenza moltissimo le considerazioni possibili sull'andamento nei vari mercati.

Per un confronto, utile allo scopo del nostro articolo, aggiungiamo la situazione dell'Italia in norme "affini" spesso associate in sistemi di gestione integrati.

Per la ISO/IEC 20000-1 (Sistemi di Gestione per i Servizi IT):

Country	certificates	sites
China	9247	9249
United States of America	265	357
Spain	187	281
India	179	578
Italy	176	299
United Kingdom of Great	134	220
Czech Republic	113	122
Japan	111	295
Bulgaria	107	126
Mexico	105	183

Ancora un quinto posto ma qui il distacco dalla Cina è abissale. Anche qui la classifica è molto lunga ma abbiamo estratto le nazioni con oltre 100 certificati per praticità.

Per la ISO 22301 (Sistemi di Gestione per la Business Continuity):

Country	certificates	sites
United Kingdom of Great Britain and Northern Ireland	447	851
Korea (Republic of)	176	289
India	159	819
Turkey	147	173
China	134	135
United Arab Emirates	113	166
Singapore	111	187
Greece	95	101
Thailand	81	151
Italy	70	145
Japan	59	306
Netherlands	51	87
Spain	51	112
United States of America	51	233
Serbia	50	50

Qui siamo giusto nella top ten (in questo caso abbiamo ampliato la ricerca alle nazioni con oltre 50 certificati emessi).

Infine, la più rilevante norma, la ISO 9001:

Country	certificates	sites
China	426716	430065
Italy	92664	135550
Germany	49298	81550
Japan	40834	96808
United Kingdom of Great Britain and Northern Ireland*	39682	55622
India	36505	45255
Spain	31318	45740
United States of America	25561	42498
France	21918	60539
Brazil	16268	25386
Korea (Republic of)	14339	15089
Thailand	12711	18291
Romania	11886	14641
Malaysia	11610	15584
Czech Republic	11429	12580
Poland	10512	16575
Taiwan, Province of China	10379	14782
Colombia	10263	15210

Qui, con una punta di orgoglio, diciamo di essere superati solo dalla Cina per ovvie dimensioni numeriche (l'elenco è limitato alle nazioni con almeno 10.000 certificati).

Delle aziende italiane censite 333 appartengono al settore ICT (IAF 33), dato particolarmente utile per le nostre successive analisi:

Country	Information technology
China	36674
Germany	981
Japan	884
Spain	711
India	677
Argentina	574
United States of America	438
United Kingdom of Great Britain and No	401
Israel	389
Romania	342
Italy	333
Colombia	331
Hungary	322
Czech Republic	300

La situazione italiana in dettaglio

Grazie al supporto di Accredia, che ringraziamo per l'aiuto offertoci, possiamo analizzare i dati delle 3 principali norme coinvolte nel settore ICT: la ISO/IEC 27001, la ISO/IEC 20000-1 e ISO 22301.

In questo caso disponiamo anche del trend rispetto all'anno precedente e i dati sono aggiornati a giugno 2022, in più possiamo attingere alla distribuzione dei certificati per regione.

Mettiamo la ISO/IEC 27001 letteralmente al centro per facilitare il confronto e l'analisi:

siti certificati al 06-2022	ISO 22301	UNI CEI ISO/IEC 27001	UNI CEI EN ISO/IEC 20000-1
Estero	35	*1.111*	79
Lombardia	56	561	58
Lazio	41	528	78
Emilia-Romagna	7	249	16
Veneto	18	190	23
Toscana	6	129	9
Piemonte	11	125	17
Campania	5	84	11
Puglia	14	83	7
Marche	-	75	2
Sicilia	1	53	3
Liguria	6	49	7
Friuli-Venezia Giulia	1	42	3
Calabria	2	37	2
Provincia autonoma di Trento	4	30	-
Abruzzo	-	29	3
Sardegna	6	24	3
Umbria	1	23	3
Basilicata	4	21	2
Provincia autonoma di Bolzano/Bozen	4	20	1
Valle d'Aosta/Vall?e d'Aoste	-	6	-
Molise	-	5	-
TOTALE	**222**	**3.474**	**327**

