




**ANCILLARY SERVICE PROVIDERS
GENERAL REQUIREMENTS
MODULE**

CONSULTATION

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
	GR (General Requirements)
Table of Contents	

		Date Last Changed
GR-A	Introduction	
	GR-A.1 Purpose	04/2016
	GR-A.2 Module History	10/2020
GR-B	Scope of Application	
	GR-B.1 Ancillary Service Provider Licensees	04/2016
GR-C	Provision of Financial Services on a Non-discriminatory Basis	
	GR-C.1 Provision of Financial Services on a Non-discriminatory Basis	10/2020
GR-1	Confidentiality	
	GR-1.1 General Requirements	04/2016
GR-2	Books and Records	
	GR-2.1 General Requirements	04/2016
	GR-2.2 Transaction Records	01/2020
	GR-2.3 Other Records	04/2016
GR-3	Publication of Documents by the Licensee	
	GR-3.1 General Requirements	04/2016
GR-4	General Requirements for TPAs	
	GR-4.1 Compensation	04/2016
	GR-4.2 Code of Conduct	04/2016
	GR-4.3 Segregation of Funds	01/2017
	GR-4.4 Content of Written Agreement	04/2016
	GR-4.5 Prohibition of Collection of Premiums/Contributions	04/2016
GR-5	General Requirements for Credit Reference Bureaus	
	GR-5.1 Code of Conduct	04/2016
GR-5A	General Requirements for Financing-Based Crowdfunding Platform Operators	
	GR-5A.1 General Requirements for Financing-Based Crowdfunding Platform Operators	01/2019
	GR-5A.2 Additional Requirements for Shari'a Compliant Financing-Based Crowdfunding Platform Operators	10/2017
GR-5B	Security Measures for Payment Service Providers Owning or Operating Cash Dispensing Machines (CDMs) or Kiosks	
	GR-5B.1 Physical Security Measures for Payment Service Providers Owning or Operating Cash Dispensing Machines (CDMs) or Kiosks	07/2020
	GR-5B.2 CDM/Kiosk Security Measures: Hardware/ Software	04/2019



MODULE:	GR (General Requirements)
Table of Contents	

		Date Last Changed
GR-5C	General Requirements for Payment Service Providers	
GR-5C.1	Fund Transfers by Customers of Payment Service Providers (PSP)	10/2020
GR-6	Dividends	
GR-6.1	CBB Non-Objection	10/2017
GR-7	Controllers	
GR-7.1	Key Provisions	04/2019
GR-7.2	Definition of Controller	04/2016
GR-7.3	Suitability of Controllers	04/2016
GR-7.4	Approval Process	04/2016
GR-8	Close Links	
GR-8.1	Key Provisions	04/2016
GR-8.2	Definition of Close Links	04/2016
GR-8.3	Assessment Criteria	04/2016
GR-9	Cessation of Business	
GR-9.1	CBB Approval	04/2020
GR -10	Customer Complaints Procedures	
GR-10.1	General Requirements	12/2018
GR-10.2	Documenting Customer Complaints Handling Procedures	12/2018
GR-10.3	Procedures for Effective Handling of Complaints	04/2020
GR-10.4	Internal Complaint Handling Procedures	12/2018
GR-10.5	Response to Complaints	04/2020
GR-10.6	Records of Complaints	12/2018
GR-10.7	Reporting of Complaints	04/2020
GR-10.8	Monitoring and Enforcement	12/2018
GR -11	Outsourcing	
GR-11.1	Outsourcing	12/2018
GR -12	Security Measures for Ancillary Service Providers	
GR-12.1	Cyber security	xx/2021



MODULE	GR: General Requirements
CHAPTER	GR-12: Security Measures for Ancillary Service Providers

GR-12 Security Measures for Ancillary Service Providers

GR-12.1 Cyber Security

GR-12.1.1 This Section applies to licensees that provide services through digital channels.

GR-12.1.2 All licensees must have in place vulnerability and patch management processes, including remediation processes to ensure that the vulnerabilities identified are addressed. Security patches must be applied where relevant within a timeframe that is commensurate with the risks posed by each vulnerability. The licensees must ensure that their systems are subject to Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST).

GR-12.1.3 All licensees must perform penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place at least twice a year. These tests must be conducted each year in June and December simulating real world cyber attacks on the technology environment and must:

- (a) Follow a risk-based approach based on an internationally recognised methodology, such as National Institute of Standards and Technology “NIST” and Open Web Application Security Project “OWASP”;
- (b) Include both Grey Box and Black Box testing in its scope;
- (c) Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services;
- (d) Be performed by external, independent third parties which must be changed at least every two years; and
- (e) Be performed on either the production environment or on non-production exact replicas of the production environment.

GR-12.1.4 Reports on penetration testing referred to in Paragraph GR-12.1.3 must be submitted to CBB before 31st August for the tests as at 30th June and 28th February for the tests as at 31st December. The penetration testing reports must include the vulnerabilities identified and a full list of ‘passed’ tests and ‘failed’ tests together with the steps taken to mitigate the risks identified.