

Control Domain	Control	SOC 2 (TSC 2017)	ISO/IEC 27001:2022	GDPR
Information Security Policies	Maintain and enforce security policies	CC1.2, CC5.3	5.1	Art. 24, Art. 32
Access Control	Role-based and least-privilege access	CC6.1, CC6.2	5.15, 5.16, 5.17, 5.18	Art. 25, Art. 32(1)(b)
Access Control	User access provisioning and de-provisioning	CC6.2	5.18, 5.20, 5.21	Art. 5(1)(f), Art. 32
Authentication	Strong user authentication and password policy	CC6.2	5.17, 5.18	Art. 32
Asset Management	Identify and manage information assets	CC9.2	5.9, 5.10	Recital 39, Art. 32
Cryptography	Use encryption for sensitive data	CC6.1, CC6.7	5.25, 5.26, 5.27	Art. 32(1)(a), Art. 34
Physical Security	Restrict physical access to systems	CC6.6	5.10, 5.11	Art. 32
Operations Security	Protection against malware, logging, and monitoring	CC7.2, CC7.3	5.8, 5.28, 5.29, 5.30	Art. 32
Change Management	Formal change control process	CC8.1	5.32	Art. 32
Logging and Monitoring	Logging security-relevant events and monitoring	CC7.2, CC7.3	5.7, 5.15, 5.31	Art. 30, Art. 33, Art. 34
Incident Management	Detect, report, and respond to security incidents	CC7.4	5.33, 5.34	Art. 33, Art. 34
Business Continuity	Continuity and disaster recovery planning	CC9.2	5.29, 5.35, 5.36	Art. 32(1)(c)
Vendor Management	Assess and monitor third-party service providers	CC9.2	5.19, 5.22	Art. 28, Art. 29
Data Subject Rights	Ensure data subjects can exercise rights	—	—	Art. 12–23
Data Minimization	Collect only necessary personal data	—	—	Art. 5(1)(c)
Privacy by Design and Default	Integrate data protection into system design	—	5.23 (related)	Art. 25
Training and Awareness	Security awareness and training programs	CC2.2, CC5.2	5.35	Art. 39(1)(b), Recital 74
DPIA	Assess impact of data processing activities	—	—	Art. 35
Legal and Regulatory Compliance	Stay current with applicable laws and regulations	CC1.2, CC4.1	5.6, 5.7	Art. 24, Art. 30
Risk Assessment	Identify and manage security risks	CC3.1–3.4	5.4, 5.5	Art. 32, Recital 76
Policy Enforcement	Regular review and enforcement of policies	CC1.2, CC5.3	5.1, 5.2	Art. 24, Art. 32