siti certificati al 06-2021	ISO 22301	UNI CEI ISO/IEC 27001	UNI CEI EN ISO/IEC 20000-1
Estero	26	*688*	83
Lombardia	15	514	40
Lazio	10	474	66
Emilia-Romagna	3	220	10
Veneto	9	181	19
Toscana	3	124	7
Piemonte	5	120	14
Campania	3	85	8
Puglia	3	81	6
Marche	-	67	-
Sicilia	1	51	3
Liguria	-	41	4
Friuli-Venezia Giulia	1	47	1
Calabria	-	43	-
Provincia autonoma di Trento	3	22	-
Abruzzo	-	24	2
Sardegna	1	23	2
Umbria	1	26	3
Basilicata	4	23	1
Provincia autonoma di Bolzano/Bozen	7	19	1
Valle d'Aosta/Vall?e d'Aoste	-	4	-
Molise	-	5	-
TOTALE	**95**	**2.882**	**270**

Il dato Estero si riferisce a certificati censiti da Accredia (perché conferiti dagli Organismi di Certificazione). È un dato che lasciamo per dovere di trasparenza ma che non influisce sulle considerazioni e sugli scopi di questo articolo.

La Lombardia e il Lazio si confermano come le regioni principali in praticamente tutte le norme, sia nel 2021 sia nell'anno in corso.

Di particolare interesse il fatto che il settore ICT (IAF 33) che risulta essere l'unico dove le norme sono applicate simultaneamente (non possiamo sapere se nelle stesse aziende ma è comunque un dato che caratterizza il settore ICT).

È doveroso ricordare che la Circolare tecnica DC N° 22/2017[2] stabilisce che le certificazioni ISO 22301 vengono rilasciate per macrosettori:

A. Industria e relativa distribuzione (es.: Farmaceutica; Alimentare)
B. Infrastrutture critiche (es.: distribuzione energia; comunicazioni; trasporti)
C. Produzione di Energia (es.: Raffinerie; Centrali elettriche)
D. Pubblica Amministrazione (se non già ricompresa nei settori precedentemente elencati)
E. Sanitario (es.: Strutture sanitarie con centri di rianimazione; sale operatorie; terapie intensive; supporto alla respirazione)
F. Servizi
G. Servizi finanziari e di spedizione (es.: banche, assicurazioni, corrieri, money transfer)
H. Servizi informatici (es.: conservatori di fatture elettroniche, Internet Service Provider)

[2] Circolare tecnica DC N° 22/2017 - Nuova informativa in merito all'accreditamento per lo schema di certificazione ISO 22301:2012 - Sistemi di gestione della business continuity (rev.1) - Accredia

Un altro dato interessante è la crescita anno su anno dei siti certificati:

Siti certificati in Italia	TOTALE	ISO 22301	UNI CEI ISO/IEC 27001	UNI CEI EN ISO/IEC 20000-
2021	151399	95	2882	270
2022	160615	222	3474	327
incr %	5,74	57,21	17,04	17,43

È evidente come le tre norme abbiano trend in crescita positivi, con la ISO 22301 in crescita significativa.

Il quadro emergente

Il quadro emergente è di sicuro interesse per l'Italia. Ci posiziona infatti ai primi posti per il settore ICT con una tendenza positiva importante.

Più complesso è determinare quante delle aziende certificate in Italia dispongano di un sistema integrato con ISO/IEC 27001, ISO/IEC 20000-1 e ISO 22301 nelle varie combinazioni possibili.

Questo dato potrebbe essere rilevante per calibrare l'effettivo effort richiesto. Infatti, è cosa diversa dover applicare la transizione alla sola ISO/IEC 27001 e dover considerare invece gli impatti sull'integrazione con gli altri standard analizzati.

Vediamo di tener conto anche di questo dato nello sviluppo della nostra analisi.

Le principali modifiche apportate alla ISO/IEC 27001

Per brevità riportiamo quanto detto dalla norma e quanto si evince da un'analisi requisito per requisito.

