International Telecommunication Union

Technical Report

(October 2023)

Digital Financial Services Security Lab

Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure

TABLE OF CONTENTS

Page

List of Tables

Page

List of Figures

Page

Preliminary elements

Context

Over the past few decades, Digital Financial Services have become among the leading methods for financial transactions for a growing number of world countries. This phenomenon is not exclusive to advanced economies; on the contrary, digital transformation, accelerated by the COVID-19 pandemic, has also concerned emerging markets. Studies show that Digital Financial Services in developing countries can be at the forefront of economic growth. This advantage has encouraged emerging economies to take action toward a more digitalised financial environment. Therefore, the DFS infrastructure is critical and should be assessed in terms of cyber resilience.

Summary

This report aims to support Digital Financial Services (DFS) regulators and DFS stakeholders in emerging economies in assessing their critical infrastructure's cyber resilience level. It is structured in four distinctive parts. The first part presents a tailored cyber resilience self-assessment toolkit for DFS regulators and DFS entities. This toolkit is proceeded by a matrix that facilitates the identification of the relevant actors managing the DFS critical infrastructure. The second part of this report looks at the DFS architecture and aims to provide a preliminary understanding of its most relevant actors. In particular, the close interconnection among the telecommunication sector, financial industry, third parties, and end users will be analysed to identify some of the most common cyber-threat actors and risks in DFS ecosystems. The third part of this report defines a comprehensive methodological framework comprising risk management processes, governance and testing procedures, and the incident response cycle. The methodology is based upon internationally recognised normative frameworks to facilitate a holistic and comprehensive assessment. Finally, the report includes an appendix aggregating all the questions in the Cyber Resilience Toolkit that can be used by regulators for the assessment of the cyber resilience of the stakeholders in DFS ecosystem.

Scope

The scope of this report is to provide DFS entities in emerging economies with technical guidelines and toolkit to conduct a self-assessment of their current cyber resilience critical infrastructure for digital financial services. To do so, this document presents a methodology tailored to the digital financial services ecosystem in developing markets and a tailored Cyber Resilience Toolkit. To build a more constructive understanding of the cyber threats targeting the DFS ecosystem, this document's scope also includes a preliminary definition of the most relevant risks facing the four main DFS actors: the telecommunication sector, the financial industry, the third-party service providers, and the end user. The high-level overview remains as open and wide-ranging as possible, with the intended purpose of including the highest number of emerging countries with different features and national security architectures. Finally, this report's scope includes the standardisation of taxonomy among emerging countries. This critical component is needed to facilitate transnational and cross-sectoral information-sharing cyber resilience initiatives. A shared taxonomy will strengthen cyber preparedness and encourage alignment with some of the most innovative worldwide cyber legislations, such as the European Union (EU) Digital Operational Resilience (DORA).

Keywords

Advanced Persistent Threat, Business Continuity Plan, Cyber Governance, Cyber Attack, Cyber Methodology, Cyber Preparedness, Cyber Resilience Framework, Cyber Resilience, Cybersecurity, DFS, Digital Financial Services, DORA, European Cyber Legislation, European Union, Financial Institution, Hacktivism, Incident Response, Indicator of Compromise (IoC), ISO 27001, ISO 27005, ISO, Malware, NIS 2, NIS, NIST, Reporting, State-Backed Hackers, Threat Acton, Threat Intelligence, Threat Source, Threat vector, Vulnerability Assessment, Vulnerability.

References

Agur, I. et al. (2020). *Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies*. International Monetary Fund

Basel Committee on Banking Supervision. (2005). *The Joint Forum. Outsourcing in Financial Services.* Bank for International Settlements. https://www.bis.org/publ/joint12.pdf

Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

Brauchle, J.P. et al. (2020). *Cyber Mapping the Financial System*. Carnegie Endowment for International Peace

Carnegie Mellon University. (2016). *Volume 9 Training and Awareness v1.1 – CRR supplemental resource Guide*
https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-TA.pdf

Cicchitto, N. (2020). *Winning the Cybersecurity Race is a team sport: How to engage your stakeholders*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/09/28/winning-the-cybersecurity-race-is-a-team-sport-how-to-engage-your-stakeholders/?sh=136e341b6667

CISA. (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf

CISA. (2023). *Partnerships and collaboration | Cybersecurity and Infrastructure Security Agency*. CISA. https://www.cisa.gov/topics/partnerships-and-collaboration

CISCO. (2023) *What is Network Security?* CISCO. Accessed April 2023. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Committee On Payments and Market Infrastructures and Board of the International Organization of Security Commissions. (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures*. Bank for International Settlements. https://www.bis.org/cpmi/publ/d146.pdf

Committee on Payments and Market Infrastructures and World Bank Group. (2016). *Payment aspects of financial inclusion.* Bank for International Settlements and World Bank Group. https://www.bis.org/cpmi/publ/d144.pdf

Deloitte. (2017). *Fintechs and regulatory compliance.* Deloitte

Duflos, E. (2022). *Rethinking Consumer Protection: A Responsible Digital Finance Ecosystem*. CGAP

ENISA. (2017). *ENISA overview of cybersecurity and related terminology*. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

ENISA. (2022). *Glossary.* https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

ENISA. (2023). *Incident Reporting.* Accessed April 2023. https://www.enisa.europa.eu/topics/incident-reporting

EU Council and Parliament. (2022). *Directive on the on the resilience of critical entities and repealing Council Directive 2008/114/EC*. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

EU. (2023). *The EU Cybersecurity Skills Academy Factsheet. EU Digital Strategy*. https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-skills-academy-factsheet

European Banking Federation. (2020). *Cloud exit strategy – testing of exit plans.* EBF. https://www.ebf.eu/wp-content/uploads/2020/09/Cloud-exit-strategy-Testing-of-exit-plans.pdf

European Central Bank. (2018). *Tiber-EU Framework*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

Financial Stability Board. (2013). *Principles for an Effective Risk Appetite Framework*. https://www.fsb.org/wp-content/uploads/r_131118.pdf

G7 Cyber Expert Group. (2020). *G-7 Fundamental Elements of Cyber Exercise Programmes*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948042/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf

G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

G7 Cyber Expert Group. (2022). *G-7 Fundamental Elements of Ransomware Resilience For The Financial Sector.* United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134062/2022-10-13-g7-fundamental-elements-ransomware-data.pdf

Greene, A., et al. (2022). *Cyber incident reporting. New rules, new timelines*. Crowe. https://www.crowe.com/cybersecurity-watch/cyber-incident-reporting-new-rules-new-timelines

Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

IMF (2004). *What is an Emerging Market?*. https://www.imf.org/en/Publications/WP/Issues/2016/12/31/What-is-An-Emerging-Market-17598

Insider, B. (2021). *The future of digital payments in Africa - an outlook of trends in 2022*. Business Insider Africa. https://africa.businessinsider.com/local/markets/the-future-of-digital-payments-in-africa-an-outlook-of-trends-in-2022/gvltq07

Interpol. (2023). *AFJOC - African Joint Operation Against Cybercrime*. INTERPOL. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

ISO. (2009). *ISO 73:2009 Risk Management Vocabulary*. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

ISO. (2011). *ISO/IEC Standard No. 27005:2011. Information technology – Security techniques – Information security risk management.* https://www.iso.org/standard/56742.html

ISO. (2014). *ISO 55000:2014 Asset Management – Overview Principles and terminology*. https://www.iso.org/obp/ui/#iso:std:iso:55000:ed-1:v2:en

ISO. (2015). *ISO/IEC 27039:2015 Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS).* *https://www.iso.org/standard/56889.html*

ISO. (2016). *ISO 37001: 2016 Anti-bribery management systems — Requirements with guidance for use*. https://www.iso.org/obp/ui/#iso:std:iso:37001:ed-1:v1:en

ISO. (2018). *ISO 31000:2018. Risk Management Guidelines.* https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

ISO. (2018). *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.* *https://www.iso.org/standard/73906.html*

ISO. (2020). *ISO/TS 23029:2020 Web-serve-based application programming interface (WAPI) in financial services.* ISO/TS 23029:2020 - Web-service-based application programming interface (WAPI) in financial services

ISO. (2022). *ISO/IEC Standard No. 27001:2022. Information security, cybersecurity, and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/82875.html

ITU. (2013). *Recommendation X.1154 (04/13)*. https://www.itu.int/rec/T-REC-X.1154-201304-I

ITU. (2014). *Recommendation X.1158 (11/14)*. https://www.itu.int/rec/T-REC-X.1158-201411-I

ITU. (2014). *Recommendation X.3500 (08/14)*. https://www.itu.int/rec/T-REC-Y.3500-201408-I/en

ITU. (2016). *DFS Glossary.* https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201701/ITU_FGDFS_DFS-Glossary.pdf

ITU. (2017). *Security Aspects of DFS.* International Telecommunication Union. https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf

ITU. (2020). *Digital Financial Services security assurance framework.* International Telecommunication Union. https://www.itu.int/hub/publication/t-tut-dfs-2021/

ITU. (2020). *Recommendation X.1254 entity Authentication Assurance Framework.* *https://www.itu.int/rec/T-REC-X.1254-202009-I/en*

Janeway,T. (2020). *The NIST Cybersecurity Framework – Third Parties Need Not Comply*. ISACA Journal. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-1/the-nist-cybersecurity-framework-third-parties-need-not-comply_joa_eng_0220.pdf

Maurer, T. et al. (2021). *The Global Cyber Threat*. The International Monetary Fund. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

MITRE ATT&CK. (2023). *Enterprise Mitigations.* Mitigations-Enterprise | MITRE ATT&CK. Accessed April 2023. https://attack.mitre.org/mitigations/enterprise/

