




ANCILLARY SERVICE PROVIDERS GENERAL REQUIREMENTS MODULE

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

	Date Last Changed
GR-A Introduction GR-A.1 Purpose GR-A.2 Module History	04/2016 10/2022
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 GR-2.2 Transaction Records GR-2.3 Other Records	04/2016 01/2020 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 GR-4.2 Code of Conduct GR-4.3 Segregation of Funds GR-4.4 Content of Written Agreement GR-4.5 Prohibition of Collection of Premiums/Contributions	04/2016 04/2016 01/2017 04/2016 04/2016
GR-5 General Requirements for Credit Reference Bureaus GR-5.1 Code of Conduct	04/2016
GR-5A [This Chapter has been deleted in April 2022 and replaced with Module CFP requirements] GR-5A.1 This Section was deleted in April 2022 GR-5A.2 This Section was deleted in April 2022	04/2022 04/2022
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 GR-5B.2 CDM/Kiosk Security Measures: Hardware/ Software	07/2020 04/2019

MODULE:	GR (General Requirements)
Table of Contents	

	Date Last Changed
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	07/2022
GR-12 Information Security	
GR-12.1 Electronic Frauds	01/2021
GR-12.2 Cyber security Risk Management	10/2022
GR-13 Fees and Charges	
GR-13.1 Merchant Fees on Payments to Zakat and Charity Fund	04/2021
GR-14 Marketing of Financial Services	
GR-14.1 Arrangements relating to Regulated Services provided by PSPs	10/2022



MODULE	GR:	General Requirements
CHAPTER	GR-A:	Introduction

GR-A.1 Purpose

Executive Summary


GR-A.1.1 Module GR presents a variety of different requirements that are not extensive enough to warrant their own stand-alone Module, but for the most part are generally applicable. These include general requirements on confidentiality, books and records, publication of documents, the distribution of dividends, controllers; close links and on suspension of business. There are also included specific requirements for TPAs and credit reference bureaus. Each set of requirements is contained in its own Chapter.

Legal Basis

GR-A.1.2

This Module contains the Central Bank of Bahrain ('CBB') Directive (as amended from time to time) regarding general requirements applicable to ancillary service provider licensees, and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 and its amendments ('CBB Law'). Requirements regarding controllers (see Chapter GR-7) are also included in Regulations, to be issued by the CBB.

GR-A.1.3 For an explanation of the CBB's rule-making powers and different regulatory instruments, see section UG-1.1.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-A:	Introduction


GR-A.2 Module History

Evolution of Module

GR-A.2.1 This Module was first issued in April 2016 by the CBB. Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made: Chapter UG-3 provides further details on Rulebook maintenance and version control.

GR-A.2.2 A list of recent changes made to this Module is detailed in the table below:


Module Ref.	Change Date	Description of Changes
GR-9.1.8	10/2016	Added a Rule in the Cessation of Business Section to be consistent with other Volumes of the CBB Rulebook.
GR-4.3.8	01/2017	Amended Paragraph reference.
GR-7.1.6	01/2017	Consistency of notification timeline rule on controllers with other Volumes of the CBB Rulebook.
GR-2.2.1	07/2017	Amended paragraph according to the Legislative Decree No. (28) of 2002.
GR-2.2.2	07/2017	Deleted paragraph.
GR-5A.1	10/2017	Added a chapter on “General Requirements for Financing-Based Crowdfunding Platform Operators”.
GR-5A.2	10/2017	Additional requirements for “Shari’a - Compliant Financing - Based Crowdfunding Platform Operators”.
GR-6.1.3	10/2017	Added additional requirement to submit when requesting no-objection letter for proposed dividends.
GR-5A.1.4	10/2018	Amended Paragraph to further clarify the scope of exemption.
GR-10	11/2018	Added new Section on Customer Complaints Procedure.
GR-11	11/2018	Added new Section on Outsourcing.
GR-5A.1.4	01/2019	Amended Paragraph on maximum credit provided to each borrower under a crowdfunding agreement.
GR-5A.1.5	01/2019	Amended Paragraph.
GR-5A.1.8	01/2019	Amended Paragraph.
GR-5A.1.11A	01/2019	Added a new Paragraph on the minimum time to withdraw a commitment.
GR-5B.1	04/2019	Added a Chapter on “Physical Security measures for Payment Service Providers owning or Operating Cash Dispensing Machines (CDMs) or Kiosks”.
GR-5B.2	04/2019	Additional requirements for “CDM/Kiosk Security Measures: Hardware/Software”.
GR-7.1.1A	04/2019	Added a new Paragraph on exposure to controllers.
GR-7.1.1B	04/2019	Added a new Paragraph on exposure to controllers.
GR-5B.1.13	07/2019	Added a new Paragraph on Europay, MasterCard and Visa (EMV) Compliance.
GR-5B.1.14 & GR-5B.1.15	10/2019	Added new Paragraphs on Contactless Payment Transactions.
GR-2.2.1	01/2020	Amended Paragraph.
GR-9.1.8	04/2020	Amended Paragraph.
GR-10.3.14	04/2020	Amended Paragraph adding reference to CBB consumer protection.
GR-10.5.6	04/2020	Amended Paragraph adding reference to CBB consumer protection.
GR-10.7.1 - GR-10.7.3	04/2020	Amended Paragraphs adding reference to CBB consumer protection.
GR-5B.1.13A	07/2020	Added a new Paragraph on contactless payment.
GR-C	10/2020	Added a new Chapter on Provision of Financial Services on a Non-discriminatory Basis.
GR-12	01/2021	Added a new Chapter on Information Security.
GR-13	04/2021	Added a new Chapter on Fees and Charges.
GR-12.2	07/2021	Added a new Section on Cyber Security.
GR-12.2	01/2022	Enhanced Section on Cyber Security Risk Management.
GR-5A	04/2022	Deleted Chapter and replaced with Module CFP requirements.
GR-12.2.59	04/2022	Amended Paragraph on cyber security incident reporting.
GR-12.2.60	04/2022	Amended Paragraph on submission period of the cyber security incident report.
GR-11	07/2022	Replaced Chapter with new Outsourcing Requirements.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-A:	Introduction

GR-A.2 Module History

GR-A.2.2 **Continued**

Module Ref.	Change Date	Description of Changes
GR-12.2.26	10/2022	Amended Paragraph on email domains requirements.
GR-12.2.26A	10/2022	Added a new Paragraph on additional domains requirements.
GR-14	10/2022	Added a new Chapter on marketing of financial services including requirements for arrangements relating to regulated services provided.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-B:	Scope of Application

GR-B.1 Ancillary Service Provider Licensees

GR-B.1.1

Unless otherwise indicated, the requirements in this Module apply to all ancillary service provider licensees, thereafter referred to in this Module as licensees.



MODULE	GR: General Requirements
CHAPTER	GR-C: Provision of Financial Services on a Non-discriminatory Basis

GR-C.1 Provision of Financial Services on a Non-discriminatory Basis

GR-C.1.1 Ancillary service provider licensees must ensure that all regulated financial services are provided without any discrimination based on gender, nationality, origin, language, faith, religion, physical ability or social standing.



MODULE	GR:	General Requirements
CHAPTER	GR-1:	Confidentiality

GR-1.1 General Requirements


GR-1.1.1

Licensees must ensure that any information in their control or custody is not used or disclosed unless:

- (a) They have the customer's or licensee's written consent;
- (b) Disclosure is made in accordance with the licensee's regulatory obligations; or
- (c) The licensee and members of the credit reference bureau are legally obliged to disclose the information in accordance with Article 117 of the CBB Law.

GR-1.1.2

Ancillary service providers must take appropriate steps to ensure the security of any information handled for its customers or held on behalf of other CBB licensees.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-2:	Books and Records

GR-2.1 General Requirements

GR-2.1.1

In accordance with Article 59 of the CBB Law, all licensees must maintain books and records (whether in electronic or hard copy form) sufficient to produce financial statements and show a complete record of the business undertaken by a licensee. These records must be retained for at least ten years according to Article 60 of the CBB Law.

GR-2.1.2 Paragraph GR-2.1.1 includes accounts, books, files and other records related to client information (e.g. trial balance, general ledger, reconciliations, list of counterparties, etc.). It also includes records that substantiate the value of the assets and liabilities.

GR-2.1.3 Separately, Bahrain Law currently requires other transaction records to be retained for at least five years (see Ministerial Order No. 23 of 2002, Article 5(2), made pursuant to the Amiri Decree Law No. 4 of 2001).

GR-2.1.4

Unless otherwise agreed to by the CBB in writing, records must be kept in either English or Arabic. Any records kept in languages other than English or Arabic must be accompanied by a certified English or Arabic translation. Records must be kept current. The records must be sufficient to allow an audit of the licensee's business or an on-site examination of the licensee by the CBB.

GR-2.1.5 Translations produced in compliance with Rule GR-2.1.4 may be undertaken in-house, by an employee or contractor of the licensee, provided they are certified by an appropriate officer of the licensee.


GR-2.1.6

Records must be accessible at any time from within the Kingdom of Bahrain, or as otherwise agreed with the CBB in writing.

GR-2.1.7 Where older records have been archived, the CBB may accept that records be accessible within a reasonably short time frame (e.g. within 5 business days), instead of immediately. The CBB may also agree similar arrangements where elements of record retention and management have been centralised in another group company, whether inside or outside of Bahrain.

GR-2.1.8

Paragraphs GR-2.1.1 to GR-2.1.7 apply to licensees, with respect to all business activities.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-2: Books and Records

GR-2.2 Transaction Records


GR-2.2.1

Licensees must keep completed transaction records for as long as they are relevant for the purposes for which they were made (with a minimum period in all cases of five years from the date when the transaction was terminated). Records of terminated transactions must be kept whether in hard copy or electronic format as per the Legislative Decree No. (54) of 2018 with respect to Electronic Transactions “The Electronic Communications and Transactions Law” and its amendments.

GR-2.2.2 [This Paragraph has been deleted in July 2017].

GR-2.2.3

Rule GR-2.2.1 applies only to transactions relating to business booked in Bahrain by the licensee.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-2:	Books and Records

GR-2.3 Other Records

Corporate Records


GR-2.3.1

Licensees must maintain the following records in original form or in hard copy at their premises in Bahrain:

- (a) Internal policies, procedures and operating manuals;
- (b) Corporate records, including minutes of shareholders', Directors' and management meetings;
- (c) Correspondence with the CBB and records relevant to monitoring compliance with CBB requirements;
- (d) Reports prepared by the licensee's internal and external auditors; and
- (e) Employee records.

Customer Records

GR-2.3.2 Record-keeping requirements with respect to customer records, including customer identification and due diligence records, are contained in Module FC (Financial Crime).