Le modifiche principali, come definite nella norma riguardano:

> This third edition cancels and replaces the second edition (ISO/IEC 27001:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001:2013/Cor 1:2014 and ISO/IEC 27001:2013/Cor 2:2015.
>
> The main changes are as follows:
>
> — the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

Le modifiche inerenti ai Technical Corrigenda erano già state recepite nella versione della UNI CEI EN ISO/IEC 27001:2017, quindi per l'Italia la principale modifica riguarda l'armonizzazione con l'HLS del 2021 e con i controlli dell'Annex A allineati alla ISO/IEC 27002:2022.

Interessante notare che l'Annex A ora segue esattamente la numerazione della ISO/IEC 27002 e quindi i controlli hanno perso la "A." che li caratterizzava.

Le modifiche apportate ai requisiti

Per ovvie ragioni non entreremo nei singoli requisiti a discutere delle singole variazioni ma riportiamo tutti i requisiti in qualche modo toccati dagli aggiornamenti:

> 4.2 Understanding the needs and expectations of interested parties
> 4.4 Information security management system
> 5.1 Leadership and commitment
> 5.3 Organizational roles, responsibilities and authorities
> 6.1.3 Information security risk treatment
> 6.2 Information security objectives and planning to achieve them

6.3 Planning of changes (NUOVO REQUISITO)
7.4 Communication
8.1 Operational planning and control
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management review
10 Improvement

Quindi un aggiornamento non proprio irrilevante, come confermato dal periodo di transizione definito da IAF in 36 mesi[3].

Quale impatto sui Sistemi di Gestione già certificati?

Innanzitutto, occorrerà rivalutare i controlli applicabili utilizzando il nuovo Annex A e soprattutto gli attributi dei controlli.

Gli attributi meritano sicuramente un minimo di commento vista la nuova struttura.

Facciamo un esempio per chiarire l'uso dei controlli: supponiamo che l'organizzazione operi in un settore fortemente orientato alla cybersecurity, in particolare alla risposta, e che i suoi contratti richiedano particolare resilienza e protezione dei dati personali dei clienti.

Con la precedente versione della norma la scelta dei controlli poteva avvenire solo sulla base dell'esperienza. A fronte dei rischi, non ritenuti accettabili, l'organizzazione doveva analizzare i 114 controlli e scegliere, senza una guida specifica, quelli ritenuti appropriati.

Nella nuova versione dell'Annex A, e grazie alla ISO/IEC 27002:2022, le organizzazioni potranno selezionare i controlli in base a 5 attributi, ciascuno orientato a specifici orientamenti della sicurezza delle informazioni (riportiamo il testo integrale in attesa della traduzione ufficiale nazionale):

Control type

Control type is an attribute to view controls from the perspective of when and how the control modifies the risk with regard to the occurrence of an information security incident.

Attribute values consist of:

- Preventive (the control that is intended to prevent the occurrence of an information security incident),
- Detective (the control acts when an information security incident occurs) and
- Corrective (the control acts after an information security incident occurs).

Information security properties

Information security properties is an attribute to view controls from the perspective of which characteristic of information the control will contribute to preserving. Attribute values consist of:

- Confidentiality,
- Integrity and
- Availability.

[3] IAF_MD_26_Transition_requirements_for_ISOIEC_27001-2022_09082022.pdf

Cybersecurity concepts

Cybersecurity concepts is an attribute to view controls from the perspective of the association of controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110. Attribute values consist of:

- Identify,
- Protect,
- Detect,
- Respond and Recover.

Operational capabilities

Operational capabilities is an attribute to view controls from the practitioner's perspective of information security capabilities. Attribute values consist of:

- Governance,
- Asset_management,
- Information_protection,
- Human_resource_security,
- Physical_security,
- System_and_network_security,
- Application_security,
- Secure_configuration,
- Identity_and_access_management,
- Threat_and_vulnerability_management,
- Continuity,
- Supplier_relationships_security,
- Legal_and_compliance,
- Information_security_event_management and
- Information_security_assurance.

