SECURITY SUMMIT

Security Summit

Milano 17-18-19 marzo 2026

Clusit

ASTREA

UNINFO

Aggiornamenti dal mondo della normazione, dalla ISO/IEC 27701:2025 allo schema EUCC

Dorotea DE MARCO | Funzionario Dipartimento tecnologie digitali e sicurezza informatica GPDP
Fabio GUASCONI | Presidente CT 510 UNI/UNINFO e CEO di Risc^3
Stefano RAMACCIOTTI | Consulente e formatore Common Criteria

Dorotea DE MARCO
Relatore Clusit

- ✓ Funzionario tecnologico **Garante protezione dati personali**
- ✓ Esperto CT 510
- ✓ Editor ISO/IEC 27555:2021
- ✓ Co-editor ISO/IEC 10267 e ISO/IEC 27555 revision

Fabio GUASCONI
Relatore Clusit

- ✓ Presidente della CT 510 di **UNINFO** "Sicurezza"
- ✓ Direttivo **CLUSIT**
- ✓ Esperto **SBS**
- ✓ CEO Risc^{3}, già cofondatore **Bl4ckswan**
- ✓ Esaminatore UNI 11697
- ✓ Certificazioni CISA, CISM, PCI-QSA/3DS/QPA, ITIL, PRINCE2, ISFS, LA 27001/22301/27701/9001, LI 27001, DPO UNI 11697

Stefano RAMACCIOTTI
Relatore Clusit

- ✓ Presidente **ISC2 Italy Chapter**
- ✓ Membro ISO/IEC JTC1 SC27 WG3 "Security Evaluation Criteria"
- ✓ Esperto tecnico ACCREDIA **accreditamento laboratori di prova EUCC**
- ✓ ex-Direttore del Centro di Valutazione della Difesa
- ✓ Certificazioni: CISSP e Valutatore Common Criteria fino a EAL4 per CSE canadese e PCM
- ✓ Attività di docenza: STELMILIT Chiavari, CIFIGE, UNIROMA TRE, Università degli studi di Genova (DITEN), Consorzio Interuniversitario SERICS, Gerico Lab srl

Agenda

- Norme sulla protezione dei dati personali
- Norme su RED e CRA
- EUCC
- EIDAS / EIDAS2

Norme "privacy" pubblicate dal 2022

2025

- ISO/IEC 27701:2025 – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
- ISO/IEC 27706:2025 – Requirements for bodies providing audit and certification of privacy information management systems to ISO/IEC 27701 in combination with ISO/IEC 27001
- ISO 27018:2025 - Code of practice for protection of PII in public clouds acting as PII processors
- ISO 27564:2025 - Privacy models

2024

- ISO 27562:2024 - Privacy guidelines for fintech services

2023

- ISO/IEC TS 27560:2023 – Structure of personal identifiable information (PII) processing records - **free**

2022

- ISO 27557:2022 - Organizational privacy risk management
- ISO 27559:2022 - Privacy enhancing data de-identification framework
- ISO 27556:2022 – User-centric privacy preferences management framework

Focus sulla ISO/IEC 27701 – versione 2019

1 Scope
2 Normative reference
3 Terms, definitions and abbreviations
4 General
5 PIMS-specific requirements related to ISO/IEC 27001
6 PIMS-specific guidance related to ISO/IEC 27002
7 Additional ISO/IEC 27002 guidance for PII controllers
8 Additional ISO/IEC 27002 guidance for PII processors
Annex A (normative) PIMS specific reference control objectives and controls (PII Controllers)
Annex B (normative) PIMS specific reference control objectives and controls (PII Processors)
Annex C (informative) Mapping to the General Data Protection Regulation
Annex D (informative) Mapping to ISO/IEC 29100
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151
Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002


INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

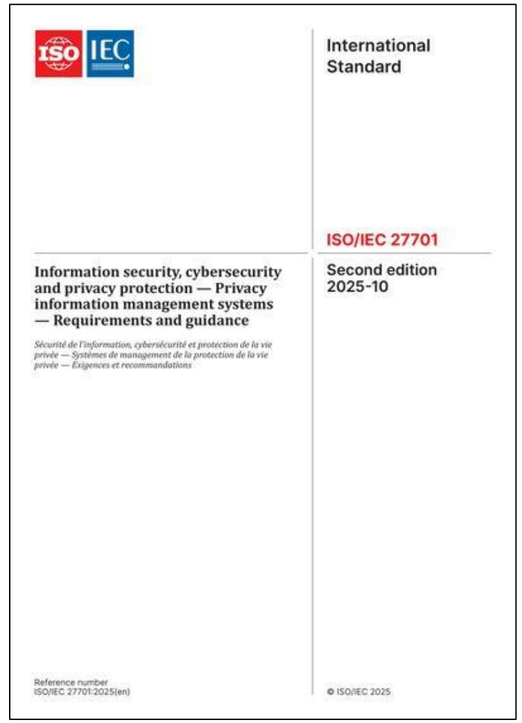
ISO IEC

Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019

Focus sulla ISO/IEC 27701 – versione 2025

1 Scope
2 Normative references
3 Terms, definitions and abbreviations
4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement
11 Further information on annexes
Annex A (normative) PIMS reference control objectives and controls for PII controllers and PII processors
Annex B (normative) Implementation guidance for PII controllers and PII processors
Annex C (informative) Mapping to ISO/IEC 29100
Annex D (informative) Mapping to the General Data Protection Regulation
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151
Annex F (informative) Correspondence with ISO/IEC 27701:2019.


ISO IEC

International Standard

ISO/IEC 27701

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations

Second edition
2025-10

Reference number
ISO/IEC 27701:2025(en)

© ISO/IEC 2025

ISO/IEC 27701:2025

PIMS separato da ISMS (ISO 27701:2019) - elementi caratterizzanti

- (4.1) la necessità di definire se si sta operando come titolare o responsabile
- (4.2) il requisito di includere tutti i soggetti dell'ecosistema della data protection, inclusa l'autorità di controllo, tra le parti interessate
- (6.1 e 8.2) l'obbligo di effettuare privacy risk assessment e privacy risk treatment, collegate ad un SoA analogo a quello richiesto dalla ISO/IEC 27001
- processo di gestione del rischio.

ISO/IEC 27701:2025

Risk management - elementi specifici per la privacy rispetto alla ISO 31000, ripresi dalla ISO/IEC 27557

- considerando sia gli impatti sugli interessati che quelli sull'organizzazione
- ampliando il contesto ai classici privacy stakeholders
- focalizzando lo scope sui trattamenti e su prodotti e servizi ad essi collegati
- introducendo due possibili approcci, asset-based ed event-based
- fornendo una utile serie di annex con esempi di "privacy events" e dei relativi "privacy impacts" sulle persone e delle conseguenze sulle organizzazioni
- (6.1) identificare e documentare un "information security programme" per il trattamento del rischio relativo

ISO/IEC 27701:2025 – Annex A

Raccolta di controlli

carattere **normativo**

parti:

- **A.1 per i titolari – 29 controlli**
- **A.2 per i responsabili – 17 controlli**
- **A.3 per entrambi i titolari e i responsabili – 28 controlli** (da ISO/IEC 27002)

A.1 e A.2 hanno in comune:

- **Conditions for collection and processing**
- **Obligations to PII principals**
- **Privacy by design and privacy by default**
- **PII sharing, transfer and disclosure**

A.3 riguarda "*Security considerations for PII controllers & processors*"

ISO/IEC 27701:2025 – Annex B

Mapping delle implementation guidance di:

- A.1 in **B.1 Implementation guidance for PII controllers**
- A.2 in **B.2 Implementation guidance for PII processors**
- A.3 in **B.3 Implementation guidance for PII controllers and PII processors**
- Es: le implementation guidance del controllo A.2.2.2 si trovano in B.2.2.2.