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR 3:	Publication of Documents by the Licensee

GR-3.1 General Requirements

GR-3.1.1	Any written communication, including stationery, business cards or other business documentation published by the <u>licensee</u> , or used by its employees must include a statement that the <u>licensee</u> is regulated by the Central Bank of Bahrain, the type of license and the legal status.
-----------------	--




MODULE	GR:	General Requirements
CHAPTER	GR-4:	General Requirements for TPAs

GR-4.1 Compensation

GR-4.1.1


A TPA's compensation may be determined:

- (a) As a percentage of the claims processed by the TPA; or
- (b) On another basis as specified in the written agreement.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-4:	General Requirements for TPAs


GR-4.2 Code of Conduct

- GR-4.2.1** TPAs are allowed to enter into agreement with more than one:
- Insurance firm; and/or
 - A self-funded scheme outside of Bahrain.
- GR-4.2.2** TPAs must not charge any kind of fees to the claimants/policyholders.
- GR-4.2.3** TPAs must not market or sell insurance nor own any part of a healthcare facility or company.
- GR-4.2.4** Where a TPA owns any part of a healthcare facility or company at the time this Module is issued, it will be permitted to retain its ownership in the company.
- GR-4.2.5** TPAs must act in the insurance firms and/or self-funded schemes (limited to outside Bahrain) best interests at all times and must fulfill their needs to the best of their ability.
- GR-4.2.6** TPAs must improve the skills of their employees and increase their knowledge through continuing education and training.
- GR-4.2.7** TPAs must disclose to the existing and prospective insurance firm and/or self-funded scheme (limited to outside Bahrain) any and all information that may affect the TPA's ability to provide services and/or advice to the clients.
- GR-4.2.8** TPAs must ensure that all funds collected and/or held by the TPA are used for the express purpose for which the funds are collected and/or held as understood by the insurance firm and/or self-funded scheme (limited to outside Bahrain).
- GR-4.2.9** TPAs must fully disclose to each insurance firm and/or self-funded scheme (limited to outside Bahrain) the terms of engagement and the services to be rendered to that client.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-4:	General Requirements for TPAs

GR-4.3 Segregation of Funds


- GR-4.3.1** All funds remitted to a TPA by an insurance firm and/or self-funded scheme (limited to outside Bahrain) must be held by the TPA in a separate account maintained in the name of the insurance firm and/or self-funded scheme (limited to outside Bahrain) or in a separate account maintained jointly in the names of the insurance firm and/or self-funded scheme (limited to outside Bahrain) and the TPA.
- GR-4.3.2** When funds are collected by a TPA from a healthcare provider on behalf of an insurance firm and/or self-funded scheme (limited to outside Bahrain), such funds must be promptly deposited in a separate account maintained in the name of the insurance firm and/or self-funded scheme (limited to outside Bahrain) or an account maintained jointly in the names of the insurance firm and/or self-funded scheme (limited to outside Bahrain) and the TPA, or remitted to the insurance firm and/or self-funded scheme (limited to outside Bahrain), as provided for in the agreement.
- GR-4.3.3** When an account is held jointly in the names of the insurance firm and/or self-funded scheme (limited to outside Bahrain) and the TPA, the TPA must provide the insurance firm and/or self-funded scheme (limited to outside Bahrain) on a monthly basis a record of all transactions in the joint account.
- GR-4.3.4** Funds must not be commingled with any other funds of the TPA nor other insurance firm and/or self-funded scheme (limited to outside Bahrain) of the TPA. Records of a TPA must clearly show funds received and paid out allocated per insurance firm and/or self-funded scheme (limited to outside Bahrain) and must be made available to the insurance firm and/or self-funded scheme (limited to outside Bahrain) upon request.
- GR-4.3.5** An insurance firm and/or self-funded scheme (limited to outside Bahrain) shall have the responsibility to make available to the TPA funds necessary to enable the TPA to pay claims in a timely manner, as provided in the agreement.
- GR-4.3.6** TPAs must process and settle claims of the policyholder/claimant within 15 calendar days from the receipt of all necessary documents.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-4:	General Requirements for TPAs

GR-4.3 Segregation of Funds (continued)

GR-4.3.7 TPAs must process and settle claims from healthcare service providers within 30 calendar days from the receipt of all necessary documents from the healthcare service providers.

GR-4.3.8 TPAs must comply with Paragraphs GR-4.3.6 and GR-4.3.7 by 30th September 2016 at the latest.


 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-4:	General Requirements for TPAs

GR-4.4 Content of Written Agreement

GR-4.4.1 A TPA must not conduct any business with an insurance firm and/or self-funded scheme (limited to outside Bahrain) in the absence of a written agreement between the TPA and the insurance firm and/or self-funded scheme (limited to outside Bahrain). The agreement must be retained as part of the official records of the TPA for the duration of the agreement.

GR-4.4.2 The agreement referred to in Paragraph GR-4.4.1 must include at a minimum:


- (a) The services to be provided by the TPA on behalf of the insurance firm and/or self-funded scheme (limited to outside Bahrain);
- (b) Financial arrangements;
- (c) Provisions setting forth the respective liability of the insurance firm and/or self-funded scheme (limited to outside Bahrain) and the TPA for the accuracy and eligibility of submitted claims, and for the prompt submission of claims; and
- (d) The responsibilities of the TPA to the insurance firm and/or self-funded scheme (limited to outside Bahrain) with respect to the maintenance of appropriate back-up systems against the loss of records, and the maintenance of appropriate insurance coverage by the TPA against the risk of loss.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-4:	General Requirements for TPAs

GR-4.5 Prohibition of Collection of Premiums/Contributions


GR-4.5.1

TPAs are prohibited from collecting premiums/contributions from policyholders. Premiums/contributions must be paid directly by the policyholders to insurance firms.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-5:	General Requirements for Credit Reference Bureaus

GR-5.1 Code of Conduct

GR-5.1.1	<u>Credit reference bureaus</u> must comply with the provisions of the Bahrain Credit Reference Bureau Code of Practice (Appendix CM-3 under Volumes 1 and 2 of the CBB Rulebook) which dictates the code of conduct to be followed by <u>credit reference bureaus</u> .
-----------------	--

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-5A:	[This Chapter was deleted in April 2022 and replaced with Module CFP]

GR-5A.1 [This Section was deleted in April 2022 and replaced with Module CFP]

GR-5A.1.1 [This Paragraph was deleted in April 2022].

GR-5A.1.2 [This Paragraph was deleted in April 2022].

GR-5A.1.3 [This Paragraph was deleted in April 2022].

GR-5A.1.4 [This Paragraph was deleted in April 2022].

GR-5A.1.5 [This Paragraph was deleted in April 2022].

GR-5A.1.6 [This Paragraph was deleted in April 2022].

GR-5A.1.7 [This Paragraph was deleted in April 2022].

GR-5A.1.8 [This Paragraph was deleted in April 2022].


GR-5A.1.9 [This Paragraph was deleted in April 2022].

GR-5A.1.10 [This Paragraph was deleted in April 2022].

GR-5A.1.11 [This Paragraph was deleted in April 2022].

GR-5A.1.11A [This Paragraph was deleted in April 2022].

GR-5A.1.12 [This Paragraph was deleted in April 2022].

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-5A:	[This Chapter was deleted in April 2022 and replaced with Module CFP]

GR-5A.1 [This Section was deleted in April 2022 and replaced with Module CFP]

GR-5A.1.13 [This Paragraph was deleted in April 2022].

GR-5A.1.14 [This Paragraph was deleted in April 2022].

GR-5A.1.15 [This Paragraph was deleted in April 2022].

GR-5A.1.16 [This Paragraph was deleted in April 2022].

GR-5A.1.17 [This Paragraph was deleted in April 2022].

GR-5A.1.18 [This Paragraph was deleted in April 2022].

GR-5A.1.19 [This Paragraph was deleted in April 2022].

GR-5A.1.20 [This Paragraph was deleted in April 2022].

GR-5A.1.21 [This Paragraph was deleted in April 2022].

GR-5A.1.22 [This Paragraph was deleted in April 2022].

GR-5A.1.23 [This Paragraph was deleted in April 2022].

GR-5A.1.24 [This Paragraph was deleted in April 2022].


GR-5A.1.25 [This Paragraph was deleted in April 2022].

GR-5A.1.26 [This Paragraph was deleted in April 2022].

GR-5A.1.27 [This Paragraph was deleted in April 2022].

GR-5A.1.28 [This Paragraph was deleted in April 2022].

GR-5A.1.29 [This Paragraph was deleted in April 2022].

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-5A:	[This Chapter was deleted in April 2022 and replaced with Module CFP]

GR-5A.2 [This Section was deleted in April 2022 and replaced with Module CFP]

GR-5A.2.1 [This Paragraph was deleted in April 2022].

GR-5A.2.2 [This Paragraph was deleted in April 2022].

GR-5A.2.3 [This Paragraph was deleted in April 2022].

GR-5A.2.4 [This Paragraph was deleted in April 2022].

GR-5A.2.5 [This Paragraph was deleted in April 2022].

GR-5A.2.6 [This Paragraph was deleted in April 2022].

GR-5A.2.7 [This Paragraph was deleted in April 2022].



MODULE	GR: General Requirements
CHAPTER	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

General Requirement

GR-5B.1.1

Where CDMs/Kiosks are installed at an outdoor location, the Payment Service Providers (PSPs) must provide adequate shade covering the area above the customers and the machine.

Record Keeping

GR-5B.1.2


PSPs must record the details of the site risk assessments and retain such records for a period of five years from the date of the CDMs/Kiosks installation, or for any other period required by the Ministry of the Interior or the CBB from time to time, whichever is the longer.

CDM/ Kiosk Alarms

GR-5B.1.3

In addition to alarming the premises, PSPs must alarm the CDM/Kiosk itself, in a way which activates audibly when the CDM/Kiosk is under attack. The system must be monitored by remote signaling to an appropriate local police response designated by the Ministry of Interior. PSPs must consider the following:

- The design of the system must ensure that the CDMs/Kiosks have a panic alarm installed;
- The design of the system must give an immediate, system-controlled warning of an attack on the CDMs/Kiosks, and all CDMs/ Kiosks must be fitted with fully operational fraud detection and inhibiting devices;
- A maintenance record must be kept for the alarm detection system and routine maintenance must be conducted in accordance with at least the manufacturer's recommendations. The minimum must be two planned maintenance visits and tests every 6 months; and
- The alarm system must be monitored by the PSP's head office 24 hours daily. It must automatically generate an alarm signal if the telephone/internet line fails or is cut.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	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 (continued)

Closed-circuit Television (CCTV)


GR-5B.1.4 PSPs must ensure that the Cash Dispensing Machines (CDMs) and Kiosks owned and operated by them are equipped with closed-circuit television (CCTV). The location of camera installation must be carefully chosen to ensure that images of the CDM/Kiosk are recorded, however keypad entry or the screen of the CDM/Kiosk must not be captured by the CCTV recording. The camera must support the detection of the attachment of alien devices to the fascia (external body) and possess the ability to generate an alarm for remote monitoring if the camera is blocked or otherwise disabled.

GR-5B.1.5 As a minimum, the CCTV activity must be recorded (preferably in digital format) and, where risk dictates, remotely monitored by the PSP's head office.

GR-5B.1.6 When a CDM or Kiosk is located in an area where a public CCTV system operates, the PSP must liaise with the authority responsible for the CCTV system to include the CDM/Kiosk site in any preset automatic camera settings and request regular sweeps of the site. The CCTV system must not be able to view the CDM/Kiosk keypad or screen, thereby preventing observation of PIN entry.

