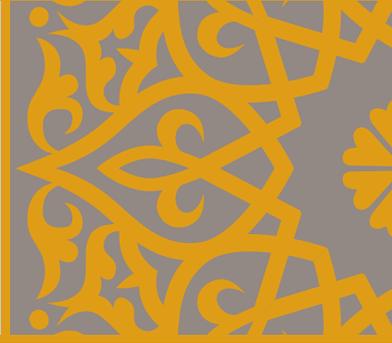


# Arab Regional Fintech Working Group

## Cyber Resilience Oversight Guidelines for the Arab Countries, Concerning Financial Market Infrastructures



No.  
137  
2020



صندوق النقد العربي  
ARAB MONETARY FUND



اتحاد منظمات  
البنوك العربية  
الائتمانية  
البنوك العربية  
الائتمانية





## Arab Regional Fintech Working Group

# Cyber Resilience Oversight Guidelines for the Arab Countries, concerning Financial Market Infrastructures

Arab Monetary Fund

2020

## ACKNOWLEDGEMENT

### Arab Regional Fintech Working Group

This document was produced within the Arab Regional Fintech Working Group activities.

The Arab Regional Fintech WG has a comprehensive structure from the different Fintech industry stakeholders, within the Arab region and outside, to enhance the proper Fintech ecosystem in Arab countries. Which implies the exchange of knowledge and expertise, strengthening the capacity-building of the Arab regulators, as well as building a network of relations between Arab and international experts from the public and private sectors to promote Fintech industry and the development of innovation.

The Cyber resilience oversight guidelines document was prepared by Kokila Alagh and Luna de Lange of KARM Legal Consultants, member of MENA Fintech Association, in collaboration with Nouran Youssef from the Arab Monetary Fund, and has benefited from the contributions and consultant support provided by Anomali Incorporated (and Anomali Solutions, Dubai, United Arab Emirates). Moreover, the paper has benefited from valuable review, comments and suggestions provided by Ahmed Albalooshi and Khalid Waheed Abdulrahman from Al Baraka Banking Group B.S.C, the Policy team from CGAP World Bank, and Fredesvinda Fatima Montes, Dorothee Delort; Finance, Competitiveness, and Innovation Department, The World Bank.

Any queries regarding this report should be addressed to:

Nouran Youssef, DBA

Senior Financial Sector Specialist, Arab Monetary Fund

Economic Department, Financial Sector Development Division

Corniche Street, P.O Box 2818, Abu Dhabi, United Arab Emirates

Tel. +971 2617 1454

E-mail: [Economic@amfad.org.ae](mailto:Economic@amfad.org.ae); [FSD@amfad.org.ae](mailto:FSD@amfad.org.ae),

[FintechWG@amf.org.ae](mailto:FintechWG@amf.org.ae), [nouran.youssef@amf.org.ae](mailto:nouran.youssef@amf.org.ae);

Website: [www.amf.org.ae](http://www.amf.org.ae)

All rights reserved. ©2019 AMF

Any reproduction, publication and reprint in the form of a different publication, whether printed or produced electronically, in whole or in part, is permitted only with the explicit written authorisation of the AMF.

## Table of Contents

<b>1. Brief introduction: Financial Market Infrastructures</b> .....	<b>14</b>
<b>2. Cyber Governance</b> .....	<b>14</b>
<b>2.1 Brief introduction: Cyber Governance:</b> .....	<b>14</b>
<b>2.2 Cyber Resilience Strategy and Framework:</b> .....	<b>15</b>
2.2.2 Risk Management and Ancillary Components: .....	15
2.2.3 Key Considerations:.....	16
<b>2.3 The Roles and Responsibilities of the Board and Management:</b> .....	<b>19</b>
<b>2.4 Guidance on the Senior Executive or Chief Information Security Officer (CISO):</b> .....	<b>24</b>
<b>2.5 Skills, Training and Accountability:</b> .....	<b>25</b>
<b>3. Information Assets Identification and Classification</b> .....	<b>26</b>
<b>3.1 Identification</b> .....	<b>26</b>
<b>3.2 Classification</b> .....	<b>26</b>
<b>3.3 Management of Interconnections with Third Parties:</b> .....	<b>28</b>
3.2.1 Impact to and from an Organisation’s Ecosystem:.....	29
3.2.2 Risks from Interconnections: .....	29
3.2.3 Data-Sharing Agreements:.....	31
3.2.4 Contagion / Contamination:.....	31
3.2.5 Crisis Communication and Reporting: .....	31
3.2.6 Responsible disclosure policy:.....	32
3.2.7 Incident handling preparation phase for anticipatory Forensic Readiness .....	32
3.2.8 Auditing and Testing: .....	32
<b>4. Protection and Risk Management:</b> .....	<b>32</b>
<b>4.1 Protection of Processes and Assets:</b> .....	<b>33</b>
4.1.2 Network and Infrastructure Management: .....	34
4.1.3 Logical and Physical Security Management:.....	36
<b>4.2 People Management:</b> .....	<b>41</b>
4.2.1 Human Resources Security: .....	41
4.2.2 Security Awareness and Training: .....	42
4.2.3 Supplier and Third-Party Interconnectivity and Security Management: .....	42
<b>5. Cyber Incidents Detection:</b> .....	<b>43</b>
<b>6. Incident Response and Recovery:</b> .....	<b>45</b>
<b>6.1 Cyber Resilience Incident Management:</b> .....	<b>46</b>
<b>6.2 Data Confidentiality, Integrity and Availability:</b> .....	<b>49</b>
<b>6.3 Communication and Collaboration:</b> .....	<b>50</b>
6.3.1 Contagion / Communicability:.....	50
6.3.2 Crisis Communication and Responsible Disclosure: .....	51
<b>6.4 Forensic Readiness:</b> .....	<b>52</b>
<b>7. Information Security Controls Testing:</b> .....	<b>53</b>

<b>7.1</b>	<b>Vulnerability Assessments:</b> .....	<b>55</b>
<b>7.2</b>	<b>Scenario-based Testing:</b> .....	<b>56</b>
<b>7.3</b>	<b>Penetration Testing:</b> .....	<b>57</b>
<b>7.4</b>	<b>Red Team Testing:</b> .....	<b>57</b>
<b>7.5</b>	<b>Taxonomy of Cyber Risk Controls:</b> .....	<b>58</b>
<b>8.</b>	<b><i>Situational Awareness:</i></b> .....	<b>59</b>
<b>8.1</b>	<b>Cyber Threat Intelligence:</b> .....	<b>60</b>
8.1.1.	Identification of potential cyber threats: .....	60
8.1.2.	Threat intelligence process: .....	60
8.1.3.	Scope of cyber threat intelligence gathering: .....	60
8.1.4.	Effective use of information:.....	60
8.1.5.	Expectations in terms of Cyber Threat Intelligence:.....	61
<b>8.2</b>	<b>Communication and Sharing of Information:</b> .....	<b>62</b>
8.2.1	Cross Industry; Cross Governmental and Cross Border / Jurisdictional Information Sharing: .....	67
8.2.2	Amongst Banks; with a brief case study of UBF-ISAC:.....	69
8.2.3	From Banks to Regulators: .....	71
8.2.4	Amongst Regulators: .....	72
8.2.5	With Security Agencies; with brief a case study of a CSIRT (Computer Security Incident Response Team): .....	74
<b>9.</b>	<b><i>Learning and Evolving:</i></b> .....	<b>76</b>
9.1	Cyber Threat Intelligence (continued): .....	76
<b>10.</b>	<b><i>Cyber Resilience assessment and performance metrics:</i></b> .....	<b>77</b>
<b>11.</b>	<b><i>Cyber Risk Insurance:</i></b> .....	<b>79</b>
<b>12.</b>	<b><i>Conclusion and Recommendations:</i></b> .....	<b>82</b>

## **Abbreviations:<sup>1</sup>**

ABAC	Attribute-based access control
AI	Artificial intelligence
AIC	Availability, integrity and confidentiality (see: CIA)
AIM	Asset inventory management
CIA	Confidentiality, integrity and availability (see: AIC)
CIRT	Cyber incident response team <u>or</u> computer incident response team
CERT	Computer emergency response team
CISO	Chief information security officer
CISSP	Certified Information Systems Security Professionals
COBIT	Control objectives for information and related technology
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CROE	Cyber resilience oversight expectations
CSD	Central securities depository
CSIRT	Computer security incident response team
DDoS	Distributed denial of service
DMZ	Demilitarised zone
e-CF	European e-Competence Framework
ENISA	European Network and Information Security Agency

---

<sup>1</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); <https://www.gartner.com/en/information-technology/glossary/cirt-cyber-incident-response-team>

FFIEC	Federal Financial Institutions Examination Council
FMI	Financial market infrastructure
FS-ISAC	Financial Services Information Sharing and Analysis Centre
GRC	Governance, risk management and compliance
HIDS	Host intrusion detection system
HIPS	Host intrusion prevention system
HKMA	Hong Kong Monetary Authority
HR	Human resources
IAM	Identity and access management
ICT	Information and communication technology / technologies; ICT can also be read as IT (information technology)
IDS	Intrusion detection system
IOSCO	International Organisation of Securities Commissions
IoT	Internet of things
IP	Internet Protocol.
IPS	Intrusion prevention system
ISAC	Information sharing and analysis centre
ISAE	International Standard on Assurance Engagements
ISAE	Assurance reports on controls at a service organisation
ISMS	Information security management system
ISO/IEC	International Organisation for Standardization/International Electrotechnical Commission
IT	Information technology

KPI	Key performance indicators
KRI	Key risk indicators
MAS	Monetary Authority of Singapore
NAC	Network access control
NCB	National central bank
NIST	National Institute of Standards and Technology
ORPS	Other retail payment systems
PFMIs	Principles for financial market infrastructures
PIRPS	Prominently important retail payment systems
RBAC	Role-based access control
RPO	Recovery point objectives
RTO	Recovery time objectives
SDLC	Software/system development life cycle
SFIA	Skills Framework for the Information Age
SIEM	Security information and event management
SIPS	Systemically important payment systems
SLA	Service level agreement
SOC	Security operations centre
SSH	Secure Shell
SSS	Securities settlement system
TIBER	Threat intelligence-based ethical red teaming
T2S	Target2-Securities

TLS	Transport layer security
TR	Trade repositories
TTP	Tactics, techniques and procedures
UBF-ISAC	United Arab Emirates Information Sharing and Analysis Centre
VPN	Virtual private network

## Executive Summary

The rapid digitization within the Arab region, as well as the global economy has led, increasingly so, to a dramatic increase in the number of cybersecurity incidents. Cybersecurity issues are becoming a day-to-day struggle for organisations. Recent trends and cybersecurity statistics reveal a huge increase in hacked and breached data from sources that are increasingly common in workplace environments of organisations, such as mobile and Internet of Things (IoT) devices. Furthermore, recent security research suggests that most organisations have unprotected data and poor cybersecurity practices in place, making them particularly vulnerable to cyber-attacks and possible data loss. To successfully fight against malicious cyber-attacks, it's imperative that organisations make cybersecurity awareness, prevention and security best practices a part of their culture, in addition to strict adherence and compliance with regulatory provisions – the said provisions in turn needing to be robust, yet with a measure of flexibility, in nature. Digital innovations should not, however, be stifled in their growth or advancement as they help serve stakeholders, curb costs and provide a competitive edge to organisations in the global market. These trends point to a growing imperative for cyber threat resilience in the digital age. It is acknowledged that governments, organisations in the private and public sectors and individuals must all play their part in building an ecosystem that is resilient to cyber threats.<sup>2</sup>

Statistics (from an international perspective) may assist to motivate the need for cyber resilience through representation of the overall impact of cyber-attacks. As such, be advised of the following reported statistics:

1. Worldwide spending on cybersecurity is forecasted to reach US\$133.7 billion in 2022<sup>3</sup>
2. 62% of businesses experienced phishing and social engineering attacks in 2018<sup>4</sup>
3. 68% of business leaders feel their cybersecurity risks are increasing<sup>5</sup>
4. Data breaches exposed 4.1 billion records in the first half of 2019<sup>6</sup>
5. 71% of breaches were financially motivated and 25% were motivated by espionage<sup>7</sup>
6. 52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively<sup>8</sup>
7. Between January 1, 2005 and April 18, 2018 there have been 8,854 recorded breaches<sup>9</sup>
8. While overall ransomware infections were down 52%, enterprise infections were up by 12% in 2018<sup>10</sup>
9. By 2020, the estimated number of passwords used by humans and machines worldwide will grow to 300 billion<sup>11</sup>

<sup>2</sup> <https://www.varonis.com/blog/cybersecurity-statistics/>

<sup>3</sup> <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

<sup>4</sup> <https://www.cybintsolutions.com/cyber-security-facts-stats/>

<sup>5</sup> [https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)

<sup>6</sup> <https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>

<sup>7</sup> <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

<sup>8</sup> <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

<sup>9</sup> <https://www.idtheftcenter.org/data-breaches/>

<sup>10</sup> <https://www.symantec.com/security-center/threat-report>

<sup>11</sup> <https://www.scmagazine.com/video-300-billion-passwords-by-2020-report-predicts/article/634848/>

Herewith highlights of the IBM Security and Ponemon Institute 2019 Cost of a Data Breach Report:

Global Averages 		Middle East Averages 	
Average total cost of a data breach <b>\$3.92M</b>		Average total cost of a data breach <b>\$5.97M</b>	
Average size of a data breach <b>25,575 records</b>		Average size of a data breach <b>38,800 records</b>	
Cost per lost record <b>\$150</b>	Time to identify and contain a breach <b>279 days</b>	Cost per lost record <b>\$173</b>	Time to identify and contain a breach <b>381 days</b>
Highest country average cost of \$8.19 million <b>United States</b>	Highest industry average cost of \$6.45 million <b>Healthcare</b>	Country rank for total cost <b>2</b>	Highest industry average for cost per record <b>Financial</b>

12

As the international community of persons (individual and organisations alike) grow more reliant on technology for their everyday activities, they are also looking to their governments to work together with the private sector to provide for a robust environment in which organisations can leverage technology and information storage, with a sense of trust, security and comfort in collecting, retaining, exchanging and destroying or erasing information or data; or facilitating transactions (financial; or otherwise). Concurrently, governments and the private sector in the GCC region are relying on digital innovations to help serve stakeholders, contain costs and provide a competitive edge in the global market. These trends point to a growing imperative for cyber threat resilience in the digital age. Governments, organisations and individuals must all play their part in building an ecosystem that is resilient to cyber threats.<sup>13</sup>

Cyber resilience is defined as an organisation's ability to continuously deliver the intended outcome, despite adverse cyber events. In other words, it is the organisational capability to sense, resist and react to disruptive cyber events, and to recover from them in a timely fashion. Strong cyber governance requires an organised, systematic and proactive approach within an organisation, in management of both the prevailing, as well as emerging cyber threats that it faces, or may face; supports efforts to

<sup>12</sup> IBM Security and Ponemon Institute are pleased to release the 2019 Cost of a Data Breach Report; [https://www.ibm.com/downloads/cas/ZBZLY7KL?\\_ga=2.83934879.749854357.1584273312-689978418.1584273312](https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.83934879.749854357.1584273312-689978418.1584273312)

<sup>13</sup> <https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6>

appropriately and adequately consider, as well as manage, cyber risks at all levels within an organisation's ecosystem; and provides for the allocation of adequate resources and expertise to manage cyber-related risks and attacks, within an organisation. Broadly speaking, an organisation's cyber resilience framework should have the necessary consideration of various components, namely the cyber risk management components, including: Governance; Identification; Protection; Detection; as well as Response and Recovery; and furthermore, ancillary components, including: Testing; Situational awareness; as well as Learning and evolving.

Cyber resilience, as a concept, essentially brings the areas of information security, business continuity and resilience together. Due to the nature of a digital economy being borderless and ever changing, it is advisable to create the capability to anticipate threats, to absorb the impacts of such threats and to react in a rapid and flexible way to ensure that an organisation's key systems and processes continue operating, without undue interruption. This ability is further enhanced through an organisation's use of smart technology.

Regulators and Supervisory Authorities play a critical role to play in the establishment of a national cyber resilient culture, where individuals and organisations are informed, aware, educated, skilled and necessarily enabled in defence. Cyber threats are real and can be as devastating as risks of terror and other catastrophic events. Regulators can establish a framework in which organisations collaborate to enhance their resilience against cyber-attacks, because the former are able to have a greater sense of the threat environment, through monitoring, reporting, participation and surveillance. When an organisation comes under a cyber-attack, the target is likely to perceive it as an isolated event, as it attempts to respond thereto. Regulatory and Supervisory Authorities, however, are able to put the event into a larger (and perhaps National) context and to respond on a regional, national or international scale, as needed. If organisations are successful in this endeavour, their members will feel more secure about the violability of data, including that exchanged in the facilitation of transactions. Innovation and investment in technology will thrive within an environment nurtured by smart, strong Authorities and organisations governed thereunder.

The Cyber Resilience Oversight Guidelines for the Arab Region, concerning Financial Market Infrastructures identifies, describes and compares the range of observed Financial Market Infrastructure regulatory and supervisory cyber-resilience practices across jurisdictions, particularly the Arab region, but too looking internationally at best practices, operational efforts of various organisations globally; and applying same in context for guidelines of expectations of regulatory and supervisory authorities, for adoption, implementation and observance by their members and organisations under their umbrella of jurisdiction.

It is to be noted that regulators generally may not presently have formally adopted or implemented or a specific cyber strategy. Despite this, all regulators do vehemently expect organisations to maintain adequate competence and capability in this area, as part of their global strategies. For this reason, it is advisable for regulators to issue an advisory notice as a mandate to this effect, in anticipation of the preparation and drafting of regulatory strategies, policies and frameworks, for formal publication, promulgation, adoption and implementation, as, when and how-ever appropriate.

Due to the fact that cyber-risks pose ever-growing, ever-evolving and unique challenges to organisations, it must be acknowledged (with a sufficient degree of understanding and appreciation) that supervisors require dedicated attention and resourcing. Regulators expect that organisations will minimise their cyber risk exposure by means of ensuring that systems are “secure-by-design”, where foundationally software and hardware development aim to ensure that systems are free from vulnerabilities (or at least best protected against vulnerabilities) and best impervious to attacks, in so far possible, through such measures as continuous testing, authentication safeguards and adherence to best programming practices. Emphasis is to be placed on resilience, having due regard of current threats, as opposed to ensuring mere compliance to a standard<sup>14</sup>, without due reflection on whether there may be unique threats that the regulations may not or do not address – particularly given the constant evolution of threats and changes in technology, the possibility of new attack mechanisms and vulnerabilities must always be taken into account. It is important that organisations adequately assess what is required for their specific organisational circumstances, size, and activities undertaken, with due regard of Regulator’s expectations, as highlighted in this report.

Please be advised that this framework builds upon existing international standards of cybersecurity for Financial Markets Infrastructures (FMIs). The framework does not specifically advise on the different levels of expectations, however, does include several recommended listed actions, which will by necessity require Organisations to adequately capture their diversity of sophistication and criticality of each FMIs individualist operations.

---

<sup>14</sup> <https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6>

## 1. Brief introduction: Financial Market Infrastructures<sup>15</sup>

Financial Market Infrastructures (FMIs) (also referred to as “organisation” for ease of reference) are multilateral systems existing and operating amongst participant institutions and operators of such systems, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.<sup>16</sup>

The efficient, effective and secure operation of organisations are of paramount importance for the preservation and advancement of financial stability and economic growth. Improper or ineffective management, or the mismanagement of organisations may result as catalysts of financial shocks, or vehicles through which these shocks are transmitted across domestic and/or international financial markets.<sup>17</sup> Financial shocks may include: liquidity dislocations<sup>18</sup> in the banking system, a stock market crash across domestic and international financial markets, unpredictable changes in monetary policy, or the rapid devaluation of a currency.<sup>19</sup> In this context, the level of cyber resilience, which contributes to an organisation’s operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy.<sup>20</sup> Due to the fact that organisations differ in terms of organisational / corporate structuring, set-up, operations and cross-border presence, each organisation should engage and closely liaise with its respective regulatory authorities to determine its requirements to establish, implement and review its cyber governance arrangements – in example: through a steering committee, common strategy and framework, *etcetera*.<sup>21</sup>

## 2. Cyber Governance

### 2.1 Brief introduction: Cyber Governance:<sup>22</sup>

Cyber governance, traditionally defined, concerns the organisational arrangements for the creation, implementation, examination and review of its approach to managing cyber-related risks (or perils), as well as cyber-attacks.

Effective cyber governance requires a clear and comprehensively formulated cyber resilience framework (as instructive directives) within the organisation’s operational ecosystem, which prioritises the security, productivity and efficiency of its operations, with the aim of mitigating the risk of cyber-attacks, the related disruptions and to maintain a cyber-resilient environment, in doing so, ultimately supporting and preserving the objectives of financial stability, financial shock resistance and economic growth.

<sup>15</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>16</sup> Bank for International Settlements and International Organisation of Securities Commissions

2012, Committee on Payment and Settlement Systems, Technical Committee of the International Organisation of Securities Commissions Principles for financial market infrastructures; <https://www.bis.org/cpmi/publ/d101a.pdf>

<sup>17</sup> <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>18</sup> Working Paper Series NO 1522 / march 2013, What does a financial shock do? First international evidence, European Central Bank, 2013; <https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1522.pdf>

<sup>19</sup> Economic Shock, reviewed by Jim Chappellow, Updated October 11, 2019: <https://www.investopedia.com/terms/e/economic-shock.asp>

<sup>20</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, December 2018

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>21</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank,

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>22</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank,

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

Strong cyber governance:

1. requires an organised, systematic and proactive approach within an organisation, in management of both the prevailing, as well as emerging cyber threats that it faces, or may face;
2. supports efforts to appropriately and adequately consider, as well as manage, cyber risks at all levels within an organisation's ecosystem; and
3. provides for the allocation of adequate resources and expertise to manage cyber-related risks and attacks, within an organisation.

## **2.2 Cyber Resilience Strategy and Framework:<sup>23</sup>**

An organisation's cyber resilience framework should be governed by a cyber resilience strategy.

A cyber resilience strategy defines, dictates and identifies:

1. the manner in which an organisation's cyber resilience objectives are determined;
2. key role players, support members or personnel, as well as internal and external resources for the implementation and proper functioning of the strategic directives and processes to follow;
3. the people, processes and technologies requirements for the proper management of cyber risks; and
4. the manner in which to communicate and timeously collaborate with relevant stakeholders or participants, in order to:
  - 4.1. effectively and expeditiously respond to; as well as
  - 4.2. to recover from cyber-attacks.

### **2.2.2 Risk Management and Ancillary Components:<sup>24</sup>**

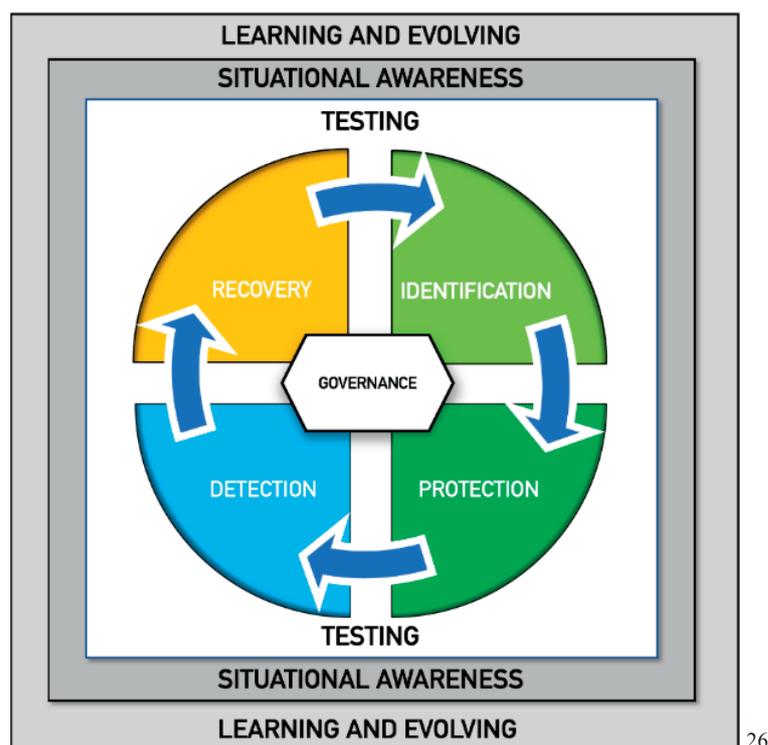
Broadly speaking, an organisation's cyber resilience framework should have the necessary consideration of various components, detailed hereunder:<sup>25</sup>

1. Cyber risk management components, including: Governance; Identification; Protection; Detection; as well as Response and Recovery.
2. Ancillary components, including: Testing; Situational awareness; as well as
3. Learning and evolving.