National Institute of Justice. (2020). *Taking on the Dark Web*. https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs

NIST. (1998). *NIST SP.800-16. Information Technology Security Training Requirements.* National Institute of Standards and Technology. *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf*

NIST. (2005). *NIST.IR.7250. Cell Phone Forensic Tools: An Overview and Analysis.* National Institute of Standards and Technology. *https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7250.pdf*

NIST. (2008). *NIST.SP.800-115. Technical Guide to Information Security Testing and Assessment (SP 800-115).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

NIST. (2010). *NIST.SP.800-122.Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

NIST. (2010). *NIST.SP.800-34 Rev.1. Contingency Planning Guide for Federal Information Systems.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

NIST. (2011). *NIST.IR.7711. Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7711.pdf

NIST. (2011). *NIST.SP.800-137. Information Security.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

NIST. (2011). *NIST.SP.800-145. The NIST Definition of Cloud Computing.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NIST. (2012). *NIST.SP.800-30 Rev.1 Information Security.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST. (2012). *NIST.SP.800-61 Rev.2. Computer Security Incident Handling Guide.* National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

NIST. (2015). *NIST.SP.800-82 Rev.2. Guide to Industrial Control Systems (ICS) Security.* National Institute of Standards and Technology. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

NIST. (2016). *NIST.SP.800-150. Guide to Cyber Threat Information Sharing.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

NIST. (2017). *NIST.IR.8183. Cybersecurity Framework Manufacturing.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

NIST. (2017). *NIST.SP.800.63-3. Digital Identity Guidelines (SP 800-63-3).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

NIST. (2017). *NIST.SP.800-12 Rev.1 An Introduction to Information Security.* National Institute of Standards and Technology. *https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final*

NIST. (2018). *NIST.CSWP.04162018. Framework for Improving Critical Infrastructure Cybersecurity* (v.1.1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2018). *NIST.IR.8011-3. Security Control Assessment*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8011-3.pdf

NIST. (2018). *NIST.SP.800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

NIST. (2019). *NIST.SP.1800-17. Multifactor Authentication for E-Commerce*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf

NIST. (2020). *NIST.IR.8286. Integrating Cybersecurity and Enterprise Risk Management.* National Institute of Standards and Technology. *(ERM).* https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

NIST. (2020). *NIST.SP.1800-16. Securing Web Transactions TLS Server Certificate Management.* National Institute of Standards and Technology. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf*

NIST. (2020). *NIST.SP.800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2021). *NIST.SP.1800-15. Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf

NIST. (2021). *NIST.SP.800-160 Ver.2 Rev. 1. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

NIST. (2021). *NIST.SP.800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information.* National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-172/final

NIST. (2022). *NIST.SP.800-161 Rev.1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

NIST. (2022). *NIST.SP.800-40 Rev.4 Guide to Enterprise Patch Management Planning.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

NIST. (2023). *NIST.FIPS.185-5.* Federal Information Processing Standards (2023), *Digital Signature Standard*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

Pazzarbasoglu, C. et al. (2020). *Digital Financial Services.* World Bank Group. https://pubdocs.worldbank.org/en/230281588169110691/Digital-Financial-Services.pdf

PCI Security Standards Council. (2013). *Payment Application Data Security Standard*. https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf

PCI Security Standards Council. (2022). *Data Security Standard*. https://www.pcisecuritystandards.org/document_library/

Rodreck, D., Ngulube, P., & Dube, A. (2013). A cost-benefit analysis of document management strategies used at a financial institution in Zimbabwe: A case study. SA Journal of Information Management,15(2), doi:10.4102/sajim.v15i2.540

Signaling System 7 (SS7). (2023). *SS7*. Available at: https://ss7.info/

The European Parliament and Council. (2022) *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

US Committee on National Security Systems. (2022). *CNSSI 4009 Glossary*. https://ww.niap-ccevs.org/Ref/CNSSI_4009.pdf

US Department of Homeland Security. (2020). *Exercise and Evaluation Program (HSEEP).* https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf)

US Government. (2023). *Financial Crimes Enforcement Network- Financial Institution Definition*. Accessed April 2023. https://www.fincen.gov/financial-institution-definition

Taxonomy and Terminology

Terms defined elsewhere:

This Technical Report uses the following terms defined elsewhere:

Account Hijacking [ITU – FIGI - Digital Financial Services: Security assurance framework][1]: The ability of an attacker to take control of an account or communication session.

Advanced Persistent Threat (APT) [NIST SP 800-30 Rev.1][2]: An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives. An APT often wants to establish and extend its presence within the information technology infrastructure of organization to continually exfiltrate information and/or to undermine or impede critical aspects of a mission, program, or organization. Moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

Application Programming Interface (API) [ISO/TS 23029:2020][3]: A set of well-defined methods, functions, protocols, routines, or commands that an application software program uses to invoke services.

Asset Management [ISO 55000:2014][4]: The coordinated activity of an organization to realize value from assets.

Authentication Factor [ITU-T X.1154][5]: A type of credential. There are three types of authentication factors: ownership, knowledge, and biometric factors.

Awareness Campaign [Adapted from NIST SP 800-16][6]: A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

Best Practice [NIST SP 1800-15B][7]: A procedure that has been shown by research and experience to produce optimal results and that is an established standard suitable for widespread adoption.

Business Continuity Plan [NIST SP 800-34 Rev.1][8]: The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

---

[1] ITU (2020), *Digital Financial Services security assurance framework*, International Telecommunication Union https://www.itu.int/hub/publication/t-tut-dfs-2021/

[2] NIST (2012). *Information Security.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[3] ISO/TS (2020). *ISO/TS 23029:2020 Web-serve-based application programming interface (WAPI) in financial services.* ISO/TS 23029:2020 - Web-service-based application programming interface (WAPI) in financial services

[4] ISO (2014). *55000:2014 Asset Management – Overview Principles and terminology.* https://www.iso.org/obp/ui/#iso:std:iso:55000:ed-1:v2:en

[5] ITU (2013). *Recommendation X.1154 (04/13)*. https://www.itu.int/rec/T-REC-X.1154-201304-I

[6] NIST (1998). *Information Technology Security Training Requirements.* *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf*

[7] NIST (2021). *Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD).* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf

[8] NIST (2010). Contingency Planning Guide for Federal Information Systems. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Cloud Service Provider (CSP) [Adapted from ITU-T Y.3500][9]: An external party that makes cloud services available.

Computer Security Incident Response Teams (CSIRTs) [NIST SP 800-61 rReeRv.2][10]: A capability set up for the purpose of assisting in responding to computer security-related incidents.

Cost-Benefit Analysis [Journal of Information Management][11]: A systematic approach to considering the weaknesses (costs) and strengths (benefits) of the choices available.

Critical Component [Adapted from CNSSI 4009-202215][12]: A component, which is, or contains, information and communications technology (ICT), including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

Critical National Infrastructure (CNI) [EU Directive on resilience of critical entities][13]: An asset, a facility, equipment, a network, or a system, which is necessary for the provision of an essential service.

Cyber Defence [ENISA Terminology][14]: A variety of defensive mechanisms that could be used to mitigate or respond to cyberattacks.

Cyber Event [NIST SP 800-61 Rev.2]: Any observable occurrence in a network or information system.

Cyber Incident [ENISA Terminology][15]: Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it's natural or human made; malicious or non-malicious intent; deliberate, accidental, or due to incompetence; due to development or due to operational interactions.

Cyber Resilience [Adapted from BIS Guidance on Cyber Resilience for FMIs][16]: An entity's/ subject's ability to anticipate, withstand, contain, and rapidly recover from a cyberattack.

Cyberattack [CNSSI 4009-202215]: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Cyber-Threat Intelligence (CTI) [NIST SP 800-150][17]: Threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes.

---

[9] ITU (2014). *Recommendation X.3500 (08/14)*. https://www.itu.int/rec/T-REC-Y.3500-201408-I/en

[10] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[11] Rodreck, D., Ngulube, P., & Dube, A. (2013). *A cost-benefit analysis of document management strategies used at a financial institution in Zimbabwe: A case study*. SA Journal of Information Management,15(2), doi:10.4102/sajim.v15i2.540

[12] U.S. Committee on National Security Systems. *CNSSI 4009 Glossary.* https://ww.niap-ccevs.org/Ref/CNSSI_4009.pdf

[13] EU Council and Parliament (2022). *Directive on the on the resilience of critical entities and repealing Council Directive 2008/114/EC*. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[14] ENISA. *Enisa overview of cybersecurity and related terminology*. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

[15] ENISA. *Enisa overview of cybersecurity and related terminology*. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

[16] Committee On Payments and Market Infrastructures and Board of the International Organization of Security Commissions (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures*. Bank for International Settlements. https://www.bis.org/cpmi/publ/d146.pdf

[17] NIST (2016). *Guide to Cyber Threat Information Sharing.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Dark Web [Adapted from the U.S. National Institute of Justice][18]: The Dark Web is a part of the World Wide Web that provides a higher level of anonymity, highly-secured communication channels, and shields data transfer operations from external interference. The Dark Web has over the past few decades provided asylum to oppressed journalists and politically exposed individuals, while also facilitated illicit activities and the establishment of a protected hub for criminal commerce.

Data Backup [NIST SP 800-34 Rev.1]: A copy of files and programs made to facilitate recovery if necessary.

Data Exposure [Adapted from NIST SP 800 161 Rev.r1][19]: The extent to which the organization's data is subject to a risk.

Data Loss Prevention [CNSSI 4009-202215]: A systems ability to identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework.