Analogamente ai controlli dell'Annex A della ISO/IEC 27001 e la ISO/IEC 27002, nell'Annex B i controlli vengono estesi (talvolta anche con "Other information«)

Privacy Risk Management

Privacy events
Appropriation
Distortion
Induced disclosure
Insecurity
Re-identification
Stigmatization
Surveillance
Unanticipated revelation
Unwarranted restriction

Privacy impacts on individuals
Dignity loss
Discrimination
Economic loss
Loss of self-determination
Loss of trust

Consequences for organizations
Noncompliance costs
Direct business costs
Damage to reputation
Harm to internal organizational culture

Information Security Programme

Raccolta di controlli di sicurezza

- information security risk management;
- policies for information security;
- organization of information security;
- human resources security;
- asset management;
- access control;
- operations security;
- network security management;
- development security;
- supplier management;
- incident management;
- information security continuity;
- information security reviews;
- cryptography; and
- physical and environmental security.

ISO Standard in sviluppo

ISO/IEC 27566 – Age assurance systems (multipart standard)

– Part 1 (FDIS) – **Framework** – key principles and confidence indicators for providers of services, decision makers and regulators

– Part 2 (1st WD) – **Technical approaches and guidance for implementation**

– Part 3 (2nd CD) – **Approaches to comparison or analysis** – measurement and testing of age verification components

ISO/IEC 27091 (FDIS) – **Artificial Intelligence – Privacy protection -** Guidelines for organizations developing AI systems and models, to address privacy risk in their lifecycle

ISO/IEC 10267 (DIS) – **Methods to quantify the amount of personal information in a dataset**

ISO Standard in sviluppo

ISO/IEC 27568 (2nd WD) – **Security and privacy of digital twins**

ISO/IEC 27573 (2nd WD) – **Privacy protection of user avatar and system avatar interactions in the metaverse**

ISO/IEC 27574 (1st WD) – **Privacy in brain-computer interface (BCI) applications**

ISO/IEC 27503 (PWI)- **Guidelines on Privacy Protection of Intelligent Travel Services**

CEN JTC13/WG 5

Revisione di EN 17529:2022 Data protection and privacy by design and by default

NWIP – revisione di 17926 - Privacy information management system per EN ISO/IEC 27701 – Refinements in European context» (ENQ)

Certification scheme as per ISO/IEC 17065 for certification against EN ISO/IEC 27701 – refinements in European context" (ENQ)

NWI from the CWA 18016 "Age appropriate design"

CEN CWA 17858:2022 Guidelines for Traditional Micro-SMEs' GDPR Compliance

Norme su RED e CRA

E' sempre più comune che gli enti di normazione europei lavorino a supporto del legislatore nell'andare a definire aspetti tecnici riguardanti la sicurezza in ambiti specifici.

Due esempi particolarmente rilevanti in questo senso sono:

- **Radio Equipment Directive** (Direttiva EU 2014/53) concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio

- **Cyber Resilience Act** (Regolamento EU 2024/2847) relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali

In entrambi i casi il CEN/CLC JTC 13 ha creato dei gruppi di lavoro dedicati, rispettivamente WG 8 (Special Working Group RED Standardization Request) e WG 9 (Horizontal cybersecurity for products with digital elements).

Norme su RED e CRA

La Direttiva RED richiede, tra le altre cose, che le apparecchiature radio siano fabbricate in modo da garantire:

- la protezione della salute e della sicurezza di persone e di animali domestici e beni (art. 3.1 a))
- la protezione delle reti (art. 3.3 d))
- la protezione dei dati personali trattati (art. 3.3 e))
- la protezione dalle frodi (art. 3.3 f))

Per definire quali **requisiti** siano necessari il JTC 13 ha quindi elaborato la serie di norme EN 18031, Common security requirements for radio equipment, composta dalle seguenti parti:

- **EN 18031-1** Part 1: Internet connected radio equipment
- **EN 18031-2** Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
- **EN 18031-3** Part 3: Internet connected radio equipment processing virtual money or monetary value