<sup>23</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>24</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>25</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)



### 2.2.3 Key Considerations:<sup>27</sup>

In the preparation, formulation and documentation of an organisation's cyber resilience strategy, the organisation is advised to ensure that the following aspects and considerations are included in the make-up and execution of such strategy:<sup>28</sup>

1. The value and importance of cyber resilience to the organisation and its key participants (in example: its stakeholders), which may include: proprietors / owners, investors, customers / clients, suppliers / vendors, employees / personnel, contractors, appropriate Legal and Regulatory authorities, appropriate industry bodies and also, competitors;
2. The organisation's overall business vision, objectives, corporate strategy and other strategies which relate to or impact its cyber resilience, which may include: safeguarding the organisation's ongoing operations, efficiency and the financial viability of its services to its users, clients and/or customers *etcetera*;
3. The timeous and effective identification, mitigation and management of its cyber risks;
4. Assessment of the organisation's cyber risk appetite, so as to ensure that it remains proportionate to the organisation's risk tolerance.

<sup>26</sup> Designed by Leon Andrew de Lange, 18 October 2019; with credit to CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>27</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank,

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>28</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank,

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

5. Maintaining and encouraging the organisation's capability to antedate, anticipate, mitigate against any cyber risks; also to withstand at the onset and contain any cyber-attacks, in addition to the effective recovery from any such attacks;
6. Clear, credible and attainable cyber maturity goals, together with a timeline and/or implementation plan for change delivery, planning and acquiring skills (capabilities) relating to its people, processes and technology. Most importantly – in doing so, also keeping up to date with an ever-evolving threat landscape, criticality rating and maintaining proportion thereof in relation to the organisation's size.
7. The cyber resilience strategy should clearly set out the manner in which this implementation plan will be delivered, as well as the tracking and monitoring of such timeous and proper delivery. This is the responsibility of the organisation's Board (or its equivalent within the organisation).
8. An organisation's cyber resilience framework must properly describe the roles and responsibilities, which includes responsibility for decision-making within the organisation, for the identification, mitigation and the management of cyber risks; and together with this: the manner in which cyber resilience initiatives will be adopted, implemented, executed, managed and funded.
9. In respect of funding considerations, a comprehensive and realistic costing and budgeting process is to be followed by the organisation, with due consideration of an organisation's organisational capabilities in terms of cyber resilience.
10. The cyber resilience strategy requires considerable and careful scrutinization, assessment for the procurement of resources, which includes sufficient budget and funding resources for payment towards the decided high-level scope of technology and assets for use of the set-up or upgrading of cyber resilience, as well as the management and maintenance thereof within an organisation.
11. Determining the governance which is necessary to enable cyber resilience to be adequately designed, transitioned, operated and improved on by means of cyber resilience maturity, skills sophistication and capability evolvment.
12. The execution and integration of cyber resilience across the entire organisation's ecosystem is of paramount importance. This ecosystem includes its people, processes, technology and new business initiatives. This further requires integration within the organisation's various commercial departments, including: business, finance, risk management, internal audit, operations, cybersecurity, information technology (IT), communications, legal and human resources - some of which may be outsourced and external to the organisation.
13. An organisation's cyber resilience framework should methodically incorporate the necessary policies, procedures and controls related to the risk management and ancillary components (referred to in paragraph 2.2.2 to *supra*). This specifically includes the governance, identification, protection, detection, response and recovery, testing, situational awareness, as well as learning and evolving within an organisation.

14. An organisation should have knowledge and make use of the prevailing, up to date international, national and industry-level standards, guidelines and recommendations, including: NIST<sup>29</sup>, COBIT<sup>30</sup>, ISO/IEC 27000<sup>31</sup>, ISO/IEC 27001<sup>32</sup> and CPMI-IOSCO Guidance<sup>33</sup> *etcetera*. These sources aim to document industry best practices in the management of cyber threats. There remains a duty upon the organisation to ensure the sources are current and valid, amidst an ever-evolving cyber threat landscape and to use such aids as a benchmark for designing its cyber resilience framework. An organisation is further expected to use these sources for the integration of the most effective and operational cyber resilience solutions, fit for purpose to the organisation in its cyber resilience framework and strategy.
15. Consistency should be observed between an organisation's cyber resilience framework and its enterprise's risk management framework<sup>34</sup>.
16. The organisation's Board should approve its cyber resilience framework and ensure that it is commensurate with the organisation's formulated cyber resilience strategy.
17. The organisation should use maturity models and define relevant cyber resilience baselines and assessment metrics to assess, measure and determine the suitability and efficacy of its cyber resilience framework, as well as the organisation's level of adherence thereto, by use of sovereign and independent compliance programmes, in addition to carrying out audits by qualified internal members of staff, or on an outsourced basis, regularly so.
18. An organisation should consider internal and external stakeholders' priorities and their noteworthy requirements.
19. An organisation should consider interactions with third party or other participants, which may include Regulators, industry bodies, peer organisations *etcetera*, in respect of information sharing.

In the continuous development and maturing of an organisation's cyber resilience strategy and framework, advancement and innovation are key considerations to be had. Such key considerations are further detailed hereunder:

20. An organisation's Board (in consultation with Senior management and the appropriately trained, skilled and informed technical personnel) should review its cyber resilience strategy and framework (including all policies, procedures and controls related thereto), at least twice a year (bi-annually), or as often as needed; and update it (as approved by the Board), whenever necessary.

---

<sup>29</sup> National Institute of Standards and Technology; <https://www.nist.gov/>

<sup>30</sup> COBIT 5: A Business Framework for the Governance and Management of Enterprise IT;

[https://books.google.ae/books/about/COBIT\\_5.html?id=1iLKVIOI9EC&source=kp\\_book\\_description&redir\\_esc=y](https://books.google.ae/books/about/COBIT_5.html?id=1iLKVIOI9EC&source=kp_book_description&redir_esc=y)

<sup>31</sup> [https://www.iso.org/search.html?q=27000&hPP=10&idx=all\\_en&p=0&hFR\[category\]\[0\]=standard](https://www.iso.org/search.html?q=27000&hPP=10&idx=all_en&p=0&hFR[category][0]=standard)

<sup>32</sup> <https://www.iso.org/isoiec-27001-information-security.html>

<sup>33</sup> CPMI-IOSCO Guidance on Cyber Resilience for Financial Market

Infrastructures (CPMI-IOSCO Guidance); <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf>

<sup>34</sup> Risk Management Framework: a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. [https://en.m.wikipedia.org/wiki/Risk\\_management\\_framework](https://en.m.wikipedia.org/wiki/Risk_management_framework)

21. In doing so, an organisation should consider the following factors:
- a.) The ever-evolving threat landscape, which includes the consideration of risks associated with: the supply chain, use of cloud services, social networking, mobile applications, the internet of things (IoT) *etcetera*;
  - b.) Threat intelligence on threat actors; new tactics, techniques and procedures which may specifically impact an organisation;
  - c.) The findings and results of risk assessments carried out of the organisation's critical functions, key roles, procedures, information assets, third-party service providers and interconnections;
  - d.) Actual cyber incidents that have impacted the organisation directly; or external cyber incidents from its ecosystem or other source(s);
  - e.) Lessons learned from audits and tests on the organisation's cyber resilience framework and strategy;
  - f.) The organisation's performance against the relevant cyber resilience baselines, aptitude or performance metrics, as well as maturity models; and
  - g.) New business developments and future strategic objectives of the organisation.
22. With proper investigation into and the review of findings, together with application of the listed considerations, the organisation's cyber resilience strategy and framework must determine how the organisation will continuously review, as well as proactively identify, mitigate and manage the cyber risks – risks which the organisation bears and that too, which it in-turn may pose to its participants, other organisations, vendors, vendor products and service providers.
23. Review and Approvals: The cyber resilience strategy should plan and document the organisation's future maturity of cyber resilience, with short and long-term goals. Senior management, together and in consultation with the appropriately trained, skilled and informed technical personnel, should continuously review, improve, amend; subject to approval by the Board, the existing cyber resilience strategy and framework as the desired cyber resilience maturity level and/or cyber risk landscape changes.
24. The organisation should establish the appropriate structures, processes and relationships with the key stakeholders in the ecosystem to continuously and proactively improve the ecosystem's cyber resilience and promote financial stability objectives as a whole.

### **2.3 The Roles and Responsibilities of the Board and Management:<sup>35</sup>**

The clearly defined roles and responsibilities of the organisation's Board (or its equivalent), as well as its management is pivotal to an organisation's cyber resilience support infrastructure.

---

<sup>35</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

An organisation is expected to establish an internal, interdisciplinary steering committee, comprised both various responsible persons, including: members of senior management and appropriate staff (personnel and/or contractors) from various commercial departments or verticals within the organisation's ecosystem [including that of: business, finance, risk management, internal audit, operations, cybersecurity, information technology (IT), communications, legal and human resources (some of which may be outsourced and external to the organisation)], all together to collaboratively develop and implement an appropriate, wide-ranging and comprehensive cyber resilience strategy and framework.

This committee should provide as a platform for the voicing of an array of opinions, interpretations, views, ideas and perspectives to ensure that the organisation's cyber resilience strategy and framework is thorough and holistic in nature.

The framework and strategy should further have due regard of all elements related to organisation's people, regulatory and policy procedures, as well as its technological resources and assets.

In reiteration of the key considerations listed *supra* in paragraph 2.2, and not to be interpreted as a closed list, the steering committee should further:

1. assess and prioritise internal and external stakeholders' needs and expectations;
2. provide direction to senior management on what cyber resilience should achieve;
3. define who makes cyber resilience decisions and in what manner those decisions should be made;
4. consider the organisation's risk landscape and risk appetite / risk tolerance when determining how cyber risks should be addressed;
5. evaluate the manner in which the various commercial units within the organisation are impacted and how they can work together, in a congruent, integrated fashion, in order to achieve enterprise-wide cyber resilience outcomes;
6. assess the manner of monitoring the performance and outcomes of cyber resilience; and intervene if and when necessary, in order to ensure that the specified directives of the cyber resilience strategy and framework are systematically and properly followed;
7. engage in interactions with other participants, organisations and third parties, on areas such as information sharing;
8. determine the governance necessary to enable cyber resilience to be designed, implemented, executed, transitioned, operated and improved;
9. determine the manner in which cyber resilience initiatives will be delivered, managed and funded, including the budgeting process and organisational capabilities;
10. determine the manner in which cyber resilience will be integrated into all aspects of the organisation, which includes people, processes, technology and new business initiatives;

The organisation's Board should in turn:

11. approve the cyber resilience strategy, and should ensure that it is regularly reviewed and updated at least annually according to the organisation's threat landscape to ensure that it remains relevant;
12. be kept regularly informed of the organisation's cyber risk and ensure consistency with the organisation's risk tolerance and appetite, so that it can achieve the organisation's overall business objectives and corporate strategy;
13. create a culture within the organisation's ecosystem which recognises that staff at all levels of the organisation, play a significant role and bare important responsibilities to ensure the organisation's cyber resilience.

In order to carry out the aforementioned responsibilities, the organisation's Board should:

1. ensure that it collectively possesses the appropriate balance of skills, knowledge and experience to understand and assess the cyber risks impacting the organisation;
2. be sufficiently informed of and be further capable of credibly challenging the recommendations and decisions of designated senior management members;
3. the Board should collectively increase its skills and knowledge on cyber security; however, it may also access specific expertise through a Board member with adequate experience, or through experienced internal members, personnel or staff and/or external independent organisation(s) reporting to and advising the Board;
4. ensure that a senior executive (someone who is independent of the organisation, possess the appropriate balance of skills, knowledge and experience, and have sufficient resources and direct access to the Board [in example: a Chief Information Security Officer (CISO)] whom has the responsibility of accountability to the Board for implementing the cyber resilience strategy and framework at the enterprise level;
5. ensure that staff (including senior management) who are responsible for cyber activities have adequate and suitable skills, knowledge and experience, and are sufficiently informed and empowered to make timely decisions;
6. ensure that cyber risks, implementation of the cyber resilience framework and any associated issues appear regularly on the Board's meeting agenda; and that the Board has adequate access to cybersecurity expertise (whether internal or external). Discussions surrounding cyber risk management should be given adequate attention and time on the Board's meeting agenda;
7. cultivate a strong level of awareness of and commitment to the organisation's cyber resilience. To that end, an organisation's Board and senior management should promote a culture that recognises that members and staff at all levels have significant responsibilities in ensuring the organisation's cyber resilience, and lead by example;
8. ensure that behavioural and cultural change is nurtured and conveyed through leadership and vision, with clear and effective messages – including that cyber resilience is everyone's responsibility and liability. This should be communicated throughout the organisation and

could form part of the organisation's charters, policies, vision statements, mandates from senior management, or through cyber awareness campaigns of the organisation;

9. ensure that situational awareness materials are made available to relevant employees when prompted by highly visible cyber incidents, changes to the threat landscape and the impacts of these threats to the organisation, or by regulatory alerts. For example, the organisation could send internal emails about cyber events or post articles on its intranet site;
10. ensure that senior management regularly conducts a cyber resilience self-assessment test, which evaluates the organisation's cyber maturity. The Board should review the self-assessment and take appropriate decisions to improve the effectiveness of cyber activities and integration with the corporate strategy across the organisation;
11. review and approve senior management's prioritisation, time-mapping and resource allocation decisions, based on the results of the cyber (self-) assessments performance against key performance indicators (KPIs) and their progression towards their target state of maturity, and further in cognizance of the organisation's overall business objectives.

Senior management should:

1. regularly provide a written report to the Board on the overall status of its cyber resilience programme, highlighting keys risks and issues. As part of the Board's updates, senior management should provide their budgeting and estimation activities plan for ongoing and future resource requirements, so as to ensure that cyber resilience objectives are continually achieved and maintained;
2. ensure that it has a programme for continuing cyber resilience training and skills development for all members and staff. Such training programmes should include the Board members and senior management; and should be conducted at least once a year (annually). These annual cyber resilience trainings should include: incident response, current cyber threats (e.g. threats, threat actors and vulnerabilities), tactics and techniques (e.g. phishing, spear phishing, social engineering and mobile security) and emerging issues, according to members and staff levels of responsibility and the risks associated with their respective roles;
3. ensure that employees and contractors with privileged account permissions and/or with access to sensitive assets and information, receive additional cyber resilience training commensurate with their respective levels of responsibility;
4. that respective business units are provided with cyber resilience training relevant to their criticality to the business;
5. ensure that it gages and identifies the competencies, skills and resources required for cyber resilience. Senior management can adopt well-known skills frameworks [in example: the Cyber Resiliency Engineering Framework<sup>36</sup>, European e-Competence Framework (e-CF)<sup>37</sup> or the Skills Framework for the Information Age (SFIA)<sup>38</sup>] to determine its organisational needs and further, to implement the cyber resilience strategy and framework within the organisation;

<sup>36</sup> The MITRE Corporation, MITRE Technical Report, Cyber Resiliency Engineering Framework, Deborah J. Bodeau & Richard Graubart, September 2011; [https://www.mitre.org/sites/default/files/pdf/11\\_4436.pdf](https://www.mitre.org/sites/default/files/pdf/11_4436.pdf)

<sup>37</sup> A common European framework for ICT Professionals in all industry sectors, <http://www.ecompetences.eu/>

<sup>38</sup> The Skills Framework for the Information Age framework, <https://www.sfia-online.org/en/framework>

6. continuously review the skills, competencies and training requirements to ensure that it has the right set of skills as technologies and cyber risks evolve;
7. establish and sustain incentives for staff and members (in example: recognition awards) to ensure behaviours and adherence consistency with the organisation's intended cyber risk culture;
8. establish and sustain incentives (e.g. staff recognition awards) to ensure behaviours are consistent with the intended cyber risk culture;
9. produce a formal cyber Code of Conduct or Policy, which can be incorporated into the organisation's enterprise Code of Conduct, and to ensure that all members and staff comply with it;
10. validate the effectiveness of its cyber resilience training programme (in example: the intentional deployment of social engineering or phishing tests) and assess whether training and awareness programmes positively influence the organisation members' behaviour. Further hereto, based on the lessons learned from its training programme, the organisation should improve the employee awareness programmes;
11. measure and report on the implementation, efficacy, consistency and persistence of cyber resilience activities;
12. establish and incorporate a programme for talent recruitment, member and staff retention, as well as succession planning for members and staff, and ensure such persons are aligned to cyber activities and deployed effectively across the organisation;
13. ensure that there are well-defined plans for the succession of high-risk and high-level members of the organisation (in example: senior management, system administrators, software developers and critical system operators *etcetera*). Also, to ensure that the recruitment necessities for key cyber roles include suitable cyber skills, knowledge and experience aligned with the organisation's defined succession plans;
14. ensure that staff performance plans are consonant with compliance with the organisation's cyber resilience policies and standards, in order to hold employees accountable for their actions and failures to act when necessary or timeously so (omission).

An organisation:

1. should ensure that the Board members' and senior managements' understanding of their roles and responsibilities with regard to cyber resilience is regularly assessed, including their knowledge of cyber risks;
2. may use this Cyber Resilience Oversight Expectation Guidelines for the Member States Central Banks of the Arab Countries, concerning Financial Market Infrastructures as the basis for their self-assessments.

## **2.4 Guidance on the Senior Executive or Chief Information Security Officer (CISO) – whichever is elected by an Organisation to fulfil this specific role:<sup>39</sup>**

An organisation should appoint an independent, senior executive, normally a Chief Information Security Officer (CISO), who is responsible for all cyber resilience issues within the organisation, as well as with regard to third parties. The Senior Executive is responsible to ensure that the cyber resilience objectives and measures defined in the organisation's cyber strategy, cyber resilience policies and guidelines are properly communicated both internally and, when relevant, externally to third parties; and that compliance with the strategy, policies and guidelines is reviewed, monitored and adhered to.

An organisation should have its own senior executive or CISO in-house or can outsource this function, depending on the organisation's specific structure and organisational set-up. To the extent permitted by the relevant national authority and in cases of group entities, this could include a group-wide CISO.

The Senior Executive or CISO is responsible for the following primary tasks:

1. Supporting senior management and the Board when defining, compiling and updating the cyber resilience policies, and advising on all cyber resilience issues. This includes helping to resolve conflicting issues, such as costing and budgetary restraints versus cyber resilience goals of an organisation;
2. Actively participating in, observing and facilitating cyber risk management;
3. Producing cyber resilience policies within an organisation and, where required, relevant rules relating thereto, as well as examination of proper compliance and adherence thereto;
4. Influencing and prompting the organisation's cyber resilience processes, monitoring IT service providers' involvement and assisting in any related tasks;
5. Helping to produce and update the organisation's contingency plan with regard to cyber issues;
6. Initiating and monitoring the implementation of cyber resilience measures;
7. Participating in projects relevant to cyber resilience, including the monitoring of security testing of new components, prior to entering the organisation's networks and infrastructures;
8. Acting as a point of contact for any comments, queries or concerns relating to an organisation's cyber resilience, from within the organisation or from external third parties;
9. Investigating cyber incidents, as well as reporting such incidents to the senior management and the Board;
10. Continuously surveying and monitoring threats applicable to an organisation's IT assets;
11. Initiating and coordinating efforts to raise awareness on cyber resilience and training sessions;

<sup>39</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

12. Reporting to senior management and the Board regularly, at least quarterly, and on *an ad hoc* basis on the status of cyber resilience issues within an organisation. This status report should include an evaluation of the cyber resilience situation, compared with the last report; information about cyber resilience projects, cyber risks, cyber incidents and the results of penetration and red team testing.

In terms of organisation and processes, the Senior Executive or CISO must be independent, so as to avoid any potential conflicts of interest and therefore, the following arrangements are expected:

1. The organisational make-up must ensure that the Senior Executive or CISO can act independently from the IT or operations department; and be able to report to senior management and the Board directly, at any time. The Senior Executive or CISO must not be involved in internal audit activities of the organisation;
2. The determination of the necessary resources required by the Senior Executive or CISO;
3. The designation of a suitable and adequate budget for cyber resilience training sessions, within the organisation; and for further training of the Senior Executive or CISO's personnel or team;
4. The requirement for all employees in the organisation and IT service providers to report any incidents relevant to the cyber resilience of the organisation, according to the decided and mandated escalation procedure, within the organisation.

Note: Organisational set-ups may exist where the CISO has a functional reporting line to the Chief Information Officer (CIO), but with guarantees for the CISO to have direct access to senior management and the Board; also, with sufficient resources for the CISO to conduct its role independently.

## **2.5 Skills, Training and Accountability<sup>40</sup>:**

Senior management should:

1. ensure that it has a programme for continuing cyber resilience training and skills development for all staff. This training programme should include the Board members and senior management and should be conducted at least once a year (annually). The annual cyber resilience training should include incident response, current cyber threats (including: threats, threat actors and cyber vulnerabilities), tactics and techniques (including: phishing, spear phishing, social engineering and mobile security) and emerging issues, according to staff members' levels of responsibility and the risks associated with their respective roles;
2. ensure that employees and contractors with privileged account permissions and/or access to sensitive assets and information, receive additional cyber resilience training commensurate with their levels of responsibility, and that business units are provided with cyber resilience training relevant to their criticality to the business;
3. ensure that it identifies the competencies, skills and resources required in order to implement the cyber resilience strategy and framework. Senior management could adopt well-known skills

<sup>40</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

frameworks, such as the Cyber Resiliency Engineering Framework<sup>41</sup>, European e-Competence Framework (e-CF)<sup>42</sup> or the Skills Framework for the Information Age (SFIA)<sup>43</sup> to determine its organisational needs;

4. ensure that it continuously reviews the skills, competencies and training requirements to ensure that it has the right set of skills as technologies and risks evolve;
5. embeds a programme for talent recruitment, retention and succession planning for the staff, and ensure such staff are aligned to cyber activities and deployed effectively across the organisation;
6. ensure that there are well-defined plans for the succession of high-risk staff (e.g. senior management, system administrators, software developers and critical system operators, etc.), and the recruitment requirements for key cyber roles include suitable cyber skills, knowledge and experience in alignment with defined succession plans;
7. regularly benchmark its cyber resilience capabilities against the market to identify its gaps in terms of governance, skills, resources and tools, treating these gaps as cyber risks and addressing them accordingly;
8. actively foster partnerships with industry associations and cybersecurity practitioners to develop solutions for future cyber resilience needs, which will be useful to the organisation and the ecosystem as a whole.

### **3. Information Assets Identification and Classification**

#### **3.1 Identification<sup>44</sup>**

It is of paramount importance that an organisation identifies which of their operations and supporting information assets should be protected against compromise, in order of importance or priority, in the aim of preventing an organisation's operational failure, which in turn can negatively impact financial stability. The ability of an organisation to understand its internal situation and external dependencies is vital to enable the effective and appropriate response to potential cyber threats which may occur.

This process requires an organisation to have full knowledge of its information assets and to fully understand its processes, procedures, systems and all dependencies thereon, in order to strengthen the organisation's overall cyber resilience.

