TECHNOLOGY RISK MANAGEMENT GUIDELINES JANUARY 2021

Monetary Authority of Singapore

**6 Software Application Development and Management**

**6.1 Secure Coding, Source Code Review and Application Security Testing**

6.1.1 Software bugs or vulnerabilities are typically targeted and exploited by threat actors to compromise an IT system, and they often occur because of poor software development practices. To minimise the bugs and vulnerabilities in its software, the FI should adopt standards on secure coding, source code review8 and application security testing.

6.1.2 The secure coding and source code review standards should cover areas such as secure programming practices, input validation, output encoding, access controls, authentication, cryptographic practices, and error and exception handling. 6.1.3 A policy and procedure on the use of third party and open-source software codes should be established to ensure these codes are subject to review and testing before they are integrated into the FI’s software.

6.1.4 To facilitate the remediation of vulnerabilities in a timely manner, the FI should keep track of updates and reported vulnerabilities for third party and open-source software codes that are incorporated in the FI’s software.

6.1.5 The FI should ensure its software developers are trained or have the necessary knowledge and skills to apply the secure coding and application security standards when developing applications.

6.1.6 It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.

6.1.7 All issues and software defects discovered from the source code review and application security testing should be tracked. Major issues and software defects should be remediated before production deployment.