Norme su RED e CRA

A partire dal 1 agosto del 2025 chi produce apparecchiature radio può rispettare i requisiti definiti nelle norme della serie 18031 come "presumption of conformity", senza obbligo di certificazione, strutturati in modo comune:

6.x.y.1 Requirement
6.x.y.2 Rationale
6.x.y.3 Guidance
6.x.y.4 Assessment criteria
6.x.y.4.1 Assessment objective
6.x.y.4.2 Implementation categories
6.x.y.4.3 Required information
6.x.y.4.4 Conceptual assessment
6.x.y.4.5 Functional completeness assessment terms of numbering
6.x.y.4.6 Functional sufficiency assessment

Tra i requisiti troviamo, ad esempio:

[ACM] Access control mechanism
- [ACM-1] Applicability of access control mechanisms
- [ACM-2] Appropriate access control mechanisms

[SUM] Secure update mechanism
- [SUM-1] Applicability of update mechanisms
- [SUM-2] Secure updates
- [SUM-3] Automated updates.

Norme su RED e CRA

Il CRA invece richiede, nel suo articolo 13, che i fabbricanti di prodotti con elementi digitali li progettino, sviluppino e producano conformemente ai **requisiti essenziali di cybersecurity** di cui all'allegato 1 parte 1, effettuando e mantenendo successivamente aggiornata una valutazione dei rischi di cybersecurity. In aggiunta, richiede che nel caso di individuazione di **vulnerabilità** entro il periodo di assistenza (5 anni), questa sia corretta secondo quanto definito all'allegato 1 parte 2 e sia segnalata, se sfruttata, a CSIRT ed ENISA.

Nell'articolo 32 sono definite specifiche procedure di valutazione della conformità per prodotti con elementi digitali a seconda della loro tipologia esplicitate nell'allegato 8.

I fabbricanti redigono una "dichiarazione di conformità UE" che attesta il rispetto dei requisiti essenziali di cybersecurity applicabili di cui all’allegato 1, basata anche in questo caso su un meccanismo di "presumption of conformity" rispetto alle norme armonizzate sviluppate.

Norme su RED e CRA

Le principali norme "*orizzontali*" in fase di sviluppo da parte del JTC 13 sono:

- **EN 40000-1-1** Vocabulary
- **EN 40000-1-2** Principles for Cybersecurity (Annex 1, Requisito 1)
- **EN 40000-1-3** Vulnerability Handling (Annex 1, Parte 2)
- **EN 40000-1-4** Generic security requirements (Annex 1, Requisito 2 (a-m))

Mentre la parte 1-2 e la parte 1-3 sono già in Enquiry, la pubblicazione finale di tutta la serie è prevista entro fine 2027.

Saranno poi previste diverse norme "*verticali*" dedicate a specifiche categorie di prodotti.

Norme su RED e CRA

La parte 1-1 è la norma "vocabolario" della serie e recepisce termini e definizioni trasversali.

La parte 1-2 definisce i 4 principi per garantire la cybersecurity di prodotto, stabilisce un quadro generale per gestire i rischi relativi ed elenca le attività da condurre durante lo sviluppo. Prevede assessment criteria per autovalutazioni.

La parte 1-3 è impostata andando a definire una serie di requisiti per la gestione delle vulnerabilità allineati alle best practices di settore e così strutturati:

5.X.X.X Requirement
[XXX-X-RQ-XX] Description of a requirement
[XXX-X-RQ-XX-RE] Description of a requirement enhancement
[XXX-X-RC-XX] Description of a recommendation
[XXX-X-PM-XX] Description of a permission