Defence-In-Depth [NIST-SP 800-172][20]: An information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Demilitarized Zones (DMZs) [Adapted from NIST SP 800-82 Rev.2] Perimeter network segment that is logically located between internal and external networks. Its purpose is to enforce the internal network's Information Assurance Policy for external information exchange and shield the internal networks from outside attacks.

Denial of Service (DoS) [NIST SP 800-12 Rev.1][21]: The prevention of authorized access to resources or the delaying of time-critical operations.

DFS End-Users [Adapted from ITU – FIGI - Digital Financial Services: Security assurance framework]: The target audience for the DFS service, and who can make use of an application to send a DFS request to the financial institution.

Digital Financial Services [ITU DFS Glossary][22]: Digital financial services include methods to electronically store and transfer funds; to make and receive payments; to borrow, save, insure, and invest; and to manage a person's or enterprise's finances.

Disaster Recovery [ENISA Glossary]: The process of restoring a system to full operation after an interruption in service, including equipment repair / replacement, and file recovery / restoration.

Distributed Control Systems (DCS) [Adapted from NIST SP 800-82][23]: Systems generally used to control production system within a local area (e.g., a factory using a supervisory and regulatory control).

---

[18] National Institute of Justice (2020). *Taking on the Dark Web*. https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs

[19] NIST. *SP 800-161 Rev.1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* *https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final*

[20] NIST (2021). *SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information.* *https://csrc.nist.gov/publications/detail/sp/800-172/final*

[21] NIST (2017). *SP 800-12 Rev.1 An Introduction to Information Security.* *https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final*

[22] ITU (2016). *DFS Glossary.* https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201701/ITU_FGDFS_DFS-Glossary.pdf

[23] NIST (2015). *Guide to Industrial Control Systems (ICS) Security.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Distributed Denial of Service (DDoS) [NIST SP 1800-15B]: A denial of service technique that uses numerous hosts to perform the attack.

Due Diligence [ISO 37001:2016][24]: Process to further assess the nature and extent of the bribery risk and help organizations make decisions in relation to specific transactions, projects, activities, business associates and personnel.

Emerging Economies [Adapted from IMF][25]: An emerging market with good growth prospects, high rates of return, and extremely volatile financial conditions.

Entities [FIPS 186-5][26]: An individual (person), organization, device, or process. In this report, it is used interchangeably with "party".

EXtensible Markup Language (XML) [ISO/TS 23029:2020]: eXtensible Markup Language, a data format standard created by W3C.

Federated Digital Identity Systems [NIST SP 800-63][27]: A particular system to identify users and facilitate authentication processes through a third-party provider.

Financial Institution (FI) [Adapted from U.S. Financial Crimes Enforcement Network][28]: Includes any person doing business in one or more of the following capacities: (1) bank; (2) broker or dealer in securities; (3) money services business;(4) telegraph company; (5) casino;(6) card club; (7) a person subject to supervision by any state or federal bank supervisory authority. For the scope of this report, this list is not considered exhaustive and may adjust according to any specific DFS ecosystems or national architectures' characteristics.

Financial Technology (FinTech) [ITU DFS Glossary]: A term that refers to companies providing software, services, and products for digital financial services: often used in reference to newer technologies.

Hacker [NIST SP 800-12 Rev.1]: Unauthorized user who attempts to or gains access to an information system. While there are many types of hackers, this report refers predominantly to black-hat hackers when discussing cyberattacks and risks related to the DFS ecosystem.

Impact [ENISA Glossary][29]: The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation of a loss of confidentiality, integrity, or availability of information or a system.

Impact Analysis [ENISA Glossary]: The identification of critical business processes, and the potential damage or loss that may be caused to the organization resulting from a disruption to those processes.

---

[24] ISO (2016). *Anti-bribery management systems — Requirements with guidance for use*. https://www.iso.org/obp/ui/#iso:std:iso:37001:ed-1:v1:en

[25] IMF (2004). *What is an Emerging Market?*. https://www.imf.org/en/Publications/WP/Issues/2016/12/31/What-is-An-Emerging-Market-17598

[26] Federal Information Processing Standards (2023), *Digital Signature Standard*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

[27] Grassi, P. et al. (2017). *Digital Identity Guidelines (SP 800-63-3).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[28] U.S. Government (2023). *Financial Crimes Enforcement Network- Financial Institution Definition*. https://www.fincen.gov/financial-institution-definition

[29] ENISA (2022). *Glossary*. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

Incident Response (IR) [ISO/IEC 27039:2015][30]: An action [or process] taken to protect and restore normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs.

Indicator of Compromise (IoC) [NIST SP 800-53][31]: Forensic artifacts from intrusions that are identified on organizational systems at the host or network level.

Information and Communications Technology (ICT) [NIST SP 800-161 Rev.1]: Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.

Information Sharing [NIST SP 800-16]: The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

International Mobile Equipment Identity (IMEI) [NISTIR 7250] [32] : A unique number programmed into GSM and UMTS mobile phones.

International Mobile Subscriber Identity (IMSI) [NISTIR 7250]: A unique number associated with every GSM mobile phone user.

Internet Protocol (IP) [NIST SP 1800-16B][33]: The Internet Protocol, as defined in IETF RFC 6864, is the principal communications protocol in the IETF Internet protocol suite for specifying system address information when relaying datagrams across network boundaries.

Intrusion Detection Systems (IDS) [NISTIR 7711][34]: Software that looks for suspicious activity and alerts administrators.

Intrusion Prevention Systems (IPS) [NIST SP 800-82 Rev.2][35]: A system that can detect an intrusive activity and attempt to stop the activity, ideally before it reaches its targets.

Man-In-The-Middle [ITU-T X.1254][36]: Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

Mitigative Action Plan [Adapted from NIST SP 800-160 Vol.2 Rev.1][37]: A process to implement decisions, actions, or practices intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.

---

[30] ISO/IEC. *27039:2015 Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS).* https://www.iso.org/standard/56889.html

[31] Joint Task Force (2020*). Security and Privacy Controls for Information Systems and Organizations (NIST.SP.800-53 Rev.5).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[32] NIST (2005), *Cell Phone Forensic Tools: An Overview and Analysis.* https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7250.pdf

[33] NIST (2020). *Securing Web Transactions TLS Server Certificate Management.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf

[34] NIST (2011). *Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters.* https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7711.pdf

[35] NIST (2015). *Guide to Industrial Control Systems (ICS) Security.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[36] ITU (2020). *Recommendation X.1254 entity Authentication Assurance Framework.* https://www.itu.int/rec/T-REC-X.1254-202009-I/en

[37] NIST (2021). *Developing Cyber-Resilient Systems.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

Mobile Network Operator (MNO) [Adapted from ITU DFS Glossary]: An enterprise which sells mobile phone services, including voice and data communication. In this report, an MNO may also include other actors and entities of the telecommunication sector.

Multi-Factor Authentication (MFA) [NIST SP 1800 17b][38]: An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors.

Patching System [NIST SP 800-40 Rev.r4][39]: The act of applying a change to installed software – such as firmware, operating systems, or applications – that corrects security or functionality problems or adds new capabilities.

Penetration Testing (Pentesting) [NIST SP 800-12 Rrev.1]: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

Personally Identifiable Information (PII) [NIST SP 800-122][40]: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Phishing [NIST SP 800-12 Rrev.1]: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

Privileged Users [NIST 800-53]: Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users.

Qualitative Assessment [NIST SP 800-30 Rev.1][41]: Use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels.

Quantitative Assessment [NIST SP 800-30 Rev.1]: Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

Red Team [CNSSI 4009-202215]: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.

Regulators [ITU DFS Glossary]: A governmental organisation given power through national law to set and enforce standards and practices. Central Banks, Finance and Treasury Departments, Telecommunications Regulators, and Consumer Protection Authorities are all regulators involved in

[38] NIST (2019). *Multifactor Authentication for E-Commerce*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf
[39] NIST (2022). *Guide to Enterprise Patch Management Planning.* *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf*
[40] NIST (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
[41] NIST (2012). *Information Security.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

digital financial services. As the DFS ecosystems analysed in this report change, regulators may adjust according to different national infrastructures.

Resilience [CNSSI 4009-202215]: A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands.

Risk [NIST SP 800-137][42]: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Acceptance [ISO 73:2009][43]: informed decision to take a particular risk.

Risk Appetite [ISO 31000:2018][44]: the amount and type of risk that an organization is prepared to pursue, retain, or take.

Risk Assessment [NIST SP 800-137]: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

Risk Avoidance [ISO 73:2009]: Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.

Risk Communication [ENISA Glossary]: A process to exchange or share information about risk between the decision-maker and other stakeholders.

Risk Criteria [NIST SP 800-160v.1 Rev.1]: Terms of reference against which the significance of a risk is evaluated.

Risk Evaluation [NIST SP 800-160v.1 Rev.1]: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is/are acceptable or tolerable.

Risk Identification [NIST SP 800-160v.1 Rev.1]: Process of finding, recognizing, and describing risks.

Risk Likelihood [ISO 31000:2018][45]: The likelihood of a risk materializing into a threat or a vulnerability.

Risk Management Process [ISO 73:2009]: Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring, and reviewing risk.

Risk Modification [ISO 27005:2018][46]: Process of managing level of risk by introducing, removing, or altering controls so that the residual risk can be reassessed as being acceptable.

[42] NIST (2011). *Information Security.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
[43] ISO (2009). *73:2009 Risk Management Vocabulary.* https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.
[44] ISO/IEC. (2018). ISO 31000, *Risk management – Guidelines*. https://www.iso.org/standard/65694.html
[45] ISO (2018). *31000:2018. Risk Management Guidelines*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.
[46] International Organisation for Standardization. (2011). *Information technology – Security techniques – Information security risk management. ISO/IEC Standard No. 27005:2011*

Risk Parameters [ISO 73:2009]: Parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.