#### **3.2 Classification<sup>45</sup>**

<sup>41</sup> The MITRE Corporation, MITRE Technical Report, Cyber Resiliency Engineering Framework, Deborah J. Bodeau & Richard Graubart, September 2011; [https://www.mitre.org/sites/default/files/pdf/11\\_4436.pdf](https://www.mitre.org/sites/default/files/pdf/11_4436.pdf)

<sup>42</sup> A common European framework for ICT Professionals in all industry sectors, <http://www.ecompetences.eu/>

<sup>43</sup> The Skills Framework for the Information Age framework, <https://www.sfia-online.org/en/framework>

<sup>44</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>45</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

An organisation should identify its business functions and supporting processes, as well as conduct a risk assessment in order to ensure that it thoroughly comprehends the importance of each function, supporting processes, as well as their interdependencies in performing its functions. Identified business functions and processes should then be classified in terms of criticality, which in turn should guide the organisation's prioritisation of its protective, detective, response and recovery efforts.<sup>46</sup>

An organisation should identify and maintain a current inventory of its information assets and system configurations, including interconnections with other internal and external systems, in order to know at all times, the assets that support its business functions and processes. An organisation should carry out a risk assessment of those assets and classify them in terms of criticality. It should identify and maintain a current log of both individual and system credentials to know the access rights to information assets and their supporting systems, and should use this information to facilitate identification and investigation of anomalous activities.<sup>47</sup>

An organisation should integrate identification efforts with other relevant processes, such as procurement and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials and its inventory of information assets so that that they remain current, accurate and complete.<sup>48</sup>

In consideration of the above, an organisation should:

1. identify and document all of its critical functions, key roles, processes and information assets that support those functions, and maintain updated records of this information on a regular basis;
2. identify and document all processes that are reliant (dependent) on third-party service providers and identify its interconnections, as well as update this information on a regular basis;
3. maintain an up-to-date inventory of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections. This inventory should assimilate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its inventory;
4. have an enterprise wide risk management framework to identify risks, as well as to conduct risk assessments on a regular basis, of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections to determine, classify and document their level of criticality;
5. create and maintain a basic network map of network resources, with an associated plan addressing Internet Protocols (IPs) which locate routing and security devices and servers supporting the organisation's critical functions, and which identify links with the outside world, or external to the organisation's network;
6. conduct risk assessments prior to deploying new and/or updated technologies, products, services and connections to identify potential threats and vulnerabilities. It should also update its risk assessment in case new information affecting cybersecurity risks is identified (in example: any new threat, vulnerability, antagonistic test result, hardware change, software change or configuration change). The findings of the risk assessments should be incorporated in terms of necessary actions into the cyber resilience strategy and framework;

<sup>46</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>47</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>48</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

7. have and maintain a fully comprehensive inventory of all individual and system accounts (in particular, privileged and remote access accounts) so that the organisation is aware of the access rights to information assets and their supporting systems. The organisation should review and update this inventory on a regular basis;
8. use automated tools and feeds [in example: a centralised asset inventory management (AIM) tool] that enables the organisation to support the identification and classification of the critical functions, processes, information assets and interconnections. The organisation should ensure that the inventory is updated accurately and that these changes are communicated with the relevant staff in a timely manner;
9. further use automated tools and feeds (as described in paragraph 8 *supra*) that enable the organisation to support the identification and classification process of roles, user profiles and individual and system credentials; and to ensure that these are updated accurately and that relevant staff are informed of the changes in a timely manner;
10. maintain an up-to-date and complete map of network resources, interconnections and dependencies, and data flows with other information assets. This includes the connections to business partners, internet-facing services, cloud services and any other third-party systems. The organisation should use these maps to undertake risk assessments of key dependencies and apply appropriate risk controls, whenever necessary;
11. update its inventory to document new, relocated, repurposed and sunset information assets, on a regular basis or when these changes occur;
12. use automated tools and feeds (as described in paragraph 8 *supra*) in order to identify emerging risks, update its risk assessments in a timely manner and take the necessary mitigating actions, in line with the organisation's risk tolerance;
13. identify the cyber risks that it bears from or poses to entities within its ecosystem. The organisation should too coordinate with relevant entities, as appropriate. This may involve identifying common vulnerabilities and threats, and taking appropriate measures collectively to address such risks, with the objective of improving the ecosystem's overall resilience.

### **3.3 Management of Interconnections with Third Parties:**<sup>49</sup>

There are evident challenges recognised in gaining the reassurance of an entity's cyber-resilience, both for regulators in relation to organisations, and for organisations in relation to their third-party service providers. Extensive use of third-party services increases the challenge for organisations and regulated institutions themselves to have full visibility of the controls and implemented measure, as well as their reciprocal level of risk.

---

<sup>49</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

For purposes of identifying the range of practices in relation to cyber-resilience, “third parties” is broadly understood to include:<sup>50</sup>

1. all forms of outsourcing, including cloud computing services;
2. standardised and non-standardised services and products that are typically not considered to be outsourcing, in example: power supply, telecommunication lines, commercial hardware and software, *etcetera*;
3. interconnected counterparties, such as other institutions (of a financial nature or not) and FMIs, in example: payment and settlement systems, trading platforms, central securities depositories and central counterparties.

In terms of Cyber-resilience practices concerning third parties, prudent analysis is to be had of the following: governance of third-party interconnections; business continuity and service availability; information confidentiality and integrity; specific expectations and practices regarding visibility of third-party interconnections; auditing and testing; as well as resources and skills.<sup>51</sup>

### **3.2.1 Impact to and from an Organisation’s Ecosystem:<sup>52</sup>**

An organisation’s systems and processes are directly or indirectly interconnected with the systems and processes of the entities within its ecosystem, including: participants, linked organisations, settlement banks, liquidity providers, service providers, critical infrastructures (in example: energy / power supply and telecommunications), as well as vendors and their products. Consequently, regard is to be had to these third parties’ interconnectivity to an organisation’s network, as their cyber resilience could have significant consequences in imposing cyber risks to other organisations which it is connected with. Further hereto, the degree of risks they may pose to an organisation may be disproportionate to the essentiality or criticality of their business relationship with the organisation.

It is essential for an organisation to identify what cyber risks it bears from and also, that which it poses to entities within its ecosystem, in terms of the interconnectivity that is shared and to synchronize with such relevant entity (entities), as appropriate, in so far as their personal design and implementation of cyber resilience efforts are concerned - with the common objective of improving the overall resilience of the overall ecosystem.

### **3.2.2 Risks from Interconnections:<sup>53</sup>**

An organisation should implement protective and defensive measures to mitigate risks arising from entities within its ecosystem, from the interconnectivity it shares with such entities. The appropriate controls for each entity will depend on the risk that such entity poses to an organisation and also, in consideration of the nature of the relationship with such entity. In view of its general and functional importance to the organisation, as well as its unique position in the financial system, an organisation

<sup>50</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>; Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbcs/publ/d454.pdf>

<sup>51</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>; Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbcs/publ/d454.pdf>

<sup>52</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>; Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbcs/publ/d454.pdf>

<sup>53</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>; Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbcs/publ/d454.pdf>

should implement measures to mitigate effectively the risk arising from its connected entities. Such measures include that:

1. an organisation's participation of interconnectivity requirements should be designed to ensure that they adequately support its cyber resilience framework;
2. an organisation's framework to manage its relationship with service providers within its ecosystem should address and be designed to mitigate cyber risks, on par or better than its level of cyber resilience. At a minimum, an organisation should ensure that its outsourced and interconnected services confer the same level of cyber resilience needed if their services were provided by the organisation itself.

Cyber resilience and risk considerations should be a fundamental part of the organisation's management and relations with service providers, vendors and vendor products in respect of contracts, performance, relationships and risk. Contractual agreements between the organisation and its service providers / vendors should ensure that the organisation, as well as relevant authorities, are provided with or have full access to the information necessary to assess the cyber risk arising from the service provider / vendor.

It is advisable that contracts be concluded between Organisations and service providers / vendors detailing the rights and responsibilities of both an Organisation and their third-party connection (service provider / vendor) with respect to risk. Within an organisation, the responsibility for reviewing, approving and signing / concluding contracts is to be allocated to an appropriate person, by the Board and Management of an Organisation. Such contracts serve to include:<sup>54</sup>

1. the generic rights, obligations, roles and responsibilities of both parties, namely: the Organisation and the service provider / vendor;
2. the possible risks and reciprocal mitigating measures which each party is exposed or responsible for, albeit stated mostly in broad, generalist terms;
3. a description of the nature of the service and or vendor product(s);
4. the expected results of the third party (outsourcing) relationship that is shared between the parties;
5. analysis and clauses addressing the:
  - a. strategic risk;
  - b. compliance risk;
  - c. security risk (such as security monitoring, patch management, authentication solutions, authorisation management and data loss/breach procedures);
  - d. business continuity risk;
  - e. service provider / vendor lock-in risk<sup>55</sup>;
  - f. counterparty risk (such as the visibility into the service provider's organisation);
  - g. country risk;
  - h. contractual risk;
  - i. access risk (in example: that financial institutions, their supervisors and/or agents cannot audit the third-party connection due to inadequate contractual agreements);
  - j. concentration risk<sup>56</sup>; and

<sup>54</sup> Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>55</sup>In economics, vendor lock-in, also known as proprietary lock-in or customer lock-in, makes a customer dependent on a vendor for products and services, unable to use another vendor without substantial switching costs. This includes the general ability of an organisation to withdraw from the service provider / vendor and to absorb the outsourced, third party service(s) / product(s), or transfer it to another service provider; [https://en.wikipedia.org/wiki/Vendor\\_lock-in](https://en.wikipedia.org/wiki/Vendor_lock-in); Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>56</sup> "Concentration risk" in this context does not refer to the potential systemic risk to the industry as a whole, but rather to the potential lack of control of an individual firm over one single provider as multiple activities are outsourced to the same service provider. These different aspects of

k. rights to inspect and audit.<sup>57</sup>

### **3.2.3 Data-Sharing Agreements:<sup>58</sup>**

In the event of a successful cyber-attack that compromises the integrity of an organisation's data, a successful recovery may require obtaining uncorrupted data from third parties and/or participants of an organisation's ecosystem of service providers, vendors, or others. Organisations should consider setting up appropriate data-sharing agreements with relevant third parties or participants in advance and prior to a cyber-attack incident, in order to enable such uncorrupted data to be received from and recovered by an affected organisation, in a timely manner.

### **3.2.4 Contagion / Contamination:<sup>59</sup>**

In the event of a large-scale cyber incident and due to the fact that an organisation's systems and processes are often interconnected with the systems and processes of other entities within its ecosystem, it is possible for an organisation to pose a contagion (contamination) risk, both to, or be exposed to contagion risk from its ecosystem. This may include the propagation of malware or corrupted data. An organisation should work together with its interconnected entities within its ecosystem in order to ensure the continuation of operations (of which critical services are primary responsibilities) as soon as it is possible, safe and practicable to do so, without causing unnecessary exposure to risk to the wider sector, if the risk has not been properly contained or ousted from the organisation's network or related infrastructure, or cause further exposure to loss in financial stability.

Please refer to paragraph 6.3.1. below on "*Contagion and Communicability*" for proposed guidelines hereon.

### **3.2.5 Crisis Communication and Reporting:<sup>60</sup>**

Organisations should plan in advance for crisis reporting to its ecosystem participants, interdependent organisations, authorities and others, including service providers and, where relevant, the media. Reporting plans should be developed through an adaptive process based on scenario-based planning and through analysis. Regard should further be had to prior experiences of an organisation or similar entities, where this information is available. The rapid escalation of cyber incidents may be necessary and organisations should determine decision-making responsibilities for incident response in advance, and implement clearly defined escalation and decision-making procedures. Organisations should inform relevant oversight and regulatory authorities promptly of potentially material or systemic events and incidents.

---

concentration risk are explained in Joint Forum, Outsourcing in financial services, February 2005; and Committee of European Banking Supervisors, Guidelines on outsourcing, December 2006; Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>57</sup> Organisations are generally required to monitor their providers' compliance by testing and auditing the security requirements for outsourcing and cloud computing providers, although no specified form of testing is provided; Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>.

<sup>58</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>59</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>60</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

Please refer to paragraph 6.3.2. below on “*Crisis Communication and Responsible Disclosure*” for proposed guidelines hereon.

### **3.2.6 Responsible disclosure policy:<sup>61</sup>**

Organisations should have a policy and procedure to enable the responsible disclosure of potential vulnerabilities. Such procedure should make provision to prioritise disclosures that could facilitate early response and risk mitigation by stakeholders, for the benefit of the ecosystem and broader financial stability.

Please refer to paragraph 6.3.2. below on “*Crisis Communication and Responsible Disclosure*” for proposed guidelines hereon.

### **3.2.7 Incident handling preparation phase for anticipatory Forensic Readiness<sup>62</sup>**

Incident handling forms part of daily operations by a security team or outsourced SOC. Organisations, as part of an incident handling preparatory (anticipatory) phase and prior to the reactive measure of conducting a forensic investigation (post serious incident), should have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process. In order to facilitate proper incident handling preparation for anticipatory forensic readiness, Organisations should establish relevant system logging policies that include both the types of logs to be maintained, as well as their data retention periods.

It is to be noted that forensic analysis, post incident, may need to be pended in certain circumstances, including in the event of contamination or contagion giving rise to financial stability concerns and in such circumstances, Information and Communications Technology (ICT) resources may be primarily focused on recovering critical systems, Organisations should take appropriate steps to ensure that investigations can still be performed after the event, through reasonable means, such as the preservation of necessary system logs and other evidence, for investigative analysis.

Please refer to paragraph 6.4. below on “*Forensic Readiness*” for proposed guidelines hereon.

### **3.2.8 Auditing and Testing:<sup>63</sup>**

Although organisations are generally required to monitor their providers’ compliance, it is further advisable that organisations secure their “rights to inspect and audit” any internal or external third-party connections and can do so by means of including such provision in a contract between the organisation and the third party. The audit and reporting service can be facilitated independently (to better ensure the audit’s effectiveness and efficiency) and should at least be carried out on the critical interconnections with third parties.

## **4. Protection and Risk Management:**

<sup>61</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>62</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>63</sup> Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>.

## 4.1 Protection of Processes and Assets<sup>64</sup>:

Cyber resilience depends on effective security controls, along with system and process design that protects the confidentiality, integrity, availability and safety of an organisation's assets and services. These measures should be proportionate to an organisation's threat landscape and systemic role in the financial system and be consistent with its risk tolerance.

### 4.1.1. Control implementation and design:<sup>65</sup>

An organisation should:

1. implement an all-inclusive and suitable set of security controls that will facilitate the achievement of the security objectives needed to meet its business requirements;
2. implement security controls based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections, as per the risk assessment in the identification phase. The security objectives may include ensuring:
  - a) the continuity and availability of its information systems;
  - b) the integrity of the information stored in its information systems, both in use and in transit;
  - c) the protection, integrity, confidentiality and availability of data while stagnant (at rest), during use and in transit;
  - d) adhering to applicable laws, regulation(s) and standards.
3. develop its security controls in order to facilitate cybersecurity, physical security and people (human) security. The controls should be designed according to the threat landscape, prioritised in accordance risk-based security controls and aligned to the organisation's business objectives;
4. evaluate the efficacy of its security controls regularly and where necessary, to adapt them to its evolving threat landscape. Security controls should be monitored and audited regularly to ensure that they remain effective and have been applied to all assets where they may be required;
5. capture security requirements, together with system and process requirements in the design, development and in acquiring its systems and processes, in order to identify the security controls necessary for protecting its systems, processes and data, at the earliest possible stage;
6. apply a defence in depth (also known as Castle Approach)<sup>66</sup> strategy in line with a risk-based approach. In example: an organisation should implement several independent security controls so that if one control fails or if a vulnerability is exploited, alternative controls will be able to protect targeted assets and/or processes;
7. develop and implement a bespoke information security management system (ISMS), which could be based on a combination of well-recognised international standards (in examples: ISO

<sup>64</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>65</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>66</sup> an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical security for the duration of the system's life cycle; [https://en.wikipedia.org/wiki/Defense\\_in\\_depth\\_\(computing\)](https://en.wikipedia.org/wiki/Defense_in_depth_(computing))

27001, ISO 20000-1 ISO 27103 and ISO 27002 *etcetera*)<sup>67</sup>, in order to create, implement, operate, continuously monitor, review, maintain and improve an organisation's comprehensive cybersecurity control framework;

8. consider cyber resilience at the initial and earliest stage of system design, development and procurement, as well as throughout the system development life cycle, so that vulnerabilities in software and hardware are minimised and further, so that security controls are incorporated into systems and processes from their inception. An organisation should adopt a bespoke system development life cycle methodology that embeds the resilience by design<sup>68</sup> approach when designing, constructing, procuring or modifying its systems, processes and products. At each stage of the system development life cycle, the organisation should manage its cyber risk and integrate resilience based on risk analysis results;
9. frequently review its information security management system using certification methods, running audits or other relevant methods of assurance;
10. develop processes, procedures and explore potential technologies to constantly alter and refine an organisation's security controls. This will help it to ensure it is protected against known and emerging threats, based on knowledge and best practices obtained from other organisations across the ecosystem and through the use of threat intelligence.

#### **4.1.2 Network and Infrastructure Management:<sup>69</sup>**

An organisation should:

1. establish a secure boundary that protects its network infrastructure, by means of tools (in example: a router, firewall, intrusion prevention system (IPS) or intrusion detection system (IDS), virtual private network (VPN), demilitarised zone (DMZ) or proxies *etcetera*). The boundary should identify trusted and untrusted regions / zones according to the organisation's risk profile and criticality of information assets, contained within each zone. Further, appropriate access requirements should be implemented within and between each security region, in accordance with the principle of least privilege;
2. seek to use an isolated and dedicated network for information system administration. At a minimum, the organisation should prohibit direct internet access from devices or servers used for information system administration, whenever possible;
3. establish a foundational system and security configurations for information systems and system components, including devices used for accessing the organisation network remotely, to help the configuration to those systems and security reinforcement thereof, as well as for components to be applied consistently. These foundations should be documented, formally reviewed and regularly updated, so as to adapt them to the organisation's evolving threat landscape;

<sup>67</sup> <https://www.iso.org/ics/35.030/x/>

<sup>68</sup> Cyber Resiliency Design Principles, Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines, MIT R 1 7 00 0 1 MIT R E T E C H N I C A L R E P O R T; © 2017 The MITRE Corporation. Approved for Public Release; Distribution Unlimited. Case No. 17-0103.

<https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf>

<sup>69</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

4. strengthen its network infrastructure and information systems utilising recognised industry security standards. Any changes to system configurations should be strictly controlled and monitored; and programmes that can alter or override system configuration should be restricted. This should also be applicable to devices and environments used for accessing the organisation network remotely;
5. pursue using secure network protocols, in example: Secure Shell<sup>70</sup> and protocols relying on transport layer security or such equivalent, when needed and appropriate, in order to guarantee the confidentiality and integrity of information and data exchanged within an organisation's network and beyond such network, as in the case of isolated and remote connections thereto.
6. define and implement procedures that limit, lock and terminate system and remote sessions after a set, pre-defined period of inactivity or when set, pre-defined conditions are met;
7. deploy a vast range of technologies and tools to detect and block actual and attempted attacks or intrusions. For this purpose, an organisation may use intrusion detection or prevention systems, end point security solutions - in example: antivirus, firewalls, a host intrusion detection system, host intrusion prevention system, an access gateway or a jump box *etcetera*, particularly so on devices and in environments used for accessing the organisation network remotely;
8. implement controls that manage or prevent non-controlled devices to connect to its internal network from within or outside the location premises, so as to ensure that activities in these areas are logged and monitored for inappropriate use or attempts to access business systems. The organisation's infrastructure should be scanned regularly to detect rogue devices and access points;
9. scan its legacy system technologies regularly to identify potential vulnerabilities and pursue upgrade opportunities. Controls and additional defence layers should be implemented and tested in order to protect unsupported or vulnerable systems;
10. have policies and controls that prevent users from installing unauthorised applications. Procedures for change controls should be in place to manage the installation of applications;
11. implement a defence in depth security architecture, based on the network and data flow diagrams which identify hardware, software and network components, internal and external connections; and types of information exchanged between systems. As required in the identification phase, the organisation should maintain current and complete network and data flow diagrams; segment its network infrastructure with security policies appropriate to its use and proportionate to its risk score, which define proper access policy to systems and applications. Sensitive traffic between systems and zones should be segregated by means of network management.
12. ensure that the organisation's IT environments and functions should be adequately separated with different security levels and controls implemented.
13. implement technical measures to prevent the execution of unauthorised code on organisation-owned or managed devices, network infrastructure and system components;

---

<sup>70</sup> Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network; <https://www.ssh.com/ssh/>; [https://en.wikipedia.org/wiki/Secure\\_Shell](https://en.wikipedia.org/wiki/Secure_Shell)

14. consider implementing technical measures, such as: network access control solutions, in order to prevent unauthorised devices from being connecting successfully;
15. employ automated mechanisms to help maintain an up to date, comprehensive, accurate and readily available baseline of system and security configurations for the information system and system components. These mechanisms may include hardware and software inventory tools, configuration management tools and network management tools;
16. implement automated mechanisms that can isolate affected information assets in the case of any adverse event;
17. in the context of a defence in depth strategy, the organisation should seek to implement cyber deception capabilities and techniques that enable it to bait / entice the attacker and trap it in a restricted and secluded environment (in example: a sandbox)<sup>71</sup> where all activities can be contained and analysed, allowing the organisation to gain vital threat intelligence that will help to improve its protection controls.

#### **4.1.3 Logical and Physical Security Management:<sup>72</sup>**

Logical Security consists of software safeguards for an organisation's systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. It is a subset of computer security.<sup>73</sup> Logical Security Management is the responsibility of an Organisation's information security teams and is implemented through Organisational policy.

Physical Security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).<sup>74</sup> Physical security involves the use of multiple layers of interdependent systems that can include Closed-circuit television (CCTV) or video surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, deterrent systems, fire protection, and other systems designed to protect persons and property.<sup>75</sup>

An organisation should:

1. identify and restrict physical and logical access to its system resources to the minimum level required for legitimate and authorised work activities, in line with the principle of least privilege;
2. establish policies, procedures and controls that oversee access privileges and the administration of access. The information system access should be evaluated regularly to identify unnecessary access or privileges. Physical, logical and/or remote access to critical systems should be

<sup>71</sup> In example: Anomali Threatstream platform with built-in sandbox capability; <https://www.anomali.com/products/threatstream>

<sup>72</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>73</sup> Logical security; Wikipedia; [https://en.wikipedia.org/wiki/Logical\\_security](https://en.wikipedia.org/wiki/Logical_security)

<sup>74</sup> Chapter 1: Physical Security Challenges". Field Manual 3-19.30: Physical Security. Headquarters, United States Department of Army. 2001. Archived from the original on 2013-03-13.

<sup>75</sup> Physical security; Wikipedia; [https://en.wikipedia.org/wiki/Physical\\_security#cite\\_note-1](https://en.wikipedia.org/wiki/Physical_security#cite_note-1)

restricted, logged and unauthorised access should be blocked. Administration rights on systems should be strictly limited to operational needs. Procedures should be in place for a periodic review of all access rights;

3. create and manage user accounts in accordance with a work role-based access control scheme that organises allowed information system access rights and privileges in line with users' roles. Role assignments should be reviewed regularly by appropriate staff (such as: management and system owners) in order to take appropriate action when privileged role assignments are no longer appropriate;
4. establish processes to manage the creation, alteration or deletion of user access rights. Such actions should be submitted to and approved by appropriate staff, and should be recorded for review if necessary;
5. implement specific procedures to allocate privileged access on a need to use or an individual event basis. Administrators should have two types of accounts: one for general purposes and another to carry out their administrative tasks. The use of privileged accounts should be closely monitored and controlled. The use of generic / common accounts for administration purpose should be strictly limited and traced. Whenever possible, user and administrator accounts should be nominative and clearly identifiable, by means of using dedicated taxonomy for usernames, which ensures that the positions and roles are not apparent therefrom;
6. have a dedicated policy that covers all the characteristics of its authentication mechanisms (in example: password, smart access cards, tokens and biometrics) and that same is in line with relevant standards, in example: the Digital Identity Guidelines of NIST-800-63).<sup>76</sup> Default and automatically saved authentication settings, including passwords and unnecessary default accounts, should be deactivated, changed or removed before systems, software and/or services go live;
7. develop appropriate controls by means of encryption, authentication and access control, in order to protect data at rest, in use and in transit. The controls should be proportionate to the criticality and the sensitivity of the data held, used or being transmitted, as per the risk assessment conducted in the identification phase;
8. have dedicated controls to prevent unauthorised access to cryptographic keys. Dedicated policy and procedures should be defined for the management of and access to cryptographic materials;
9. implement controls to prevent unauthorised privileged increase or escalation thereof, such as: technical controls that trigger automated notification to appropriate staff in the case of changes to user access profiles;
10. encrypt data as a result of its data classification and risk assessment processes. The organisation should also use encryption and general cryptographic controls in line with recognised standards and processes, which cover aspects such as algorithm, key length and key generation, *etcetera*;
11. implement automated mechanisms to support the management of information system access accounts, which may include implementing security controls embedded in the information

<sup>76</sup> NIST Digital Identity Guidelines; <https://pages.nist.gov/800-63-3/>

system, allowing it to automatically disable and/or remove inactive, temporary and emergency accounts after a set period of time;

12. establish strong governance on identity and access management, enforced by the use of dedicated tools such as Identity and Access Management in a system integrated manner, ensuring all systems update each other consistently;
13. seek to use an attribute-based access control model that allows it to manage access to its IT environment context-sensitive and dynamic manner;
14. employ automated mechanisms that allow user account creation, modification, enabling, disabling and removal actions to be monitored and audited continuously, in order to notify appropriate staff when potential malicious, irregular behaviour or damage is detected.
15. implement adaptive access controls to prevent potential malicious behaviour or damage.

#### **4.1.4 Change and Patch Management:<sup>77</sup>**

Change management is a collective term for all approaches to prepare, support, and help individuals, teams, and organisations in making organisational change. In an IT context, it is an IT service management discipline. The objective of change management is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in the IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes; or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Change management can ensure standardised methods, processes and procedures which are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes.<sup>78</sup>

Patch management is a critical process that can help alleviate many of the challenges of securing computing systems. A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it.<sup>79</sup> A component of configuration management, it includes acquiring, testing, applying, and monitoring patches to a computer system. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws.<sup>80</sup>

The function change management team will be to assess the risk(s) or potential problems that could occur by effecting patches or in the updating of critical business systems. The patch management team will require authorisation and clearance from the change management team, in addition to

<sup>77</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>78</sup> [https://en.wikipedia.org/wiki/Change\\_management\\_\(ITSM\)](https://en.wikipedia.org/wiki/Change_management_(ITSM))

<sup>79</sup> "Microsoft issues biggest software patch on record". Reuters. 2009-10-14. Archived from the original on 16 October 2009. Retrieved 14 October 2009.