GR-5B.1.7 PSPs must ensure that the specifications of CCTV cameras meet the following minimum requirements:

- (a) Analogue Cameras:
 - Resolution – Minimum 700 TVL
 - Lens – Vari-focal lenses from 2.8 to 12mm
 - Sensitivity – Minimum 0.5 Luminance (Lux) without Infrared (IR), 0 Lux with IR
 - IR – At least 10 to 20 meters (Camera that detects motion); and
- (b) IP Cameras:
 - Resolution – 2 MP – 1080 p
 - Lens – Vari-focal lenses from 2.8 to 12mm
 - Sensitivity – Minimum 0.5 Lux without IR, 0 Lux with IR
 - IR – At least 10 to 20 meters.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	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 (continued)

CCTV Network Systems

GR-5B.1.8 Notices of CCTV cameras in operation must be put up for the attention of the public. CCTV records must be maintained for a minimum 45-day period. The transmission rate (in terms of the number of frames per second) must be high enough to make for effective monitoring. The CCTV system must be operational 24 hours per day.

CDMs/Kiosks Lighting

GR-5B.1.9 Banks must ensure that adequate and effective lighting is operational at all times within the CDMs/Kiosks environment. The standard of the proposed lighting must be agreed with the Ministry of the Interior and other relevant authorities and tested at least once every three months to ensure that the lighting is in good working order.

Fire Alarm


GR-5B.1.10 PSPs must ensure that effective fire alarm and fire defense measures, such as a sprinkler, are installed and functioning for all CDMs/Kiosks. These alarms must be linked to the main offices of the PSP.

Cash Replenishment

GR-5B.1.11 All physical cash movements between PSP offices and offsite CDMs/Kiosks must be performed by specialized service providers.

CDMs/Kiosks Service and Maintenance

GR-5B.1.12 PSPs must maintain a list of all details on maintenance, replenishment and inspection visits by staff or other authorized parties.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	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 (continued)


Europay, MasterCard and Visa (EMV) Compliance

GR-5B.1.13 Prepaid cards issued by PSPs in the Kingdom of Bahrain must be EMV compliant. Moreover, all POSs, CDMs and Kiosks must be EMV compliant for accepting cards issued in the Kingdom of Bahrain. In this context, EMV compliant means using chip and online PIN authentication. However, contactless card payment transactions, where no PIN verification is required, are permitted for small amounts i.e. up to BD 20 per transaction, provided that licensees bear full responsibility in case of fraud occurrence.

GR-5B.1.13A Where contactless payments use Consumer Device Cardholder Method (CDCVM) for payment authentication and approval, then the authentication required for transactions above BD20 limit mentioned in Paragraph GR-5B.1.13 is not applicable given that the customer has already been authenticated by his device using PIN, biometric or other authentication methods. This is only applicable where the debit/credit card of the customer has already been tokenized in the payment application.

GR-5B.1.14 Licensees must ensure, with effect from 1st October 2019, that any new POS terminals or devices support contactless payment using Near Field Communication “NFC” technology.

GR-5B.1.15 Licensees must ensure, that any payment card issued or reissued on or after 12th October 2019 supports contactless payment using Near Field Communications “NFC” technology.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-5B: Security Measures for Payment Service Providers Owning or Operating Cash Dispensing Machines (CDMs) or Kiosks

GR-5B.2 CDM/Kiosk Security Measures: Hardware/ Software

GR-5B.2.1

Entry to sensitive areas by the PSP staff or other authorized parties into the CDM/Kiosk environment/surroundings must be controlled, monitored and recorded. The names of the persons accessing the area; the date; and the time of access to and exit from the area must be recorded. CCTV cameras must be installed and used to record all activities within the CDM/Kiosk environment.

GR-5B.2.2

The applicable standards relating to Payment Card Industry (PCI), PIN Transaction Security (PTS), and Point of Interaction (POI) requirements must, in all instances, be fully complied with.

GR-5B-2.3

PSPs must ensure that the integration of Secure Card Readers, (SCRs) and, if applicable, any mechanism protecting the SCRs are properly implemented and fully comply with the guidelines provided by the device vendor. SCRs must be approved by and fully comply with all Payment Card Industry standards at all times.

GR-5B-2.4

PSPs must ensure that all CDMs/Kiosks are equipped with mechanisms which prevent skimming attacks. There must be no known or demonstrable way to disable or defeat the above-mentioned mechanisms, or to install an external or internal skimming device.



MODULE	GR:	General Requirements
CHAPTER	GR-6:	Dividends

GR-6.1 CBB Non-Objection

GR-6.1.1

Licensees must obtain a letter of no-objection from the CBB to any dividend proposed, before announcing the proposed dividend by way of press announcement or any other means of communication and prior to submitting a proposal for a distribution of profits to a shareholder vote.


GR-6.1.2

The CBB will grant a no-objection letter where it is satisfied that the level of dividend proposed is unlikely to leave the licensee vulnerable – for the foreseeable future – to breaching the CBB’s capital requirements, taking into account (as appropriate) the licensee’s liquidity.

GR-6.1.3

To facilitate the prior approval required under Paragraph GR-6.1.1, licensees must provide the CBB with:

- (a) The licensee’s intended percentage and amount of proposed dividends for the year;
- (b) A letter of no objection from the licensee’s external auditor on such profit distribution; and
- (c) A detailed analysis of the impact of the proposed dividend on the capital requirements outlined in Section AU-2.5 and liquidity position of the licensee.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-7:	Controllers

GR-7.1 Key Provisions

GR-7.1.1 Licensees must obtain prior written approval from the CBB for any changes to their controllers (as defined in Section GR-7.2).

GR-7.1.1A Licensees must not incur or otherwise have an exposure (either directly or indirectly) to their controllers, including subsidiaries and associated companies of such controllers.

GR-7.1.1B For the purpose of Paragraph GR-7.1.1A, licensees that already have an exposure to controllers must have an action plan agreed with the CBB's supervisory point of contact to address such exposures within a timeline agreed with the CBB.

GR-7.1.2 Condition 3 of the CBB's licensing conditions specifies, among other things, that licensees must satisfy the CBB that their controllers are suitable and pose no undue risks to the licensee (See Paragraph AU-2.3.1). There are also certain procedures which are set out in Articles 52 to 56 of the CBB Law on controllers.


GR-7.1.3 Applicants for a license must provide details of their controllers, by submitting a duly completed Form 2 (Application for Authorisation of Controller). (See sub-Paragraph AU-4.1.4(a)).

GR-7.1.4 Where a controller is a legal person, the controller must notify the CBB of any change in its shareholding at the earlier of:

- (a) When the change takes effect; and
- (b) When the controller becomes aware of the proposed change.

GR-7.1.5 For approval under Paragraph GR-7.1.1 to be granted, the CBB must be satisfied that the proposed controller or increase in control poses no undue risks to the licensee or the financial system. The CBB may impose any restrictions that it considers necessary to be observed where approval is given for a new or a change in controller. A duly completed Form 2 (Controllers) must be submitted as part of the request for a change in controllers. An approval of controller will specify the applicable period for effecting the proposed acquisition of shares.

GR-7.1.6 If, as a result of circumstances outside the licensee's knowledge and/or control, a change in controller is triggered prior to CBB approval being sought or obtained, the licensee must notify the CBB no later than 15 calendar days on which those changes have occurred.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-7:	Controllers


GR-7.1 Key Provisions (continued)

GR-7.1.7 The approval provisions outlined above do not apply to existing holdings or existing voting control by controllers already approved by the CBB. The approval provisions apply to new/prospective controllers or to increases in existing holdings/voting control.

GR-7.1.8 Licensees are required to notify the CBB as soon as they become aware of events that are likely to lead to changes in their controllers.

GR-7.1.9 The criteria by which the CBB assesses the suitability of controllers are set out in Section GR-7.3. The CBB aims to respond to requests for approval within 30 calendar days and is obliged to reply within 3 months to a request for approval. The CBB may contact references and supervisory bodies in connection with any information provided to support an application for controller. The CBB may also ask for further information, in addition to that provided in Form 2, if required to satisfy itself as to the suitability of the applicant.

GR-7.1.10 Licensees must submit, within 3 months of their financial year-end, a report on their controllers (See Subparagraph BR-1.1.3(d)). This report must identify all controllers of the licensee, as defined in Section GR-7.2, the extent of their shareholding interests and any change in their legal status or any adverse information on the controllers.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-7: Controllers

GR-7.2 Definition of Controller

GR-7.2.1

A controller of a licensee is a natural or legal person who either alone, or with his associates:

- (a) Holds 10% or more of the shares in the licensee ("L"), or is able to exercise (or control the exercise of) 10% or more of the voting power in L;
- (b) Holds 10% or more of the shares in a parent undertaking ("P") of L, or is able to exercise (or control the exercise of) 10% or more of the voting power in P; or
- (c) Is able to exercise significant influence over the management of L or P.


GR-7.2.2

For the purposes of Paragraph GR-7.2.1, "associate" includes:

- (a) The spouse, son(s) or daughter(s) of a controller;
- (b) An undertaking of which a controller is a director;
- (c) A person who is an employee or partner of the controller; and
- (d) If the controller is a corporate entity, a director of the controller, a subsidiary of the controller, or a director of any subsidiary undertaking of the controller.

GR-7.2.3


Associate also includes any other person or undertaking with which the controller has entered into an agreement or arrangement as to the acquisition, holding or disposal of shares or other interests in the licensee, or under which they undertake to act together in exercising their voting power in relation to the licensee.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-7:	Controllers

GR-7.3 Suitability of Controllers


GR-7.3.1 All new controllers or prospective controllers (as defined in Section GR-7.2) of a licensee must obtain the prior written approval of the CBB. Any increases to existing controllers' holdings or voting control must also have prior written approval from the CBB and are subject to the conditions outlined in this Section. Such changes in existing controllers (as defined in the Section GR-7.2) or new/prospective controllers of a licensee must satisfy the CBB of their suitability and appropriateness. The CBB will issue an approval notice or notice of refusal of a controller according to the approval process outlined in Section GR-7.4.

GR-7.3.2 All controllers or prospective controllers (whether natural or legal persons) of all licensees are subject to the approval of the CBB. Persons who intend to take ownership stakes of 10% or above of the voting capital of a licensee are subject to enhanced scrutiny, given the CBB's position as home supervisor of such licensees. The level of scrutiny and the criteria for approval become more onerous as the level of proposed ownership increases.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-7:	Controllers


GR-7.3 Suitability of Controllers (continued)

- GR-7.3.3 In assessing the suitability and the appropriateness of new/prospective controllers (and existing controllers proposing to increase their shareholdings) who are natural persons, the CBB has regard to their professional and personal conduct, including, but not limited to, the following:
- The propriety of a person's conduct, whether or not such conduct resulted in conviction for a criminal offence, the contravention of a law or regulation, or the institution of legal or disciplinary proceedings;
 - A conviction or finding of guilt in respect of any offence, other than a minor traffic offence, by any court or competent jurisdiction;
 - Any adverse finding in a civil action by any court or competent jurisdiction, relating to fraud, misfeasance or other misconduct in connection with the formation or management of a corporation or partnership;
 - Whether the person has been the subject of any disciplinary proceeding by any government authority, regulatory agency or professional body or association;
 - The contravention of any financial services legislation or regulation;
 - Whether the person has ever been refused a license, authorisation, registration or other authority;
 - Dismissal or a request to resign from any office or employment;
 - Disqualification by a court, regulator or other competent body, as a Director or as a manager of a corporation;
 - Whether the person has been a Director, partner or manager of a corporation or partnership which has gone into liquidation or administration or where one or more partners or managers have been declared bankrupt whilst the person was connected with that partnership or corporation;
 - The extent to which the person has been truthful and open with regulators;
 - Whether the person has ever been adjudged bankrupt, entered into any arrangement with creditors in relation to the inability to pay due debts, or failed to satisfy a judgement debt under a court order or has defaulted on any debts;
 - The person's track record as a controller of, or investor in financial institutions;
 - The financial resources of the person and the likely stability of their shareholding;
 - Existing Directorships or ownership of more than 20% of the capital or voting rights of any financial institution in the Kingdom of Bahrain or elsewhere, and the potential for conflicts of interest that such Directorships or ownership may imply;
 - The legitimate interests of creditors and minority shareholders of the licensee;
 - If the approval of a person as a controller is or could be detrimental to the subject licensee, Bahrain's banking and financial sector or the national interests of the Kingdom of Bahrain; and
 - Whether the person is able to deal with existing shareholders and the board in a constructive and co-operative manner.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)	
MODULE	GR: General Requirements		
CHAPTER	GR-7: Controllers		