Risk Profile [Adapted from NISTIR 8286][47]: A prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete risk inventory.

Risk Retention [ISO 73:2009]: Acceptance of the potential benefit of gain, or burden of loss, from a particular risk.

Risk Sharing (also known as Risk Transfer) [ENISA Glossary]: Sharing with another party the burden of loss or benefit of gain, for a risk.

Risk Treatment Plan [NIST SP 800-160v.1 Rev.1]: Plan to implement processes to modify risk.

Root Cause Analysis [NIST SP 800-30]: A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.

Service Providers [NIST SP 1800 16-B]: A provider of basic services or value-added services for operation of a network; generally, refers to public carriers and other commercial enterprises.

Session Hijacking [Adapted from NIST SP 800-63-3]: A technique in which the attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to control session data exchange.

Signalling System 7 [SS7][48]: A set of protocols used for communication between different elements of a public switched telephone network.

SIM Swap [ENISA Glossary]: A technique used by attackers to transfer the victim's phone number to another SIM card and, in doing so, bypassing MFA security mechanisms.

Social Engineering [NIST SP 800-63-3][49]: The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.

Software as a Service (SaaS) [NIST SP 800-145][50]: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Supervisory Control and Data Acquisition (SCADA) [NIST SP 800-82]: A system generally used to control dispersed assets using centralized data acquisition and supervisory control.

Supplier [NIST SP 800-160 v.1 Revr.1]: Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the

[47] NIST (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf
[48] Signaling system 7 (SS7) (*2023) SS7*. Available at: https://ss7.info/
[49] Grassi, P. et al. (2017). *Digital Identity Guidelines (SP 800-63-3).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[50] NIST (2011). *The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

supply chain, developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; product resellers; and third-party partners.

Supply Chain [NIST SP 800-37 Rev.2][51]: Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

Tactics, Techniques, and Procedures (TTPs) [NIST SP 800-150]: The behaviour of an actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Third-party Providers [Adapted from NIST IR 8183][52]: Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization.

Threat [ISO/IEC 27000:2018, 3.74] [53]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

Threat actor [NIST SP 800-150][54]: An individual or a group posing a threat to a system, a network, an entity.

Threat Sources [NIST 800-137]: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

Two-Factor Authentication (2FA) [ITU-T X.1158 (11/2014)][55]: Two-factor authentication is a process that confirms a user's identity using two distinctive factors.

Vulnerability [ISO/IEC 27000:2018, 3.77]: Weakness of an asset or control that can be exploited by one or more threats.

Vulnerability Scanning (VS) [NIST SP 800-115] [56]: A technique used to identify hosts/host attributes and associated vulnerabilities.

Zero-Day-Attack [NISTIR 8011 Vol.3][57]: An attack that exploits a previously unknown hardware, firmware, or software vulnerability.

[51] NIST (2018). *SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* SP 800-37 Rev. 2, RMF: A System Life Cycle Approach for Security and Privacy | CSRC (nist.gov)
[52] NIST (2017). *Cybersecurity Framework Manufacturing.* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf
[53] ISO/IEC (2018). *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.* https://www.iso.org/standard/73906.html
[54] NIST (2016). *Guide to Cyber Threat Information Sharing.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
[55] ITU (2014). *Recommendation X.1158 (11/14)*. https://www.itu.int/rec/T-REC-X.1158-201411-I
[56] NIST. (2008). *Technical Guide to Information Security Testing and Assessment (NIST.SP-115)*. National Institute of Standards and Technology. Technical guide to information security testing and assessment (nist.gov)
[57] NIST (2018). *Security Control Assessment*. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8011-3.pdf

Terms defined here

This Technical Report defines the following terms:

Cyber Resilience for DFS Infrastructure: The ability of DFS ecosystems to withstand, respond to, and recover from disruptive and non-disruptive cyber events.

DFS Actors: Any individual, entity, corporation, or group directly involved in critical or non-critical DFS operations.

DFS Infrastructure: A digital and physical infrastructure that sees the cooperation between telecommunication and financial sectors to provide a digital financial service to an end-user.

DFS Operation: Any financial, or non-financial, operation involving a user-initiated DFS request.

DFS Request: A user-initiated operation that necessitates the evolvement of DFS actors, such as the telecommunication or financial sectors, for the provision of a digital financial service.

Abbreviations and Acronyms

2FA	Two-Factor Authentication
API	Application Programming Interface
APT	Advanced Persistent Threat
BIA	Business Impact Analysis
C2	Command and Control
CEO	Chief Executive Officer
CERT	Computer Emergency and Response Team
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CNI	Critical National Infrastructure
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic & International Studies
CSP	Cloud Service Provider
DCS	Distributed Control Systems
DDoS	Distributed Denial-of-Service
DFS	Digital Financial Services
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name Server
DORA	Digital Operational Resilience Act
DoS	Denial-of-Service
EMDEs	Emerging and Developing Economies
EU	European Union
FI	Financial Institution
Fintech	Financial Technology
HKMA	Hong Kong Monetary Authority
HTTPs	HyperText Transfer Protocol over Secure Socket Layer
ICT	Information and Communication Technologies
IMEI	International Mobile Equipment Identity
IMF	International Monetary Fund
IMSI	International Mobile Subscriber Identity
InfoSec	Information Security
IoC	Indicator of Compromise
ISO	International Organisation for Standardization
ISP	Internet Service Provider

IT	Information Technology
ITU	International Telecommunication Union
MFA	Multi-Factor Authentication
MITM	Man-In-The-Middle
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NIST	National Institute of Standards and Technology
OTP	One Time Password
PAFI	Payment Aspect for Financial Inclusion
PAN	Primary Account Number
PII	Personally Identifiable Information
PIN	Personal Identification Number
PR	Public Relations
PSK	Pre-Shared Key
PUK	Personal Unlocking Key
RAF	Risk Appetite Framework
RM	Risk Management
RPO	Recovery Point Objective
RTO	Recovery Time Objective
R&R	Roles and Responsibilities
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SIM	Subscriber Identity Module
SMS	Short Message Service
SS7	Signaling System 7
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCP/IP	Transmission Control Protocol / Internet Protocol
Telco	Telecommunication Company
TIBER	Threat Intelligence-based Ethical Red Teaming
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
UN	United Nations
US	United States
USSD	Unstructured Supplementary Service Data
vCard	Virtual Card
VS	Vulnerability Scanning
XML	eXtensible Markup Language

Cybersecurity Resilience Assessment Toolkit for DFS Critical Infrastructure

1 Overview

Over the past few decades, and especially since the COVID-19 pandemic, a growing number of individuals are making use of Digital Financial Services (DFS). These include private citizens, public institutions, and major organisations using DFS for a variety of different activities, including money transfers, e-payments, social benefit payments and monthly salary accreditations. According to IMF research[58], payment value linked to digital commerce and virtual transactions increased in Emerging and Developing Economies (EMDEs) between 2017 to 2019 from USD 1.2. trillion to USD 1.5 trillion.

This phenomenon differs from country to country, and studies demonstrate that it is associated with the projected economic growth of nations. According to a report published by the World Bank[59], a mature DFS environment can assist low-income residents and support national economic growth by lowering living costs and increasing security and transparency in widespread financial transactions. Similarly, studies conducted in Africa and South-East Asia demonstrate that digital payments supported the fight against world hunger and decreased the likelihood of users forgoing expenses due to market shocks[60]. As the uptake of digital payments in emerging markets is expected to increase over the foreseeable future[61], national DFS ecosystems will be required to guarantee, given the growing reliance on digital services, a higher level of cyber resilience of their DFS infrastructures.

As the demand for DFS in EMDEs increase, the developing world suffers a methodological and technological gap to secure critical assets and enhance network resilience. In fact, while developed countries and regions have initiated procedures to protect their DFS ecosystems emerging economies are at times struggling to keep pace. This issue has left local DFS critical components and assets often not compliant with established leading practices (e.g., *Principles for Operational Resilience*[62], *Payment aspects of financial inclusions*[63], and *Guidance on Cyber Resilience for Financial Market Infrastructures)*[64] and therefore susceptible to disruptive cyberattacks. To close the methodological gap and achieve higher levels of digital cyber resilience, EMDEs must entertain a structured cyber path to understand their current DFS cybersecurity posture, determine vulnerabilities and technological shortcomings, and define roadmaps that target areas of improvement. To this end, this report presents a tailored Cyber Resilience Toolkit to provide DFS regulators and DFS entities in emerging economies with the instruments to assess their security posture and define how to strengthen their resilience. In addition, the report provides guidelines to DFS regulators on identifying relevant actors, and defines the most common threats, risks, and vulnerabilities in DFS environments. Finally, it presents the methodology used to structure the Cyber Resilience Toolkit.

[58] Agur, I. et al. (2020). *Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies.* International Monetary Fund
[59] Pazzarbasoglu, C. et al. (2020). *Digital Financial Services.* World Bank Group
[60] Duflos, E. (2022). *Rethinking Consumer Protection: A Responsible Digital Finance Ecosystem*. CGAP
[61] Insider, B. (2021). *The future of digital payments in Africa - an outlook of trends in 2022*. Business Insider Africa
[62] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf
[63] Committee on Payments and Market Infrastructures and World Bank Group. (2016). *Payment aspects of financial inclusion.* Bank for International Settlements and World Bank Group. https://www.bis.org/cpmi/publ/d144.pdf
[64] Committee On Payments and Market Infrastructures and Board of the International Organization of Security Commissions (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures*. Bank for International Settlements. https://www.bis.org/cpmi/publ/d146.pdf

2 Cyber Resilience Toolkit

2.1 Objectives

The primary purpose of this tool is to facilitate cyber resilience self-assessments and enhance the resiliency of the Digital Financial Services (DFS) infrastructure by reinforcing both peripheral and internal defences. This tool is designed for use by DFS entities, users, and actors, including those within the telecommunications and financial sectors of the DFS ecosystem. By utilising this tool, these stakeholders can gain a better understanding of how to prepare for potential malicious cyber operations and establish best practices to defend against unauthorized access attempts.