La parte 1-4 utilizza la medesima struttura della EN 18031

Norme su RED e CRA

EN 18031

- [ACM] Access control mechanism
- [AUM] Authentication mechanism
- [SUM] Secure update mechanism
- [SSM] Secure storage mechanism
- [SCM] Secure communication mechanism
- [LGM] Logging mechanisms
- [DLM] Deletion mechanisms
- [UNM] User notification mechanism
- [RLM] Resilience mechanism
- [NMM] Network monitoring mechanism
- [TCM] Traffic control mechanism
- [CCK] Confidential cryptographic keys
- [GEC] General equipment capabilities
- [CRY] Cryptography

WD EN 40000-1-4

- [ACM] Access control mechanism
- [AUM] Authentication mechanism
- [SUM] Secure update mechanism
- [SSM] Secure storage mechanism
- [SCM] Secure communication mechanism
- [LGM] Logging mechanisms
- [DLM] Deletion mechanisms
- [UNM] User notification mechanism
- [RLM] Resilience mechanism
- [NMM] Network monitoring mechanism
- [TCM] Traffic control mechanism
- [CCK] Confidential cryptographic keys
- [GEC] General equipment capabilities
- [CRY] Cryptography
- [DTM] Data minimization
- [LIM] External impact limitation
- [MON] Monitoring of security activities

NEW

EUCC

EIDAS / EIDAS2

Architettura degli standard: ETSI, CEN e CENELEC

Policy generale TSP ETSI EN 319 401 v3.1.1	Requisiti generali di policy per tutti i prestatori di servizi fiduciari — baseline orizzontale
Requisiti CAB ETSI EN 319 403-1 v2.3.1 + TS 119 403-3	Requisiti per gli organismi di valutazione della conformità — accreditamento e specificità QTSP
Policy specifiche per servizio ETSI EN 319 411, 421, 521 / CEN/TS 18170 ...	Requisiti di policy e sicurezza per ciascun tipo di servizio fiduciario
Specifiche tecniche ETSI EN 319 122, 132, 162, 522, 532 - CEN/TS 18264 ...	Formati, protocolli, interoperabilità, protection profile — referenziati dagli atti di esecuzione
Identity proofing ETSI TS 119 461	Verifica dell'identità dei soggetti dei servizi fiduciari — trasversale a tutti i servizi

EIDAS / EIDAS2

Mappa degli standard per servizio fiduciario

Certificati qualificati (firme e sigilli)

ETSI EN 319 411-1/2
ETSI EN 319 412 series

Reg. 2025/1943

Marche temporali elettroniche

ETSI EN 319 421
ETSI EN 319 422

Reg. 2025/1929

Servizi di validazione

ETSI TS 119 441
ETSI TS 119 172-4

Reg. 2025/1942

Servizi di conservazione

ETSI TS 119 511
ETSI EN 319 162-1

Reg. 2025/1946

SERCQ (Recapito certificato)

ETSI EN 319 521/522
ETSI EN 319 531/532

Reg. 2025/1944

Gestione QSCD remoti

ETSI TS 119 431-1
CEN PP (CEN/TC 224/WG2)

Reg. 2025/1567

Formati firma / sigillo e contenitori ASiC

ETSI EN 319 122/132/162
ETSI TS 103 171/172/173

Reg. 2026/248

Archiviazione elettronica

CEN/TS 18170
ISO 14721

Reg. 2025/2532

EIDAS / EIDAS2

Punti chiave

- 30+ atti di esecuzione adottati tra luglio 2025 e febbraio 2026 — il pacchetto normativo più ampio dalla entrata in vigore di eIDAS nel 2014, tuttora in evoluzione
- Gli standard ETSI e CEN sono referenziati con versioni specifiche negli atti di esecuzione, creando una catena vincolante per la presunzione di conformità ma questo crea frizioni per i continui aggiornamenti
- La doppia conformità eIDAS2 + NIS2 trasforma il perimetro di audit — i servizi fiduciari non possono più essere valutati in isolamento dalla governance di cybersecurity NIS2
- I lavori di standardizzazione in corso colmano gap critici tra gli atti di esecuzione e gli standard tecnici vigenti

Q&A

Contatti:

d.demarco@gpdp,it
fabio.guasconi@risc3.com
Stefano