GR-7.3 Suitability of Controllers (continued)

- GR-7.3.4 In assessing the suitability and appropriateness of legal persons as controllers (wishing to increase their shareholding) or new/potential controllers, the CBB has regard to their financial standing, judicial and regulatory record, and standards of business practice and reputation, including, but not limited to, the following:
- (a) The financial strength of the person, its parent(s) and other members of its group, its implications for the licensee and the likely stability of the person's shareholding;
 - (b) Whether the person or members of its group have ever entered into any arrangement with creditors in relation to the inability to pay due debts;
 - (c) The person's jurisdiction of incorporation, location of head office, group structure and connected counterparties and the implications for the licensee as regards effective supervision of the licensee and potential conflicts of interest;
 - (d) The person's (and other group members') propriety and general standards of business conduct, including the contravention of any laws or regulations including financial services legislation on regulations, or the institution of disciplinary proceedings by a government authority, regulatory agency or professional body;
 - (e) Any adverse finding in a civil action by any court or competent jurisdiction, relating to fraud, misfeasance or other misconduct;
 - (f) Any criminal actions instigated against the person or other members of its group, whether or not this resulted in an adverse finding;
 - (g) The extent to which the person or other members of its group have been truthful and open with regulators and supervisors;
 - (h) Whether the person has ever been refused a licence, authorisation, registration or other authority;
 - (i) The person's track record as a controller of, or investor in financial institutions;
 - (j) The legitimate interests of creditors and shareholders of the licensee;
 - (k) Whether the approval of a controller is or could be detrimental to the subject licensee, Bahrain's financial sector or the national interests of the Kingdom of Bahrain;
 - (l) Whether the person is able to deal with existing shareholders and the board in a constructive manner; and
 - (m) Existing Directorships or ownership of more than 20% of the capital or voting rights of any financial institution in the Kingdom of Bahrain or elsewhere, and the potential for conflicts of interest that such Directorships or ownership may imply.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-7: Controllers

GR-7.4 Approval Process

- GR-7.4.1 Within 3 months of receipt of an approval request under Paragraph GR-7.1.1, the CBB will issue an approval notice (with or without restrictions) or a written notice of refusal if it is not satisfied that the person concerned is suitable to increase his shareholding in, or become a controller of the licensee. The notice of refusal or notice of approval with conditions will specify the reasons for the objection or restriction and specify the applicant's right of appeal in either case. Where an approval notice is given, it will specify the period for which it is valid and any conditions that attach. These conditions will include the maximum permitted limit of holding or voting control exercisable by the controller.
- GR-7.4.2 Notices of refusal have to be approved by an Executive Director of the CBB. The applicant has 30 calendar days from the date of the notice in which to make written representation as to why his application should not be refused. The CBB then has 30 calendar days from the date of receipt of those representations to reconsider the evidence submitted and make a final determination, pursuant to Article 53 of the Central Bank of Bahrain and Financial Institutions Law (Decree No. 64 of 2006) ("CBB Law") and Module EN (Enforcement).
- GR-7.4.3 Pursuant to Article 56 of the CBB Law, where a person has become a controller by virtue of his shareholding in contravention of Paragraph GR-7.1.1, or a notice of refusal has been served to him under Paragraph GR-7.4.1 and the period of appeal has expired, the CBB may, by notice in writing served on the person concerned, direct that his shareholding shall be transferred or until further notice, no voting right shall be exercisable in respect of those shares.
- GR-7.4.4 Article 56 of the CBB Law empowers the CBB to take appropriate precautionary measures, or sell such shares mentioned in Paragraph GR-7.4.3, if the licensee fails to carry out the order referred to in the preceding Paragraph.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-8:	Close Links

GR-8.1 Key Provisions

GR-8.1.1 Condition 3 of the CBB's licensing conditions specifies, amongst other things, that licensees must satisfy the CBB that their close links do not prevent the effective supervision of the licensee and otherwise pose no undue risks to the licensee. (See Paragraph AU-2.3.1).

GR-8.1.2 Applicants for a license must provide details of their close links, as provided for under Form 1 (Application for a License). (See Paragraph AU-4.1.1).

GR-8.1.3 Licensees must submit to the CBB, within 3 months of their financial year-end, a report on their close links (See Subparagraph BR-1.1.3(b)). The report must identify all undertakings closely linked to the licensee, as defined in Section GR-8.2.

GR-8.1.4 Licensees may satisfy the requirement in Paragraph GR-8.1.3 by submitting a corporate structure chart, identifying all undertakings closely linked to the licensee.

GR-8.1.5 Licensees must provide information on undertakings with which they are closely linked, as requested by the CBB.




MODULE	GR:	General Requirements
CHAPTER	GR-8:	Close Links

GR-8.2 Definition of Close Links

GR-8.2.1


A licensee ('L') has close links with another undertaking ('U'), if:

- (a) U is a parent undertaking of L;
- (b) U is a subsidiary undertaking of L;
- (c) U is a subsidiary undertaking of a parent undertaking of L;
- (d) U, or any other subsidiary undertaking of its parent, owns or controls 20% or more of the voting rights or capital of L; or
- (e) L, any of its parent or subsidiary undertakings, or any of the subsidiary undertakings of its parent, owns or controls 20% or more of the voting rights or capital of U.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-8:	Close Links

GR-8.3 Assessment Criteria

- GR-8.3.1 In assessing whether a licensee's close links may prevent the effective supervision of the licensee, or otherwise poses no undue risks to the licensee, the CBB takes into account the following:
- (a) Whether the CBB will receive adequate information from the licensee, and those with whom the licensee has close links, to enable it to determine whether the licensee is complying with CBB requirements;
 - (b) The structure and geographical spread of the licensee, its group and other undertakings with which it has close links, and whether this might hinder the provision of adequate and reliable flows of information to the CBB, for instance because of operations in territories which restrict the free flow of information for supervisory purposes; and
 - (c) Whether it is possible to assess with confidence the overall financial position of the group at any particular time, and whether there are factors that might hinder this, such as group members having different financial year ends or auditors, or the corporate structure being unnecessarily complex and opaque.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-9:	Cessation of Business

GR-9.1 CBB Approval

GR-9.1.1 As specified in Article 50 of the CBB Law, a licensee wishing to cease to provide or suspend any or all of the licensed regulated services of its operations and/or liquidate its business must obtain the CBB's prior approval.

GR-9.1.2 Licensees must notify the CBB in writing at least six months in advance of their intended suspension of any or all the licensed regulated services or cessation of business, setting out how they propose to do so and, in particular, how they will treat any of their liabilities.


GR-9.1.3 If the licensee wishes to liquidate its business, the CBB will revise its license to restrict the firm from entering into new business. The licensee must continue to comply with all applicable CBB requirements until such time as it is formally notified by the CBB that its obligations have been discharged and that it may surrender its license.

GR-9.1.4 A licensee in liquidation must continue to meet its contractual and regulatory obligations to its clients and creditors.

GR-9.1.5 Once the licensee believes that it has discharged all its remaining contractual obligations to clients and creditors, it must publish a notice in two national newspapers in Bahrain approved by the CBB (one being in English and one in Arabic), stating that it has settled all its dues and wishes to leave the market. According to Article 50 of the CBB Law, such notice shall be given after receiving the approval of the CBB, not less than 30 days before the actual cessation is to take effect.

GR-9.1.6 The notice referred to in Paragraph GR-9.1.5 must include a statement that written representations concerning the liquidation may be sent to the CBB before a specified day, which shall not be later than thirty days after the day of the first publication of the notice. The CBB will not decide on the application until after considering any representations made to the CBB before the specified day.


GR-9.1.7 If no objections to the liquidation are upheld by the CBB, then the CBB may issue a written notice of approval for the surrender of the license.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-9:	Cessation of Business

GR-9.1 CBB Approval (continued)

GR-9.1.8

Upon satisfactorily meeting the requirements set out in GR-9.1, the licensees must surrender the original license certificate issued by the Licensing Directorate at the time of establishment, and submit confirmation of the cancellation of its commercial registration from the Ministry of Industry, Commerce and Tourism.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-10: Customer Complaints Procedures

GR-10.1 General Requirements

GR-10.1.1

All licensees must have appropriate customer complaints handling procedures and systems for effective handling of complaints, whether received directly by the licensee or through other parties connected to the licensee.

GR-10.1.2


Customer complaints procedures must be documented appropriately and their customers must be informed of their availability.

GR-10.1.3

All licensees must appoint a customer complaints officer and publicise his/ her contact details at all departments and branches and on the licensee's website. The customer complaints officer must be of a senior level at the licensee and must be independent of the parties to the complaint to minimise any potential conflict of interest.

GR-10.1.4

The position of customer complaints officer may be combined with that of compliance officer.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-10: Customer Complaints Procedures

GR-10.2 Documenting Customer Complaints Handling Procedures

GR-10.2.1

In order to make customer complaints handling procedures as transparent and accessible as possible, all licensees must document their customer complaints handling procedures. These include setting out in writing:


- (a) The procedures and policies for:
 - (i) Receiving and acknowledging complaints;
 - (ii) Investigating complaints;
 - (iii) Responding to complaints within appropriate time limits;
 - (iv) Recording information about complaints;
 - (v) Identifying recurring system failure issues;
- (b) The types of remedies available for resolving complaints; and
- (c) The organisational reporting structure for the complaints handling function.

GR-10.2.2

Licensees must provide a copy of the procedures to all relevant staff, so that they may be able to inform customers. A simple and easy-to-use guide to the procedures must also be made available to all customers, on request, and when they want to make a complaint.

GR-10.2.3

Licensees are required to ensure that all financial services related documentation provided to the customer includes a statement informing the customer of the availability of a simple and easy-to-use guide on customer complaints procedures in the event the customer is not satisfied with the services provided.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-10: Customer Complaints Procedures

GR-10.3 Principles for Effective Handling of Complaints

GR-10.3.1 Adherence to the following principles is required for effective handling of complaints:

Visibility

GR-10.3.2 “How and where to complain” must be well publicised to customers and other interested parties, in both English and Arabic languages.

Accessibility

GR-10.3.3 A complaints handling process must be easily accessible to all customers and must be free of charge.

GR-10.3.4 While a licensee’s website is considered an acceptable mean for dealing with customer complaints, it should not be the only means available to customers as not all customers have access to the internet.

GR-10.3.5 Process information must be readily accessible and must include flexibility in the method of making complaints.


GR-10.3.6 Support for customers in interpreting the complaints procedures must be provided, upon request.

GR-10.3.7 Information and assistance must be available on details of making and resolving a complaint.