<sup>80</sup> [https://itlaw.wikia.org/wiki/Patch\\_management](https://itlaw.wikia.org/wiki/Patch_management)

being assigned “change windows” or dedicated / pre-scheduled time slots in which the patch management teams can operate, such as after business hours, so as to not interfere with usual organisational operations.

An organisation should:

1. have policies, procedures and controls in place for change management, which should include criteria for prioritising and classifying the changes, such as a normal or emergency change. Prior to any change, the organisation should ensure that the change request is:
  - 1.1 reviewed to ensure that it meets organisation’s business needs;
  - 1.2 categorised and assessed for identifying potential risks and to ensure that it will not negatively impact confidentiality, integrity, availability of the organisation’s systems and data; and
  - 1.3 approved before it is implemented by the appropriate level of management;
2. ensure that the organisation’s cybersecurity team is involved throughout the life cycle of the change management process, as may be appropriate;
3. put necessary procedures in place, such as: code review and unit testing, so as to guarantee that changes are implemented correctly and efficiently. The organisation should employ best practices when implementing changes;
4. test, validate and document changes to the information system prior to implementing them into production, which may require integration testing, non-regression testing and user acceptance testing. The changes to information systems include, but are not limited to, modifying hardware, software or firmware components and system and security configuration settings. An organisation should ensure that processes are in place to schedule change implementation and communicate to any persons / departments impacted thereby, prior to implementation thereof, which may include consulting them if and when necessary;
5. have in place processes to identify, assess and approve legitimate emergency changes. Post-implementation reviews should be conducted to validate that emergency procedures were appropriately followed and to determine the impact of the emergency change;
6. have a comprehensive patch management policy and processes that includes: maintaining current knowledge of available patches; identifying appropriate patches for particular systems and analysing impacts if installed; assuring that patches are installed properly, such as: by applying the four-eyes principle<sup>81</sup> and tested prior to and monitored after installation; as well as documenting all associated procedures, such as: specific configurations required. The policies, procedures and controls must make use of the information AIM process described in the identification phase that provides information on the installed programs and binaries;
7. consider using standardised configuration of IT resources to facilitate its patch management process;

---

<sup>81</sup> The four-eyes principle means that a certain activity, i.e. a decision, transaction, etc., must be approved by at least two people. This controlling mechanism is used to facilitate delegation of authority and increase transparency; <https://www.unido.org/overview/member-states/change-management/faq/what-four-eyes-principle>

8. ensure that the installations of new patches have prior approval from the appropriate level of management;
9. have in place necessary procedures for recovering quickly when changes or patches fail. Any changes to the production environment must have a related contingency plan, when applicable;
10. have policies and procedures to prohibit changes and patch installation to the information system that have not been pre-approved;
11. establish its change management process based on well-established and industry-recognised standards and best practices, such as: the information technology infrastructure library;<sup>82</sup>
12. consider automating its patch management process when possible to guarantee that all its systems remain consistently up to date;
13. consider building a segregated or separate environment that mirrors the production environment, allowing rapid testing and changes and patches to be implemented, and providing for rapid fallback when needed;
14. implement automatic mechanisms to prohibit changes and patches from being installed on the information system that have not been pre-approved.

---

<sup>82</sup> <https://en.wikipedia.org/wiki/ITIL>

## 4.2 **People Management:**

### 4.2.1 **Human Resources Security:**<sup>83</sup>

An organisation should:

1. Integrate cybersecurity at each stage of the employment life cycle of an employee, specifying security-related actions required during the orientation of each employee, during their ongoing management and upon the termination of their employment.
2. This cybersecurity integration process includes: -
  - 2.1 Prior to employment: an organisation should carry out background security checks on all candidates (including: employees and/or contractors) proportionate to their intended work role and depending on the criticality of the assets and information they may have access to in order to fulfil their duty. Responsibilities for cybersecurity should be clearly stated in the employment / service contractual agreement;
  - 2.2 During employment: an organisation should ensure that employees and contractors comply with existing policies, procedures and controls of an organisation. When and if an employee changes roles or responsibilities, an organisation should ensure that all access rights that are related to his/her previous position and are not necessary for his/her new responsibilities be cancelled and timeously so. Employees in sensitive positions (in example: employees whom change to roles requiring privileged access to critical systems or who become high-risk staff) should be pre-screened.
3. establish procedures to revoke all exiting employees' access rights from the information assets in a timely manner. Upon termination of employment, staff should be required to return all assets that belong to the organisation, including important documentation (such as that which is related to business processes, technical procedures, certain contact details), equipment, software and authentication hardware, *etcetera*;
4. establish policies, procedures and controls for granting or revoking employees physical and logical access to its systems based on work responsibilities, principles of least privilege and the segregation of duties. Procedures for regularly reviewing such access should be in place;
5. establish capabilities, including that of its people, processes and technologies to monitor privileged users' activity and access to critical systems, so as to identify and prevent irregular behaviour and to notify appropriate staff;
6. implement mechanisms that prompt automatic notifications to be sent to staff in charge of granting or revoking access to the information system, upon change to employment status;
7. implement automatic mechanisms<sup>84</sup> to grant or revoke staff access to its information system upon change to employment status;

<sup>83</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>84</sup> The automatic mechanism refers to mechanisms supported by its information systems (e.g. directory services and IAM systems); Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

8. monitor and analyse pattern behaviour, such as: network usage patterns, work hours and known devices *etcetera*, in order to identify irregular activities and evaluate the implementation of innovative solutions, by means of data analytics, machine learning and artificial intelligence *etcetera*, to support detection and response to insider threat activity in real time.

#### **4.2.2 Security Awareness and Training:<sup>85</sup>**

An organisation should:

1. ensure that its employees have a proper understanding of the cyber risk they may face when conducting their work; and too that they understand their roles and responsibilities in protecting the organisation's assets;
2. on a regular basis, but at least once a year, provide its entire staff (employees and/or contractors) with training to support cybersecurity policy compliance and its incident reporting process. This training should include fundamentals aimed at upholding appropriate awareness of cyber-related risks and good practices for dealing with potential cyber incidents, including the manner of reporting unusual activity. Cybersecurity awareness training should be part of the onboarding programme for new staff;
3. ensure that high-risk staff receive dedicated security awareness training that is relevant to their responsibilities;
4. Prior to going into service operations, staff operating new systems should receive appropriate user training and be familiar with the operating procedures;
5. validate the effectiveness of its training, through the deployment of social engineering or phishing tests, in order to assess whether the training and awareness positively influences the behaviour and ensures that staff comply with the cybersecurity policy and incident reporting process of the organisation;
6. ensure its cultural awareness of cyber risk continuously improves across the organisation and its ecosystem, under the guidance, instruction and involvement of the organisation's senior management;
7. training programmes should be updated regularly to take the evolving threat landscape of the ecosystem into account.

#### **4.2.3 Supplier and Third-Party Interconnectivity and Security Management:<sup>86</sup>**

An organisation should:

<sup>85</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>86</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

1. maintain and regularly update an inventory of its participants and third-party service providers, and ensure that its cyber resilience framework addresses its interconnections with the aforementioned entities from a cyber risk perspective;
2. ensure that third-party risk assessments be carried out frequently, taking into account the evolution of its threat landscape. An organisation should ensure that the provision of outsourced services are afforded the appropriate level of cyber resilience, using a risk-based approach
3. assess the third-party service provider's security capabilities, at the very least through third-party self-assessment. Note that: the provision of payment settlement services to ancillary systems by overseen entities is not considered to be third-party service provision;
4. design security controls that detect and prevent intrusions from third-party connections;
5. ensure that there are appropriate procedures in place to isolate or block its third-party connections in a timely manner, if there is a cyber-attack and/or a risk of contagion;
6. ensure that independent audit function validates the organisation's third-party relationship management and outsourcing;
7. obtain assurance of the third-party service provider's cyber resilience capabilities and may do so through certification, external audits (such as: Assurance Reports on Controls at a Service Organisation; Internal Control Framework over Financial Reporting - ISAE 3402)<sup>87</sup>, summaries of test reports, service level agreements and KPIs *etcetera*;
8. work closely with its third-party service providers and other organisations in the ecosystem to maintain and improve the security of interconnections and end point security. For example, the organisation could conduct response and recovery tests with its third-party service providers and other organisations.

## 5. Cyber Incidents Detection:<sup>88</sup>

An organisation's ability to recognise signs of a potential cyber incident, or to detect that an actual breach has taken place, is essential to strong cyber resilience. Early detection provides an organisation with useful lead time to launch appropriate countermeasures against a potential breach, and allows for the proactive containment of actual breaches. In the latter case, early containment could effectively mitigate the impact of the attack – in example, by preventing an unauthorised intruder from gaining access to confidential data or the exfiltration of such data. Given the generalist stealthy and sophisticated nature of cyber-attacks and the numerous entry points through which a compromise could take place, an organisation should maintain effective capabilities to extensively monitor for irregular activities.

An organisation should:

<sup>87</sup>Assurance Reports on Controls at a Service Organisation; Internal Control Framework over Financial Reporting; <https://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isa-3402.pdf>

<sup>88</sup>CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

1. define, consider and document the baseline profile of system activities to help detect deviation from the baseline, including irregular activities and events, based on the risk assessment performed in the identification phase;
2. develop the appropriate capabilities, which involves the organisation's people, processes and technology, to monitor and detect irregular activities and events, by setting appropriate criteria, parameters and triggers to prompt alerts;
3. have capabilities in place to monitor user activity, exceptions and cybersecurity events;
4. have capabilities in place to monitor connections, external service providers, devices and software;
5. analyse information collected and use as threat intelligence it to further enhance its detection and monitoring capabilities and incident response process;
6. ensure that its detection capabilities, baseline profile of system activities and the criteria, parameters and triggers are periodically reviewed, tested and updated appropriately, in a controlled and authorised manner;
7. ensure that its relevant staff (employees and/or contractors) are trained to be able to identify and report irregular activity and events;
8. build multi-layered detection controls covering people, processes and technology, which supports attack detection and isolation of infected / contaminated points;
9. ensure that its detection capabilities are informed by threat or vulnerability information, which can be collected from different sources and providers. Please refer to paragraphs 8 and 9 below on "*Situational Awareness*" and "*Threat Intelligence*".
10. define alert thresholds for its monitoring and detection systems in order to trigger and facilitate the incident response process;
11. ensure that its monitoring and detection capabilities support information collection for the forensic investigation. To facilitate forensic investigation, the organisation should ensure that its logs are backed up at a secure location, with controls in place to mitigate the risk of alteration or which compromises the integrity of the information;
12. develop and implement automated mechanisms, such as a security information and event management system, which correlates all the network and system alerts, as well as any other irregular activity across its business units, in order to detect multi-layered attacks, in example: simultaneous account takeover or a distributed denial of service (DDoS)<sup>89</sup> attack;
13. have a process to collect, centralise and correlate event information from multiple sources and log analysis to continuously monitor the IT environment (such as: databases, servers and end points *etcetera*) and detect irregular activities and events. This should include information on irregular activity and other network and system alerts across business units. This capability could be achieved through a security operations center (SOC) or such equivalent;

---

<sup>89</sup> Denial-of-service attack; [https://en.wikipedia.org/wiki/Denial-of-service\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)

14. have processes in place to monitor activities that are not in line with its security policy and which may lead to theft, integrity compromise or destruction of data;
15. ensure that its monitoring and detection capabilities allow the appropriate staff who can respond to be alerted automatically;
16. have the capabilities, in collaboration with other stakeholders, to detect cyber events and adapt its security controls swiftly. Such events may include attempted infiltration, movement of an attacker across systems, exploitation of vulnerabilities, unlawful access to systems and exfiltration of information or data;
17. continuously monitor connections among information assets and cyber risk levels throughout the information assets' life cycles, and store and analyse this data. The information gathered this way should enable the organisation to support timely responses to cyber threats (including insider threats) or vulnerabilities and investigation of irregular activities;
18. continuously monitor and inspect the network traffic, including remote connections and end point configuration activity, to identify potential vulnerabilities or irregular events in a timely manner;
19. compare the network traffic and the end point configuration with the expected traffic, configuration baseline profile and data flows;
20. use multiple external sources of intelligence, correlated log analysis, alerts, traffic flows, and geopolitical events to predict potential future attacks and attack trends, and proactively take the appropriate measures to improve its cyber resilience capabilities;
21. develop threat detection capabilities which can detect both known and unknown threats, with a proactive identification of vulnerabilities, state of the art threat detection and the correlation between vulnerabilities and threats;
22. seek to continuously explore new technologies and techniques inhibiting lateral movement (in example: deception mechanisms) which trigger alerts and inform the organisation of potential malicious activity when accessed. To do this, an organisation could create and place fictitious sensitive data with alerting tags attached to them.

## 6. Incident Response and Recovery:<sup>90</sup>

An organisation's response to an incident can either contain or escalate an incident. A poor response can even create a crisis. Vigorous, coordinated responses to incidents limit lost time, money, and customers, as well as damage to reputation and the costs of recovery.<sup>91</sup>

Financial stability may depend on an organisation's ability to settle obligations when they are due. Therefore, an organisation's arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to

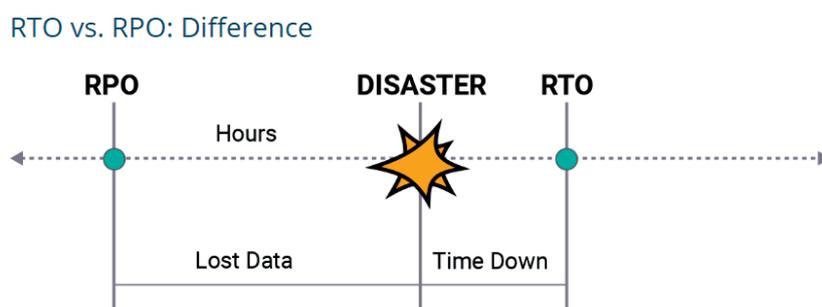
<sup>90</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/pub/l/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank,

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)  
<sup>91</sup> <https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/cyber-crisis-management.pdf>

meet such obligations, when participants are expecting it to meet them. Business continuity planning is essential for meeting the organisation's objectives.

### 6.1 Cyber Resilience Incident Management:<sup>92</sup>

RTO and RPO (recovery time objective and recovery point objective) are two key metrics that organizations must consider in order to develop an appropriate disaster recovery plan that can maintain business continuity after an unexpected event.<sup>93</sup>



94

An organisation should:

1. based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections – plan as to how to operate in a reduced / weakened capacity or how to safely restore services over time, based on services' relative priorities, and with accurate data. In order to make the best decisions about its recovery objectives following a cyber incident, the organisation must first define its recovery point objectives and its recovery time objectives, proportionate to its business needs and systemic role in the ecosystem. The Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.<sup>95</sup> The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.<sup>96</sup>
2. consider (Based on expectation '1' above) a range of different cyber circumstances, including extreme, but plausible ones, to which the organisation may be exposed, and conduct a business impact analyses to assess the potential impact such scenarios might have on the organisation. The organisation should review its range of scenarios and conduct a business impact analysis in line with the evolving threat landscape, on a regular basis;
3. based on the different cyber scenarios, develop a contingency plan that achieves recovery objectives, restoration priorities and determines the required capacities for continuous availability of the system. The plan should define roles and responsibilities, and set out options

<sup>92</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>93</sup> <https://www.msp360.com/resources/blog/rto-vs-rpo-difference/>

<sup>94</sup> <https://www.msp360.com/resources/blog/rto-vs-rpo-difference/>

<sup>95</sup> <https://www.forbes.com/sites/sungardas/2013/10/29/three-reasons-you-cant-meet-your-disaster-recovery-time-objectives>

<sup>96</sup> <https://whatis.techtarget.com/definition/recovery-point-objective-RPO>

to reroute or substitute critical functions and/or services that may be affected for a significant period by a successful cyber-attack;

4. develop a comprehensive cyber incident response, resumption and recovery plan, to manage cybersecurity events or incidents in a way that mitigates damage and prioritises resumption and recovery actions, in order to facilitate the processing of critical transactions, increase the confidence of external stakeholders, and reduce recovery time and costs. Such plans should define policies and procedures, as well as roles and responsibilities for escalating, responding to, and recovering from cybersecurity incidents. An organisation should ensure all relevant business units, including that of telecommunications, are integrated into such plans;
5. ensure that its cyber incident response, resumption and recovery processes be closely integrated with crisis management, business continuity, and disaster recovery planning and recovery operations;
6. define the Recovery Time Objectives (RTO) and Recovery Point objectives (RPO) for critical systems and functions
7. ensure that its incident response team has the requisite skills and training to address cyber incidents;
8. define alert parameters and thresholds for detecting cybersecurity incidents, which trigger the incident management processes and procedures, which in turn include alerting and conveying information to the appropriate staff;
9. regularly test its cyber contingency, response, resumption and recovery plans against a range of different plausible scenarios;
10. have processes and procedures in place for collating and reviewing information from its cybersecurity incidents and testing results in order to continuously improve its contingency, response, resumption and recovery plans;
11. have processes and procedures in place to conduct a post-incident root cause analysis of its cybersecurity incidents. The organisation should integrate its findings from the root cause analysis into its cyber response, resumption and recovery plans, as set out in expectation 4 above;
12. design and test its systems and processes to enable critical operations to be resumed safely within a few hours (in example: 2 hours, depending on the systems and technological capacity of the systems in place within an Organisation) of a cyber disruption and to enable it to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Notwithstanding this capability to resume critical operations within a few hours, organisations should undertake careful problem analysis and exercise judgement (in consultation and agreement with competent authorities and relevant stakeholders) when resuming operations so that risks to the organisation or its ecosystem do not escalate as a result, while taking into account the fact that completion of settlement by the end of day is crucial;
13. plan for scenarios in which resumption within a few hours cannot be achieved. The organisation should analyse critical functions, transactions and interdependencies to prioritise resumption and recovery actions, which may, depending on the design of the organisation (in example:

help critical transactions to be processed) while remediation efforts continue. The organisation should also plan for situations in which critical people, processes or systems may be unavailable for significant periods – in example: by potentially reverting to manual processing if automated systems are unavailable; where it is feasible, safe and practicable to do so.

14. implement an effective incident handling capability for cybersecurity incidents which includes:
  - a. preparation;
  - b. detection;
  - c. analysis;
  - d. containment;
  - e. eradication; and
  - f. recovery.
  - g. lessons learned

Such capability should allow the organisation to perform, at an early stage, analysis of cybersecurity incidents upon their detection, with minimal service disruption. This capability might include direct cooperative or contractual agreements with incident response organisations or providers to assist rapidly with mitigation effort;

15. define and develop functional and security dependency maps of identified information assets supporting critical functions to understand and prioritise the order in which they should be restored;
16. be able to use lessons learned from actual, real-life cyber-attacks on an organisation and its ecosystem to improve its contingency, response, resumption and recovery plans;
17. consult with relevant external stakeholders, such as: main participants, service providers and other organisations within the ecosystem to further enhance its contingency, response, resumption and recovery plans
18. continuously monitor, evaluate and consider technological developments and solutions in the market that may enhance its contingency, response, resumption and recovery capabilities;
19. implement processes to continuously improve its cyber response, resumption and recovery plans, taking into account cyber threat intelligence feeds, information sharing with its ecosystem and lessons learned from previous events;
20. consult, collaborate and coordinate with relevant external stakeholders (as described in expectation 16 *supra*) within the ecosystem to develop common contingency, response, resumption and recovery plans for cyber scenarios which may impact the ecosystem as a whole. The organisation should conduct regular scenario tests with the relevant external stakeholders, such as: industry-wide and organisation specific simulation exercises.
21. implement a computer security incident response team (CSIRT), whether in-house or outsourced, that is responsible for responding to security incidents and intrusions, and coordinating activities among the relevant internal and external stakeholders. Such a team should have the authority to direct the organisation to make the changes necessary to recover from the incident;

22. establish and implement processes to manage cybersecurity incidents and enable automated responses, triggered by predefined criteria, parameters and thresholds. For example, the organisation could develop configurable capability to isolate or disable automatically affected information systems if cyber-attacks or security violations are detected.

## 6.2 Data Confidentiality, Integrity and Availability:<sup>97</sup>

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an Organisation. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the United States of America's Central Intelligence Agency.<sup>98</sup>

In this context, confidentiality is the policy governed set of rules which limits access to information. Integrity is the assurance that the information is trustworthy and accurate. Availability is a guarantee of reliable access to the information by authorised persons. The elements of the CIA / AIC triad are considered the three most crucial components of security.

Security threats to data, its confidentiality, quality (integrity) and accessibility (availability), represent potential losses to the integrity of the operations of an organisation. Security personnel and managers of an organisation, in assessing the potential risks, should be interested in the relationship between the contagious threats to these different security attributes. The nature of the interrelationship between the threats provides additional information to assist security personnel and managers in making their choices of mitigating responses. In example, if the inter-relationship between threats is constant, independently of the frequency and intensity of threats, security personnel and managers can adopt smooth mitigation profiles to meet the threat. In the absence of such stable relationships, the managers' responses must be adjusted dynamically: for given temporal relationships between the number of attacks, their change (or 'jump') in frequency, and their change in size (extent of impact).<sup>99</sup> Contagion of threats is discussed further at section 6.3.1. below.

An organisation should:

1. develop a formal backup policy ("Data Backup Policy"), with detailed procedures specifying the minimum frequency and scope of data, based on data sensitivity, the frequency with which that new information is introduced and designed to achieve the Organisation's objectives;
2. develop backup and recovery methods and strategies to be able to restore system operations with minimum downtime and limited disruption;
3. regularly back up all data necessary to replay participants' transactions;
4. ensure that backups should be protected at rest, during use and in transit to ensure the confidentiality, integrity and availability of data. Backups should be tested regularly to verify their availability and integrity;

<sup>97</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>

<sup>98</sup> <https://www.cia.gov/index.html>

<sup>99</sup> <http://www0.cs.ucl.ac.uk/staff/D.Pym/contagion.pdf>

5. store backup copies at an alternate, safe site with a different risk profile to the main site, and with transfer rates consistent with actual recovery point objectives. The alternate site and backups should be safeguarded by stringent protective and detective controls;
6. ensure that its information systems implement transaction recovery mechanisms for transaction-based systems, which might include transaction rollback and logging;
7. conduct frequent periodic reconciliation of participants' positions, with the assistance of participants where needed;
8. develop capabilities to restore information system components within the actual recovery time objectives using a predefined and standardised configuration of IT resources, the integrity of which is protected;
9. ensure that its backup and recovery methods and strategies are integrated into the organisation's system infrastructure at the development and/or acquisition phase;
10. back up its information system by maintaining a redundant secondary system that is not located in the same place as the primary system and that can be activated without information being lost or operations disrupted;
11. consider having a data-sharing agreement with third parties and/or participants in order to obtain uncorrupted data from them for recovering its business operations in a timely manner and with accurate data.

### 6.3 **Communication and Collaboration:**<sup>100</sup>

#### 6.3.1 **Contagion / Communicability:**<sup>101</sup>

“Given FMIs’ systemic importance and extensive interconnections and hence, potential for risk contagion [spread of infection] between FMIs and entities within their ecosystems, [they] should take appropriate, swift and sustained actions to enhance their cyber-resilience.” - International Organization of Securities Commissions.<sup>102</sup>

The containment of the propagation of threats (in example: malicious code / malware) on a network system / systems, mobile or other devices etcetera, or at least the minimisation of its noxious effects, so as to prevent the communicability thereof and to enable the testing of the effectiveness of countermeasures, in order to make suitable decisions regarding the threat, is of vital importance as part

<sup>100</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

<sup>101</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

<sup>102</sup> International Organization of Securities Commissions; <https://www.treasurers.org/fmis-urged-prevent-cyberattack-%E2%80%9Ccontagion%E2%80%9D>; CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

of an organisation's incident response plan, following detection of an incident and as part of the response and recovery plan of an organisation<sup>103</sup> and further, aids learning and evolving.

An organisation should:

1. identify, document and regularly review systems and processes supporting its critical functions and/or operations that are dependent on external connectivity;
2. develop policies and procedures that define how it should work together with relevant interconnected entities to enable operations to be resumed (the first priority being its critical functions and services) as soon as it is safe and practicable to do so;
3. closely cooperate with its interconnected entities within the ecosystem, establishing rollback processes in order to restore all its services accurately and safely. Moreover, the organisation should test the effectiveness of these procedures regularly;
4. design its network connection infrastructure in a way that allows connections to be segmented or severed instantaneously to prevent contagion arising from cyber-attacks.

