Your story matters

Third-Party Control Obligations Information and Cybersecurity

Version 10

19 May 2025

Absa Group Chief Security Office

Third-Party Control Obligations | Information and Cybersecurity

At Absa Bank, safeguarding the confidentiality, integrity, and availability of information assets is a fundamental priority. As part of our commitment to maintaining a resilient and secure digital ecosystem, we require third parties to adhere to clearly defined information and cybersecurity control obligations. These requirements are designed to align with industry best practices and regulatory standards, ensuring that our partners uphold the same high standards of security that we do. Through a collaborative approach to cyber risk management, Absa aims to foster trusted relationships while protecting the interests of our customers, stakeholders, and the broader financial system.

Control	Control Requirements
Access Control	The organisation must implement and enforce a structured access control framework to ensure that users and systems have only the minimum necessary access to perform their functions. This includes role-based access controls (RBAC), privileged access management (PAM), periodic access reviews, and security testing to prevent unauthorised access and reduce insider threats.
Data Security	The organisation must implement and maintain robust data security measures to protect sensitive information from unauthorised access, loss, or exposure. This includes enforcing encryption, continuous breach monitoring, access restrictions, regulatory compliance, and secure data-sharing mechanisms to uphold confidentiality, integrity, and availability.
Endpoint Security: Anti-virus	The organisation must implement and maintain robust endpoint security controls to protect devices from malware, unauthorised access, and cyber threats. This includes ensuring comprehensive anti-virus coverage, regular updates, and documented threat response procedures to detect, prevent, and respond to security incidents effectively.
Endpoint Security: Endpoint Detection and Response	The organisation must deploy and maintain an Endpoint Detection and Response (EDR) solution across all endpoints and servers to proactively detect, investigate, and respond to security threats. This includes ensuring comprehensive EDR coverage, continuous monitoring, behavioral analytics, anomaly detection, and regular updates to strengthen endpoint security and threat mitigation.
Information Security Governance	The organisation must establish and maintain a structured Information Security Governance framework to ensure alignment with business objectives, regulatory requirements, and industry best practices. This includes the development, implementation, and communication of a comprehensive Information Security Policy and supporting security standards to provide clear guidance on protecting assets, mitigating risks, and responding to security incidents.

Third-Party Control Obligations | Information and Cybersecurity

Control	Control Requirements
Logging and Monitoring	The organisation must implement and maintain a centralised logging and monitoring framework to detect, investigate, and respond to security threats in real-time. This includes integration with a Security Information and Event Management (SIEM) system, adherence to log retention policies, and continuous monitoring through security dashboards to ensure effective anomaly detection and threat mitigation.
Multi-factor Authentication	The organisation must enforce Multi-Factor Authentication (MFA) as a mandatory security control to protect privileged accounts, remote access, and critical systems from unauthorised access. This includes implementing MFA for all privileged accounts, securing remote work access, and ensuring proper configuration and enforcement of MFA policies.
Network Security	The organisation must implement, maintain, and regularly assess robust network security controls to protect critical assets from unauthorised access, cyber threats, and malicious activities. This includes the deployment of firewalls, intrusion detection and prevention systems (IDS/IPS), network segmentation, Zero Trust principles, and DDoS protection measures to ensure continuous network resilience and threat mitigation.
Personnel Security	The organisation must establish and enforce personnel security controls to mitigate risks associated with human factors in cybersecurity. This includes mandatory security awareness training, confidentiality agreements, strict access management, insider threat monitoring, and secure remote work policies to ensure employees and contractors adhere to security best practices.
Quantum-Safe Encryption	The organisation must implement and transition towards quantum-safe cryptographic algorithms to protect sensitive data from emerging quantum computing threats. This includes assessing cryptographic dependencies, adopting post-quantum encryption standards, and ensuring future-proof security controls to maintain the confidentiality, integrity, and availability of critical information assets.
Technology Asset Management	The organisation must establish and maintain a comprehensive Technology Asset Management framework to ensure the accurate tracking, security, and lifecycle management of all IT assets. This includes maintaining an up-to-date asset inventory, ensuring timely patch and firmware updates, and enforcing secure asset disposal and sanitisation procedures to mitigate security risks.

Third-Party Control Obligations | Information and Cybersecurity

Control	Control Requirements
Third Party Cyber Risk Management	The organisation must establish and enforce a structured Third-Party Cyber Risk Management framework to identify, assess, and mitigate security risks associated with external vendors, subcontractors, and fourth parties. This includes defining a formal vendor risk management policy, conducting periodic risk assessments, and ensuring that third parties comply with security requirements aligned with the organisation's risk posture.
Vulnerability Management	The organisation must establish and maintain a comprehensive Vulnerability Management framework to identify, assess, prioritise, and remediate security vulnerabilities in a timely manner. This includes conducting regular penetration testing, enforcing secure configuration baselines, mitigating zero-day threats, and ensuring critical vulnerabilities are remediated within defined timeframes to reduce the organisation's attack surface.
Information Security Incident Management	The organisation must establish, implement, and maintain an Information Security Incident Management framework to ensure timely detection, response, containment, and recovery from cybersecurity incidents. This includes maintaining an up-to-date incident response plan, conducting regular testing, defining clear communication protocols, and ensuring forensic analysis capabilities for effective incident investigation and mitigation.

Third-Party Control Assessment Approach

Absa adopts a robust risk-based approach to third-party cybersecurity governance, grounded in the nature and extent of connectivity between third-parties and our internal systems or data. Each third-party’s risk profile is evaluated based on the level of access and integration they have with Absa’s digital environment. This assessment informs the scope and frequency of evidence-based control assurance activities, ensuring that security expectations are proportionate to the potential risk posed. By aligning control obligations with actual exposure, Absa promotes targeted oversight, operational resilience, and continuous improvement in our extended cybersecurity ecosystem.