GR-10.3.8 Supporting information must be easy to understand and use.

Responsiveness

GR-10.3.9 Receipt of complaints must be acknowledged in accordance with Section GR-10.5 “Response to Complaints”.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-10:	Customer Complaints Procedures

GR-10.3 Principles for Effective Handling of Complaints (continued)

GR-10.3.10 Complaints must be addressed promptly in accordance with their urgency.

GR-10.3.11 Customers must be treated with courtesy.

GR-10.3.12 Customers must be kept informed of the progress of their complaint, in accordance with Section BC-10.5.

GR-10.3.13 If a customer is not satisfied with a licensee's response, the licensee must advise the customer on how to take the complaint further within the organisation.


GR-10.3.14 In the event that they are unable to resolve a complaint, licensees must outline the options that are open to that customer to pursue the matter further, including, where appropriate, referring the matter to the Consumer Protection Unit at the CBB.

Objectivity and Efficiency

GR-10.3.15 Complaints must be addressed in an equitable, objective, unbiased and efficient manner.


GR-10.3.16 General principles for objectivity in the complaints handling process include:

- (a) Openness:
The process must be clear and well publicised so that both staff and customers can understand;
- (b) Impartiality:
 - (i) Measures must be taken to protect the person the complaint is made against from bias;
 - (ii) Emphasis must be placed on resolution of the complaint not blame; and
 - (iii) The investigation must be carried out by a person independent of the person complained about;

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-10: Customer Complaints Procedures


GR-10.3 Principles for Effective Handling of Complaints (Continued)

- (c) **Accessibility:**
 - (i) The licensee must allow customer access to the process at any reasonable point in time; and
 - (ii) A joint response must be made when the complaint affects different participants;
- (d) **Completeness:**
The complaints officer must find relevant facts, talk to both sides, establish common ground and verify explanations wherever possible;
- (e) **Equitability:**
Give equal treatment to all parties;
- (f) **Sensitivity:**
Each complaint must be treated on its merits and paying due care to individual circumstances;
- (g) **Objectivity for personnel – complaints handling procedures must ensure those complained about are treated fairly which implies:**
 - (i) Informing them immediately and completely on complaints about performance;
 - (ii) Giving them an opportunity to explain and providing appropriate support;
 - (iii) Keeping them informed of the progress and result of the complaint investigation;
 - (iv) Full details of the complaint are given to those the complaint is made against prior to interview; and
 - (v) Personnel must be assured they are supported by the process and should be encouraged to learn from the experience and develop a better understanding of the complaints process;
- (h) **Confidentiality:**
 - (i) In addition to customer confidentiality, the process must ensure confidentiality for staff who have a complaint made against them and the details must only be known to those directly concerned;
 - (ii) Customer information must be protected and not disclosed, unless the customer consents otherwise; and
 - (iii) Protect the customer and customer's identity as far as is reasonable to avoid deterring complaints due to fear of inconvenience or discrimination;

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-10:	Customer Complaints Procedures

GR-10.3 Principles for Effective Handling of Complaints (continued)

- (i) Objectivity monitoring:
Licensees must monitor responses to customers to ensure objectivity which could include random monitoring of resolved complaints;
- (j) Charges:
The process must be free of charge to customers;
- (k) Customer Focused Approach:
 - (i) Licensees must have a customer focused approach;
 - (ii) Licensees must be open to feedback; and
 - (iii) Licensees must show commitment to resolving problems;
- (l) Accountability:
Licensees must ensure accountability for reporting actions and decisions with respect to complaints handling;
- (m) Continual improvement:
Continual improvement of the complaints handling process and the quality of products and services must be a permanent objective of the licensee.

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR: General Requirements
CHAPTER	GR-10: Customer Complaints Procedures

GR-10.4 Internal Complaint Handling Procedures

GR-10.4.1


A licensee's internal complaint handling procedures must provide for:

- (a) The receipt of written complaints;
- (b) The appropriate investigation of complaints;
- (c) An appropriate decision-making process in relation to the response to a customer complaint;
- (d) Notification of the decision to the customer;
- (e) The recording of complaints; and
- (f) How to deal with complaints when a business continuity plan (BCP) is operative.

GR-10.4.2

A licensee's internal complaint handling procedures must be designed to ensure that:

- (a) All complaints are handled fairly, effectively and promptly;
- (b) Recurring systems failures are identified, investigated and remedied;
- (c) The number of unresolved complaints referred to the CBB is minimised;
- (d) The employee responsible for the resolution of complaints has the necessary authority to resolve complaints or has ready access to an employee who has the necessary authority; and
- (e) Relevant employees are aware of the licensee's internal complaint handling procedures and comply with them and receive training periodically to be kept abreast of changes in procedures.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-10:	Customer Complaints Procedures

GR-10.5 Response to Complaints

GR-10.5.1 A licensee must acknowledge in writing customer written complaints within 5 working days of receipt.

GR-10.5.2 A licensee must respond in writing to a customer complaint within 4 weeks of receiving the complaint, explaining their position and how they propose to deal with the complaint.


Redress

GR-10.5.3 A licensee should decide and communicate how it proposes (if at all) to provide the customer with redress. Where appropriate, the licensee must explain the options open to the customer and the procedures necessary to obtain the redress.

GR-10.5.4 Where a licensee decides that redress in the form of compensation is appropriate, the licensee must provide the complainant with fair compensation and must comply with any offer of compensation made by it which the complainant accepts.

GR-10.5.5 Where a licensee decides that redress in a form other than compensation is appropriate, it must provide the redress as soon as practicable.

GR-10.5.6 Should the customer that filed a complaint not be satisfied with the response received as per Paragraph GR-10.5.2, he can forward the complaint to the Consumer Protection Unit at the CBB within 30 calendar days from the date of receiving the letter.


 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-10:	Customer Complaints Procedures

GR-10.6 Records of Complaints

GR-10.6.1

A licensee must maintain a record of all customers' complaints. The record of each complaint must include:

- (a) The identity of the complainant;
- (b) The substance of the complaint;
- (c) The status of the complaint, including whether resolved or not, and whether redress was provided; and
- (d) All correspondence in relation to the complaint. Such records must be retained by the licensees for a period of 5 years from the date of receipt of the complaint.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-10:	Customer Complaints Procedures

GR-10.7 Reporting of Complaints

GR-10.7.1

A licensee must submit to the CBB's Consumer Protection Unit, 20 days after the end of the quarter, a quarterly report summarising the following:


- (a) The number of complaints received;
- (b) The substance of the complaints;
- (c) The number of days it took the licensee to acknowledge and to respond to the complaints; and
- (d) The status of the complaint, including whether resolved or not, and whether redress was provided.

GR-10.7.2

The report referred to in Paragraph GR-10.7.1 must be sent electronically to complaint@cbb.gov.bh.


GR-10.7.3

Where no complaints have been received by the licensee within the quarter, a 'nil' report should be submitted to the CBB's Consumer Protection Unit.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-10:	Customer Complaints Procedures

GR-10.8 Monitoring and Enforcement

GR-10.8.1 Compliance with these requirements is subject to the ongoing supervision of the CBB as well as being part of any CBB inspection of a licensee. Failure to comply with these requirements is subject to enforcement measures as outlined in Module EN (Enforcement).

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-11:	Outsourcing Requirements

GR-11.1 Outsourcing Arrangements

GR-11.1.1 This Chapter sets out the CBB's approach to outsourcing by licensees. It also sets out various requirements that licensees must address when considering outsourcing an activity or function.

GR-11.1.2 In the context of this Chapter, 'outsourcing' means an arrangement whereby a third party performs on behalf of a licensee an activity which commonly would have been performed internally by the licensee. Examples of services that are typically outsourced include data processing, cloud services, customer call centres and back-office related activities.

GR-11.1.3 In the case of branches of foreign entities, the CBB may consider a third-party outsourcing arrangement entered into by the licensee's head office/regional office or other offices of the foreign entity as an intragroup outsourcing, provided that the head office/regional office submits to the CBB a letter of comfort which includes, but is not limited to, the following conditions:


- The head office/regional office declares its ultimate responsibility of ensuring that adequate control measures are in place; and
- The head office/regional office is responsible to take adequate rectification measures, including compensation to the affected customers, in cases where customers suffer any loss due to inadequate controls applied by the third-party service provider.

GR-11.1.4 The licensee must not outsource the following functions:

- Compliance;
- AML/CFT;
- Financial control;
- Risk management; and
- Business line functions offering regulated services directly to the customers (refer to Regulation No. (1) of 2007 and its amendments for the list of CBB regulated services).

GR-11.1.5 For the purposes of Paragraph GR-11.1.4, certain support activities, processes and systems under these functions may be outsourced (e.g. call centres, data processing, credit recoveries, cyber security, e-KYC solutions) subject to compliance with Paragraph GR-11.1.7. However, strategic decision-making and managing and bearing the principal risks related to these functions must remain with the licensee.

GR-11.1.6 Branches of foreign entities may be allowed to outsource to their head office, the risk management function stipulated in Subparagraph GR-11.1.4 (iv), subject to CBB's prior approval.

 Central Bank of Bahrain Rulebook		Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE	GR:	General Requirements
CHAPTER	GR-11:	Outsourcing Requirements

GR-11.1 Outsourcing Arrangements (continued)

GR-11.1.7

Licensees must comply with the following requirements:

- (i) Prior CBB approval is required on any outsourcing to a third-party outside Bahrain (excluding cloud data services). The request application must:
 - a. include information on the legal and technical due diligence, risk assessment and detailed compliance assessment; and
 - b. be made at least 30 calendar days before the licensee intends to commit to the arrangement.
- (ii) Post notification to the CBB, within 5 working days from the date of signing the outsourcing agreement, is required on any outsourcing to an intragroup entity within or outside Bahrain or to a third-party within Bahrain, provided that the outsourced service does not require a license, or to a third-party cloud data services provider inside or outside Bahrain.
- (iii) Licensees must have in place sufficient written requirements in their internal policies and procedures addressing all strategic, operational, logistical, business continuity and contingency planning, legal and risks issues in relation to outsourcing.
- (iv) Licensees must sign a service level agreement (SLA) or equivalent with every outsourcing service provider. The SLA must clearly address the scope, rights, confidentiality and encryption requirements, reporting and allocation of responsibilities. The SLA must also stipulate that the CBB, external auditors, internal audit function, compliance function and where relevant the Shari'a coordination and implementation and internal Shari'a audit functions of the licensee have unrestricted access to all relevant information and documents maintained by the outsourcing service provider in relation to the outsourced activity.
- (v) Licensees must designate an approved person to act as coordinator for monitoring and assessing the outsourced arrangement.
- (vi) Licensee must submit to the CBB any report by any other regulatory authority on the quality of controls of an outsourcing service provider immediately after its receipt or after coming to know about it.
- (vii) Licensee must inform its normal supervisory point of contact at the CBB of any material problems encountered with the outsourcing service provider if they remain unresolved for a period of three months from its identification date.



MODULE	GR: General Requirements
CHAPTER	GR-11: Outsourcing Requirements

GR-11.1 Outsourcing Arrangements (continued)

GR-11.1.8 For the purpose of Subparagraph GR-11.1.7 (iv), licensees as part of their assessments may use the following:

- a) Independent third-party certifications on the outsourcing service provider's security and other controls;
- b) Third-party or internal audit reports of the outsourcing service provider; and
- c) Pooled audits organized by the outsourcing service provider, jointly with its other clients.