### **6.3.2 Crisis Communication and Responsible Disclosure:<sup>104</sup>**

An organisation's Senior Management must be prepared to communicate, as needed, across all media, including social media, in ways that assure stakeholders that the organisation's response is equal to the situation.<sup>105</sup> Typical information exchanged among teams include threat intelligence, indicators of compromise (IoCs), malware samples and details about relevant incidents.

Crisis Communication and Responsible disclosure should be effected in a secure manner, with due consideration of the appropriate medium (or method) used to convey information to and from an organisation, concerning an incident response crisis. The communication medium is required and should facilitate the needs for proper crisis communication, having regard to end-to-end encryption, mature multi-platform support, a secure group chat, open specification.

An organisation should:

1. identify and determine staff who are essential for mitigating the risk of a cyber incident, and make them aware of their roles and responsibilities regarding incident escalation;
2. ensure that its incident response plan identifies the internal and external stakeholders that must be notified, as well as the information that has to be shared and reported, and when this should take place;
3. establish criteria and procedures for escalating cyber incidents or vulnerabilities to the Board and senior management based on the potential impact and criticality of the risk;

<sup>103</sup> <https://www.securitymetrics.com/blog/6-phases-incident-response-plan>

<sup>104</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Secure Group Communications for incident response and operational communities -<https://www.enisa.europa.eu/publications/secure-group-communications>

<sup>105</sup> <https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/cyber-crisis-management.pdf>

4. have a communication plan and procedures in place to notify, as required or necessary, all relevant internal and external stakeholders (including oversight, regulatory authorities, media and customers) in a timely manner, when the institution becomes aware of a cyber incident. The organisation should notify the appropriate internal and external stakeholders when a cyber incident occurs;
5. have a policy and procedures to enable potential vulnerabilities to be disclosed responsibly. In particular, the organisation should prioritise disclosures that could help stakeholders to respond promptly and mitigate risk, which could benefit the ecosystem and broader financial stability;
6. establish and regularly review information-sharing rules, agreements and modalities in order to control the publication and distribution of such information, and to prevent sensitive information that may have adverse consequences if disclosed improperly from being disseminated;
7. after developing a range of cyber incident scenarios based on the incident criteria established in the evolving level, the organisation should develop appropriate incident response and communication plans and procedures to address the scenarios. These incident response and communication plans and procedures should take into consideration the legal and regulatory reporting requirements at a jurisdictional level;
8. develop mechanisms that instantaneously notify its senior management, relevant employees and relevant stakeholders (including oversight and regulatory authorities) of cyber incidents through appropriate communication channels with tracking and verification of receipt. Such mechanisms should be based on predefined criteria and informed by scenario-based planning and analysis, as well as prior experience.

Also refer to section 8.2 below in respect of information and intelligence sharing communities / teams.

#### **6.4 Forensic Readiness:<sup>106</sup>**

To be read together with the content under section 3.2.7 in being an Incident Handling Procedure, an organisation should:

1. identify the threat scenarios that might have a potential impact on its business and determine which pieces of digital evidence (in example: types of logs) should be collected to facilitate forensic investigation;
2. identify and document the digital evidence available on its systems and its location, and understand how the evidence should be handled throughout its life cycle;
3. Based on expectations 1 and 2 above, the organisation should develop and implement a forensic readiness policy and the capability to support forensic investigation, which also outlines the relevant system logging policies that include the types of logs to be maintained and their

<sup>106</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

retention periods. An organisation may outsource the conduct of forensic investigations to external specialists;

4. establish procedures for securely collecting digital evidence in a forensically acceptable manner and in accordance with the requirements defined in the forensic readiness policy, taking into account the requirements of the local jurisdiction. These procedures should describe how investigative staff should produce step-by-step documentation of all activities performed on digital evidence and their impact;
5. establish policies for securely handling and storing the collected digital evidence, ensuring its authenticity and integrity. The organisation should develop procedures to demonstrate that the evidence's integrity is preserved whenever it is accessed, used or moved (in example: chain of custody)<sup>107</sup>;
6. train its personnel and staff so that all those involved in an incident understand their responsibilities related to handling the digital evidence, ensuring it is not compromised and remains valid as per the requirements of the local jurisdiction;
7. ensure that staff specifically involved in the forensic investigation have the appropriate degree of competence in handling the digital evidence, ensuring its authenticity and integrity is not compromised and remains valid as per the requirements of the local jurisdiction;
8. closely integrate plans for forensic readiness with plans for incident management and other related business planning activities;
9. have a management review process that improves forensic readiness plans in accordance with experience and new knowledge;
10. take an open and collaborative approach with the ecosystem to improve lawful forensic investigation and incident handling methodologies and tools;
11. to facilitate a lawful forensic investigation, to mandate an external (independent), trusted third-party, for legal considerations.

## **7. Information Security Controls Testing:<sup>108</sup>**

Testing is an integral component of any cyber resilience framework. All elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an organisation, and regularly thereafter. This includes the extent to which the framework is implemented correctly, operating as intended and producing desired outcomes. Understanding the overall effectiveness of the cyber resilience framework in the organisation and its environment is essential in determining the residual cyber risk to the organisation's Management Information operations, assets, and ecosystem. Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the organisation's

<sup>107</sup> Chain of Custody is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence; [https://en.wikipedia.org/wiki/Chain\\_of\\_custody](https://en.wikipedia.org/wiki/Chain_of_custody)

<sup>108</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cyber resilience posture and reduce or eliminate identified gaps.

An organisation should:

1. establish and maintain a comprehensive testing programme as an integral part of its cyber resilience framework. The testing programme should consist of a broad spectrum of methodologies, practices and tools for monitoring, assessing and evaluating the effectiveness of the core components of the cyber resilience framework;
2. adopt a risk-based approach in developing the comprehensive testing programme. This should be reviewed and updated on a regular basis taking into due account the evolving landscape of threats and the criticality of information assets;
3. develop appropriate capabilities and involve, if deemed necessary, all relevant internal stakeholders (including: business lines and operational units) when implementing its testing programme;
4. ensure that the tests are undertaken by independent parties, whether internal or external;
5. for continuous improvement of its cyber resilience posture, the organisation should establish policies and procedures to prioritise and remedy issues identified from the various tests and perform subsequent validation to assess whether gaps have been fully addressed;
6. incorporate lessons learned from the test results should be incorporated, through the organisation's Board and senior management;
7. test critical systems, applications and data recovery plans at least annually;
8. test response, resumption and recovery plans, including governance and coordination, and crisis communication arrangements and practices, at least annually;
9. test the information backups periodically to verify they are accessible and readable (to be read together with Section 6.2 *supra*);
10. include testing practices as an integrated part of its enterprise risk management process with the aim of identifying, analysing and fixing cybersecurity vulnerabilities stemming from new products, services or interconnections;
11. develop capabilities to seek, analyse and use cyber threat intelligence to help inform and update its testing programme to ensure it is in line with the latest threat landscape, attackers' modus operandi and vulnerabilities;
12. adopt best practices and automated tools to support the processes and procedures in place to fix technical and organisational weaknesses identified during the testing exercises and to check for compliance with approved policy and configurations;
13. perform security assessments and tests when applicable at all phases of the software or system development life cycle and at any level (be it: business, application and technology) for the entire application portfolio, including mobile applications;

14. develop, monitor and analyse baselines and metrics to assess the performance and effectiveness of its testing programme. An organisation should use the analysis conducted to further improve its testing programme;
15. regularly conduct tests in collaboration with its peers, participants and third parties;
16. proactively engage in industry-wide exercises in order to test cooperation and coordination protocols and communication plans. These exercises should foster the organisation's awareness on cross-sector cooperation and third-party risks;
17. promote and participate in cross-sector cyber testing exercises to assess the soundness and security of its value chain as a whole;
18. test the cooperation arrangements in place with relevant external entities at least annually (e.g. third-party security service providers, law enforcement agencies, computer emergency response teams or information sharing and analysis centres (ISACs), *etcetera*) in order to validate their effectiveness;
19. consider discussing relevant test conclusions with other stakeholders to boost the cyber resilience of its ecosystem and the financial sector as a whole, as far as possible and under specific information-sharing arrangements.

## **7.1 Vulnerability Assessments:<sup>109</sup>**

An organisation should:

1. develop a documented and regularly updated vulnerability management process in order to classify, prioritise and remedy potential weaknesses identified in vulnerability assessments and perform subsequent validation to assess whether gaps have been fully addressed;
2. ensure that the organisation's vulnerability management process assists any type of exploitable weakness to be identified (such as: technical, processual, organisational and emergent) in the critical functions, their supporting processes and information assets where they reside;
3. conduct vulnerability scanning for their external-facing services and the internal systems and networks on a regular basis;
4. perform vulnerability assessments before any deployment or redeployment of new or existing services supporting critical functions, applications and infrastructure components for fixing bugs and weaknesses, consistently with change and release management processes in place;
5. periodically conduct vulnerability assessments on running services, applications and infrastructure components for compliance checks against regulations, policy and configurations, as well as for monitoring and evaluating the effectiveness of security controls to address the identified vulnerabilities;

<sup>109</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

6. perform vulnerability scanning on an ongoing basis, rotating among environments in order to scan all environments throughout the year;
7. develop and adopt a range of effective practices and tools (in example: a Bug Bounty programme<sup>110</sup> and static and dynamic code reviews *etcetera*) as part of its vulnerability management process, and have appropriate safeguards in place to manage them

## 7.2 Scenario-based Testing:<sup>111</sup>

An organisation should:

1. perform different scenario-based tests, including extreme but plausible scenarios, to evaluate and improve its incident detection capability, as well as response, resumption and recovery plans. Scenario-based tests can take the form of desktop exercises or simulations;
2. ensure that its Board and senior management are engaged in the scenario-based test, when appropriate;
3. in order to improve the organisation's staff awareness and enhance the risk culture within the organisation, the scenario-based tests should include social engineering and phishing simulation;
4. test of the extent to which internal skills, processes and procedures can adequately respond to extreme but plausible scenarios, with a view to achieving stronger operational resilience;
5. test its response, resumption and recovery plans against cyber-attack scenarios which include data destruction, data integrity corruption, data loss, and system and data availability;
6. use cybersecurity incident scenarios involving significant financial loss, as part of its stress testing process, to better understand potential spillovers and risk to its business model. The organisation should use such stress tests to further improve its risk management framework;
7. conduct scenario-based tests that cover breaches affecting multiple portions of the organisation's ecosystem in order to identify and analyse potential complexities, interdependencies and possible contagion both at business and operational level which should be taken into account in the organisation's cyber resilience framework;
8. collaborate with the ecosystem to develop cybersecurity incident scenarios involving significant financial loss and use them for stress tests to better understand potential spillovers and contagion risk to the ecosystem. The organisation should use such stress tests to further improve its cyber resilience posture, which contributes to improving the ecosystem's resilience as a whole.

<sup>110</sup> A bug bounty program is a deal offered by many websites, organisations and software developers by which individuals can receive recognition and compensation [1] for reporting bugs, especially those pertaining to exploits and vulnerabilities; [https://en.wikipedia.org/wiki/Bug\\_bounty\\_program](https://en.wikipedia.org/wiki/Bug_bounty_program)

<sup>111</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

### 7.3 Penetration Testing:<sup>112</sup>

An organisation should:

1. conduct penetration tests on their external-facing services and the internal systems and networks to identify vulnerabilities in the adopted technology, organisation and operations regularly, or at least on an annual basis. Penetration tests should be conducted using a risk-based approach and, at the very least, in cases of major changes and new system deployment;
2. perform penetration tests, engaging all critical internal and external stakeholders in the penetration testing exercises: system owners, business continuity, and incident and crisis response teams; and
3. design and perform penetration tests to simulate realistic attack techniques on systems, networks, applications and procedures.

### 7.4 Red Team Testing:<sup>113</sup>

An organisation should:

1. conduct red team exercises to test critical functions for possible vulnerabilities and the effectiveness of an organisation's mitigating controls, including its people, processes and technology;
2. perform red team exercises using reliable and valuable cyber threat intelligence, based on specific and plausible threat scenarios;
3. conduct independent red team exercises, utilising regulatory and industry frameworks, such as the European Framework for Threat-Intelligence Based Ethical Red teaming<sup>114</sup>;
4. build its internal processes and capabilities to prepare for undertaking the independent red team exercise, in example: establishing an internal white team, developing incident escalation procedures, following appropriate methodologies and establishing robust risk management controls.
5. develop an internal red team capability with the appropriate methodologies, sophisticated tools and appropriately skilled staff, in addition to periodic independent and external red team exercises. The internal red team should regularly conduct red team exercises and engage with the internal blue team to share its findings and make improvements to the organisation's cyber resilience posture.

<sup>112</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>113</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>114</sup> TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming May 2018; [https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber\\_eu\\_framework.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf)

## 7.5 Taxonomy of Cyber Risk Controls:<sup>115</sup>

Putting cyber-risk controls in place is only one aspect of building cyber-resilience. Examples of taxonomy of cyber or information security controls, per the Basel Committee on Banking Supervision: Cyber resilience: Range of practices report of December 2018, is included below:<sup>116</sup>

Control objective	Control description	Example controls and practices	Example testing approaches
Restrict access and usage to only those who have been authorised	Access is limited to what has been authorised based on job role and principle of least privilege	Identity and access management (IAM), user identification and authentication, physical security, employee awareness and training	Social engineering test
	User is authenticated whereby strength of authentication is commensurate with the sensitivity of the asset being accessed	Password policy, system authentication controls	Audits of user access
	Networks are protected from unauthorised traffic	Firewalls, routers, network segmentation	Penetration tests
	Systems are protected from malicious attacks	Anti-malware, web and email filtering	Non-functional testing
	System-to-system communication (including exchange of data) is protected from unauthorised access and use	Encryption, key management	Key management review
Detect unauthorised access and usage (including change)	Detect unauthorised access and use of systems in a timely manner	Logs, security information and event management (SIEM), security cameras, intrusion detection solutions (IDS), integrity change detection solutions, event analysis and escalation procedures	Penetration tests, red team tests

117

<sup>115</sup> Bank for International Settlements and International Organisation of Securities Commissions 2016, Committee on Payments and Market Infrastructures, Board of the International Organisation of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016 -

[https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI\\_IOSCO\\_Guidance\\_on\\_cyber\\_resilience\\_for\\_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5](https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5) CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>116</sup> Bank for International Settlements and International Organisation of Securities Commissions 2016, Committee on Payments and Market Infrastructures, Board of the International Organisation of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016 -

[https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI\\_IOSCO\\_Guidance\\_on\\_cyber\\_resilience\\_for\\_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5](https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5); Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>117</sup> Bank for International Settlements and International Organisation of Securities Commissions 2016, Committee on Payments and Market Infrastructures, Board of the International Organisation of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016 -

[https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI\\_IOSCO\\_Guidance\\_on\\_cyber\\_resilience\\_for\\_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5](https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5); Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

Control objective	Control description	Example controls and practices	Example testing approaches
Restrict access and usage to only those who have been authorised	Access is limited to what has been authorised based on job role and principle of least privilege	Identity and access management (IAM), user identification and authentication, physical security, employee awareness and training	Social engineering test
	User is authenticated whereby strength of authentication is commensurate with the sensitivity of the asset being accessed	Password policy, system authentication controls	Audits of user access
	Networks are protected from unauthorised traffic	Firewalls, routers, network segmentation	Penetration tests
	Systems are protected from malicious attacks	Anti-malware, web and email filtering	Non-functional testing
	System-to-system communication (including exchange of data) is protected from unauthorised access and use	Encryption, key management	Key management review
Detect unauthorised access and usage (including change)	Detect unauthorised access and use of systems in a timely manner	Logs, security information and event management (SIEM), security cameras, intrusion detection solutions (IDS), integrity change detection solutions, event analysis and escalation procedures	Penetration tests, red team tests

## 8. Situational Awareness:<sup>119</sup>

Situational awareness refers to an organisation’s understanding of the cyber threat environment within which it operates, the implications of being in that environment for its business and the adequacy of its cyber risk mitigation measures. Strong situational awareness can significantly enhance an organisation’s ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber-attacks that are not prevented.

An organisation’s solid understanding of the threat landscape can help it better identify and appreciate the vulnerabilities in its critical business functions, and facilitate the adoption of appropriate risk mitigation strategies, vulnerabilities in its critical business functions, as well as facilitate the adoption of appropriate risk mitigation strategies. It can also enable an organisation to validate its strategic direction, resource allocation, processes, procedures and controls with respect to building its cyber resilience. A key means of achieving situational awareness for an organisation and its ecosystem is an organisation’s active participation in information-sharing arrangements and collaboration with trusted stakeholders within and outside the industry.

<sup>118</sup> Bank for International Settlements and International Organisation of Securities Commissions 2016, Committee on Payments and Market Infrastructures, Board of the International Organisation of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016 -

[https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI\\_IOSCO\\_Guidance\\_on\\_cyber\\_resilience\\_for\\_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5](https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5); Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>119</sup> Bank for International Settlements and International Organisation of Securities Commissions 2016, Committee on Payments and Market Infrastructures, Board of the International Organisation of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016 -

[https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI\\_IOSCO\\_Guidance\\_on\\_cyber\\_resilience\\_for\\_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5](https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf?69e99441d6f2f131719a9cada3ca56a5); CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

## **8.1 Cyber Threat Intelligence:<sup>120</sup>**

### **8.1.1. Identification of potential cyber threats:<sup>121</sup>**

An organisation should identify cyber threats that could materially affect its ability to perform or to provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem. In doing so, an organisation should consider threats to the confidentiality, integrity and availability of the organisation's business processes and to its reputation that could arise from internal and external sources. In addition, an organisation should include in its threat analysis those threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. The organisation should regularly review and update this analysis.

### **8.1.2. Threat intelligence process:<sup>122</sup>**

An organisation should establish a process to gather and analyse relevant cyber threat information. Its analysis should be in conjunction with other sources of internal and external business and system information so as to provide business-specific context, turning the information into usable cyber threat intelligence that provides timely insights and informs enhanced decision-making by enabling the organisation to anticipate a cyber attacker's capabilities, intentions and *modus operandi*.

### **8.1.3. Scope of cyber threat intelligence gathering:<sup>123</sup>**

The scope of cyber threat intelligence gathering should include the capability to gather and interpret information about relevant cyber threats arising from the organisation's participants, service and utility providers and other organisations, and to interpret this information in ways that allow the organisation to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems.<sup>124</sup> In this context, relevant cyber threat intelligence could include information on geopolitical developments that may trigger cyber-attacks on any entity within the organisation's ecosystem.

### **8.1.4. Effective use of information:<sup>125</sup>**

Organisations should ensure that cyber threat intelligence is made available to appropriate staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels within the organisation. Cyber threat intelligence should be used to ensure that the implementation of any cyber resilience measures is threat-informed. When properly contextualised, cyber threat information enables an organisation to validate and inform the prioritisation of resources, risk mitigation strategies and training programmes.

<sup>120</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

<sup>121</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>122</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>123</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>124</sup> An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>125</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

### 8.1.5. Expectations in terms of Cyber Threat Intelligence:<sup>126</sup>

An organisation should:

1. identify cyber threats that could materially affect its ability to perform or provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem;
2. have capabilities in place to gather cyber threat information from internal and external sources, such as: application, system and network logs; security products (including firewalls and intrusion detection systems); trusted threat intelligence providers and publicly available information;
3. belong or subscribe to a threat and vulnerability information-sharing source and/or Information Sharing and Analysis Center (ISAC) that provides information on cyber threats and vulnerabilities. Cyber threat information gathered by the organisation should include analysis of tactics, techniques and procedures (TTPs) of real-life attackers, their *modus operandi* and information on geopolitical developments that may trigger cyber-attacks on any entity within the organisation's ecosystem;
4. have the capabilities to analyse the cyber threat information gathered from different sources, whilst taking into account the business and technical characteristics of the organisation, in order to:
  - a) determine the motivation and capabilities of threat actors (including their TTPs) and the extent to which the organisation is at risk of a targeted attack from them;
  - b) assess the risk of technical vulnerabilities in operating systems, applications and other software, which could be exploited to perform attacks on the organisation;
  - c) analyse cybersecurity incidents experienced by other organisations, where available, including types of incident and origin of attacks, target of attacks, preceding threat events and frequency of occurrence, and determine the potential risk these pose to the organisation;
5. analyse the information gathered above to produce relevant cyber threat intelligence, and continuously use it to assess and manage security threats and vulnerabilities for the purpose of implementing appropriate cybersecurity controls in its systems and, on a more general level, enhancing its cyber resilience framework and capabilities on an ongoing basis;
6. ensure that the gathering and analysis of cyber threat information and the production of cyber threat intelligence are reviewed and updated regularly;
7. that cyber threat intelligence is made available to appropriate staff who are responsible for mitigating cyber risks at the strategic, tactical and operational levels within the organisation;
8. incorporate lessons learned from its analysis of the cyber threat information into the employee training and awareness programmes;

<sup>126</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank; [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

9. continuously use its cyber threat intelligence to anticipate, as much as possible, a cyber attacker's capabilities, intentions and modus operandi, and subsequently possible future attacks;
10. develop / make use of a cyber threat risk dashboard<sup>127</sup>, which uses the cyber threat information and intelligence to outline, among other things:
  - a) the most likely threat actors for the organisation;
  - b) the TTPs that may be used by such threat actors;
  - c) the likely vulnerabilities that may be exploited by such threat actors;
  - d) the likelihood of attack from such threat actors and the impact on the confidentiality, integrity and availability of the organisation's business processes and its reputation that could arise from such attacks;
  - e) the impact of attacks already conducted by such threat actors on the ecosystem;
  - f) the risk mitigation measures in place to manage a potential attack.
11. Ensure that the cyber threat risk dashboard should be continuously reviewed and updated in the light of new threats and vulnerabilities; and be discussed by the Board and senior management;
12. include in its threat analysis those threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. The organisation should review and update this analysis regularly;
13. ensure that the scope of cyber threat intelligence gathering includes the capability to gather and interpret information about relevant cyber threats arising from the organisation's participants, service and utility providers and other organisations, and to interpret this information in ways that allow the organisation to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems;
14. integrate and align its cyber threat intelligence process with its SOC. The organisation should use information gathered from its SOC to further enhance its cyber threat intelligence; and conversely, use its cyber threat intelligence to inform its SOC.

## **8.2 Communication and Sharing of Information:<sup>128</sup>**

To facilitate sector-wide response to large-scale incidents, organisations should plan for information-sharing through trusted channels in the event of an incident, collecting and exchanging timely information that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber-attack. Organisations should, as part of their response programmes, determine beforehand which types of information will be shared, with whom, and how information provided to the organisation will be acted upon. Reporting requirements and capabilities should be consistent with information-sharing arrangements within the organisation's communities and the financial sector.

In respect of information-sharing, organisations should participate actively in information-sharing groups and collectives, including cross-industry, cross-government and cross-border groups to gather,

<sup>127</sup> This is a conceptual output, which may be integrated into existing risk reporting processes; <https://www.anomali.com/products>

<sup>128</sup> Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf> and Bank for International Settlements, Basel Committee on Banking Supervision, Guidance on cyber resilience for financial market infrastructures; <https://www.bis.org/cpmi/publ/d138.pdf>

distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats. Organisations should, where appropriate, share information both bilaterally and multilaterally. As appropriate, an organisation should consider exchanging information on its cyber resilience framework bilaterally with trusted stakeholders, so as to promote understanding of each other's approach to securing systems that are linked or interfaced. Such information exchange would facilitate an organisation and its stakeholders' efforts at merging their respective security measures to achieve greater cyber resilience. Multilateral information-sharing arrangements should be designed to facilitate a sector-wide response to large-scale incidents.

Cyber-security information-sharing mechanisms, may be mandatory or voluntary, to facilitate sharing of cyber-security information among banks, regulators and security agencies. These communications are established for multiple purposes, including helping relevant parties defend themselves against emerging cyber-threats.

CSIRTs: the formal definition and description of CSIRTs outlined in the 2007 Carnegie Mellon document "Defining Computer Security Incident Response Teams"<sup>129</sup> reads: "A computer security incident response team (CSIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident." Computer Security Incident Response Teams (CSIRTs) around the world deal with security events, such as malware outbreaks or vulnerability discoveries, *etcetera*. Incident response teams are often organised in communities such as CSIRTs Network<sup>130</sup>, TF-CSIRT<sup>131</sup>, Forum of Incident Response and Security Teams (FIRST)<sup>132</sup> and other regional, sub regional or sectorial communities.

