

How Zimperium's MAPS Capabilities Help Ensure Compliance with RMIT Malaysia Regulation



The Central Bank of Malaysia has recently mandated a critical regulation, acknowledging the importance of fortifying digital platforms and mobile applications in safeguarding a bank's integrity, See how Zimperium's [Mobile Application Protection Suite \(MAPS\)](#) can help financial institutions comply.

s/g	#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
S	11.9	A financial institution must conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems including web, mobile and all external-facing applications.	✓			
S	11.16	A financial institution must implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to prevent unauthorized access to data.		✓		
S	10.81	A financial institution must perform continuous surveillance to assess the vulnerability of the operating system and the relevant technology platform used for its digital delivery channels to security breaches and implement appropriate corresponding safeguards. In view of the evolving threat landscape, these safeguards must be continuously reviewed and updated to protect against fraud and to secure the confidentiality and integrity of customer and counterparty information and transactions.			✓	
S	10.82	Appendix 4: Control Measures on Mobile Applications and Devices 1- A financial institution should ensure digital payment, banking and insurance services involving sensitive customer and counterparty. Information offered via mobile devices are adequately secured.	✓	✓	✓	

s/g	#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
S	10.82	(continued) 2- In addition to the guidance in paragraph 1, a financial institution should also ensure the following measures are applied specifically for applications running on mobile devices used by the financial institution, appointed agents or intermediaries for the purpose of processing customer and counterparty information.	✓	✓	✓	
S	14.6	A financial institution must ensure that the independent external party providing the assurance is competent and has a good track record. The assurance shall address the matters covered in, and comply with, Appendix 9. Appendix 9: Supervisory Expectations on External Party Assurance PART B - Minimum controls to be assessed by the independent External Service Provider, where applicable.	✓	✓	✓	✓

MAPS™ Security Across the Lifecycle