When conducting on-site examinations, licensees should ensure that the data of the outsourcing service provider's other clients is not negatively impacted, including impact on service levels, availability of data and confidentiality.

GR-11.1.9 For the purpose of Subparagraph GR-11.1.7 (i), the CBB will provide a definitive response to any prior approval request for outsourcing within 10 working days of receiving the request complete with all the required information and documents.



MODULE	GR:	General Requirements
CHAPTER	GR-12:	Information Security

GR-12.1 Electronic Frauds

GR-12.1.1

PSPs must implement enhanced fraud monitoring of movements in customers' accounts to guard against electronic frauds using various tools and measures, such as limits in value, volume and velocity.

GR-12.1.2

PSPs must have in place customer awareness communications, pre and post onboarding process, using video calls, short videos or pop-up messages, to alert and warn natural persons using online channels or applications about the risk of electronic frauds, and emphasise the need to secure their personal credentials and not share them with anyone, online or offline.



MODULE	GR:	General Requirements
CHAPTER	GR-12:	Information Security

GR-12.2 Cyber Security Risk Management

GR-12.2.1

This Section applies to ancillary service provider licensees that provide services through digital channels.

GR-12.2.2

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.

GR-12.2.3

PSPs, AISP, and PISP 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 and all other licensees offering services through digital means must perform such tests at least once a year. The tests must be conducted simulating real world cyber-attacks on the technology environment and must:

- 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”;
- Include both Grey Box and Black Box testing in its scope;
- Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services;
- Be performed by external, independent third parties which must be changed at least every two years; and
- Be performed on either the production environment or on non-production exact replicas of the production environment.

GR-12.2.4

The tests referred to in Paragraph GR-12.2.3 must be conducted each year in June and December by licensees required to perform the tests twice a year and in June for licensees required to perform the tests at least once a year. Reports on penetration testing must be submitted to CBB before 30th September for the tests as at 30th June and 31st March 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.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

Role of the Board and Senior Management

GR-12.2.5

The Board of licensees must ensure that the licensee has a robust cyber security risk management framework to comprehensively manage the licensee's cyber security risk and vulnerabilities. The Board must establish clear ownership, decision-making and management accountability for risks associated with cyber-attacks and related risk management and recovery processes.

GR-12.2.6

Licensees must ensure that the cyber security risk management framework encompasses, at a minimum, the following components:

- Cyber security strategy;
- Cyber security policy; and
- Cyber security risk management approach, tools and methodology and, an organization-wide security awareness program.

GR-12.2.7

The cyber security risk management framework must be developed in accordance with the National Institute of Standards and Technology (NIST) Cyber security framework which is summarized in Appendix A – Cyber security Control Guidelines. At the broader level, the Cyber security framework should be consistent with the licensee's risk management framework.

GR-12.2.8

Senior management, and where appropriate, the boards, should receive comprehensive reports; covering cyber security issues such as the following:

- Key Risk Indicators/ Key Performance Indicators;
- Status reports on overall cyber security control maturity levels;
- Status of staff Information Security awareness;
- Updates on latest internal or relevant external cyber security incidents; and
- Results from penetration testing exercises.

GR-12.2.9

The Board must ensure that the cyber security risk management framework is evaluated for scope of coverage, adequacy and effectiveness every three years or when there are significant changes to the risk environment, taking into account emerging cyber threats and cyber security controls.



MODULE	GR:	General Requirements
CHAPTER	GR-12:	Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.10

Licensees must have in place arrangements to handle cyber security risk management responsibilities. Licensees may, commensurate with their size and risk profile, assign the responsibilities to a qualified Chief Information Security Officer (CISO) reporting to an independent risk management function or incorporate the responsibilities of cyber security risk into the risk management function. Overseas licensees must be governed under a framework of cyber security risk management policies which ensure that an adequate level of oversight is exercised by the regional office or head office.

GR-12.2.11

Licensees should ensure that appropriate resources are allocated to the cyber security risk management function for implementing the cyber security framework.

GR-12.2.12

Licensees must ensure that the cyber security risk management function is headed by suitably qualified Chief Information Security Officer (CISO), with appropriate authority to implement the Cyber Security strategy.

GR-12.2.13

Licensees may establish a cyber security committee that is headed by an independent senior manager from a control function (like CFO / CRO), with appropriate authority to approve policies and frameworks needed to implement the cyber security strategy, and act as a governance committee for the cyber security function. Membership of this committee should include senior management members from business functions, IT, Risk and Compliance.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.14 The senior management must be responsible for the following activities:

- (a) Create the overall cyber security risk management framework and adequately oversee its implementation;
- (b) Formulate an organisation-wide cyber security strategy and cyber security policy;
- (c) Implement and consistently maintain an integrated, organisation-wide, cyber security risk management framework, and ensure sufficient resource allocation;
- (d) Monitor the effectiveness of the implementation of cyber security risk management practices and coordinate cyber security activities with internal and external risk management entities;
- (e) Ensure that internal management reporting caters to cyber threats and cyber security risk treatment;
- (f) Prepare quarterly or more frequent reports on all cyber incidents (internal and external) and their implications on the licensee; and
- (g) Ensure that processes for identifying the cyber security risk levels across the licensee are in place and annually evaluated.

GR-12.2.15 The senior management must ensure that:

- (a) The licensee has identified clear internal ownership and classification for all information assets and data;
- (b) The licensee has maintained an inventory of the information assets and data which is reviewed and updated regularly;
- (c) The cyber security staff are adequate to manage the licensee's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls;
- (d) It provides and requires cyber security staff to attend regular cyber security update and training sessions (for example Security+, CEH, CISSP, CISA, CISM, CCSP) to stay abreast of changing cyber security threats and countermeasures.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.16 With respect to Subparagraph GR-12.2.15(a), data classification entails analyzing the data the licensee retains, determining its importance and value, and then assigning it to a category. When classifying data, the following aspects of the policy should be determined:

- a) Who has access to the data;
- b) How the data is secured;
- c) How long the data is retained (this includes backups);
- d) What method should be used to dispose of the data;
- e) Whether the data needs to be encrypted; and
- f) What use of the data is appropriate.

The general guideline for data classification is that the definition of the classification should be clear enough so that it is easy to determine how to classify the data. In other words, there should be little (if any) overlap in the classification definitions. The owner of data (i.e. the relevant business function) should be involved in such classification.

Cyber Security Strategy

GR-12.2.17

An organisation-wide cyber security strategy must be defined and documented to include:

- (a) The position and importance of cyber security at the licensee;
- (b) The primary cyber security threats and challenges facing the licensee;
- (c) The licensee's approach to cyber security risk management;
- (d) The key elements of the cyber security strategy including objectives, principles of operation and implementation approach;
- (e) Scope of risk identification and assessment, which must include the dependencies on third party service providers;
- (f) Approach to planning response and recovery activities; and
- (g) Approach to communication with internal and external stakeholders including sharing of information on identified threats and other intelligence among industry participants.

GR-12.2.18 The cyber security strategy should be communicated to the relevant stakeholders and it should be revised as necessary and, at least, once every three years. Appendix A provides cyber security control guidelines that can be used as reference to support the licensee's cyber security strategy and cyber security policy.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

Cyber Security Policy

GR-12.2.19

Licensees must implement a written cyber security policy setting forth its policies for the protection of its electronic systems and client data stored on those systems, which must be reviewed and approved by the licensee's senior management, as appropriate, at least annually. The cyber security policy areas including but not limited to the following must be addressed:

- (a) Definition of the key cyber security activities within the licensee, the roles, responsibilities, delegated powers and accountability for these activities;
- (b) A statement of the licensee's overall cyber risk tolerance as aligned with the licensee's business strategy. The cyber risk tolerance statement should be developed through consideration of the various impacts of cyber threats including customer impact, service downtime, potential negative media publicity, potential regulatory penalties, financial loss, and others;
- (c) Definition of main cyber security processes and measures and the approach to control and assessment;
- (d) Policies and procedures (including process flow diagrams) for all relevant cyber security functions and controls including the following:
 - (a) Asset management (Hardware and software);
 - (b) Incident management (Detection and response);
 - (c) Vulnerability management;
 - (d) Configuration management;
 - (e) Access management;
 - (f) Third party management;
 - (g) Secure application development;
 - (h) Secure change management;
 - (i) Cyber training and awareness;
 - (j) Cyber resilience (business continuity and disaster planning);
 - and
 - (k) Secure network architecture.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

Approach, Tools and Methodology

GR-12.2.20

Licensees must ensure that the cyber security policy is effectively implemented through a consistent risk-based approach using tools and methodologies that are commensurate with the size and risk profile of the licensee. The approach, tools and methodologies must cover all cyber security functions and controls defined in the cyber security policy.

GR-12.2.21

Licensees should establish and maintain plans, policies, procedures, process and tools (“playbooks”) that provide well-defined, organised approaches for cyber incident response and recovery activities, including criteria for activating the measures set out in the plans and playbooks to expedite the licensee’s response time. Plans and playbooks should be developed in consultation with business lines to ensure business recovery objectives are met and are approved by senior management before broadly shared across the licensee. They should be reviewed and updated regularly to incorporate improvements and/or changes in the licensee. Licensees may enlist external subject matter experts to review complex and technical content in the playbook, where appropriate. A number of plans and playbooks should be developed for specific purposes (e.g. response, recovery, contingency, communication) that align with the overall cyber security strategy.

Prevention Controls

GR-12.2.22

A Licensee must develop and implement preventive measures across all relevant technologies to minimise the licensee’s exposure to cyber security risk. Such preventive measures must include, at a minimum, the following:

- Deployment of End Point Protection (EPP) and Endpoint Detection and Response (EDR) including anti-virus software and anti-malware programs to detect, prevent, and isolate malicious code;
- Use of firewalls for network segmentation including use of Web Application Firewalls (WAF) where relevant, for filtering and monitoring HTTP traffic between a web application and the Internet, and access control lists to limit unauthorized system access between network segments;
- Rigorous security testing at software development stage as well as after deployment to limit the number of vulnerabilities;
- Use of a secure email gateway to limit email based cyber attacks such as malware attachments, malicious links, and phishing scams (for example use of Microsoft Office 365 Advanced Threat Protection tools for emails);



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

- (e) Use of a Secure Web Gateway to limit browser based cyber-attacks, malicious websites and enforce organization policies;
- (f) Creating a list of whitelisted applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on the organization's systems; and
- (g) Implementing Bring Your Own Device "BYOD" security policies to secure all mobile devices with any access to licensee systems, applications, and networks through security measures such as encryption, remote wipe capabilities, and password enforcement.

GR-12.2.23 Licensees should also implement the following prevention controls in the following areas:

- (a) Data leakage prevention to detect and prevent confidential data from leaving the licensee's technology environment;
- (b) to Controls or solutions to secure, control, manage and monitor privileged access to critical assets, (e.g. Privileged Access Management (PAM);
- (c) Controls to secure physical network ports against connection to computers which are unauthorised to connect to the licensee's network or which do not meet the minimum-security requirements defined for licensee computer systems (e.g. Network access control); and
- (d) Identity and access management controls to limit the exploitation and monitor the use of privileged and non-privileged accounts.