CERT: Computer emergency response (or readiness) team; also known as CIRT (cyber incident response team or computer incident response team). The term CERT, although many companies use the term generically, has been a registered mark of Carnegie Mellon University since 1997. Organisations can and must apply for authorisation to use the CERT mark, if desired. Carnegie Mellon's CERT designation has a particular focus and niche it occupies; it operates as a "...partner with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks..." A CERT studies "...problems that have widespread cybersecurity implications and develop[s] advanced methods and tools".<sup>133</sup> One example is that of ADGovCERT<sup>134</sup>

To facilitate information exchange among teams and improve reaction time to security incidents, tailored communication solutions are required. These teams are often organised in groups forming a decentral community that needs to co-operate and have secure and reliable communication channels to share information. The type of work and decentralized organisational structure of these communities impose tough requirements on the chosen communication solutions. First and foremost, solutions must implement end-to-end encryption protocols for group messaging because highly sensitive information is exchanged. Thus, to reduce the amount of required trust in providers, solutions must implement end-to-end encryption with verifiable keys defined in an open specification. To allow archive of previous incidents lesson learnt, these solutions must provide a way to archive conversations and storage of attachments. Finally, on premise hosting and the selection of free software allows independent operation and extensibility by the managing member of the community. This community could be a

<sup>129</sup> [https://resources.sei.cmu.edu/asset\\_files/WhitePaper/2007\\_019\\_001\\_294579.pdf](https://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_294579.pdf)

<sup>130</sup> CSIRTs Network <http://csirtsnetwork.eu/>

<sup>131</sup> TF-CSIRT <https://tf-csirt.org/>

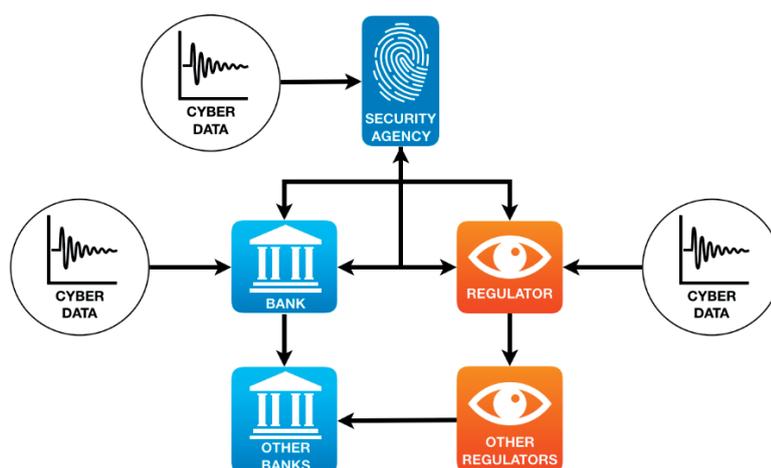
<sup>132</sup> FIRST - Forum of Incident Response and Security Teams <https://www.first.org/>

<sup>133</sup> [https://resources.sei.cmu.edu/asset\\_files/WhitePaper/2007\\_019\\_001\\_294579.pdf](https://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_294579.pdf)

<sup>134</sup> <https://www.tamm.abudhabi/adgovcert>

group of incident response teams forming a decentral community or an operational community grouped in an information sharing and analysis centre (ISAC)<sup>135</sup> – See section 8.2.2. below.

An organisation may already have in place a chat group, encrypted emails and a shared secure space on the web, where to share information, like many existent communities. The idea is to move from a (traditional) set of tools and systems, created over time, to a more scalable and integrated set of tools. These, as guidelines, serve as a starting point for other operational communities (with organisations included as part thereof) to conduct their own evaluation and see how various tools could fit their sizes and needs.<sup>136</sup>



137

An organisation should:<sup>138</sup>

1. define the goals and objectives of information sharing, in line with its business objectives and cyber resilience framework, in order to facilitate sector-wide response to large scale incidents. At the very least, the objectives should include collecting and exchanging information in a timely manner that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber-attack;
2. define the scope of information-sharing activities by identifying the types of information available to be shared (in example: an attackers' *modus operandi*, indicators of compromise, and threats and vulnerabilities *etcetera*), the circumstances under which sharing this information is permitted (as in the case of a cyber incident), those with whom the information can and should be shared (such as: the organisation's direct stakeholders such as critical service providers, participants and other interconnected organisations *etcetera*), as well as how information provided to an organisation and other sector participants will be acted upon;
3. establish and regularly review the information-sharing rules and agreements and implement procedures that allow information to be shared promptly and in line with the objectives and scope established above, while at the same time meeting its obligations to protect potentially sensitive data that may have adverse consequences if disclosed improperly;

<sup>135</sup> <https://www.enisa.europa.eu/publications/secure-group-communications>

<sup>136</sup> <https://www.enisa.europa.eu/publications/secure-group-communications>

<sup>137</sup> Designed by Leon Andrew de Lange, 18 October 2019; with credit to Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcb/publ/d454.pdf>

<sup>138</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank;

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber resilience oversight expectations for financial market infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber%20resilience%20oversight%20expectations%20for%20financial%20market%20infrastructures.pdf)

4. establish trusted and safe channels of communication with its direct stakeholders for exchanging information;
5. have in place a process to access and share information with external stakeholders in a timely manner, such as regulators, law enforcement or other organisations within the FMI's ecosystem;
6. participate actively in existing information-sharing groups and facilities, including cross-industry, cross-government and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats;
7. establish and implement protocols for sharing information relating to threats, vulnerabilities and cyber incidents with employees, based on their specific roles and responsibilities;
8. share information with relevant stakeholders in the ecosystem to achieve broader cyber resilience situational awareness, including promoting an understanding of each other's approach to achieving cyber resilience;
9. make use of threat intelligence capabilities that provide internal and external threat and vulnerability information, analyse this information, and disseminate it to the relevant stakeholders in the ecosystem promptly, so as to help stakeholders to respond quickly and mitigate risks;
10. participate in efforts to identify the gaps in current information-sharing mechanisms and seek to address them, in order to facilitate a sector-wide response to large-scale incidents.

**Case Study- European financial infrastructures launch Cyber Information and Intelligence Sharing Initiative (CIISI-EU)<sup>139</sup>**

1. Quoting *Fabio Panetta*, Member of the Executive Board of the European Central Bank, at the fourth meeting of the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures:

- 1.1 "Protecting the integrity of the financial system, and maintaining confidence in it, is critical. Specifically, financial market infrastructures are crucial for intermediation between market participants and end users. They are critical for the everyday livelihood of European citizens, for instance by transmitting salary and pension payments. They are also vital for the functioning of the financial system and the financing of the real economy, as they settle market transactions through a web of settlement banks, clearing houses, settlement systems and custodians.
- 1.2 The setting up the ECRB itself as a forum for strategic discussions on cyber resilience has been an important step. Building on what we have achieved so far, we today wish to launch the Cyber Information and Intelligence Sharing Initiative (CIISI-EU), which members overwhelmingly backed at our meeting in June 2019. This initiative would support our aim of catalysing joint initiatives to develop effective market solutions, working together for the public good and fostering trust.
- 1.3 By addressing cyber risks that can be systemic and highly costly in an increasingly sophisticated threat landscape, CIISI-EU will contribute to protecting the European economy

<sup>139</sup> <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html>;  
<https://www.paymentscardsandmobile.com/european-financial-infrastructures-launch-ciisi-eu/>

and security. The initiative will allow the most important financial infrastructures to share vital technical information among themselves using an automated platform. Members will create a trusted community where they will meet to discuss cybersecurity threats and share related intelligence and best practices. The ECRB members will receive bi-annual threat reports informing them of strategic issues pertinent to their businesses.

- 1.4 Exchanging cyber information and intelligence among peers within a trusted community allows financial infrastructures to leverage the collective knowledge, experience and capabilities of that community to address the threats they may face. It enables them to make informed decisions about their defensive capabilities, threat detection techniques and mitigation strategies. By sharing cyber information and intelligence, financial infrastructures act in the public interest to support the safe and sound operation of the financial system as a whole.
- 1.5 We should not underestimate the significance of taking this step. Never before have the largest pan-European financial infrastructures, in close liaison with Europol and the European Union Agency for Cyber Security, come together and agreed to share information and intelligence. For years, the industry has talked about sharing information and intelligence, but few have actually done it.
- 1.6 The ECRB working group on information sharing, comprised of ECRB members and authorities, has worked very hard over the last year to push forward this unique and ground-breaking model of cooperation. The CIISI-EU operating model has the potential to serve as an example to other communities and jurisdictions on how to work together, share information and catalyse new initiatives.
- 1.7 The work we do within the ECRB also supports the ambitions set by the European Commission as part of its Digital Single Market strategy. Strengthening trust and security is a key element of that strategy, and the Commission has recently launched a public consultation on a potential legal initiative to improve the resilience of financial services against cyberattacks<sup>140</sup>. We look forward to hearing more about this today from the European Commission.”

2. A group of Europe’s largest and most important financial infrastructures, members of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB), chaired by the European Central Bank (ECB), launched an initiative to share vital cybersecurity threat information to help protect European citizens’ savings against cybercriminals.
3. The core objectives of the initiative, known as Cyber Information and Intelligence Sharing Initiative (CIISI-EU), are to protect the financial system by preventing, detecting and responding to cyberattacks; to facilitate the sharing of information and good practices between financial infrastructures; and to raise awareness of cybersecurity threats.
4. “This is the first time that major financial infrastructures, Europol and the European Union Agency for Cybersecurity (ENISA) have jointly taken steps against cyber risk,” said ECB Executive Board member and ECRB Chair, Fabio Panetta. “We hope this will be an inspiring model for other jurisdictions to tackle one of the biggest threats of our time. Cybercriminals are increasingly stealing money, and therefore sharing information will help us to prevent attacks and ultimately protect people’s money.”
5. “Protecting the integrity of the financial system, and maintaining confidence in it, is critical. Specifically, financial market infrastructures are crucial for intermediation between market participants and end users. They are critical for the everyday livelihood of European citizens, for instance by transmitting salary and pension payments. They are also vital for the functioning of the financial system and the financing of the real economy, as they settle market transactions through a web of settlement banks, clearing houses, settlement systems and custodians.

<sup>140</sup> [https://ec.europa.eu/info/sites/info/files/business\\_economy\\_euro/banking\\_and\\_finance/documents/2019-financial-services-digital-resilience-consultation-document\\_en.pdf](https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf)

6. Cyberattacks are already used to harm companies and to interfere with national and international politics. Cyberattacks against financial market infrastructures would undermine confidence in the financial system, with repercussions on the economy as a whole. Fending off these attacks is therefore a matter of European security.”
7. In the coming months, the ECB will publish the framework for the CIISI-EU sharing initiative to encourage other jurisdictions to follow suit.
8. Cyber threats pose a serious risk to the stability of the European and global financial system. Cyber threats are borderless and the capabilities of the attackers are constantly evolving, threatening to disrupt the interconnected global financial systems. To successfully combat cyber risk, financial infrastructures need to actively participate in information and intelligence sharing arrangements and collaborate with trusted stakeholders within the industry as a whole.

### **8.2.1 Cross Industry; Cross Governmental and Cross Border / Jurisdictional Information Sharing:**<sup>141</sup>

Different kinds of cyber-security information are shared, on a voluntary or mandatory basis, by organisations and regulators, including cyber-threat information, information related to cyber-security incidents, regulatory and supervisory responses in case of cyber-security incidents and/or identifications of cyber-threat and best practices related to cyber-security risk management. Depending on the type of arrangement, the kind of information shared varies.

For some of the jurisdictions, both mandatory and voluntary information-sharing arrangements are noted for the same type of information-sharing arrangement. This is because voluntary/mandatory sharing is sometimes applicable when different types of information are being shared, or when information is shared with different parties. In Example: In the jurisdiction of Singapore, there is a mandatory requirement for financial institutions to report relevant cyber-security incidents to the Monetary Authority of Singapore (MAS), while cyber-threat information exchange between MAS and the Cyber Security Agency (CSA) Singapore is voluntary.

Other types of information-sharing arrangements are observed, which include: public announcement or the disclosure of information about cyber-security incidents; as well as cross-sector information sharing with public and private institutions. In particular, the range of stakeholders involved in cyberattacks typically includes non-bank critical infrastructure operators, third-party service providers and customers who could contribute to sharing information with security agencies for further distribution to other sectors, or be part of other setups such as a joint-industry groups.<sup>142</sup>

Legislative Options for Cyber-Information Sharing:<sup>143</sup> Two categories of cyber-information sharing exist, namely:

1. the sharing of information in the possession of the government, regulatory or supervisory bodies; and

<sup>141</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>142</sup> This “other” type of information is shown in Figure 3. One example is the EBA guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05) and recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), which assumed good information-sharing of IT risks between banks and supervisors, although there was no specific requirement for banks to report security incidents to their supervisors; Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>143</sup> <https://fas.org/sgp/crs/intel/R43941.pdf>

2. the sharing of information in the possession of the private sector.

A myriad of legal issues arise with respect to each category. Ultimately of benefit, Legislators and Regulators need to address any legal obstacles that may prevent more robust cyber-intelligence sharing, whether by removing legal barriers to information sharing or by effectuating more comprehensive change with regard to the distribution of cyber-intelligence within and amongst the public and private sectors, as well as for government, regulatory or supervisory bodies.

Various legislative proposals on cybersecurity information sharing could merit a lengthy discussion, however, six identified themes permeate the various proposals aimed at promoting cybersecurity information sharing, including:

1. Creating a Broader Legal Framework for the Sharing of Cyber Information – a framework that contemplates broader cybersecurity information sharing, addressing:
  - a. the types of cybersecurity information that is authorised for dissemination within the private sector and between the private and public sectors;
  - b. the entities that can receive such information; and
  - c. the purposes for which such information can be used.
2. Clarifying Which Government Agency Leads the Efforts on Cyber Information Sharing:
  - a. the legislation may need to resolve what entity in the government needs to be the liaison between the public and private sector with regard to such sharing of information.
3. Increasing the Amount and Quality of Government Cyber Information Disclosed to the Private Sector ensuring that the underlying information that is disseminated from the government is both voluminous and helpful.
4. Minimising liability related to distributing privately held cyber intelligence.
5. Adopting and implementing a tailored approach to minimising liability, with two approaches:
  - a. more narrowly tailored immunity provisions, such that a provision is tied to a particular law that could be the source of civil or criminal liability for private entities that engage in cyber-information sharing; or
  - b. cyber-security exception to any antitrust laws, by creating an explicit “legislative carve-out” allowing for the exchange of “vulnerability, threat, and countermeasure information and the development of common security protocols.”
6. Adopting and implementing a broad approach to minimizing liability proposing more sweeping language that broadly immunises private entities involved in collecting and disclosing cyber intelligence and then drafting tailored exceptions to curb the scope of the immunity, possibly incorporating:
  - a. Notwithstanding Clauses;
  - b. Limitation of Liability Clauses;
  - c. Good Faith Safe Harbours; and
  - d. Pre-emption Clauses.

Preventing Government, Regulatory / Supervisory Bodies’ misuse of acquired cyber intelligence: A balance is to be struck through means of the legislative provisions that govern cyber information sharing so as to ensure the prevention of forfeiting of certain intellectual property rights; where such information sharing be used against a private entity in a subsequent regulatory action; or the risk of the privacy rights of individuals whose information may be encompassed in disclosed cyber-intelligence.

In reiteration of the principles of the CIA / AIC triad: Rules concerning the confidentiality, integrity and availability of data should be observed by all entities, at all given times. Confidentiality is the policy governed set of rules which limits access to information. Integrity is the assurance that the information is trustworthy and accurate. Availability is a guarantee of reliable access to the information by authorised persons.

### 8.2.2 Amongst Banks; with a brief case study of UBF-ISAC:<sup>144</sup>

Banks share information (in example: knowledge of a cyber-security threat) with peer banks through established channels, mainly to allow peer banks to take more timely action in response to similar threats. Although there is no common standard for automated information-sharing, regulators in most jurisdictions are not directly involved in bank-to-bank information-sharing but do play a role in facilitating the establishment of voluntary sharing mechanisms for cyber-vulnerability, threat and incident information, and in some cases indicators of compromise. Some jurisdictions have established public sector platforms to accomplish information-sharing initiatives while others have encouraged private sector development of information-sharing organisations. Three jurisdictions (Brazil, Japan and Saudi Arabia<sup>145</sup>) have mandated cyber-security information-sharing among banks through regulations or statutes.

Sharing of information and collaboration among banks depend on the financial industry's culture and level of trust among participants. Experience shows that a two-level information-sharing structure through which information would be first shared on the interpersonal level with a closer group and then be exchanged at the company level with a broader group of banks helps build trust into the system.

#### Case Study: United Arab Emirates Banking Federation ISAC<sup>146</sup> (UBF-ISAC):

## **UBF launches first cyber threat sharing platform for UAE banks**

Banks to share cyber security intelligence on Anomali ThreatStream

147

*The Power of Active Collaboration in ISACs, ISAOs and Security Interest Groups<sup>148</sup>*

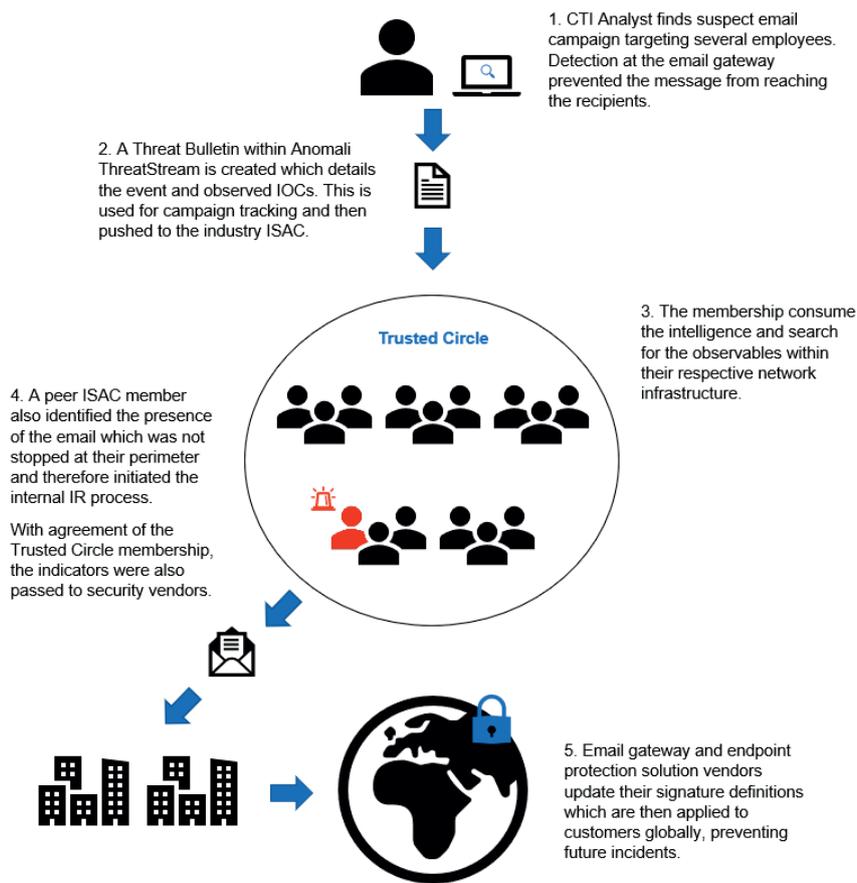
<sup>144</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>145</sup> Cyber Security Framework, Saudi Arabian Monetary Authority, May 2017; <http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf>

<sup>146</sup> United Arab Emirates Banking Federation-ISAC; <http://www.uaebf.ae/en/>

<sup>147</sup> UBF launches first cyber threat sharing platform for UAE banks, Banks to share cyber security intelligence on Anomali ThreatStream; Published: September 14, 2017 16:00, By Babu Das Augustine, Banking Editor - <https://gulfnews.com/business/banking/ubf-launches-first-cyber-threat-sharing-platform-for-uae-banks-1.2090165> ; <https://www.anomali.com/files/data-sheets/ThreatStream-Datasheet.pdf>

<sup>148</sup> <https://www.anomali.com/blog/the-power-of-active-collaboration-in-isacs-isaos-and-security-interest-groups>



149

*The Power of Active Collaboration in ISACs, ISAOs and Security Interest, continued:* “Encouraging and supporting information sharing and collaboration within and across industries is a vital component for security programs worldwide. Making information on threats discoverable and accessible using the appropriate medium within a timely and secure manner will help minimize the impact and effectiveness of cyber-attacks for all organisations.”<sup>150</sup>

### Case Study- FS-ISAC – key features and benefits:<sup>151</sup>

9. The Financial Services Information-sharing and Analysis Center (FS-ISAC) is a non-profit entity established in 1999 to collect and provide financial services sector member organisations with information on potential vulnerabilities as well as timely, accurate and actionable warnings of physical, operational and cyber-threats or attacks on the national financial services infrastructure. Its members include banks, credit unions, insurance companies, investment companies, financial services regulators and law enforcement entities.

<sup>149</sup> The Power of Active Collaboration in ISACs, ISAOs and Security Interest Groups, Marc Green, Anomali Inc. 2018, <https://www.anomali.com/blog/the-power-of-active-collaboration-in-isacs-isaos-and-security-interest-groups>

<sup>150</sup> The Power of Active Collaboration in ISACs, ISAOs and Security Interest Groups; <https://www.anomali.com/blog/the-power-of-active-collaboration-in-isacs-isaos-and-security-interest-groups>

<sup>151</sup> Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

10. In addition to the core information-sharing platform, the FS-ISAC hosts conferences and educational seminars, conducts sector and cross-sector contingency planning exercises, and is an internationally recognised source for threat intelligence information. Core elements of the FS-ISAC include:
  - 10.1 Rapid response: the FS-ISAC analyses and disperses information and threat intelligence information among its members through their proprietary real-time Critical Infrastructure Notification System (CINS).
  - 10.2 Information analysis and sharing: the FS-ISAC receives information from many sources that is verified and classified by type and severity. The information is then sent out by CINS and reaches members instantly. FS-ISAC also conducts crisis calls if necessary, and has a team working 24/7 to analyse any incoming data and disseminate information.
  - 10.3 Anonymised data: Information received and disseminated through the FS-ISAC is considered confidential and stored in a standalone, secure portfolio so that no threat or information can be traced back to its source by any members and all information is anonymously shared. This makes the FS-ISAC a safe place for its members and encourages sharing.
  - 10.4 Member-driven: The members of the FS-ISAC run the organisation, tailoring it specifically for the needs of the financial industry.
  - 10.5 Recognised by US Financial Services Regulators: the Federal Financial Institutions Examination Council, a group consisting of federal and state US financial services regulators, has recognised the FS-ISAC as a key threat intelligence source and recommends financial institutions participate in its process to identify, respond to and mitigate cyber-security threats and vulnerabilities.

### **8.2.3 From Banks to Regulators:<sup>152</sup>**

The sharing of cyber-security information from a bank to its regulator(s)/supervisor(s) is generally limited to cyber-incidents based on regulatory reporting requirements. Such requirements are mainly established to:

1. enable systemic risk monitoring of the financial industry by regulator(s);
2. enhance regulatory requirements or issue recommendations by regulator(s) to adjust policies and strategies based on information collected;
3. allow appropriate oversight of incident resolution by regulator(s); and
4. facilitate further sharing of information with industry and regulators to develop a cyber-risk response framework.

Reporting requirements are established by different authorities for specific purposes, depending on their mandate. Different scopes and perimeters may depend on the:

1. type of authority - supervisors, regulators, national security;
2. their mandate- national cyber-security agencies, consumer protection, banking supervision *etcetera*;
3. sector(s) involved - multisector or specific: banks, significant banks, systemic operators, payment); and
4. geographical range - national, multi-regional.

<sup>152</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbst/publ/d454.pdf>

Incident reporting by banks to regulator(s) is a mandatory requirement in many jurisdictions, with different scopes of requirements and ranges of application. Some requirements also include the obligation to submit a root cause analysis for the incident, or a full post-mortem or lessons learnt after the incident. While many of the supervisors focus only on reporting and tracking incidents that have already taken place, some require proactive monitoring and tracking of potential cyber-threats because concerns about reputational risk may lead to a delay in incident reporting by the regulated entity.

Based on these considerations, different reporting frameworks are also observed. These range from formal communications to informal communications, such as free-text updates via email or telephonic verbal updates. Differences are noted in:

1. taxonomy for reporting;
2. reporting time frame (immediately, after two hours, after four hours and after 72 hours are examples of practices observed);
3. templates; and
4. threshold to trigger an incident reporting.

These differences highlight the fragmentation issue facing the banks operating in multiple jurisdictions or supervised by different authorities, as these banks are likely to be obliged to fill in various templates with different taxonomy, reporting time frame and threshold. This may increase their regulatory burden, consuming significant resources to ensure compliance. It may be possible for an authority with multiple functions to receive from a bank multiple reports with distinct formats for multiple times.

All incident reporting processes have a single direction flow, by a bank to an authority, although an informal flow back can be used for alerting firms in case of an incoming threat. By normalising the prompt exchange of information between banks and supervisors, reciprocal flow mechanisms can help remove the possible stigma associated with incident reporting by banks, thereby fostering effective and timely incident reporting.

#### **8.2.4 Amongst Regulators:<sup>153</sup>**

Regulators share information with fellow regulators (domestic or cross-border), as appropriate according to established mandatory or voluntary information-sharing arrangements shared between them. Cyber-security information shared among regulators may include regulatory actions, responses and measures.