The toolkit proposed in this study does not claim to be exhaustive nor to present all the solutions to threats targeting DFS servers, critical information, or the overall architecture. However, contrary to existing frameworks, it offers solutions and questions tailored to the EMDES' digital financial services ecosystem and common threats that can potentially impact their growing and interconnected ecosystems.

2.2 DFS Critical Entity Identification Matrix

This report presents a Critical Entity Identification Matrix to identify the entities relevant to the cyber resilience assessment proposed in the toolkit (Table 1). The matrix identifies four different categories of entities (i.e., non-significant, minor, major, and critical) based on their roles in the DFS ecosystem and the assessed impact on users and the national population in case they are targeted by a cyberattack.

For instance, in the unfortunate event of a cyberattack targeting a state-owned public telecommunication company providing the cabling network for critical national entities, the magnitude and relevance of the cyber incident are likely going to be much higher than a low-level ransomware attack targeting a private or private-government owned local FinTech. Therefore, this scenario demonstrates that regulators must coordinate with all critical entities (e.g., the telco company) and with other regulators to strengthen the overall DFS infrastructure's cyber resilience and its ability to withstand cyberattacks.

DFS Critical Entity Identification Matrix

		Entity ownership			
		Private	Private – Government Owned Corporation	Government - Local	Government - Federal
Entity's Customers (as % of the overall potential national consumer base) impacted by a disruption of services provided	< 20%	Non-Significant	Minor Entity	Minor Entity	Critical Entity
	20%	Minor Entity	Minor Entity	Major Entity	Critical Entity
	40%	Minor Entity	Major Entity	Major Entity	Critical Entity
	60%	Major Entity	Major Entity	Critical Entity	Critical Entity
	80%	Major Entity	Critical Entity	Critical Entity	Critical Entity
	> 80%	Critical Entity	Critical Entity	Critical Entity	Critical Entity

Disclaimer	Due to the nature of the DFS ecosystem, small and private enterprises may retain a close relationship with government and federal organisations, potentially representing a point of entry for malicious actors or malevolent lateral movement. For this reason, this toolkit warns that while the presented categorisation of private, government, and federal organisations stands in most cases, the interconnected nature of the DFS architecture urges a closer analysis of each entity before judging their positions and role in the ecosystem.

Table 1: DFS Critical Entity Identification Matrix

The first dimension, entity's ownership, groups entities into four categories (i.e., Private, Private - Government Owned, Government - Local, Government - Federal). The second dimension, entity's customers as "%" of the overall potential national consumer base impacted by a disruption of services provided, groups entities into six categories assessing the level of service disruption for the national population base in case of a cyberattack targeting the DFS entity itself (i.e., less than 20%, 20%, 40%, 60%, 80% and more than 80%). In other words, it prioritises companies based on the expected impact of a cyberattack on the population if successful. For instance, an offensive operation targeting the leading telecommunication company of a given nation is expected to cause a higher negative impact than a cyberattack against a small company with a limited number of private users. This distinction facilitates the definition of the relevant entities that require a higher level of cyber resilience to avoid widespread service disruption.

The crosscheck between these two variables' results defines the entities' role within the DFS ecosystem and, in turn, dictates whether they are to be considered relevant for the self-assessment. While non-significant and minor entities may still undergo the self-assessment and should be monitored for potential lateral supply chain attacks, major and critical entities must be prioritised to mitigate the risk of service disruption.

Nevertheless, it is essential to note that this matrix may not cover all scenarios due to the intricately interconnected nature of the DFS infrastructure. A seemingly non-significant entity can still present a potential point of failure, as it may serve as an entry point for malicious actors to infiltrate and move laterally. Likewise, a smaller entity offering a critical service that is widely used and/or exclusively sourced could create substantial disruption within the entire ecosystem if compromised. Because of their small size and perceived limited role in the architecture, indicators of compromise (IoCs) may be harder to detect and/or easier to ignore. Therefore, while protecting federal, critical, and major entities is paramount to strengthening overall cyber resilience, regulators and cybersecurity specialists must pay close attention to the interconnections and roles played by private suppliers and external service providers.

This prioritisation effort facilitates the identification of critical infrastructure and the work of regulators and specialists in analysing the current cyber resilience level. Therefore, before using the toolkit, the reader is advised to use the relevant matrix (Section 2.2, DFS Critical Entity Identification Matrix) to identify the relevant DFS actors involved in the self-assessment.

2.3 Structure of the Cyber Resilience Assessment Toolkit

The toolkit presents straightforward questions and controls to facilitate self-assessment and the evaluation of mitigation measures in place.

Among multiple cybersecurity standards and principles used for the development of the proposed methodology, the Cyber Resilience Toolkit leverages the following sources:

- The NIST Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53) provides customisable security controls that have wide-ranging applicability, thus facilitating its implementation to entities with varying characteristics (e.g., organisational, systems and networks used, the criticality of assets managed).
- The EU's Digital Operational Resilience Act (DORA) provides both robust cybersecurity requirements and guidance on information security measures to be implemented specifically by financial entities.
- The ISO/IEC 27000-series, in particular the Standards ISO 27001 and ISO 27005, provides security controls that specifically target the predominant elements of cyber resilience identified in the Methodology presented below, such as controls on risk assessments and risk management.

- The Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA DSS) provide security controls and requirements specific to payment protection and financial data.

This toolkit outlines four levels of cyber resilience maturity, which detail the characteristics needed to be more cyber resilient. To use the toolkit and initiate the cyber resilience assessment, regulators and officials must go through each question and select the appropriate level based on the response they assess closer to the company's status. The results will be aggregated and presented through a series of infographics, which will show the finalised cyber resilience assessment and indicate areas of improvement.

As an example, this report takes into consideration a question assessing the cybersecurity Training and Awareness level of a given DFS entity:

Are your personnel and staff properly trained in the risks connected to the internet? These include phishing, fraud, malware characteristics, and other social engineering schemes. (ID TA.01)

To respond to this question, a DFS entity may select one of the following resilience levels:

0. No, the corporate staff is not trained.
1. Yes, the staff is given training, although this does not count towards working hours and it is not encouraged.
2. Yes, the staff is given free and easily accessible training, although courses are not coded, and their attendance is not mandatory.
3. Yes, the staff is properly trained, and additional hours are given to those interested in honing their understanding of cybersecurity.
4. Yes, the entity schedules quarterly mandatory training sessions for all staff, organises drills, and evaluates personnel accordingly. Training counts towards working hours.

The selected answer will define the entity's cyber resilience level and count towards the final resilience score. The toolkit's cyber resilience levels are defined as follows:

"*None*" - Resiliency Level 0

Based on the principles outlined in the methodology, the entity/country does not have coverage of cyber resilience requirements.

A Mitigative Action Plan needs to be defined to fill the highlighted deficiencies.

"*Basic*" - Resiliency Level 1

Based on the principles outlined in the methodology, the entity/country does not have sufficient coverage of cyber resilience requirements.

A Mitigative Action Plan needs to be defined to fill the highlighted gaps.

"*Intermediate*" - Resiliency Level 2

Based on the principles outlined in the methodology, the entity/country has partial coverage of cyber resilience requirements.

Multiple actions are required to increase cyber resiliency, and several areas of improvement are indicated.

"*Advanced*" - Resiliency Level 3

Based on the principles outlined in the methodology, the entity/country has sufficient coverage of cyber resilience requirements.

Some improvement actions are required, and a few areas of improvement are indicated.

"*Expert*" - Resiliency Level 4

Based on the principles outlined in the methodology, the entity/country has a mature coverage of cyber resilience requirements. Therefore, no particular compensatory action is required.

The aforementioned cyber resiliency levels are applied to entities and countries. As regulators collect and aggregate data from the identified relevant DFS entities, they are able to assess the country's current cyber posture and resilience level.

2.4 How regulators would use the Toolkit for the cyber resilience assessment of DFS entities

The Cyber Resilience Toolkit targets both DFS regulators and entities, who are asked to respond to all questions relevant to their roles within the DFS ecosystem and their current cybersecurity standards. When receiving the Toolkit, regulators are encouraged to filter the applicable questions and identify the significant DFS entities under their jurisdiction. This exercise is facilitated by the matrix provided in this report (Table 1, Section 2.2, DFS Critical Entity Identification Matrix). The matrix identifies relevant entities based on their significance within the DFS ecosystem and the projected impact a cyberattack against them would have on the wider national infrastructure. Based on the matrix evaluation, regulators can define the operational perimeter of their cyber resilience assessment and provide entities with the relevant controls. As the Toolkit is of self-assessment nature, regulators need to trust that entities will conduct a fair and transparent evaluation of their current resilience status. When applicable or necessary, the regulator could request for evidence of what entities responded in the questionnaire.

