Annex C: Initial reporting trigger reference material

Survey conducted in January 2022

Jurisdiction	Authority	Trigger	RD (hrs)	Source
Australia	**APRA**	Threshold	72 hrs	An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than **72 hours, after becoming aware** of an information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions. Source: CPS 234
China	**CBIRC**	Occurrence	Immediate	When cyber security incidents **occur**, network operators should **immediately** initiate an emergency response plan, adopt corresponding remedial measures, and **report to the relevant competent departments** in accordance with relevant provisions. Source: CAC Cybersecurity Law, article 25 (translated) Where the breach, tampering, or loss of personal information **occurs or may occur**, a personal information processor shall **immediately** take remedial measures and **notify the departments** with personal information protection duties and the relevant individuals. *Source: Personal Information Protection Law (PIPL)*
EU	**ECB**	Threshold	2 hrs (SIs)	Initial information on the cyber incident must be submitted within two hours after the reporting thresholds are exceeded or within two hours after the point in time when the Supervised Entity can reasonably assume that an identified cyber incident will exceed the reporting thresholds, whichever occurs earlier. *Source: ECB Decisions (issued directly to the banks in scope)*
	EIOPA	None	N/A	EIOPA does not have incident reporting in place

Jurisdiction	Authority	Trigger	RD (hrs)	Source
	ESMA	Detection	24 hrs	Item 55 / Guideline 62: TRs should send to ESMA an initial incident notification **within 24 hours of becoming aware** of the incident and a follow-up notification within one month. *Source: Guidelines on periodic information and notification of material changes to be submitted to ESMA by Trade Repositories*
	EBA	Threshold	4 hrs	Payment service providers should send the initial report to the competent authority within **four hours** from the moment the operational or security incident has been classified as **major**. *Source: Revised guidelines on major incident reporting under PSD*
France	**BdF**	Threshold Detection Detection	2 hrs (SIs) 4 hrs (retail PSs) 72 hrs (wholesale PSs)	Payment service providers should send the initial report to the competent authority within **4 hours** from the moment the major operational or security incident was first **detected**, or, if the reporting channels of the competent authority are known not to be available or operational at that time, as soon as they become available/operational again. Should business be back to normal before 4 hours have passed since the incident was detected, payment service providers should aim to submit both the initial and the last intermediate report simultaneously (i.e. filling out sections A and B of the template) by the 4-hour deadline. *Source: PSDII (for retail payment systems)* Incident reporting shall occur without any delay **after incident detection** and in less than **72 hours**. *Source: ECB framework for wholesale payment systems (for wholesale payments)*
Hong Kong	**HKMA**	Detection	Same-day	As the nature of every operational incident is different, authorized institutions (AIs) are expected to exercise their judgement and establish internal guidelines endorsed by the management for deciding whether an operational incident should be regarded as significant and thus should be reported to the HKMA. The HKMA expects AIs to report to it suspected or confirmed cyber attacks that

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				may cause potential loss/leakage of sensitive data of the AI or its customer(s), potential financial loss (albeit small) to the affected customer(s), potential material financial loss to the AI, or significant impact on the AI's reputation. The Retail Payment Oversight Division of the HKMA asks SVF licensees to report suspected or confirmed cyber attacks **as soon as practicable**, and to provide prompt updates as and when the information and assessment is available. As for designated CSSs, as long as the incident affects the operation or service level of the system or the safety and efficiency of the system, they should be reported to the HKMA **as soon as possible**. No matter whether the incident is known or unknown to the CSS participant, or whether the incident is caused by a third party or the CSS participant, it should be reported to the HKMA
India	**RBI**	Detection	6 hrs	Guidelines clearly specify reporting requirements for unusual incidents specifying types of incidents to be reported/not reported. At the same time, they also allow for some discretion where FIs can exercise own judgement for reporting the incidents Security Incident Reporting (SIR) to RBI (**within two to 6 hours**) *Source: RBI/2015-16/418*
Indonesia	**BI**	Occurrence	1 hr (PSs)	BI has set qualitative criteria as a reference for CIR; however, no explicit quantitative criteria/ thresholds have been set by the authority. The qualitative criteria includes: potential breaches to the legal/regulatory requirements and the materiality of impact to the critical information systems or services which could cover malfunctioning data centres, network failures, and fraud incidents. Article 254.6: The disruption as referred to in paragraph (5) point c and force majeure as referred to in paragraph (5) point d must be notified to Bank Indonesia **not later than 1 (one) hour after the disruption occurrence**.