Considering different types of cyber-security information-sharing, information-sharing among regulators is the least observed practice across jurisdictions, although it is expected that many informal and ad hoc communication channels exist, such as through supervisory colleges and memoranda of understanding. Cyber-fraud is becoming more sophisticated and cross-jurisdiction, and sharing of cyber-security information among regulators could assist in maintaining awareness of the cyber-threat situation for timely guidance to be provided to banks to protect financial systems against cyber-frauds.

#### **Case study – Bilateral cyber-security information-sharing between the Hong Kong Monetary Authority (HKMA) and the Monetary Authority of Singapore (MAS)**

<sup>153</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

Given the importance of facilitating more cross-border cyber-security information-sharing, the Hong Kong Monetary Authority (HKMA) and the Monetary Authority of Singapore (MAS) established a bilateral cyber-security information-sharing framework in the first quarter of 2018.

As part of the framework, the HKMA and MAS have agreed upon four (4) important guiding principles and key design features of the governance arrangement, the scope of information-sharing, a traffic light protocol, standard taxonomy and dedicated communication channels.

1. Voluntary: Given that some cyber-security information may be highly sensitive, the sharing of information under the framework should be voluntary, without creating any legal obligations for the participating authorities.
2. Timely: The HKMA and MAS recognise that timely sharing of cyber-security information is of paramount importance to building an effective framework. The authorities have therefore agreed that information about cyber-security incidents should be shared as soon as possible to the extent permitted by law. If a cyber-security incident is assessed to have the potential to spread to other jurisdictions, the related information should be shared within 24 hours. Incomplete information about cyber-security incidents can be shared so long as a reasonable degree of validity has been ascertained.
3. Effective: To ensure the efficacy of the framework, sharing of cyber-security information should not be limited to information related to those financial institutions with an operation in both jurisdictions (i.e. unlike typical supervisory college or memoranda of understanding, “supervisory locus” is not required to be established). A taxonomy was also established with reference to the Structured Threat Information eXpression (STIX) framework.
4. Confidential: The confidentiality of any information shared between the authorities should be properly protected. The framework will focus on the sharing of general information such as the modus operandi of the attacks. The authorities also adopted a Traffic Light Protocol (TLP) for subsequent sharing of information.

The HKMA and MAS have been exchanging information regarding real-life cyber-threats and cybersecurity-related regulatory responses and measures since April 2018.

### **From Regulators to Banks:<sup>154</sup>**

Information-sharing from regulators to banks occurs through established channels, based on the information the regulator receives both from banks and other sources. Various jurisdictions, including: Australia, China, Korea, Saudi Arabia<sup>155</sup>, Singapore, Turkey and the US, have established clear guidance in the form of standards and practices to enable cyber-security information-sharing by regulators to banks. In these jurisdictions, information flows from the bank to the regulator, and the regulator assesses the risk to the financial industry and shares the information with the industry, as appropriate, based on the risk assessment. In cases where the information is sensitive (in example that which contains customer-specific or bank-specific information), the regulator anonymises or summarises it to allow sharing.

<sup>154</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>155</sup> Cyber Security Framework, Saudi Arabian Monetary Authority, May 2017; <http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf>

Regulators with a regulator to bank sharing mechanism more readily share publicly available information such as cyber-security risk management best practices. They use informal channels such as industry sharing platforms (in example: participation in industry forums), meetings and informal communications to disseminate information to the banks.

In cases where non-public information is obtained by regulators, the information is shared with selected parties via informal meetings or other informal communication vehicles, so as to preserve anonymity and confidentiality of the institution(s)/bank(s) impacted by a cyber-attack, and maintain banks' confidence and trust in the regulators generally.

Mandatory requirements for regulators to share information with banks have only been established for a few jurisdictions, such as: China). A few other jurisdictions have put in place practices for voluntary sharing, in example: Singapore and the UK.

Many jurisdictions, however, have not put in place any standard practices for regulators in the sharing of information with banks, nor established any process or time frame to enable timely, risk-based information-sharing. Classification of information could ensure that the appropriate audience could receive the appropriate information and help to build trust between regulators and banks.

### **8.2.5 With Security Agencies; with brief a case study of a CSIRT (Computer Security Incident Response Team):<sup>156</sup>**

Given that cyber-security incidents encountered by banks or regulators could potentially be experienced by entities in other sectors, effective communication of relevant cyber-security incidents with security agencies could facilitate broader awareness of cyber-threats in a timely manner, and enhance defensive measures against adversaries.

For jurisdictions with operations of Computer Emergency Readiness Team (CERT) or similar security agencies, these agencies may act as focal points for cyber-security incident notification. Banks or regulators share cyber-security information with these agencies for broader circulation of information and collaboration with other sectors within the country, such as the public sector, civilian sector and computer community. Jurisdictions have generally set out standards and practices for critical infrastructure entities and regulators to share cyber-security information with national security agencies. While most jurisdictions adopt a voluntary approach, a few jurisdictions mandate formal sharing requirements. Some jurisdictions (like: Luxembourg, the US) have established sharing platforms to facilitate multilateral sharing of cyber-security incident or cyber-threat information. In the US, an online portal is available for cyber-security information to be submitted to the National Cyber-security and Communications Integration Center<sup>157</sup> and the US CERT<sup>158</sup>. In Luxembourg, the Computer Incident Response Center (CIRCL)<sup>159</sup> has established a Malware Information-sharing Platform (MISP) to gather, review, report and respond to computer security threats and incidents. The MISP allows organisations to share information about malware and their indicators. The aim of this trusted platform is to help improve the counter-measures used against targeted attacks and set up preventive actions and detection.

<sup>156</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf> & Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>157</sup> National Cybersecurity and Communications Integration Center; <https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center>

<sup>158</sup> <https://www.us-cert.gov/>

<sup>159</sup> <https://www.circl.lu/>

For jurisdictions with mandatory requirements for cyber-security incident information-sharing with national security agencies (such as: Canada, France, Singapore and Spain), the sharing arrangements are bilateral in general. Instead of requiring banks or regulators to share all cyber-security incidents, these jurisdictions require cyber-security incidents affecting key operators of critical infrastructure to be reported.

Some jurisdictions have established procedures for relevant information to be exchanged voluntarily and bring together relevant parties for coordination of responses to incidents. In the UK, the Authorities Response Framework can be invoked by financial authorities to bring together the Financial Conduct Authority (FCA), the Bank of England, the Treasury, the National Crime Agency and the National Cyber-security Centre to coordinate their response to a cyber-security incident. Meetings and formal communications can be triggered as appropriate.

### Case study – Computer Security Incident Response Teams (CSIRTs) in the European Union (EU)<sup>160</sup>

The Network and Information Security (NIS) Directive<sup>161</sup> is a component of the European Union’s legislation with the explicit aim of improving cyber-security throughout the EU. The directive was promulgated on 10 May 2018 and defines various obligations across the EU, one of which concerns the establishment of one or more Computer Security Incident Response Teams (CSIRTs) at National level, for purposes of ensuring comprehensive incident management across the EU.

Mandatory incident reporting and notification to national CSIRTs (directly or through a competent authority) is directed for entities identified as “*Operators of Essential Services*” (OES)<sup>162</sup> and “*Digital Service Providers*” (DSP)<sup>163</sup>. Notably, some banks have been included in the first category – that of OES. In some countries, competent supervisory authorities for banks have identified certain banks as OES, whilst other banks may be declared to be OES by the Ministry of Finance or another governmental authority.

The NIS Directive<sup>164</sup> has also detailed the requirements to have a CSIRTs European network, existing as a dedicated network for all national CSIRTs and run by the member states, with its secretariat provided by the European Network and Information Security Agency (ENISA)<sup>165</sup>, with the following competencies:

1. Exchange information on services, operations and cooperation capabilities.
2. Exchange and discussing information related to incidents and associated risks (upon receipt of request and responded to on a voluntary basis)
3. Identify a coordinated response to an incident (upon receipt of request)

<sup>160</sup> Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>161</sup> DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

<sup>162</sup> **Operators of essential services** are private businesses or public entities with an important role to provide security in healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply; [https://europa.eu/rapid/press-release MEMO-18-3651\\_en.htm](https://europa.eu/rapid/press-release_MEMO-18-3651_en.htm); seven categories of activity, including energy, transport, and the health sector. Non-traditional utilities in the form of providers of digital infrastructure, consisting of IXPs, DNS service providers and TLD name registries, also fall within the definition of OES; <http://www.arthurcox.com/wp-content/uploads/2019/07/Network-and-Info-Systems-Directive-July-2019.pdf>

<sup>163</sup> These include: Online marketplaces; Online search engines (a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase, or other input, and returns links in which information related to the requested content can be found); and Cloud computing services, including IaaS, PaaS and SaaS operators (Defined by the 2018 Regulations as “a digital service that enables access to a scalable and elastic pool of shareable computing resources”); DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union; [https://europa.eu/rapid/press-release MEMO-18-3651\\_en.htm](https://europa.eu/rapid/press-release_MEMO-18-3651_en.htm)

<sup>164</sup> The Directive on security of network and information systems (NIS Directive); <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

<sup>165</sup> <https://www.enisa.europa.eu/>

4. Providing member states support in addressing cross-border incidents (responded to on a voluntary basis).
5. Issue guidelines concerning operational cooperation.
6. Discuss, explore and identify further forms of operational cooperation (risks and incidents, early warnings, mutual assistance, coordination).
7. Discuss the capabilities and preparedness of certain CSIRTs upon request from that CSIRT).

## 9. Learning and Evolving:<sup>166</sup>

An organisation's cyber resilience framework needs to achieve continuous cyber resilience amid a changing threat environment. To be effective in keeping pace with the rapid evolution of cyber threats, an organisation should implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the organisation to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. An organisation should aim to instill a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

### 9.1 Cyber Threat Intelligence (continued):<sup>167</sup>

An organisation should:

1. have capabilities in place to gather information on common vulnerabilities, cyber threats, events and incidents occurring both within and outside the organisation;
2. have the capabilities to analyse the information gathered and assess the potential impact on its cyber resilience framework;
3. distil and classify the lessons learned (in example: strategic, tactical and operational), identify the key stakeholders to whom these apply, incorporate them to improve the organisation's cyber resilience framework and capabilities, and convey them to each relevant stakeholder on an ongoing basis;
4. ensure that senior management has a programme for continuing cyber resilience training and skills development for all staff. This training programme should include the Board members and senior management and should be conducted at least annually. The annual cyber resilience training should include incident response, current cyber threats (such as: phishing, spear phishing, social engineering and mobile security) and emerging issues. The organisation should ensure that the training programme equips staff to deal with cyber incidents, including how to report unusual activity;
5. ensure that cybersecurity awareness materials are made available to staff when prompted by highly visible cyber events or by regulatory alerts;

<sup>166</sup> CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>167</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); Anomali Incorporated, <https://www.anomali.com/>

6. incorporate lessons learned into the staff training, awareness programmes and materials, on an ongoing and dynamic basis. The organisation should utilise industry and authority initiatives related to awareness and training, where possible;
7. set a range of indicators and develop management information to measure and monitor the effective implementation of the cyber resilience strategy and framework on a regular basis and its evolution over time. For example, relevant information and indicators could be: the percentage of the organisation's staff that have received cybersecurity training; the percentage of incidents reported within the required timeframe per applicable incident category; the percentage of vulnerabilities mitigated within a defined time period after discovery; and yearly reports monitoring progress of indicators, *etcetera*;
8. validate the effectiveness of incorporating lessons learned into the employee training and awareness programmes on a regular basis;
9. actively monitor technological developments and keep abreast of new cyber risk management processes that could effectively counter existing and newly developed forms of cyber-attack. An organisation should consider acquiring such technology and know-how to maintain its cyber resilience;
10. analyse and correlate findings from audits, management information, incidents, near misses, tests (e.g. vulnerability assessment, penetration testing and red team testing, etc.), exercises and external and internal intelligence in order to enhance and improve its cyber resilience capabilities. An internal cross-disciplinary steering committee could drive this activity;
11. incorporate lessons learned from real-life cyber events and/or from testing results on the organisation and/or other organisations, to improve the its risk mitigation capabilities, as well as its cyber contingency, response, resumption and recovery plans;
12. continuously track its progress in developing its cyber resilience capabilities from a current state to a defined future state. A maturity model can assist the organisation in documenting this progress;
13. have capabilities in place to use multiple sources of intelligence, correlated log analysis, alerts, traffic flows, cyber events across other sectors and geopolitical events to better understand the evolving threat landscape and proactively take the appropriate measures to improve its cyber resilience capabilities.

## **10. Cyber Resilience assessment, baselines and performance metrics:<sup>168</sup>**

An Organisation should define the cybersecurity baselines, serving as minimum security controls that must be complied with, further subject to Organisations being encouraged encouraged to implement additional, enhanced controls based on each individualist Organisation's risk appetite, always being mindful of the aimed objective to the desired level of cybersecurity and resilience. Organisations are further encouraged to collaborate across industries, sectors, jurisdictions and the

<sup>168</sup> Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

like on such enhanced controls in the aim to improve overall industry, sector or jurisdictional risk posture and too, which may influence future updates, additions or amendments to baselines.

### **Before compromise:<sup>169</sup>**

#### **Event:**

1. External scanning blocked connections (count)
2. New vulnerabilities (by OWASP type: count)
3. Malware stopped (count)
4. Phishing sites known (count)
5. Phishing site takedown (count, hours open)
6. Unique malware targeting bank (count)
7. Vulnerabilities per line of code (count)
8. Applications going into production with code vulnerabilities (count)
9. Security events detected (count)

#### **Practices:**

1. Penetration testing (by type: count and finding rating)
2. Systems protected by IAM (count)
3. Internally developed systems which cannot be updated (by type: count)
4. Systems with out-of-vendor support components (by type: count)
5. Systems without anti-malware solutions (count)
6. Non-authorized (compliant) devices (by type: count)
7. Information security configuration compliance (coverage %)
8. Awareness exercises (coverage %, count)
9. Staff responding to phishing tests (% of total staff);
10. User access review (coverage %)
11. Security assessments of providers over 12 months (% coverage of relevant third parties)
12. Patch ageing (by criticality: days)
13. Assurance report on information security (findings by rating, ageing to remediation)

### **At compromise:<sup>170</sup>**

#### **Event:**

1. Detected malicious software endpoints (count)
2. Detected malicious software on servers (count)
3. Online directories containing staff/customer info (count)
4. Incident type over period (count per: denial of service, malicious code, misuse, reconnaissance, social engineering, unauthorised access, other)

#### **Practices:**

1. Resolution and recovery plans developed (by type: count)
2. Incident rehearsals (by type: count)

<sup>169</sup> Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>170</sup> Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

### After compromise:<sup>171</sup>

#### Event:

1. Detected APT (count)
2. Blocked connections to malicious websites (count)
3. Data breaches detected (count)
4. Bank losses (value)
5. Customer loss (value)

#### Practices:

1. Post-incident reports (count)

## **11. Cyber Risk Insurance:**

As data mega-breaches are now commonplace, organisations worldwide are focusing on how to best manage and mitigate cyber-risk, in addition to the necessary safeguards addressed in this report. The fact is: the current threat environment means that breaches are inevitable and should be viewed as such, so that organisations appropriately and best safeguard themselves and the data they hold. As such, Cyber Risk Insurance should not be regarded as an optional extra, or luxury commodity, but rather and a necessity. It is crucial for Organisations to obtain the correct and adequate coverage, whilst too having full understanding of their risk posture.

First party coverage protects against losses incurred directly by the company in response to a cyber incident (direct expenses), and typically includes theft and fraud, forensic investigation, business interruption, extortion, and computer data loss and restoration. Third party coverage, in contrast hereto, protects against losses incurred by third parties in response to a cyber incident, and typically includes litigation, dealings with regulators, notification costs, crisis management and credit monitoring. Cyber insurance is written and priced to suit individual customers. As such, cyber insurance policies may stipulate exclusions, impose limits, or add clauses to protect the insurer from higher risks (e.g. non-performance of a cloud-computing provider, unencrypted devices that contain personal or other sensitive data, computer software malfunctions due to programming errors.)<sup>172</sup>

In consideration of risk, organisations are subject to overwhelming exposure to financial losses, costs of a breach, possible punitive legal / regulatory consequences, or payment of civil damages legal which could arise as a result of any such breach. Reputational ruin and the diminishment of trust and investor security are of paramount concern in the context of financial stability. Data breaches have the clear potential to negatively affect an organisation's valuation or a Nation's currency, depending on the veracity of the breach suffered.

In a bid to transfer the risks of a cyber breach, Organisations may look to cyber insurance for added protection – again, in addition to the necessary safeguards of cyber resilience. Organisations need to be confident that their insurance effectively transfers risk, considering the current threat and regulatory environment and be reminded that the threat landscape is an ever-evolving landscape. Insurers, in turn, need a comprehensive view of the organisation's security posture. An Organisation

<sup>171</sup> Bank for International Settlements, Basel Committee on Banking Supervision, Cyber-resilience: Range of practices, December 2018; <https://www.bis.org/bcbs/publ/d454.pdf>

<sup>172</sup> [https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY\\_Risk\\_CyberInsurance\\_Noexp.PDF](https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF)

too must be mindful that: “Cyber insurance is only one element of risk management and it will never be able to remove cyber risk entirely”.<sup>173</sup>

Organisations are advised to ensure clarity in any cyber insurance policy wording and exclusions, in order to be confident that the policy that will meet their expectations in the event of a claim.

Key considerations for Organisations when contracting and onboarding Cyber Insurance coverage:<sup>174</sup>

1. If at all possible, contract to include retroactive cyber insurance coverage when first signing a contract. Given the fact the identification of a cyber-attack may only become evident after a considerable lapse of time - on average, globally, it takes 279 days to detect and contain a breach, whereas in the Middle East in 2019 it was reported that it takes on average 381 days.<sup>175</sup> Some insurers will allow and cover this (perhaps subject to the payment of an additional or higher premium), however, some will not. It is worth bearing in mind that Organisations can lower their risk of having to make a claim/claims retroactively through employing advanced testing, in example: penetration testing whereby previous breaches or attempts at attacking an Organisation’s network are often identified.
2. Make sure to get coverage for claims resulting from vendor or third-party supplier negligent or intentional acts / errors which result in breaches, in addition to an Organisation’s own negligent or intentional acts / errors which result in same. Vendor, Supplier and Third-Party management is further applicable here. Similarly, if an Organisation handles, controls, processes, stores or in any way handles any sensitive and/or personal data on behalf of others, an Organisation must duly ensure that they are sufficiently covered to compensate such claimant in the event of any breach of such data.
3. Ensure that coverage is included for any loss of data, which includes (but is not limited to) incidents due to employees or others who could unintentionally contribute to a data breach, exposure or loss. This is particularly relevant in the context of a breach occurring from within (inside) an Organisation and not as a result of outside penetration.
4. Ensure to clearly understand the insurance policy’s coverage to ensure that physical systems (networks and servers) are covered sufficiently therein, in addition to every physical asset of an Organisation as well in need of coverage as well. This will include: door locks, security cameras, phone systems, HVAC infrastructure (heating, ventilation, and air conditioning), and all types of control systems which are vulnerable to access and exploitation. This adds complexity to cyber insurance policies and as such, it is prudent to understand which insurance product covers the physical aspect of a breach.
5. Cyber risk is extremely difficult for insurers to quantify, leading to policies that are more customized than non-cyber policies, and therefore could potentially be more costly. Negotiate with an insurer for a lower premium or rate after an advanced penetration test is conducted and findings have been remediated – Sophisticated Insurers should understand the benefits of this offensive approach to cybersecurity and gaining valuable insight as to the Organisation’s present or potential risk exposure through this exercise.
6. An Organisation must ensure to have adequate understanding of the claims process. Not all cyber claims are treated equally and as such, Organisations should know what will be needed to file a claim and ensure that they will be able to satisfy the Insurers’ requirements before

<sup>173</sup> [https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY\\_Risk\\_CyberInsurance\\_Noexp.PDF](https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF)

<sup>174</sup> <https://www.cio.com/article/3202079/5-considerations-when-purchasing-cyber-insurance.html>;  
[https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY\\_Risk\\_CyberInsurance\\_Noexp.PDF](https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF)

<sup>175</sup> IBM Security and Ponemon Institute are pleased to release the 2019 Cost of a Data Breach Report;  
[https://www.ibm.com/downloads/cas/ZBZLY7KL?\\_ga=2.83934879.749854357.1584273312-689978418.1584273312](https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.83934879.749854357.1584273312-689978418.1584273312)

purchasing insurance coverage. Of particular relevance here may an Organisation’s Incident Response processes and procedures, for assessment by an Insurer in the event of a claim.

- An Organisation must be able to balance the cost of premiums, in addition to that of implementing controls. Whilst insurance policies may assist in transferring risk (and not eliminating risk), organisations should conduct a ‘cost-benefit analysis’ to determine the appropriateness of investing in cyber insurance coverage.

Coverage provided by cyber insurance: Although traditional insurance policies may offer the option to cover some specific areas related to cyber risk, they are not designed to fully cover all the potential costs and losses.<sup>176</sup> Consideration of the following coverage areas are to be adequately considered and addressed by Organisations in relation to their Cyber Insurance Policies, in addition to other insurance policies which they may have.

**Figure 2: Comparison between traditional insurance and cyber policies**

	General liability 	Property 	E&O/D&O 	Crime 	Cyber 
Network security	+	+	+	+	✓
Privacy breach	+	+	+	+	✓
Media liability	+		+		✓
Professional services	+		+	+	✓
Virus transmission	+	+	+	+	✓
Damage to data	+	+	+	+	✓
Breach notification	+		+	+	✓
Regulatory investigation	+		+	+	✓
Extortion	+		+	+	✓
Virus/hacker attack	+	+	+	+	✓
Denial of service attack	+	+	+	+	✓
Business interruption loss		+	+		✓

 Possible  
 Coverage

177

Estimated costs of Cyber Insurance Coverage:<sup>178</sup>

<sup>176</sup> [https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY\\_Risk\\_CyberInsurance\\_Noexp.PDF](https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF)

<sup>177</sup> [https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY\\_Risk\\_CyberInsurance\\_Noexp.PDF](https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF)

<sup>178</sup> [https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY\\_Risk\\_CyberInsurance\\_Noexp.PDF](https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF)

Size of Company (Based on Revenue)	Small Companies (Less than \$100 Million)	Midsized Companies (\$100 Million - \$1 Billion)	Large Companies (More than \$1 Billion)
Coverage	\$1 - 5 million	\$5 - 20 million	\$15 - 25+ million
Yearly Premium (Cost for Coverage)	\$7,000 - \$15,000 per million in coverage	\$10,000 - \$30,000 per million in coverage	\$20,000 - \$50,000 per million in coverage
<b>Typical Coverage Sublimits (Restrictions on Payout)</b>			
Sub-limits can restrict payouts on a single aspect of coverage from 10 - 50% of the total coverage			
Notification Cost	\$100,000 - \$500,000 limit	\$500,000 - \$2 million limit	\$1.5 - \$2.5 million limit
Crisis Management Cost	\$250,000 - \$1.25 million limit	\$1.25 - \$5 million limit	\$3.75 - \$6.25 million limit
Legal and Regulatory Defense Expense	\$500,000 - \$2.5 million limit	\$2.5 million - \$10 million limit	\$7.5 - \$12.5+ million limit

Source: Deloitte research on insurance provider Web sites

## 12. Conclusion and Recommendations:

1. Strong cyber governance requires an organised, systematic and proactive approach within an organisation, in management of both the prevailing, as well as emerging cyber threats that it faces, or may face; supports efforts to appropriately and adequately consider, as well as manage, cyber risks at all levels within an organisation's ecosystem; and provides for the allocation of adequate resources and expertise to manage cyber-related risks and attacks, within an organisation.
2. Risk management components include Governance; Identification; Protection; Detection; as well as Response and Recovery. Ancillary components, include Testing; Situational awareness; as well as Learning and evolving. An organisation's cyber resilience framework should methodically incorporate the necessary policies, procedures and controls related to the risk management and ancillary components.
3. The value and importance of cyber resilience to the organisation and its key participants (in example: its stakeholders), which may include: proprietors / owners, investors, customers / clients, suppliers / vendors, employees / personnel, contractors, appropriate Legal and Regulatory authorities, appropriate industry bodies and also, competitors. An organisation should consider internal and external stakeholders' priorities and their noteworthy requirements
4. The organisation's overall business vision, objectives, corporate strategy and other strategies which relate to or impact its cyber resilience, which may include: safeguarding the organisation's ongoing operations, efficiency and the financial viability of its services to its users, clients and/or customers *etcetera*;
5. Whilst Regulators generally do not require a specific cyber resilience strategy, all Regulators do and should expect institutions to maintain and suitable cyber resilience capability on the part of organisations. The timeous and effective identification, mitigation and management of its cyber risks is expected of organisations, in addition to a proper assessment of the

organisation's cyber risk appetite, so as to ensure that it remains proportionate to the organisation's risk tolerance.

