Information Security Controls Checklist for Fintech

Access Control

Control	In Place?	Notes
Unique user authentication for all systems		
Multi-factor authentication (MFA) enforced		
Periodic review of user access rights		
Timely revocation of access upon role change or termination		

Data Security

Control	In Place?	Notes
Encryption of sensitive data at rest and in transit		
Data classification and labeling		
Secure data disposal procedures		
Regular backups and restoration testing		

Network Security

Control	In Place?	Notes
Firewalls configured and maintained		
Intrusion detection/prevention systems (IDS/IPS)		
Regular vulnerability scanning		
Segmentation of critical networks		

Incident Response

Control	In Place?	Notes
Documented incident response plan		
Defined incident reporting procedures		
Regular incident response training and testing		
Forensic readiness procedures		

Vendor & Third-Party Management

Control	In Place?	Notes
Due diligence before onboarding vendors		
Regular risk assessment of third parties		
Security requirements in vendor contracts		
Monitoring of vendor compliance		

This checklist is intended as a starting point for developing and assessing information security controls in the fintech sector. Additional controls may be necessary based on business needs, technology, and regulatory requirements.