Control ID	Control Title	Applicable
5.1	Policies for Information Security	Yes
5.23	Use of Cloud Services	Yes
5.24	Information Security for Use of Supplier Services	Yes
6.1	Screening	Yes
6.4	Disciplinary Process	Yes
7.4	Physical Security Monitoring	Yes
8.7	Protection Against Malware	Yes
8.16	Monitoring Activities	Yes
8.28	Secure Coding	Yes
8.32	Change Management	Yes
8.34	Protection of Log Information	Yes
5.3	ICT Readiness for Business Continuity	Yes
7.8	Physical Entry Controls	No
8.2	Use of Cryptography	No

Justification	References
Core to ISMS framework and governance	ISO 27001
Cloud-based banking services in scope	ISO 27001, EBA
Vendor and third-party risk management	ISO 27001, NIS2
Pre-employment checks required for banking staff	ISO 27001
Formal disciplinary policies to enforce ISMS	ISO 27001
Monitoring of data centers and secure areas	ISO 27001, EBA
Anti-malware controls on endpoints and servers	ISO 27001, NIS2
Log review and SIEM monitoring	ISO 27001, GDPR
Secure development practices for banking applications	ISO 27001
Control changes in critical systems	ISO 27001, EBA
Logs provide audit evidence for compliance	ISO 27001, GDPR
Regulatory requirement for resilience	ISO 27001, EBA
Managed by third-party security vendor	
Handled by separate crypto team	