Therefore, once the regulator has obtained the Toolkit and identified the significant entities, it can distribute the self-assessment material to companies and organizations deemed of importance for the DFS ecosystem. After filtering the controls and responding to all questions, entities are requested to provide regulators with the finalised evaluation. Based on the needs and specificities of each entity taking the assessment, data can be rendered in a twofold way:

a) Holistically, by showing only the final score that accounts for the average grade received for each pillar. The holistic overview is recommended only in particular cases, as it fails to point out areas of improvements or domains that require a more focused review.
b) Granularly, by emphasising the results received for each domain. This method is recommended for most entities; it facilitates the definition of customisable roadmaps, and the presentation of more detailed results to the regulators and relevant stakeholders.

To aggregate such data, the regulator could, for instance, utilise a table that combines the following information: entities' names, their roles in the DFS ecosystem, and the scores obtained at the domains level. The information will allow the regulator to have a general overview of the entire ecosystem and to identify criticalities. More specifically, this effort could:

a) Support the regulator's understanding of the average cyber resilience level of the DFS ecosystem.
b) Help regulators to identify entities, who are below the desired level of cyber resiliency in specific domains or do not meet the minimum-security standards mandated by the regulator, by confronting entities' data and identify weak points and liabilities.
c) Promptly verify the entity's responses by cross-checking the minim-maximum results and requesting evidence of the cybersecurity standards and measures currently in place.

Furthermore, regulators are encouraged to meet with relevant entities and stakeholders on a regular basis following the distribution of the Toolkit material. In fact, periodic meetings will not only promote cross-department cooperation to aggregate data and understand entity's issues, but will also

facilitate compliance among parties, shared understanding and knowledge transfer, and ensure that all significant entities are onboard before initiating mitigation or correction plans.

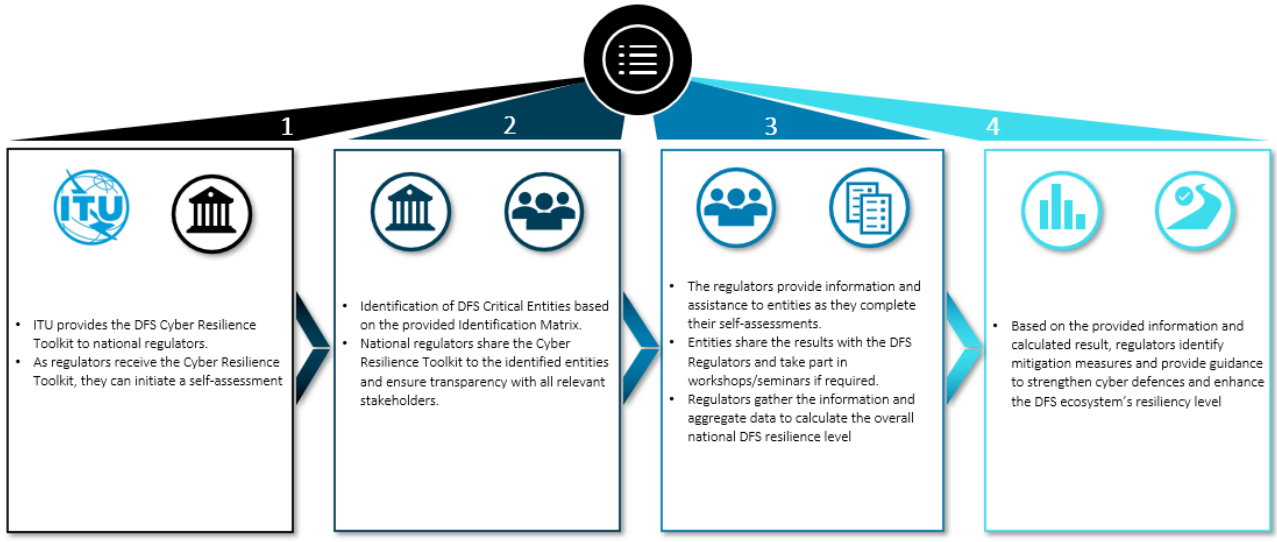

Figure 1: Cyber Resilience Assessment

As regulators receive the toolkit, they follow a four-step process to collect, aggregate and analyse the data. The process is as follows:

- **Step One:** The regulator receives the Cyber Resilience Toolkit from ITU and initiates a self-assessment filtering the applicable content.
- **Step Two:** The regulator identifies the relevant entities to be involved in the assessment through the provided DFS Critical Entity Identification Matrix (to be found in Section 2.2). This identification process facilitates a prioritization for the most critical entities within the country's DFS ecosystem. As the regulator completes the identification process, it passes on the Cyber Resilience Toolkit at the entity level.
- **Step Three:** The engaged entities initiate their own self-assessment and reach out to regulators in case of any difficulties. Regulators aggregate the data received back from the entities and, by doing so, obtain a preliminary overview of the DFS CNIs' current cyber resilience status. The information can be aggregated through virtual communication, or through other methods (e.g., workshops, seminars). This process is left entirely to the decision of the regulator and can vary depending on national priorities, and preferences.
- **Step Four:** The completely aggregated data facilitates the identification of DFS national weaknesses and the definition of specific national cyber resilience roadmaps.

2.5 Example

To further explicate the aforementioned process, this report takes the example of a DFS regulator assessing the national cybersecurity preparedness of an unspecified country. The regulator is aggregating the data coming from three different entities (i.e., entity A, entity B, entity C). These entities represent – in this example - actors involved in any DFS operation (Section 3.1, Identified Actor): the telecommunication and the financial sectors. These actors are only illustrative of the entities' roles that can be listed in this table; they should not be considered exhaustive. Instead, within this table, regulators should aggregate results coming from significant entities previously identified through the provided matrix (Section 2.2, DFS Critical Entity Identification Matrix), which facilitates the classification of entities' roles and their significance in the DFS system. Therefore, the "Role" column of the table should be completed with the specific role that the assessed entity plays in the ecosystem, and not necessarily with the "telco" and/or "financial" label. Upon recognising and

defining its role in the DFS ecosystem, entities are expected to answer all applicable questions and provide the relevant information.

Below, this report includes an illustrative example of the table that the regulator can utilise to aggregate the data.

Name	Role	Overall Score	Pillars					
			Risk Management	Governance	Testing	Training and Awareness	Protection	Incident Response & Protection
Entity A	Telco Entity							
Entity B	Financial Entity							
Entity C	Telco Entity							

Table 2: Entities Data Aggregation Table

Once the regulator starts receiving the self-test assessment information from the three DFS entities, the data needs to be populated on the applicable columns. By following this exercise, the regulator can ensure transparency with all stakeholders and provide analysts with a structured and clear way to reference the information. In this scenario, the entities record scores in a range of two to four (Section 2.3, Structure of the Cyber Resilience Toolkit).

Name	Role	Overall Score	Pillars					
			Risk Management	Governance	Testing	Training and Awareness	Protection	Incident Response & Protection
Entity A	Telco Entity	3	3	2.5	3	3.5	2	4
Entity B	Financial Entity	2.5	2.5	3	3	2	2.5	2
Entity C	Telco Entity	3.5	4	2.5	4	4	2.5	4

Table 3: Example of Entities Data Aggregation Table

The aggregation of the data in the table further illustrates the weak points in the ecosystem; in this example represented as the Governance and Protection pillars for entity A and C, and Incident Response/Training for entity B. The regulator can identify low scores focusing on any grades below a pre-determined threshold; for this instance, this report assumes the threshold of three as an advanced level. If a mistake is made, the system automatically warns the user. More specifically, in specific cases, such as the selection of two mutually exclusive answers to a question, the toolkit prompts an error message asking the user to only select one single entry. Upon receiving the message, users are encouraged to revise the table and provide the updated results to the regulators. A more detailed

example of the exercise is also provided in the Cyber Resilience Toolkit's document in the "Example" sheet.

Based on the self-assessments data from the entities' completed questionnaire, the regulator can also calculate three important metrics:

a) The **column "Overall Score",** which is automatically calculated by the toolkit**,** indicates the average score of each entity. It can be calculated summing the results of each pillar and dividing by the number of the values being added (i.e., six). In this specific instance, and taking entity A as an example, the regulator sums all the grades (3 + 2.5 + 3 + 3.5 + 2 + 4 = 18) and divides the result (18 / 6 = 3). The overall score for the entity (i.e., the average of all the pillars' scores) is therefore three.
b) The **average for pillars or domains**. Although this computation may not be critical while cross-referencing entities' data, they illustrate what are the areas that need improvement for each specific entity. For instance, should entity B score three in pillar "Testing", but more specifically five in Red Teaming (Section 4.3.1, Red Teaming) and one in Vulnerability Scanning (Section 4.3.3, Vulnerability Scanning), it is clear that a functioning roadmap must include structural improvements on the entity's Vulnerability Scanning capabilities.
c) The **average of the overall scores** indicates the average resilience score of the national DFS infrastructure as it takes into account all significant entities and their calculated overall scores. This computation can be determined by considering all the grades under the "Overall Score" column. Given a country that only has three DFS significant entities (as in this example, i.e., Entity A, Entity B, and Entity C), the regulator can calculate the averaged resilience by summing the three values and dividing by the added numbers (i.e., in this scenario, 3 + 2.5 + 3.5 = 9 /3 = 3). Therefore, the final cyber resilience DFS score would be three out of four.

This exercise, extended to all the tested entities, facilitates the identification of the ecosystems' weaknesses, focusing on any grades that do not meet the threshold set by the regulator. While this report considers three out of five to be an advanced level (Section 2.3, Structure of the Cyber Resilience Toolkit), this may not be the case in all DFS environments as operational needs and, consequently, minimum standards can vary greatly. It is therefore important that expectations and thresholds are set in advance by the regulator and properly communicated to the relevant stakeholders.

