La nuova norma

ISO/IEC 27001:2022

sui sistemi di gestione della sicurezza delle informazioni, cybersecurity e privacy

Privacy Day 25 maggio 2023 Pisa CNR - Monica Perego

LA NUOVA NORMA ISO/IEC 27001:2022 SUI SISTEMI DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI, CYBERSECURITY E PRIVACY

ISO/IEC 27001:2022

ISO/IEC 27000:2018

ISO/IEC 27002:2022

ISO/IEC 27001:2022

FRAMEWORK DI REQUISITI

FRAMEWORK DI GESTIONE DEL RISCHIO

FRAMEWORK DI CONTROLLO

ISO/IEC 27001:2022

FRAMEWORK DI REQUISITI

Richiede il soddisfacimento di una serie di requisiti riportati nei capitoli da 4 a 10 dello standard

FRAMEWORK DI GESTIONE DEL RISCHIO

FRAMEWORK DI CONTROLLO

ISO/IEC 27001:2022

FRAMEWORK DI GESTIONE DEL RISCHIO

Sulla base del contesto e delle esigenze
ed aspettative delle parti interessate, individuino,
valutino e trattino i rischi che impattano sulla RID

FRAMEWORK DI REQUISITI

FRAMEWORK DI CONTROLLO

ISO/IEC 27001:2022

FRAMEWORK DI CONTROLLO

In quanto riporta nell'Allegato A 93 controlli suddivisi in 4 clausole.

FRAMEWORK DI REQUISITI

FRAMEWORK DI GESTIONE DEL RISCHIO

ISO/IEC 27000:2018

TECNOLOGIE INFORMATICHE - TECNICHE PER LA SICUREZZA - SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

- VISIONE D'INSIEME E VOCABOLARIO

ISO/IEC 27001:2022

ISO/IEC 27002:2022

LA NUOVA NORMA ISO/IEC 27001:2022 SUI SISTEMI DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI, CYBERSECURITY E PRIVACY

STRUTTURA

ISO/IEC 27002:2022

INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION - INFORMATION SECURITY CONTROL

ISO/IEC 27001:2022

ISO/IEC 27000:2018

PUNTI IN COMUNE

ISO/IEC 27001:2022 E IL GDPR

ISO/IEC 27001:2022	REG. EU 2016/679
Dati del campo di applicazione del sistema di gestione della sicurezza delle informazioni	Dati personali
Ambito di applicazione worldwide	Ambito di applicazione secondo artt. 2 e 3

(1 di 3)

PUNTI IN COMUNE

ISO/IEC 27001:2022 E IL GDPR

ISO/IEC 27001:2022

REG. EU 2016/679

Applicazione delle normative cogenti compresa la protezione dei dati personali

→

Requisiti per garantire la libertà e i diritti degli interessati tra cui informativa e consenso

(2 di 3)

PUNTI IN COMUNE

ISO/IEC 27001:2022 E IL GDPR

ISO/IEC 27001:2022	REG. EU 2016/679
Analisi dei rischi da cui derivano i controlli da applicare (vedi ISO/IEC 27002:2022) ed eventuali ulteriori misure tecniche ed organizzative	Analisi dei rischi da cui derivano le misure tecniche e organizzative

(3 di 3)

ART. 42 - CERTIFICAZIONE

ART. 43 - ORGANISMO DI CERTIFICAZIONE

GDPR-ARTT.42 E 43

ART. 42 - CERTIFICAZIONE

1 Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati

ART. 43 - ORGANISMO DI CERTIFICAZIONE

GDPR-ARTT.42 E 43

ART. 42 - CERTIFICAZIONE

2 | Allo scopo di dimostrare la conformità al presente regolamento

3 | La certificazione è volontaria e accessibile tramite una procedura trasparente.

ART. 43 - ORGANISMO DI CERTIFICAZIONE

GDPR-ARTT.42 E 43

ART. 42 - CERTIFICAZIONE

4 La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento.

ART. 43 - ORGANISMO DI CERTIFICAZIONE

GDPR-ARTT.42 E 43

ART. 43 - ORGANISMO DI CERTIFICAZIONE

Gli stati membri garantiscono
che tali organismi di certificazione
siano accreditati da uno o entrambi dei seguenti organismi:

- dall'autorità di controllo competente ai sensi degli articoli 55 o 56.

ART. 42 - CERTIFICAZIONE

GDPR-ARTT.42 E 43

ART. 43 - ORGANISMO DI CERTIFICAZIONE

- dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del parlamento europeo e del consiglio conformemente alla norma EN-ISO/IEC 17065/2012.