GR-12.2.24

Licensees must set up anti-spam and anti-spoofing measures to authenticate the licensee's mail server and to prove to ISPs, mail services and other receiving mail servers that senders are truly authorized to send the email. Examples of such measures include:

- SPF "Sender Policy Framework";
- DKIM "Domain Keys Identified Mail"; and
- DMARC "Domain-based Message Authentication, Reporting and Conformance".

GR-12.2.25 Licensees should subscribe to one of the Cyber Threat Intelligence services in order to stay abreast of emerging cyber threats, cybercrime actors and state of the art tools and security measures.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.26

Licensees must use a single unified private email domain or its subdomains for communication with customers to prevent abuse by third parties. Licensees must not utilise third-party email provider domains for communication with customers. The email domains must comply with the requirements with respect to SPF, DKIM and DMARC in this Module. With respect to URLs or other clickable links in communications with customers, licensees must comply with the following requirements:

- (a) Limit the use of links in SMS and other short messages (such as WhatsApp) to messages sent as a result of customer request or action. Examples of such customer actions include verification links for customer onboarding, payment links for customer-initiated transactions etc;
- (b) Refrain from using shortened links in communication with customers;
- (c) Implement one or more of the following measures for links sent to customers:
 - i. ensure customers receive clear instructions in communications sent with the links;
 - ii. prior notification to the customer such as through a phone call informing the customer to expect a link from the licensee;
 - iii. provision of transaction details such as the transaction amount and merchant name in the message sent to the customer with the link;
 - iv. use of other verification measures like password or biometric authentication; and
- (d) Create customer awareness campaigns to educate their customers on the risk of fraud related to links they receive in SMS, short messages and emails with clear instructions to customers that licensees will not send clickable links in SMS, emails and other short messages to request information or payments unless it is as a result of customer request or action.

GR-12.2.26A

For the purpose of Paragraph GR-12.2.26, subject to CBB's approval, licensees may be allowed to use additional domains for email communications with customers under certain circumstances. Examples of such circumstances include emails sent to customers by:

- (a) Head/regional office of a licensee; and
- (b) Third-party service providers subject to prior arrangements being made with customers. Examples of such third-party services include informational subscription services (e.g. Bloomberg) and document management services (e.g. DocuSign).



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

Cyber Risk Identification and Assessments

GR-12.2.27

Licensees must conduct periodic assessments of cyber threats. For the purpose of analysing and assessing current cyber threats relevant to the licensee, it should take into account the factors detailed below:

- (a) Cyber threat entities including cyber criminals, cyber activists, insider threats;
- (b) Methodologies and attack vectors across various technologies including cloud, email, websites, third parties, physical access, or others as relevant;
- (c) Changes in the frequency, variety, and severity of cyber threats relevant to the region;
- (d) Dark web surveillance to identify any plot for cyber attacks;
- (e) Examples of cyber threats from past cyber attacks on the licensee if available; and
- (f) Examples of cyber threats from recent cyber attacks on other organisations.

GR-12.2.28

Licensees must conduct periodic assessments of the maturity, coverage, and effectiveness of all cyber security controls. Cyber security control assessment must include an analysis of the controls' effectiveness in reducing the likelihood and probability of a successful attack.

GR-12.2.29

Licensees should ensure that the periodic assessments of cyber threats and cyber security controls cover all critical technology systems. A risk treatment plan should be developed for all residual risks which are considered to be above the licensee's risk tolerance levels.

GR-12.2.30

Licensees must conduct regular technical assessments to identify potential security vulnerabilities for systems, applications, and network devices. The vulnerability assessments must be comprehensive and cover internal technology, external technology, and connections with third parties. Assessments for external public facing services and systems must be more frequent.

MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.31 With respect to Paragraph GR-12.2.30, external technology refers to the licensee's public facing technology such as websites, apps and external servers. Connections with third parties includes any API or other connections with fintech companies, technology providers, outsourcing service providers etc.

GR-12.2.32 CBB may require additional third-party security reviews to be performed as needed.

Cyber Incident Detection and Management

GR-12.2.33 Licensees must implement cyber security incident management processes to ensure timely detection, response and recovery for cyber security incidents. This includes implementing a monitoring system for log correlation and anomaly detection.

GR-12.2.34 Licensees should receive data on a real time basis from all relevant systems, applications, and network devices including operational and business systems. The monitoring system should be capable of identifying indicators of cyber incidents and initiate alerts, reports, and response activities based on the defined cyber security incident management process.

GR-12.2.35 Licensees should retain the logs and other information from the monitoring system for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations, for 12 months or longer.

GR-12.2.36 Once a cyber incident is detected, licensees should activate their containment measures, processes and technologies best suited to each type of cyber incident to prevent a cyber incident from inflicting further damage. This may involve, after considering the costs, business impact and operational risks, shutting down or isolating all or affected parts of their systems and networks as deemed necessary for containment and diagnosis.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.37

Licensees must define roles and responsibilities and assign adequate resources to detect, identify, investigate and respond to cyber incidents that could impact the licensee's infrastructure, services and customers. Such responsibilities must include log correlation, anomaly detection and maintaining the licensee's asset inventory and network diagrams.

GR-12.2.38

Licensees must regularly identify, test, review and update current cyber security risk scenarios and the corresponding response plan. This is to ensure that the scenarios and response plan remain relevant and effective taking into account changes in the operating environment, systems or the emergence of new cyber security threats. If any gaps are identified, the monitoring system must be updated with new use cases and rule sets which are capable of detecting the current cyber incident scenarios.

GR-12.2.39

The cyber incident scenario tests should include high-impact-low-probability events and scenarios that may result in failure. Common cyber incident scenarios include distributed denial of service (DDoS) attacks, system intrusion, data exfiltration and system disruption. Licensees should regularly use threat intelligence to update the scenarios so that they remain current and relevant. Licensees should periodically review current cyber incident scenarios for the purpose of assessing the licensee's ability to detect and respond to these scenarios if they were to occur.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.40

Licensees must ensure that critical cyber security incidents detected are escalated to an incident response team, management and the Board, in accordance with the licensee's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly. See also Paragraph GR-12.2.59 for the requirement to report to CBB.

GR-12.2.41 Licensees should clearly define the roles, responsibilities and accountabilities for cyber incident detection and response activities to one or more named individuals that meet the pre-requisite role requirements. Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible. The roles should include:

- **Incident Owner:** An individual that is responsible for handling the overall cyber incident detection and response activities according to the incident type and services affected. The Incident Owner is delegated appropriate authority to manage the mitigation or preferably, removal of all impacts due to the incident.
- **Spokesperson:** An individual, from External Communications Unit or another suitable department, that is responsible for managing the communications strategy by consolidating relevant information and views from subject matter experts and the licensee's management to update the internal and external stakeholders with consistent information.
- **Record Keeper:** An individual that is responsible for maintaining an accurate record of the cyber incident throughout its different phases, as well as documenting actions and decisions taken during and after a cyber incident. The record serves as an accurate source of reference for after-action reviews to improve future cyber incident detection and response activities.

GR-12.2.42 For the purpose of managing a critical cyber incident, the licensee should operate a situation room, and should include in the incident management procedure a definition of the authorities and responsibilities of staff members, internal and external reporting lines, communication channels, tools and detailed working procedures. The situation room or a war room is a physical room or a virtual room where relevant members of the management gather to handle a crisis in the most efficient manner possible.

GR-12.2.43 Licensees should record and document in an orderly manner the incidents that have been handled and the actions that were taken by the relevant functions. In particular, the licensee should maintain an "incident log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence. It should also include the status of the issue whether it is open or has been resolved and person in charge of resolving the issue/incident. The logs should be stored and preserved in a secure and legally admissible manner.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.44 Licensees should utilise pre-defined taxonomy for classifying cyber incidents according to, for example, the type of incident, threat actors, threat vectors and repercussions; and a pre-established severity assessment framework to help gauge the severity of the cyber incident. For example, taxonomies that can be used when describing cyber incidents:

- (a) Describe the cause of the cyber incident (e.g. process failure, system failure, human error, external event, malicious action)
- (b) Describe whether the cyber incident due to a third-party service provider
- (c) Describe the attack vector (e.g. malware, virus, worm, malicious hyperlink)
- (d) Describe the delivery channel used (e.g. e-mail, web browser, removable storage media)
- (e) Describe the impact (e.g. service degradation/disruption, service downtime, potential impact to customers, data leakage, unavailability of data, data destruction/corruption, tarnishing of reputation)
- (f) Describe the type of incident (e.g. zero-day attack, exploiting a known vulnerability, isolated incident)
- (g) Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic)
- (h) Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state)

The cyber incident severity may be classified as:

- (a) **Severity 1** incident has or will cause a serious disruption or degradation of critical service(s) and there is potentially high impact on public confidence in the licensee.
- (b) **Severity 2** incident has or will cause some degradation of critical services and there is medium impact on public confidence in the licensee.
- (c) **Severity 3** incident has little or no impact to critical services and there is no visible impact on public confidence in the licensee.

GR-12.2.45 Licensees should determine the effects of the cyber incident on customers and to the wider financial system as a whole and report the results of such an assessment to CBB if it is determined that the cyber incident may have a systemic impact.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.46 Licensees should establish metrics to measure the impact of a cyber incident and to report to management the performance of response activities. Examples include:

1. Metrics to measure impact of a cyber incident
 - (a) Duration of unavailability of critical functions and services
 - (b) Number of stolen records or affected accounts
 - (c) Volume of customers impacted
 - (d) Amount of lost revenue due to business downtime, including both existing and future business opportunities
 - (e) Percentage of service level agreements breached
2. Performance metrics for incident management
 - (a) Volume of incidents detected and responded via automation
 - (b) Dwell time (i.e. the duration a threat actor has undetected access until completely removed)
 - (c) Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied

Recovery

GR-12.2.47 Licensees must identify the critical systems and services within its operating environment that must be recovered on a priority basis in order to provide certain minimum level of services during the downtime and determine how much time the licensee will require to return to full service and operations.

GR-12.2.48 Critical incidents are defined as incidents that trigger the BCP and the crisis management plan. Critical systems and services are those whose failure can have material impact on any of the following elements:

- a) Financial situation;
- b) Reputation;
- c) Regulatory, legal and contractual obligations; and
- d) Operational aspects and delivery of key products and services.

GR-12.2.49 Licensees must define a program for recovery activities for timely restoration of any capabilities or services that were impaired due to a cyber security incident. Licensees must establish recovery time objectives (“RTOs”), i.e. the time in which the intended process is to be covered, and recovery point objectives (“RPOs”), i.e. point to which information used must be restored to enable the activity to operate on resumption”. Licensees must also consider the need for communication with third party service providers, customers and other relevant external stakeholders as may be necessary.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

GR-12.2.50 Licensees must ensure that all critical systems are able to recover from a cyber security breach within the licensee's defined RTO in order to provide important services or some level of minimum services for a temporary period of time.

GR-12.2.51 Licensees should validate that recovered assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations. This includes performing checks on data to ensure data integrity. In some cases, licensees may need to use backup data kept in a disaster recovery site or plan for the reconstruction of data from external stakeholders such as business partners and customers.

GR-12.2.52 Licensees must define a program for exercising the various response mechanisms, taking into account the various types of exercises such as attack simulations, "war games" and "table top" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers and spokespersons.

GR-12.2.53 Licensees must define the mechanisms for ensuring accurate, timely and actionable communication of cyber incident response and recovery activities with the internal stakeholders, including to the board or designated committee of the board.