3 Mapping the DFS Infrastructure

3.1 Identified Actors

This report defines DFS actors as all individuals, entities, or organisations directly involved in a digital transaction. Depending on the nature and architecture of each DFS system (whether global, regional, or national) and the complexity of the financial infrastructure, the actors at play may change. However, as a fundamental methodological basis, this document recognises four main actors[65] to be critical in any DFS operation: the client, mobile network operators, financial institutions, and third-parties. Their significance in the system is based on their roles in the DFS infrastructure and their importance in financial operations, defining them as pivotal actors in any Digital Financial Services environment.

a) **Client / User**: The end user is considered the target or the initiator of a DFS request, may that entail a money-less interaction with the bank and/or the transfer of an undefined capital. In this report, the terms "client" and "user" will be used interchangeably; by requesting a digital

[65] ITU. (2020). *Digital Financial Services security assurance framework*. International Telecommunication Union. https://www.itu.int/hub/publication/t-tut-dfs-2021/

service through an application or a webpage, a bank client also becomes a service user. In fact, in a DFS user-bank exchange, possibly conducted through a mobile money application downloaded on a device belonging to the user and accessed with pre-determined login credentials, sees the client/user requesting a financial service to be conducted remotely. The details needed to access the users' accounts are stored in centralised servers and crossed-checked through a Pre-Shared Key (PSK) encryption mechanism.
The request and connection to the mobile network can be completed through the owner's SIM card or through a cabled/wireless network infrastructure, which remains potentially exposed to invasive cyberattacks and/or compromises. Therefore, a SIM card in this document is acknowledged as a physical or virtual card (vCard or e-SIM), and it is a bridge between the user and the next DFS stakeholder: the Mobile Network Operator.

b) **Mobile Network**: The Mobile Network Operator (MNO) is responsible for the transit connectivity between the Financial Institution (FI) to the end users and vice versa. The MNO provides the wireless or cabled network infrastructure connecting the two actors. Depending on the sophistication level of the overall DFS infrastructure, the MNO may also interact with a DFS provider, here intended as a DFS actor that provides the necessary web/device applications managing the relationship with the financial institutions.
The MNO infrastructure remains exposed to potential infiltration. Threat actors may use the mobile network infrastructure to operate man-in-the-middle schemes or facilitate the disruption of DFS critical services. For example, hackers tend to capitalise on unsecured MNO environments to create an evil twin and intercept user data in transit. Furthermore, given the interconnections between the four stakeholders (i.e., the end user, the MNO, the financial institution, and third-parties), and the importance of the mobile network in transmitting critical information, hackers may leverage a compromised telco operator to elude DFS defence mechanisms and move laterally in the supply chain. Further details on identified cyber-threat actors in DFS ecosystems can be found in Section 3.2.

c) **Financial Institution**: The financial institution receives and responds to requests from the user, playing a pivotal role in any DFS operation. Under specific circumstances, it can also be considered the initiator of direct interactions with the customer. For instance, the financial institution could respond directly to a money-transfer request and verify the DFS user through an identity management software. Alternatively, the financial institution may link to the requestor through a software program or hardware infrastructure (e.g., a DFS application, or an Ethernet connection on a personal computer) created internally or through external third-parties. This may not be the case in federated or brokered digital identity systems, where a third-party acts as an intermediary between the parties and facilitates the necessary financial actions and exchanges between the financial institutions and the users.

d) **Third-Parties**: This study defines third-parties as entities external to the leading, or analysed organisation[66]. These include, but are not limited to, service providers, vendors, suppliers, demand-side partners, consortiums, alliances, and investors. Due to the central role third-parties may have in a DFS entity's internal structure, especially in providing external tools and services, third-parties could threaten a given organisation's cyber resilience. This, commonly referred to as *third-party risk*, is widely acknowledged as the result of the probability of the third party effectively causing a disruption impacting the service utilised by the leading entity. For example, a financial institution using a front-end Software as a Service (SaaS) solution (e.g., an application or graphical interface) may see its operations disrupted if the third-party managing the SaaS solution is targeted by a cyberattack and its servers are

[66] Janeway,T. (2020). *The NIST Cybersecurity Framework – Third Parties Need Not Comply*. ISACA Journal. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-1/the-nist-cybersecurity-framework-third-parties-need-not-comply_joa_eng_0220.pdf

temporarily unavailable. In a wireless setting, this document also considers other potential DFS stakeholders, such as a mobile application developer, a mobile handset manufacturer, and an external service provider who continues the transaction monetisation and ensures the complete finalisation of the initiated operation[67]. On top of the minimum four actors (i.e., client, MNO, financial institutions, and third-parties), these additional stakeholders can directly facilitate cross-sectoral interactions and provide a financial service to the client. For instance, in a wireless DFS environment, an application developer can enable user-friendly applications that connect the client to an Internet Service Provider (ISP) and, ultimately, their banks.

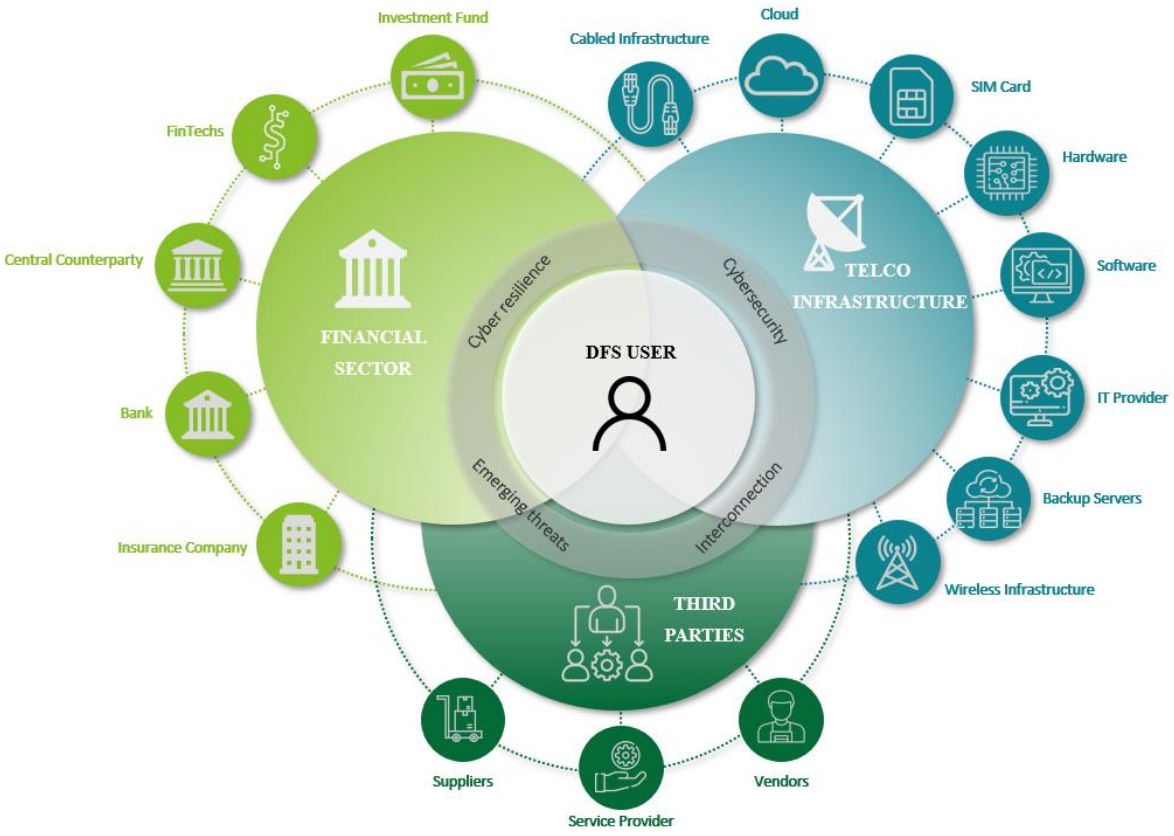

Figure 3: DFS Actors

The four aforementioned actors (user, telecommunication sector, financial sector, and third-parties) are critical in any DFS ecosystems and represent the backbone to complete any digital financial operations. They are strongly interconnected and continuously cooperate to provide the final user a service. Due to their role and significance in the DFS infrastructure, they must be considered in any DFS cyber resilience assessment. However, they are not the only actors. In advanced DFS ecosystems, the DFS provider-created Digital Financial Service Application (DFS application) often functions as the intermediary between the user and the financial institution. A DFS application consists of a user-friendly Graphical User Interface (GUI) that facilitates the reception and revision of users' requests, enhancing communication and transparency. However, these requests are carried through electronic or wave signals in the MNO's infrastructure and, in unfavourable circumstances, can be exploited for malicious use (e.g., credential harvesting, account hijacking, or remote malware execution).

[67] ITU-T, F. G. (2017). *Security Aspects of DFS.* International Telecommunication Union

Additionally, a functioning DFS environment will likely include Financial Technology (here acknowledged also as FinTechs) firms, which are global and/or regional entities driving digital payments innovation and transforming how users invest, save, and borrow money[68]. This situation further demonstrates the volatility of the environment and suggests that these digital mechanisms will likely continue to adapt and change over the next few years.

In different terms, a DFS ecosystem can be widely understood as an interaction between the financial and mobile networks to provide a service to a client[69]. A DFS ecosystem encompasses, but is not limited to, banks, insurers, financial market infrastructures, credit assessment institutions, investment funds, telco companies, and private citizens. The DFS ecosystem requires close collaboration between the financial and telecommunication sectors. While the first may involve private or public monetary authorities or private entities, the second may include state-of-the-art communication infrastructures facilitating data flow. This includes cloud computing, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) mechanism, and broader Information Technology (IT) services.