Security domains

Security domains is an attribute to view controls from the perspective of four information security domains:

- "Governance and Ecosystem" includes:
  - "Information System Security Governance & Risk Management" and
  - "Ecosystem cybersecurity management" (including internal and external stakeholders);
- "Protection" includes:
  - "IT Security Architecture",
  - "IT Security Administration",
  - "Identity and access management",
  - "IT Security Maintenance" and
  - "Physical and environmental security";
- "Defence" includes:
  - "Detection" and
  - "Computer Security Incident Management";
- "Resilience" includes:
  - "Continuity of operations" and
  - "Crisis management".

Tornando al nostro esempio e filtrando i controlli con le "parole chiave": cybersecurity risposta, resilienza, riservatezza, utilizzate negli attributi, si ottiene un insieme ben definito di controlli che corrispondono alle "parole chiave".

Questo permetterà a ciascuna organizzazione di dimostrare alle parti interessate la scelta dei controlli sulla base di requisiti specifici, siano essi legali, contrattuali o volontari.

Per agevolare la selezione abbiamo realizzato una SoA in grado di filtrare i controlli secondo le chiavi necessarie e supportare le aziende alla identificazione dei controlli necessari. La stessa SoA permette di inserire ulteriori funzionalità a supporto del SGSI: correlazione con controlli della precedente edizione, documenti di riferimento, eventuali KPI associati per la misura di efficacia del controllo, funzioni coinvolte nella gestione del controllo ecc.

Questa struttura si è rilevata nel tempo di particolare praticità ed efficacia, non solo nelle fasi progettuali ma anche in quelle inerenti alla formazione e agli audit (interni ed esterni).

La scelta dei controlli

Da quanto appena esposto è chiaro che le organizzazioni saranno agevolate nella scelta dei controlli e nella correlazione dei controlli con il proprio business.

Rilevante quanto descritto nella sezione 0 della ISO/IEC 27002:2022, indispensabile per la corretta utilizzazione dei controlli e per risolvere "errori interpretativi" rilevati nell'utilizzazione della precedente versione dei controlli elencati nell'Annex A della ISO/IEC 27001:

> There are three main sources of information security requirements:
>
> a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;
> b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their sociocultural environment;
> c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

Altri impatti attesi

Una volta riallineato il trattamento dei rischi, sarà necessario aggiornare la Dichiarazione di Applicabilità (o SoA) in modo da recepire quanto richiesto dai nuovi controlli.

Dovranno essere anche recepite tutte le modifiche apportate ai requisiti elencati nei paragrafi della norma, attraverso un approccio strutturato, che tenga conto del ciclo di vita del Sistema e della documentazione esistente.

A titolo di esempio, sarà necessario riprogrammare ed effettuare la formazione per il personale coinvolto, ridefinire i parametri per la verifica di efficacia dei controlli, riprogrammare e rieseguire gli audit interni ecc.

Non si tratta quindi di mere modifiche documentali passive, c'è un impatto effettivo.

Ovviamente questo potrebbe essere gestito come un miglioramento, sfruttando la norma stessa e il SGSI per farsi condurre lungo la strada giusta.

Impatto sui sistemi integrati ISO/IEC 20000-1 e ISO 22301

Poco dibattuto finora il tema dei sistemi integrati e dei sistemi dotati di varie "estensioni" della ISO/IEC 27001.

In questa sezione vogliamo trattare queste casistiche, visti anche i dati raccolti nella prima parte dell'articolo.

L'impatto analizzato finora sarà caratterizzato da altri elementi aggiuntivi per i sistemi integrati, soprattutto con norme come la ISO/IEC 20000-1 e la ISO 22301.

Per la ISO/IEC 20000-1 era stata preparata una linea guida specifica[4] per l'allineamento alla ISO/IEC 27001:2013, che a questo punto si trova disallineata e quindi non più utilizzabile, almeno non in modo immediato.

Le aziende dovranno provvedere autonomamente all'allineamento dei requisiti (operazione relativamente complessa) e dei controlli (questa operazione sarà sicuramente più articolata). Sicuramente gli attributi dei controlli potranno essere di aiuto nel creare una cross reference.