GR-12.2.54 Licensee must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber security incident.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

Cyber Security Insurance

GR-12.2.55

Licensees must arrange to seek cyber risk insurance cover from a suitable insurer, following a risk-based assessment of cyber security risk is undertaken by the respective licensee and independently verified by the insurance company. The insurance policy may include some or all of the following types of coverage, depending on the risk assessment outcomes:

- (a) Crisis management expenses, such as costs of notifying affected parties, costs of forensic investigation, costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs to analyse the insured's legal response obligations;
- (b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations; and
- (c) Policy also provides coverage for a variety of torts, including invasion of privacy or copyright infringement. First-party coverages may include lost revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the insured.

Training and Awareness

GR-12.2.56

Licensees must evaluate improvement in the level of awareness and preparedness to deal with cyber security risk to ensure the effectiveness of the training programmes implemented.

GR-12.2.57

The licensee must ensure that all employees receive adequate training on a regular basis, in relation to cyber security and the threats they could encounter, such as through testing employee reactions to simulated cyber-attack scenarios. All relevant employees must be informed on the current cyber security breaches and threats. Additional training should be provided to 'higher risk staff'.

GR-12.2.58

The licensees must ensure that role specific cyber security training is provided on a regular basis to relevant staff including:

- (a) Executive board and senior management;
- (b) Cyber security roles;
- (c) IT staff; and
- (d) Any high-risk staff as determined by the licensee.



MODULE	GR: General Requirements
CHAPTER	GR-12: Information Security

GR-12.2 Cyber Security Risk Management (continued)

Incident Reporting to CBB

GR-12.2.59 Upon occurrence or detection of any cyber security incident, whether internal or external, that compromises customer information or disrupts critical services that affect operations, licensees must contact the CBB, immediately (within one hour), on 17547477 and submit Section A of the Cyber Security Incident Report (Appendix RM-1) to CBB's cyber incident reporting email, incident.ancillary@cbb.gov.bh (for Ancillary Service Providers) or incident.tpa@cbb.gov.bh (for TPAs), within two hours.

GR-12.2.60 Following the submission referred to in Paragraph GR-12.2.59, the licensee must submit to CBB Section B of the Cyber Security Incident Report (Appendix RM-1) within 10 calendar days of the occurrence of the cyber security incident. Licensees must include all relevant details in the report, including the full root cause analysis of the cyber security incident, its impact on the business operations and customers, and all measures taken by the licensee to stop the attack, mitigate its impact and to ensure that similar events do not recur. In addition, a weekly progress update must be submitted to CBB until the incident is fully resolved.

GR-12.2.61 With regards to the submission requirement mentioned in Paragraph GR-12.2.60, the licensee should submit the report with as much information as possible even if all the details have not been obtained yet.



MODULE	GR:	General Requirements
CHAPTER	GR-13:	Fees and Charges

GR-13.1 Merchant Fees on Payments to Zakat and Charity Fund

GR-13.1.1

PSPs must exempt the Zakat and Charity Fund (“the Fund”) of the Ministry of Justice, Islamic Affairs and Awqaf from merchant fees for payments made to the Fund.



MODULE	GR: General Requirements
CHAPTER	GR-14: Marketing of Financial Services

GR-14.1 Arrangements relating to Regulated Services provided by PSPs

GR-14.1.1

Pursuant to Article 3(b) of Resolution No. (16) of 2012 relating to marketing financial services in the Kingdom of Bahrain, and in relation to regulated services provided by PSPs:

- (a) Where a PSP has entered into an arrangement with a third party offering, as part of its services, marketing services relevant to the regulated services, the said third party may market the regulated services, subject to the following conditions:
 - (i) The arrangement between the PSP and third party must be subject to a contract that governs all aspects of the relationship including, but not limited to, the marketing of the regulated services and all rights, responsibilities and obligations of both the PSP and the third party; and
 - (ii) The arrangement must be in full compliance with the CBB Law, its regulations, resolutions and directives (including the CBB Rulebook) and all other applicable laws and regulations;
- (b) The PSP shall remain fully responsible for the regulated services provided in connection with the arrangement and for any violations of the CBB Law, its regulations, resolutions and directives (including the CBB Rulebook) that arise out of, or in connection with, the said arrangement;
- (c) Any arrangement involving the provision of regulated services by the aforementioned third party shall be illegal and be subject to the relevant penal provisions in the CBB law.



Appendix A – Cyber Security Control Guidelines

The Control Guidelines consists of five Core tasks which are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cyber security risk.

Identify – Develop an organisation-wide understanding to manage cyber security risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Cyber Security Risk Management Framework. Understanding the business context, the resources that support critical functions, and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cyber security incident.

Detect – Develop and implement appropriate activities to identify the occurrence of a cyber security incident. The Detect Function enables timely discovery of cyber security events.

Respond – Develop and implement appropriate activities to take action regarding a detected cyber security incident. The Respond Function supports the ability to contain the impact of a potential cyber security incident.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cyber security incident.

Below is a listing of the specific cyber security activities that are common across all critical infrastructure sectors:

IDENTIFY

Asset Management: The data, personnel, devices, systems, and facilities that enable the licensee to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the licensee's risk strategy.

1. Physical devices and systems within the licensee are inventoried.
2. Software platforms and applications within the licensee are inventoried.
3. Communication and data flows are mapped.
4. External information systems are catalogued.
5. Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
6. Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.



Business Environment: The licensee's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions.

1. Priorities for the licensee's mission, objectives, and activities are established and communicated.
2. Dependencies and critical functions for delivery of critical services are established.
3. Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

Governance: The policies, procedures, and processes to manage and monitor the licensee's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk.

1. licensee's cyber security policy is established and communicated.
2. Cyber security roles and responsibilities are coordinated and aligned with internal roles and external partners.
3. Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed.
4. Governance and risk management processes address cyber security risks.

Risk Assessment: The licensee understands the cyber security risk to licensee's operations (including mission, functions, image, or reputation), licensee's assets, and individuals.

1. Asset vulnerabilities are identified and documented.
2. Cyber threat intelligence is received from information sharing forums and sources.
3. Threats, both internal and external, are identified and documented.
4. Potential business impacts and likelihoods are identified.
5. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
6. Risk responses are identified and prioritized.

Risk Management Strategy: The licensee's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

1. Risk management processes are established, managed, and agreed to by licensee's stakeholders.
2. The licensee's risk tolerance is determined and clearly expressed.
3. The licensee's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

Third Party Risk Management: The licensee's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing third party risk. The licensee has established and implemented the processes to identify, assess and manage supply chain risks.

1. Cyber third-party risk management processes are identified, established, assessed, managed, and agreed to by the licensee's stakeholders.



2. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber third party risk assessment process.
3. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of a licensee's cyber security program.
4. Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
5. Response and recovery planning and testing are conducted with suppliers and third-party providers.

PROTECT

Identity Management, Authentication and Access Control: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
2. Physical access to assets is managed and protected.
3. Remote access is managed.
4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
5. Network integrity is protected (e.g., network segregation, network segmentation).
6. Identities are proofed and bound to credentials and asserted in interactions
7. Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Awareness and Training: The licensee's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security-related duties and responsibilities consistent with related policies, procedures, and agreements.

1. All users are informed and trained on a regular basis.
2. Licensee's security awareness programs are updated at least annually to address new technologies, threats, standards, and business requirements.
3. Privileged users understand their roles and responsibilities.
4. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
5. The Board and senior management understand their roles and responsibilities.
6. Physical and cyber security personnel understand their roles and responsibilities.
7. Software development personnel receive training in writing secure code for their specific development environment and responsibilities.

Data Security: Information and records (data) are managed consistent with the licensee's risk strategy to protect the confidentiality, integrity, and availability of information.



1. Data-at-rest classified as critical or confidential is protected through strong encryption.
2. Data-in-transit classified as critical or confidential is protected through strong encryption.
3. Assets are formally managed throughout removal, transfers, and disposition
4. Adequate capacity to ensure availability is maintained.
5. Protections against data leaks are implemented.
6. Integrity checking mechanisms are used to verify software, firmware, and information integrity.
7. The development and testing environment(s) are separate from the production environment.
8. Integrity checking mechanisms are used to verify hardware integrity.

Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational units), processes, and procedures are maintained and used to manage protection of information systems and assets.

1. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
2. A System Development Life Cycle to manage systems is implemented
3. Configuration change control processes are in place.
4. Backups of information are conducted, maintained, and tested.
5. Policy and regulations regarding the physical operating environment for licensee's assets are met.
6. Data is destroyed according to policy.
7. Protection processes are improved.
8. Effectiveness of protection technologies is shared.
9. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
10. Response and recovery plans are tested.
11. Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening).
12. A vulnerability management plan is developed and implemented.

Maintenance: Maintenance and repairs of information system components are performed consistent with policies and procedures.

1. Maintenance and repair of licensee's assets are performed and logged, with approved and controlled tools.
2. Remote maintenance of licensee's assets is approved, logged, and performed in a manner that prevents unauthorized access.

Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.



2. Removable media is protected and its use restricted according to policy.
3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
4. Communications and control networks are protected.
5. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

DETECT

Anomalies and Events: Anomalous activity is detected and the potential impact of events is understood.

1. A baseline of network operations and expected data flows for users and systems is established and managed.
2. Detected events are analyzed to understand attack targets and methods.
3. Event data are collected and correlated from multiple sources and sensors
4. Impact of events is determined.
5. Incident alert thresholds are established.

Security Continuous Monitoring: The information system and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.

1. The network is monitored to detect potential cyber security events.
2. The physical environment is monitored to detect potential cyber security events
3. Personnel activity is monitored to detect potential cyber security events.
4. Malicious code is detected.
5. Unauthorized mobile code is detected.
6. External service provider activity is monitored to detect potential cyber security events.
7. Monitoring for unauthorized personnel, connections, devices, and software is performed.
8. Vulnerability scans are performed at least quarterly.

Detection Processes: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

1. Roles and responsibilities for detection are well defined to ensure accountability.
2. Detection activities comply with all applicable requirements.
3. Detection processes are tested.
4. Event detection information is communicated.
5. Detection processes are continuously improved.

RESPOND

Response Planning: Response processes and procedures are executed and maintained, to ensure response to detected cyber security incidents. Response plan is executed during or after an incident.

Communications: Response activities are coordinated with internal and external stakeholders.



1. Personnel know their roles and order of operations when a response is needed.
2. Incidents are reported consistent with established criteria.
3. Information is shared consistent with response plans.
4. Coordination with internal and external stakeholders occurs consistent with response plans.
5. Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.
6. Incident response exercises and scenarios across departments are conducted at least annually.

Analysis: Analysis is conducted to ensure effective response and support recovery activities.

1. Notifications from detection systems are investigated.
2. The impact of the incident is understood.
3. Forensics are performed.
4. Incidents are categorized consistent with response plans.
5. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the licensee from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

1. Incidents are contained.
2. Incidents are mitigated.
3. Newly identified vulnerabilities are mitigated or documented as accepted risks.

Improvements: The response activities are improved by incorporating lessons learned from current and previous detection/response activities.

1. Response plans incorporate lessons learned.
2. Response strategies are updated.

RECOVER

Recovery Planning: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cyber security incidents. Recovery plan is executed during or after a cyber security incident.

Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.

1. Recovery plans incorporate lessons learned.
2. Recovery strategies are updated.



Communications: Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

1. Public relations are managed.
2. Reputation is repaired after an incident.
3. Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.