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				Source: Bank Indonesia Regulation Number 23/6/PBI/2021 (Payment Service Providers)
Italy	**BdI**	Threshold Threshold Detection	2 hrs (SIs) 4 hrs (LSIs) 3 hrs (PSs)	Regarding the timing of notification of incidents, the initial report must be sent: • for less significant banks, payment and electronic money institutions within **4 hours** from the moment when the reporting criteria are met • for significant banks within **2 hours** from the moment when the reporting criteria are met • for retail payment systems, payment schemes and financial technology providers within **3 hours of incident detection**
	MEF	Threshold	1-6 hrs (OES/ DSPs)	As for the national security cyber regulation n. 81/2021 for the financial operators included in the National Cybernetic Perimeter (Law n. 109/2019), the notification mechanism is threshold-less and based on the definitions of relevant cyber events. Designated critical national infrastructure must notify CSIRT Italy without delay of any incident having a significant impact on the continuity of the essential services provided, including information that makes it possible to identify cross-border impact of the incident. The notification must be made **within six hours or one hour** depending on the severity of the incident. *Source: Italian Legislative Decree no. 85/2018*
Japan	**JFSA**	Detection	Immediate	The FSA requires FIs to report **immediately** when a computer system failure or a cyber security incident meeting certain criteria is **detected**. Criteria for reportable incidents are provided in FSA's supervisory guidelines. Similar provisions are in place in FSA's supervisory guidelines for other types of FIs. Form 4-45 'Report of System Failure and Other Incidents' in the 'Forms and Other Materials' shall be submitted as part of the reporting. Additional reporting is required upon recovery and/or when cause of the incident is identified. A status update shall

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				be reported within one month if the recovery or identification of the cause has not been completed. *Source: Comprehensive Guidelines for Supervision of Major Banks, III-3-7-1-3: Supervisory methods and actions*
Russia	**CBR**	Detection Detection	3 hrs (SIs) 24 hrs (Other)	Significant Institutions: within **three hours** from the moment of **detection** of the incident. Other institutions: within **24 hours** from the moment of **detection** of the incident *Source: Bank of Russia Standard STO BR BFBO-1.5-2018 (Section 6)*
Saudi Arabia	**SAMA**	Threshold	Immediate	The Member Organisation should inform 'SAMA IT Risk Supervision' **immediately** when a medium or high classified security incident has **occurred and identified**. *Source: Cyber Security Framework v1.0, Article 3.3.15.5*
Singapore	**MAS**	Detection+ Threshold	1 hr	A bank shall notify the Authority **as soon as possible, but not later than 1 hour**, **upon the discovery** of a relevant incident. • 'relevant incident' means a system malfunction or IT security incident, which has a severe and widespread impact on the bank's operations or materially impacts the bank's service to its customers. *Source: MAS Notice on Technology Risk Management*
Spain	**BdE**	Threshold	2 hrs	**Two hours from its qualification** as relevant *Source: LSI reporting template (ECB Framework)*
Switzerland	**FINMA**	Detection	24 hrs	If a cyber attack on critical assets results in one or more of the protective goals of critical functions and their business processes being put at risk, this must be reported to FINMA immediately. Immediate reporting to FINMA means that the affected supervised institution informs FINMA through the responsible (Key) Account Manager **within 24 hours of detecting such a cyber attack** and conducting an initial assessment of its criticality. The actual report should be **submitted within 72 hours** via the FINMA

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				web-based survey and application platform (EHP). *Source: FINMA*
Türkiye	**BRSA**	Occurrence	N/A	A firm must notify the BRSA **immediately** if any sensitive or personal data are disclosed or leaked such that Information Systems Continuity Plan or secondary centres are activated. *Source: Regulation on Information Systems and Electronic Banking Services of Banks*
UK	**BoE (PRA)**	Threshold	Immediate	A firm must notify the PRA **immediately if it becomes aware**, or has information which reasonably suggests, that any of the following has occurred, may have occurred or may occur in the foreseeable future: (1) the firm failing to satisfy one or more of the threshold conditions; or (2) any matter which could have a significant adverse impact on the firm's reputation; or (3) any matter which could affect the firm's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm; or (4) any matter in respect of the firm which could result in serious financial consequences to the UK financial system or to other firms. *Source: PRA Rulebook, 2.1 General Notification Requirements*
	FCA	Threshold	Immediate	A firm must notify the FCA **immediately if it becomes aware**, or has information which reasonably suggests, that any of the following has occurred, may have occurred or may occur in the foreseeable future: (1) the firm failing to satisfy one or more of the threshold conditions; or (2) any matter which could have a significant adverse impact on the firm's reputation; or (3) any matter which could affect the firm's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm; or

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				(4) any matter in respect of the firm which could result in serious financial consequences to the UK financial system or to other firms. *Source: FCA Rulebook, SUP 15.3 General Notification Requirements*
US	**FRB**	Threshold	36 hrs (Banks)	The Federal Reserve Board, OCC, and FDIC issued a final rule that requires a banking organisation to notify its primary federal regulator of any 'computer-security incident' that rises to the level of a 'notification incident,' as soon as possible and no later than **36 hours** after the banking organisation determines that a **notification incident has occurred**. A bank service provider is required to notify at least one bank-designated point of contact at each affected customer bank as soon as possible when it determines it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to disrupt or degrade, covered services provided to the bank for four or more hours. *Source: Computer-Security Incident Notification Requirements for Banking Organisations and Their Bank Service Providers*
	SEC Rule (SCI Entities)	Threshold	Immediate	SCI personnel having a reasonable basis to conclude that an SCI event has occurred must notify the Commission. *Source: SEC Regulation SCI (17 C.F.R. §§ 242-1002)*