Ad esempio: il change management (req. 8.5.1 della ISO/IEC 20000-1) potrebbe essere messo in correlazione con i controlli:

5.20 Addressing information security within supplier agreements

5.22 Monitoring, review and change management of supplier services

8.7 Protection against malware

8.8 Management of technical vulnerabilities

8.9 Configuration management

8.32 Change management

Ovviamente la conoscenza di entrambe le norme e l'esperienza nella loro gestione giocano un ruolo sostanziale per la scelta dei controlli correlati.

Stesso processo può essere ipotizzato per la ISO 22301 ma in questo caso si è aiutati dagli attributi dei controlli, ad esempio sono correlabili tutti i controlli che hanno i seguenti attributi

Operational capabilities

- Continuity,

Security domains

- "Resilience" includes:
  - "Continuity of operations" and
  - "Crisis management".

Quindi potremmo, ad esempio, considerare i controlli che richiamano la continuità e la resilienza, ottenendo così l'applicabilità dei seguenti controlli:

5.29 Information security during disruption

5.30 ICT readiness for business continuity

8.14 Redundancy of information processing facilities

[4] ISO/IEC TR 20000-7:2019 - Information technology — Service management — Part 7: Guidance on the integration and correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015 and ISO/IEC 27001:2013

Non un lavoro semplicissimo ma conoscendo le tematiche e le norme diventa un lavoro interessante, anche per controllare (e dimostrare) l'integrità del sistema e la sua coerenza con il business aziendale.

Impatto sui sistemi estesi alle ISO/IEC 27017, ISO/IEC 27018 e/o ISO/IEC 27701

In attesa delle inevitabili revisioni di questi standard di estensione della ISO/IEC 27001 possiamo ipotizzare un percorso analogo a quello visto per le altre norme, solo che in questo caso dovremo rivedere tutti i controlli citati per capirne eventuali cambiamenti e integrazioni.

Facciamo un esempio trasversale, applicabile a tutti e tre gli standard, supponiamo di voler allineare le estensioni per il controllo di "event logging", la tabella seguente evidenzia le correlazioni tra la ISO/IEC 27001 e le sue estensioni:

ISO/IEC 27701	ISO/IEC 27018	ISO/IEC 27017	ISO/IEC 27001:2022
6.9.4.1 Event logging – collegato all'art. 5 del GDPR.1 f)	12.4.1 Event logging	12.4.1 Event logging	8.15 Logging cui potrebbero essere collegati: • 5.25 Assessment and decision on information security events • 5.28 Collection of evidence • 5.34 Privacy and protection of PII • 8.11 Data masking • 8.16 Monitoring activities • 8.17 Clock synchronization

Quindi, un altro esercizio che comporta la conoscenza/esperienza trasversale di questi standard e il contesto dell'organizzazione per poter eseguire un lavoro corretto.

A titolo di cronaca, alla data di pubblicazione di questo articolo, in Italia sono presenti:

- 362 organizzazioni con estensione alla ISO/IEC 27017
- 359 organizzazioni con estensione alla ISO/IEC 27018
- 57 organizzazioni con estensione alla ISO/IEC 27701

Per l'Italia, le estensioni di cui sopra, sono certificabili sotto accreditamento, secondo quanto descritto nel sito Accredia[5].

[5] Circolare informativa DC N° 01/2019 - Accreditamento ISO/IEC 27001:2013 con integrazione linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2014 - Information Technology, Security techniques, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors - Accredia e Circolare tecnica DC N° 10/2019 - Disposizioni in merito all'accreditamento norma ISO/IEC 27701 - Accredia

Considerazioni finali

La definizione di "modifica documentale" non mi trova pienamente d'accordo, dati gli elementi visti sopra.

Vero che cambiano i testi ma è anche vero che le ripercussioni su un sistema di gestione non sono solo documentali. Anche solo dimostrare che la nuova organizzazione dei controlli è efficace significa comunque mettere le mani su parecchi elementi del Sistema di Gestione.

Molte aziende attendevano la nuova norma per iniziare la certificazione, altre la attendevano per cogliere l'occasione per una revisione e una "svecchiata". In ogni caso sarà una grande opportunità per tutti.

Restiamo a vostra disposizione per una gap analysis e per un progetto di transizione ben fatto, da persone che hanno esperienze e competenze trasversali pluriennali.