ART. 42 - CERTIFICAZIONE

GLI STANDARD

SODDISFANO L'ART 42

EURO PRIVACY APPROVATA DA EPBD RICHIAMA LA ISO/IEC 27001:2022 COME POSSIBILE REQUISITO

VALENZA PANEUROPEA

GDPR-CARPA - ©EUROPRICE

GLI STANDARD

SODDISFANO L'ART 42

EURO PRIVACY APPROVATA DA EPBD RICHIAMA LA ISO/IEC 27001:2022 COME POSSIBILE REQUISITO

VALENZA PANEUROPEA

GDPR-CARPA - ©EUROPRICE

VALENZA NAZIONALE

GLI STANDARD

NON SODDISFANO L'ART 42
CONSIDERATI COME MISURE DI ACCOUNTABILITY (1 di 2)

ISDP© 10003 SCHEMA DI CERTIFICAZIONE
DATA PROTECTION – GDPR ACCREDITATO IN ACCORDO
CON LA NORMA EN ISO/IEC 17065:2012 ED AVVIATO ITER DI APPROVAZIONE AI
SENSI DELL'ART. 42.5

GLI STANDARD

NON SODDISFANO L'ART 42
CONSIDERATI COME MISURE DI ACCOUNTABILITY (1 di 2)

ISDP© 10003 SCHEMA DI CERTIFICAZIONE
DATA PROTECTION – GDPR ACCREDITATO IN ACCORDO
CON LA NORMA EN ISO/IEC 17065:2012 ED AVVIATO ITER DI APPROVAZIONE AI
SENSI DELL'ART. 42.5

BS 10012:2017 SPECIFICATION FOR A PERSONAL INFORMATION
MANAGEMENT SYSTEM

GLI STANDARD

NON SODDISFANO L'ART 42
CONSIDERATI COME MISURE DI ACCOUNTABILITY (2 di 2)

ISO/IEC 27001:2022 INFORMATION SECURITY, CYBERSECURITY
AND PRIVACY PROTECTION — INFORMATION SECURITY MANAGEMENT SYSTEMS
— REQUIREMENTS

GDPR-ARTT.42 E 43

GLI STANDARD

NON SODDISFANO L'ART 42
CONSIDERATI COME MISURE DI ACCOUNTABILITY (2 di 2)

ISO/IEC 27001:2022 INFORMATION SECURITY, CYBERSECURITY
AND PRIVACY PROTECTION — INFORMATION SECURITY MANAGEMENT SYSTEMS
— REQUIREMENTS

ISO/IEC 27701:2019 SECURITY TECHNIQUES — EXTENSION TO ISO/IEC 27001 AND
ISO/IEC 27002 FOR PRIVACY INFORMATION MANAGEMENT — REQUIREMENTS
AND GUIDELINES

ISO/IEC 27001:2022

L'IMPIANTO DELLA NORMA È CONGRUENTE A QUELLO DI TUTTE LE ALTRE NORME SUI SISTEMI DI GESTIONE

1 SCOPE

2 NORMATIVE REFERENCES

3 TERMS AND DEFINITIONS

4 CONTEXT OF THE ORGANIZATION

5 LEADERSHIP

6 PLANNING

7 SUPPORT

8 OPERATION

9 PERFORMANCE EVALUATION

10 IMPROVEMENT

ISO/IEC 27001:2022

QUATTRO MACRO-CONTROLLI CHE COINCIDONO CON I TRADIZIONALI PILASTRI ASSOCIATI ALLA SICUREZZA DELLE INFORMAZIONI

- CONTROLLI ORGANIZZATIVI
- CONTROLLI SULLE PERSONE
- CONTROLLI FISICI
- CONTROLLI TECNOLOGICI

ISO/IEC 27001:2022

QUATTRO MACRO-CONTROLLI CHE COINCIDONO CON I TRADIZIONALI PILASTRI ASSOCIATI ALLA SICUREZZA DELLE INFORMAZIONI

- CONTROLLI ORGANIZZATIVI → 37
- CONTROLLI SULLE PERSONE → 8
- CONTROLLI FISICI → 14
- CONTROLLI TECNOLOGICI → 34

ISO/IEC 27001:2022

Caratteristiche (5 famiglie di attributi), linee guida ed istruzione per l'applicazione dei controlli sono disponibili in ISO/IEC 27002:2022

Grazie!