6. An organisation's cyber resilience strategy should clearly set out the manner in which this implementation plan will be delivered, as well as the tracking and monitoring of such timeous and proper delivery. This is the responsibility of the organisation's Board (or its equivalent within the organisation).
7. An organisation's cyber resilience framework must properly describe the roles and responsibilities, which includes responsibility for decision-making within the organisation, for the identification, mitigation and the management of cyber risks; and together with this: the manner in which cyber resilience initiatives will be adopted, implemented, executed, managed and funded.
8. Cyber-related risks pose mounting, ever-evolving and unique challenges to organisations and as such, require dedicated attention and adequate resourcing.
9. Regulators expect that organisations are to mitigate and minimise their cyber risk exposure in ensuring that their cyber resilience systems and organisational arrangements are secure by-design and that emphasis is placed on resilience in light of current and possible future threats, as opposed to simply ensuring "compliance to a certain standard" type approach.
10. An organisation should have knowledge and make use of the prevailing, up to date international, national and industry-level standards, guidelines and recommendations, including: NIST , COBIT 5 , ISO/IEC 27000 , ISO/IEC 27001 and CPMI-IOSCO Guidance *etcetera*. These sources aim to document industry best practices in the management of cyber threats. There remains a duty upon the organisation to ensure the sources are current and valid, amidst an ever-evolving cyber threat landscape and to use such aids as a benchmark for designing its cyber resilience framework. An organisation is further expected to use these sources for the integration of the most effective and operational cyber resilience solutions, fit for purpose to the organisation in its cyber resilience framework and strategy.
11. In terms of cyber-risk management, IT and operational risk management practices are used to address cyber-risk and supervise cyber-resilience. Organisations are expected to have a strategy and framework to comprehensively map and actively manage their IT system architecture and define the organisation's clear tolerance and appetite levels for cyber-risk, which too is to be approved and adequately challenged at board level.
12. In terms of an organisation's corporate governance/organisation, management models need to specifically incorporate cyber-resilience and clearly articulated across same across the technical, business and strategic management perspectives of an organisation. The organisation's Board should approve its cyber resilience framework and ensure that it is commensurate with the organisation's formulated cyber resilience strategy.
13. In terms of an organisation's workforce, skills shortages lead to recruitment challenges. Organisations can implement or leverage specific cyber-certifications to address this issue.
14. In respect of funding considerations, a comprehensive and realistic costing and budgeting process is to be followed by the organisation, with due consideration of an organisation's organisational capabilities in terms of cyber resilience.

15. The cyber resilience strategy requires considerable and careful scrutinization, assessment for the procurement of resources, which includes sufficient budget and funding resources for payment towards the decided high-level scope of technology and assets for use of the set-up or upgrading of cyber resilience, as well as the management and maintenance thereof within an organisation.
16. Determining the governance which is necessary to enable cyber resilience to be adequately designed, transitioned, operated and improved on by means of cyber resilience maturity, skills sophistication and capability evolvment
17. The execution and integration of cyber resilience across the entire organisation's ecosystem is of paramount importance. This ecosystem includes its people, processes, technology and new business initiatives. This further requires integration within the organisation's various commercial departments, including: business, finance, risk management, internal audit, operations, cybersecurity, information technology (IT), communications, legal and human resources - some of which may be outsourced and external to the organisation
18. Consistency should be observed between an organisation's cyber resilience framework and its enterprise's risk management framework Protection and detection testing, as well as response, recovery and continuity testing are of vital importance. Maintaining and encouraging the organisation's capability to antedate, anticipate, mitigate against any cyber risks; also to withstand at the onset and contain any cyber-attacks, in addition to the effective recovery from any such attacks is of paramount importance.
19. Incident response capabilities: An incident management framework may not necessarily be required as being mandatory of an organisation, but is recommended. Incident response plans must, however, be made mandatory, to deal with material cyber-related incidents, with regard to the classification of an organisation's information assets and services, according to their operational sensitivity and business criticality.
20. An organisation must ensure that it has clear, credible and attainable cyber maturity goals, together with a timeline and/or implementation plan for change delivery, planning and acquiring skills (capabilities) relating to its people, processes and technology. Most importantly – in doing so, also keeping up to date with an ever-evolving threat landscape, criticality rating and maintaining proportion thereof in relation to the organisation's size.
21. No standard set of assessment metrics exist, which makes it more difficult for organisations to articulate and engage on cyber-resilience. Such metrics need to be developed through foresight-inspired activities. The organisation should use maturity models and define relevant cyber resilience assessment metrics to assess, measure and determine the suitability and efficacy of its cyber resilience framework, as well as the organisation's level of adherence thereto, by use of sovereign and independent compliance programmes, in addition to carrying out audits by qualified internal members of staff, or on an outsourced basis, regularly so.
22. Communication and Information-sharing: An organisation should consider interactions with third party or other participants, which may include Regulators, industry bodies, peer organisations *etcetera*, in respect of information sharing.  
In general, mechanisms surrounding same, the content and use of information collected or shared (as discussed above) are of paramount importance in the greater sense of security and resilience. Various

channels for the sharing of information, such as: *memoranda* of understanding, supervisory colleges, ISACs, trusted circles *etcetera*, not to mention the active participation of members and parties of such organisations are vital for the sustenance, existence and value of such arrangements. Considerations are to be had of the speed, latitude, security and fluidity of communications.

23. Third-party risks in the outsourcing of activities in relation to organisations' management of third-party dependencies remain of vital importance. Third parties generally speaking may provide cost-effective solutions to increase resilience levels of organisations, however, the onus remains on organisations to demonstrate their adequate understanding and active management of the third-party dependencies and concentration across the organisation's value chain. A balanced accountability model is to be established amongst organisations – particularly in respect of organisations not subject to stringent regulator supervision prerogatives.
24. Cyber Threat Intelligence: An organisation's cyber resilience framework needs to achieve continuous cyber resilience amid a changing threat environment. To be effective in keeping pace with the rapid evolution of cyber threats, an organisation should implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the organisation to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. An organisation should aim to instill a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.
25. An organisation's Board should review its cyber resilience strategy and framework (including all policies, procedures and controls related thereto), at least once a year (annually) and update it, whenever necessary. In doing so, an organisation should consider the following factors:
  1. The ever-evolving threat landscape, which includes the consideration of risks associated with: the supply chain, use of cloud services, social networking, mobile applications, the internet of things (IoT) *etcetera*;
  2. Threat intelligence on threat actors; new tactics, techniques and procedures which may specifically impact an organisation;
  3. The findings and results of risk assessments carried out of the organisation's critical functions, key roles, procedures, information assets, third-party service providers and interconnections;
  4. actual cyber incidents that have impacted the organisation directly; or external cyber incidents from its ecosystem or other source(s);
  5. lessons learned from audits and tests on the organisation's cyber resilience framework and strategy;
  6. the organisation's performance against the relevant cyber resilience aptitude or performance metrics, as well as maturity models; and
  7. new business developments and future strategic objectives of the organisation.
26. With proper investigation into and the review of findings, together with application of the listed considerations, the organisation's cyber resilience strategy and framework must determine how the organisation will continuously review, as well as proactively identify, mitigate and manage the cyber risks – risks which the organisation bears and that too, which it in-turn may pose to its participants, other organisations, vendors, vendor products and service providers.
27. The cyber resilience strategy should plan and document the organisation's future maturity of cyber resilience, with short and long-term goals. Senior management should continuously

review, improve and amend the existing cyber resilience strategy and framework as the desired cyber resilience maturity level and/or cyber risk landscape changes.

28. The organisation should establish the appropriate structures, processes and relationships with the key stakeholders in the ecosystem to continuously and proactively improve the ecosystem's cyber resilience and promote financial stability objectives as a whole.

## **Reference List**

Bank for International Settlements and International Organisation of Securities Commissions (2012), “Principles for financial market infrastructures”, April 2012, <https://www.bis.org/cpmi/publ/d101a.pdf>

Bank for International Settlements (2015), “Guidance on cyber resilience for financial market infrastructures”, Basel Committee on Banking Supervision, November 2015, <https://www.bis.org/cpmi/publ/d138.pdf>

Bank for International Settlements (2018), “Cyber-resilience: Range of practices”, Basel Committee on Banking Supervision, December 2018, <https://www.bis.org/bcbs/publ/d454.pdf>

Bodeau, D. and Graubart R. (2011), “Cyber Resiliency Engineering Framework”, MITRE Technical Report, The MITRE Corporation, September 2011; [https://www.mitre.org/sites/default/files/pdf/11\\_4436.pdf](https://www.mitre.org/sites/default/files/pdf/11_4436.pdf)

CPMI-IOSCO (2016), “Guidance on cyber resilience for financial market infrastructures”, June 2016, <https://www.bis.org/cpmi/publ/d146.pdf>

European Parliament and of the Council (2016), “DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”, <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

European Central Bank (2018), “Cyber resilience oversight expectations for financial market infrastructures”, December 2018, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)

European Central Bank (2018), “TIBER-EU FRAMEWORK-How to implement the European framework for Threat Intelligence-based Ethical Red Teaming”, May 2018, [https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber\\_eu\\_framework.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf)

European Commission (2019), “The Directive on security of network and information systems (NIS Directive)”, <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> , <https://www.enisa.europa.eu/>

Fornari, F. and Stracca, L. (2013), “What does a financial shock do? First International Evidence”, March 2013, European Central Bank, Working Paper Series NO 1522, <https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1522.pdf>

International Standards on Assurance Engagements (2011), “Assurance Reports on Controls at a Service Organisation; Internal Control Framework over Financial Reporting, June 15, 2011, <https://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf>

Saudi Arabian Monetary Authority (2017), “Cyber Security Framework”, May 2017; <http://www.sama.gov.sa/en/US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf>

United Arab Emirates Banking Federation-ISAC (2017); “UAE banks launch ISAC”, September 2017, <http://www.uaebf.ae/en/>

## **Annex I: Glossary of Terms**<sup>179</sup>

Actionable intelligence	Information that can be acted upon to address, prevent or mitigate a cyber threat.
Attack surface	The sum of an information system's characteristics in the broad categories (software, hardware, network, processes and human) which allows an attacker to probe, enter, attack or maintain a presence in the system and potentially cause damage to an FMI. A smaller attack surface means that the FMI is less exploitable and an attack less likely. <sup>180</sup> However, reducing attack surfaces does not necessarily reduce the damage an attack can inflict. <sup>181</sup>
Availability	The property of being accessible and usable as expected upon demand. <sup>182</sup>
Business process	A collection of linked activities that takes one or more kinds of input and creates an output that is of value to an FMI's stakeholders. A business process may comprise several assets, including information, ICT resources, personnel, logistics and organisational structure, which contribute either directly or indirectly to the added value of the service.
Critical operations	Any activity, function, process, or service, the loss of which, for even a short period of time, would materially affect the continued operation of an FMI, its participants, the market it serves, and/or the broader financial system.
Cyber	Refers to the interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions. <sup>183</sup>

<sup>179</sup> For general definitions of terms not found in this glossary, please see CPMI, Glossary of payments and market infrastructure terminology, <https://www.bis.org/cpmi/publ/d00b.htm>

CPSS, A glossary of terms used in payments and settlement systems, March 2003; and European Central Bank and Eurosystem, Glossary of terms related to payment, clearing, and settlement systems, December 2009; Cyber resilience oversight expectations for financial market infrastructures, European Central Bank,

[https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf); CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>180</sup> NICCS, Glossary of common cybersecurity terminology, <http://niccs.us-cert.gov/glossary>

<sup>181</sup> CPMI, Cyber resilience in financial market infrastructures, November 2014.

<sup>182</sup> NICCS, Glossary of common cybersecurity terminology, <http://niccs.us-cert.gov/glossary>

<sup>183</sup> NICCS, Glossary of common cybersecurity terminology, <http://niccs.us-cert.gov/glossary>

Cyber attack	The use of an exploit by an adversary to take advantage of a weakness(es) with the intent of achieving an adverse effect on the ICT environment. <sup>184</sup>
Cyber event	An observable occurrence in an information system or network. <sup>185</sup>
Cyber governance	Arrangements an organisation puts in place to establish, implement and review its approach to managing cyber risks. cyber maturity model A mechanism to have cyber resilience controls, methods and processes assessed according to management best practice, against a clear set of external benchmarks.
Cyber maturity model	A mechanism to have cyber resilience controls, methods and processes assessed according to management best practice, against a clear set of external benchmarks. <sup>186</sup>
Cyber resilience	An FMI's ability to anticipate, withstand, contain and rapidly recover from a cyber attack.
Cyber resilience framework	Consists of the policies, procedures and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces.
Cyber resilience strategy	An FMI's high level principles and medium term plans to achieve its objective of managing cyber risks.
Cyber risk	The combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation.
Cyber risk management	The process used by an FMI to establish an enterprise-wide framework to manage the likelihood of a cyber-attack and develop strategies to mitigate, respond to, learn from and  coordinate its response to the impact of a cyber attack. The management of an FMI's cyber risk should support the business processes and be integrated in the FMI's overall risk management framework.

<sup>184</sup> Adapted from MITRE definition of "attack". <https://capec.mitre.org/about/glossary.html>

<sup>185</sup> NICCS, Glossary of common cybersecurity terminology, <http://niccs.us-cert.gov/glossary>

<sup>186</sup> Adapted from APMG International Definition, <http://www.apmg-international.com/en/consulting/what-maturity-model.aspx>

Cyber risk profile	The cyber risk actually assumed, measured at a given point in time.
Cyber risk tolerance	The propensity to incur cyber risk, being the level of cyber risk that an FMI intends to assume in pursuing its strategic objectives.
Cyber threat	A circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in an FMI's systems, resulting in a loss of confidentiality, integrity or availability.
Cyber threat intelligence	Information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event (may also be referred to as "cyber threat information"). <sup>187</sup>
Defence in depth	The security controls deployed throughout the various layers of the network to provide for resiliency in the event of the failure or the exploitation of a vulnerability of another control (may also be referred to as "layered protection").
Detection	Development and implementation of the appropriate activities in order to identify the occurrence of a cyber event. <sup>188</sup>
Disruption	A disruption is an event affecting an organisation's ability to perform its critical operations.
Ecosystem	A system or group of interconnected elements, formed linkages and dependencies. For an FMI, this may include participants, linked FMIs, service providers, vendors and vendor products.
Financial Market Infrastructure	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions.
Forensic investigation	The application of investigative and analytical techniques to gather and preserve evidence from a digital device impacted by a cyber attack.

<sup>187</sup> Bank of England – CBEST, *Qualities of a threat intelligence provider*.

<sup>188</sup> NIST, *Framework for improving critical infrastructure cybersecurity*, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

Forensic readiness	The ability of an FMI to maximise the use of digital evidence to identify the nature of a cyber attack.
Identification	To develop the organisational understanding required to manage cyber risk to systems, assets, data and capabilities. <sup>189</sup>
Information asset	Any piece of data, device or other component of the environment that supports information-related activities. In the context of this report, information assets include data, hardware and software. <sup>190</sup> Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services. <sup>191</sup>
indicator	An occurrence or sign which reveals that an incident may have occurred or be in progress. <sup>192</sup>
Information asset	Any piece of data, device or other component of the environment that supports information-related activities. In the context of this report, information assets include data, hardware and software. <sup>193</sup> Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services.
Integrity	With reference to information, an information system or a component of a system, the property of not having been modified or destroyed in an unauthorised manner. <sup>194</sup>
Layered protection	As relying on any single defence against a cyber threat may be inadequate, an FMI can use a series of different defences to cover the gaps in and reinforce other protective measures. For example, the use of firewalls, intrusion detection systems, malware scanners, integrity auditing procedures and local storage encryption tools can serve to

<sup>189</sup> NIST, *Framework for improving critical infrastructure cybersecurity*, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

<sup>190</sup> UK National Archives, *What is an information asset?*, <http://www.nationalarchives.gov.uk/documents/informationmanagement/information-assets-factsheet.pdf>.

<sup>191</sup> CPMI-IOSCO – *Guidance on cyber resilience for financial market infrastructures* – June 2016; <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>192</sup> NICCS, *Glossary of common cybersecurity terminology*, <http://niccs.us-cert.gov/glossary>

<sup>193</sup> UK National Archives, *What is an information asset?*, <http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf>

<sup>194</sup> NICCS, *Glossary of common cybersecurity terminology*, <http://niccs.us-cert.gov/glossary>

protect information assets in a complementary and mutually reinforcing manner. May also be referred to as “defence in depth”.

Leading standards, guidelines  
and practices

Standards, guidelines and practices which reflect industry best approaches to managing cyber threats, and which incorporate what are generally regarded as the most effective cyber resilience solutions.

Malware

Malicious software used to disrupt the normal operation of an information system in a manner that adversely impacts its confidentiality, availability or integrity.

Operational resilience

The ability of an FMI to: (i) maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and (ii) recover to effective operational capability in a time frame consistent with the provision of critical economic services.

Protection

Development and implementation of appropriate safeguards, controls and measures to enable reliable delivery of critical infrastructure services.

Recover

To restore any capabilities or services that have been impaired due to a cyber event.

Red team

An independent group that challenges the cyber resilience of an organisation to test its defences and improve its effectiveness. A red team views the cyber resilience of an FMI from an adversary’s perspective.

Resilience by design

The embedding of security in technology and system development from the earliest stages of conceptualisation and design.

Respond

Of an FMI, to develop and implement appropriate activities to be able to take action when it detects a cyber event.

Resume

To recommence functions following a cyber incident. An FMI should resume critical services as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability. The plan of action should incorporate the use of a secondary site and be designed to ensure that critical ICT systems can resume operations within two hours following a disruptive event.

Risk-based approach	An approach whereby FMIs identify, assess and understand the risks to which they are exposed to and take measures commensurate with these risks.
Risk tolerance	The amount and type of risk that an organisation is willing to take in order to meet its strategic objectives (may also be referred to as “risk appetite”).
Security operations centre	A function or service responsible for monitoring, detecting and isolating incidents.
Situational awareness	The ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event.
Threat	A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organisational operations, organisational assets (including information and information systems), individuals, other organisations or society in general. <sup>195</sup>
Threat intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. <sup>196</sup>
Vulnerability	A weakness, susceptibility or flaw in a system that an attacker can access and exploit to compromise system security. Vulnerability arises from the confluence of three elements: the presence of a susceptibility or flaw in a system; an attacker's access to that flaw; and an attacker's capability to exploit the flaw.
Vulnerability assessment	Systematic examination of an information system and its controls and processes, to determine the adequacy of security measures, identify

<sup>195</sup> NICCS, [http://niccs.us-cert.gov/glossary#letter\\_t](http://niccs.us-cert.gov/glossary#letter_t)

<sup>196</sup> [https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1\\_webroot.pdf](https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf)

security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. Source: Adapted from NIST/FSB Cyber Lexicon<sup>197</sup>

---

<sup>197</sup> Cyber resilience oversight expectations for financial market infrastructures, European Central Bank, [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf);

## **Annex II: Members of the Working Group on Cyber Resilience and Consultant Contributors**

We acknowledge with much appreciation the crucial role of the research and drafting team, co-led by Kokila Alagh and Luna de Lange of KARM Legal Consultants.

The Group's work has also benefited from the contributions and consultant support provided by Anomali Incorporated (and Anomali Solutions, Dubai, United Arab Emirates) whom for several months have availed resources and a team of skilled, knowledgeable and experienced persons to assist the drafters of this report in their research, benefiting their technical know-how and operationality of the proposed guidelines.

We further acknowledge the valued contributions of the editors of this report and their organisation, Al Baraka Banking Group, whom have availed resources and a team of skilled, knowledgeable and experienced persons to assist the drafters of this report, too benefiting from their technical know-how and operationality of the proposed guidelines.

We express gratitude to all.

### **Members:**

- |  |   |
|--|---|
| 1. Mrs Kokila Alagh Rajeev Malhotra <sup>198</sup> | KARM Legal Consultants <sup>199</sup><br>Founder & Managing Partner<br>United Arab Emirates |
| 2. Mrs Luna de Lange <sup>200</sup>                | KARM Legal Consultants<br>Partner<br>United Arab Emirates                                   |

### **Editors:**

- |                                  |  |
|----------------------------------|--|
| 1. Mr Ahmed Albalooshi           | Al Baraka Banking Group B.S.C.<br>Chief Information Officer<br>Kingdom of Bahrain  |
| 2. Mr Khalid Waheed Abdulrahman  | Al Baraka Banking Group B.S.C.<br>CISM, CISSP, ISO27001 Lead<br>Auditor; Manager - Information<br>Technology<br>Kingdom of Bahrain |
| 3. Ms. Fredesvinda Fatima Montes | Senior Financial Sector Specialist<br>Finance, Competitiveness, and<br>Innovation Department; The World Bank                       |
| 4. Ms. Dorothee Delort           | Senior Financial Sector Specialist<br>Finance, Competitiveness, and<br>Innovation Department; The World Bank                       |

<sup>198</sup> Co-lead on both the research and drafting team; <https://ae.linkedin.com/in/kokila-alagh-6662315>

<sup>199</sup> <http://karmadv.com/>

<sup>200</sup> Co-lead on both the research and drafting team; <https://ae.linkedin.com/in/luna-de-lange-54593459>

**AMF Technical Secretariat:**

5. Ms. Nouran Youssef, DBA  
Senior Financial Sector Specialist  
Coordinator of the Arab Regional  
Fintech WG, Arab Monetary Fund

**Consultant Contributors:**

1. Mr Hugh Njemanze<sup>201</sup>  
Anomali Incorporated<sup>202</sup>  
Chief Executive Officer
2. Mr Jamie Stone<sup>203</sup>  
Anomali Incorporated  
Vice President, EMEA
3. Mr Jonathan Martin<sup>204</sup>  
Anomali Incorporated  
Operations Director, EMEA
4. Mr Khaled Chatila<sup>205</sup>  
Anomali Incorporated  
Regional Sales Director, Middle East
5. Mr Leon Andrew de Lange<sup>206</sup>  
Anomali Incorporated  
Senior Solutions Consultant, EMEA
6. Mr Marc Green<sup>207</sup>  
Anomali Incorporated  
Senior Principal Security Analyst, EMEA
7. Ms Angela Nichols  
Anomali Incorporated  
Vice President of Global Marketing

<sup>201</sup> <https://www.anomali.com/company/leadership>; <https://www.linkedin.com/in/hugh-njemanze-603721>

<sup>202</sup> Trusted and vetted Consultants to the Arab Monetary Fund: <https://www.anomali.com/>

<sup>203</sup> <https://uk.linkedin.com/in/jamie-stone-03a39917>

<sup>204</sup> <https://uk.linkedin.com/in/ionathanmartin5>

<sup>205</sup> <https://ae.linkedin.com/in/khaledchatila>

<sup>206</sup> <https://ae.linkedin.com/in/andrew-de-lange-anomali>

<sup>207</sup> <https://uk.linkedin.com/in/marc-green-a0571163>



**Copies of publications issued by the Arab Monetary Fund  
may be requested from:**

**Arab Monetary Fund**

**P.O. Box 2818**

**Abu Dhabi, U.A.E.**

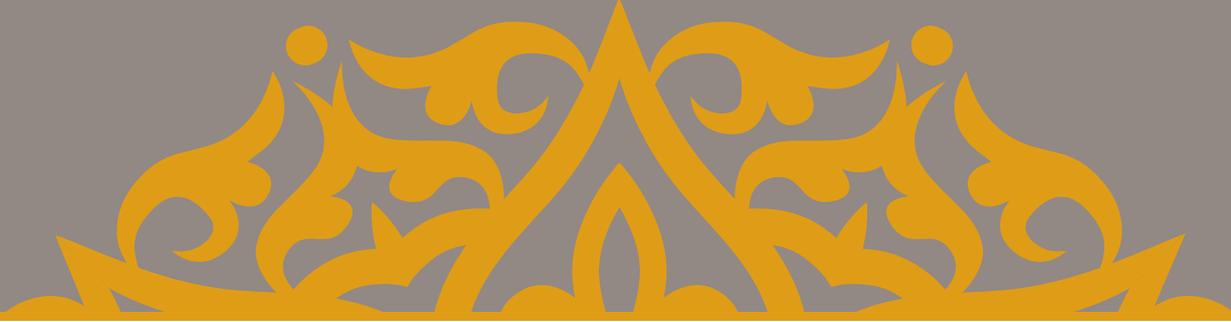
**Tel. : (+9712) 6215000**

**Fax : (+9712) 6326**

**E-mail: [publications@amfad.org.ae](mailto:publications@amfad.org.ae)**

**\*Available in PDF format at: [www.amf.org.ae](http://www.amf.org.ae)**





<http://www.amf.org.ae>

