ANCILLARY SERVICE PROVIDERS GENERAL REQUIREMENTS MODULE

MODULE:	GR (General Requirements)

Table of Contents

MODULE:	GR (General Requirements)

Table of Contents

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

GR-12.2 Cyber Security

GR-12.2.1 This Section applies to 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. The licensees must ensure that their systems are subject to Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST).

GR-12.2.3 All licensees must perform penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place at least twice a year. These tests must be conducted each year in June and December simulating real world cyber attacks on the technology environment and must:

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

GR-12.2.4 Reports on penetration testing referred to in Paragraph GR-12.2.3 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.