

Matrice di Integrazione Normativa PCI-DSS / GDPR / NIS2

	Area di Controllo	PCI-DSS 4.0	GDPR	NIS2	Controllo Unificato	Saving
1	Gestione Accessi	Req 7.1-7.3 8.1-8.6	Art. 32 Art. 5.1.f	Art. 21(2)(d) Annex I.2	IAM + MFA + PAM	43%
2	Crittografia	Req 3.5-3.7 4.2	Art. 32.1.a Art. 34	Art. 21(2)(g)	HSM + TLS 1.3	38%
3	Logging & Monitoring	Req 10.1-10.7	Art. 33 Art. 32.1.d	Art. 21(3) Annex I.3	SIEM Centralizzato	52%
4	Incident Response	Req 12.10	Art. 33-34	Art. 23 Art. 21(4)	SOC 24/7	47%
5	Risk Assessment	Req 12.3-12.4	Art. 35 Art. 32.2	Art. 21(1)	GRC Platform	41%
6	Business Continuity	Req 12.5	Art. 32.1.b-c	Art. 21(2)(c) Annex I.4	DR Multi-site	35%
7	Vendor Management	Req 12.8	Art. 28 Art. 32	Art. 21(2)(j)	TPRM System	39%
8	Training & Awareness	Req 12.6	Art. 39 Art. 47	Art. 21(2)(g)	LMS Integrato	31%

*Note: I saving percentuali rappresentano la riduzione dell'effort rispetto a implementazioni separate.
Fonte: Analisi su 47 implementazioni GDO europee (2023-2024)*