Due to the nature of the DFS requests, this ecosystem mandates communication among these two networks and multiple elements, including software, hardware, and cabled infrastructure. In addition, communication nodes may remain exposed to the internet. As a result, inefficient or weak encryption algorithms may not protect them, making them potential entry points for cyber-enabled threats targeting financial systems.

As the interactions between the actors change, existing literature [70]list four distinctive business models on the nature and functioning of the DFS ecosystems. These models are the following:

1. Bank-Led Business model
2. MNO-Led Business model
3. Mobile Virtual Network Operator (MVNO) Business model
4. Hybrid Model

They all dictate a specific interaction among the various stakeholders and indicate one of the actors as a central pillar of the ecosystem. For example, the first model (i.e., the Bank-Led Business model) emphasises the bank's centralised role as a financial aggregator and provider of DFS services. In this scheme, the bank functions as the central hub for DFS users' requests, and the network framework is the link between the bank itself and citizens or entities in need.

Regardless of the designated model, this document will not consider in depth the various schemes but will maintain a more holistic and comprehensive understanding of the DFS ecosystem to include as many architectures as possible. Considering the scope of this document, the analysis will aim to structure the methodology, maintaining a broader view of the DFS ecosystems and their actors. This will facilitate the establishment of the toolkit and a holistic methodology that will address the needs of a larger number of readers. However, a published International Telecommunication Union (ITU) study will serve the purpose of those interested in deepening their understanding of the various models[71].

3.2 DFS Vulnerabilities, Most Common Threats, and Related Mitigation Measures

Different DFS ecosystems' actors face threats that often share several commonalities. For this reason, ITU proposed[72] a comprehensive framework to categorise and map threats, vulnerabilities, and risks,

[68] Deloitte. (2017). *Fintechs and regulatory compliance.* Deloitte
[69] Brauchle, J.P. et al. (2020). *Cyber Mapping the Financial System*. Carnegie Endowment for International Peace
[70] ITU. (2020). *Digital Financial Services security assurance framework*. International Telecommunication Union https://www.itu.int/hub/publication/t-tut-dfs-2021/
[71] ITU. (2020). *Digital Financial Services security assurance framework*. International Telecommunication Union. https://www.itu.int/hub/publication/t-tut-dfs-2021/
[72] ITU. (2020). *Digital Financial Services security assurance framework*. International Telecommunication Union. https://www.itu.int/hub/publication/t-tut-dfs-2021/

suggesting mitigation procedures. This categorisation effort has been analysed and included in the following paragraphs to define a preliminary shared understanding of some risks common to DFS ecosystems.

As an initial disclaimer, it must be stated that the threat list provided in this document is not exhaustive; it highlights the most common threats according to the present literature and international standards[73]. As the ever-changing nature of the cyber world remains a central figure of the digital ecosystem, threats and risks change according to the local DFS and social structure, as well as the single nation's technological, economic, and political sophistication. Furthermore, while representing various degrees of cyber maturity and technical know-how, each threat listed below can occur as a single event or be combined in a more complex and invasive digital or hybrid offensive cyber operation.

This document will refrain from presenting threat scenarios based on actual intelligence or broader geopolitical dynamics. Instead, it will limit itself to giving technical details of identified threats to facilitate regulators and DFS officials in defining cybersecurity risks and mitigation measures. This operation will better prepare the reader to approach the methodological discussion and utilise the created toolkit to its intended capabilities.

Account and Session Hijacking Attacks

In an Account or Session Hijacking incident, DFS Providers or MNOs face the risk of data exposure and modification. Cyber-threat actors would capitalise on exposed vulnerabilities to complete an unauthorised account takeover, where an attacker impersonates an authorised user and harvests confidential data and credentials.

In this scenario, attackers exploit inadequate user sessions and accounts management vulnerabilities. This can be done in multiple ways, such as leveraging weak encryption mechanisms to store credentials or unpatched software that may not be properly monitored.

DFS actors must strengthen the user ID management process, impose user session timeouts, and ensure robust cryptographic hashing algorithms to mitigate the risk of account and session hijack. In turn, authorisation tokens or Multi-factor Authentication (MFA) will limit the risk of malicious activity, and a strong no-trust mechanism will likely mitigate the risk of lateral movement.

Credentials Attacks

In a credential-harvesting incident, DFS Providers or Mobile Devices risk unauthorised access and takeover of a user's DFS account. Once the genuine profile is compromised, threat actors may proceed with on-path attacks (also known as Man-in-the-Middle, or MITM), intercepting data in transit, potentially modifying its content, and stealing confidential login credentials. A MITM scenario may also facilitate phishing attacks, capitalising on close relations between co-workers. For instance, the hackers may leverage a compromised account to reach out to connected individuals and lure other employees into willingly giving up privileged information or access controls.

In such a scenario, attackers exploit vulnerabilities related to inadequate Personal Identification Number (PIN) and password policies, often leveraging the lack of an MFA or Two-factor Authentication (2FA). If robust MFA or 2FA mechanisms are not in place, hackers can capitalise on multiple complex credential-harvesting schemes, including but not limited to credential stuffing, sniffing, or spoofing. Similarly, server misconfigurations or unlimited user login attempts are among the logical vulnerabilities malicious actors can easily exploit to access sensitive information.

To limit the risk of a MITM attack or the leak of confidential information, DFS actors must define strong authentication mechanisms and robust password and PIN policies. In addition, limiting the

[73] PCI Security Standards Council. (2022). *Data Security Standard*. https://www.pcisecuritystandards.org/document_library/
PCI Security Standards Council. (2013). *Payment Application Data Security Standard*. https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf

maximum number of consecutive login attempts is strongly recommended to mitigate the risk of a brute force or dictionary attack.

Systems and Platforms Attacks

When targeting DFS environments, cyber-threat actors often attempt to spy on and remotely steal credentials from user devices. To achieve this, hackers often capitalise on account access privileges and conduct denial-of-service (DoS) attacks to, for instance, divert corporate attention while infiltrating the network. This could facilitate unwanted intrusion through, for example, a sophisticated phishing attempt or a more subtle watering hole.

In this scenario, attackers exploit vulnerabilities related to the unsafe transfer of customer credentials and insufficient network protection. When inside, hackers may attempt lateral movement to access confidential information to be sold on the Dark Web or to be encrypted in a ransomware incident. In more complex and severe attacks, hackers may capitalise on low-level incidents to create distractions, penetrate the system, and maintain undetected persistence. Such operations, often conducted by Advanced Persistent Threat (APT) actors, sees hackers establishing communication channels with their controlled servers and exfiltrating data of corporate interest from the compromised systems and platforms.

As DFS actors often maintain a pivotal role in the national interest of their countries, the harvested data may also include information about the state's national security, such as financial transactions related to contracts affecting the country's critical national infrastructure.

The entity may undertake multiple controls and procedures to mitigate the risk of DoS attacks. These include, for instance, creating Demilitarized Zones (DMZs) in the network, distrusting binary-based Short Message Service (SMS) messages and limiting network exposure. In this case, the entity may strengthen peripheral and internal defence to limit the risk of platform compromise. This may consist of a defence-in-depth mechanism based on pre-defined security layers, a no-trust access policy, or a complex architecture of firewalls and Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS). A robust defence-in-depth mechanism, as an example, can be constituted of three main security layers: the Infrastructure Security Layer, a Services Security Layer, and an Applications Security Layer. These divisions can prevent in-depth attacks and preventively intercept operations targeting core functions of the entities' service[74].

Code Exploitation Attacks

In a Code Exploitation Attack, a DFS Provider faces the risk of application compromise. In these operations, attackers exploit vulnerabilities related to unpatched software and not-updated security libraries.

To mitigate the risk of this exploitation, DFS actors must ensure continuous monitoring of security libraries, define a patching revising cycle, and coordinate with operating system providers to keep up with the latest updates.

Data Misuse Attacks

In a data misuse incident, an MNO, a DFS Provider, or a Third-party Provider risks unauthorised access to and interception of user data. Threat actors may capitalise on weak encryption mechanisms and inadequate data protection controls to infiltrate servers and manipulate or exfiltrate information. Depending on the data's nature and value, threat actors may decide to obtain and transfer it to high-level foreign actors or sell it to third parties on the cyber black market.

Under severe circumstances, threat actors may also manipulate the data to bring about corporate or market disruptions to pursue a political or economic personal objective. An example of severe data

[74] ITU. (2020). *Digital Financial Services security assurance framework*. International Telecommunication Union. https://www.itu.int/hub/publication/t-tut-dfs-2021/

misuse is the compromising and/or interception of users' financial information, such as the Primary Account Number (PAN) or account number. Through such information, hackers may, among multiple malicious activities, complete unapproved transfer funds or identity theft/social engineering schemes. Therefore, regardless of the method used for producing receipts (e.g., e-mail, SMS, or attached printer), the DFS entity should mask the PAN in support of applicable laws, regulations, and payment-card policies, to mitigate the risk of data misuse and avoid releasing users' confidential information.

Data misuse is a widespread cyber occurrence that targets various environments and can be highly profitable for insider trading. For this reason, it remains one of the most common and used cyberattacks in today's cyber world.

Potential controls and procedures mitigating the risk include encryption solutions, data management processes, data anonymisation mechanisms, and third-party monitoring.

Denial of Service Attacks

In a Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack, cyber-threat actors target a DFS provider (e.g., MNO), flooding the network or servers with superfluous Transmission Control Protocol/Internet Protocol (TCP/IP) requests to disrupt the regular data traffic. In a DDoS attack, the threat actor capitalises on multiple infected machines (i.e., zombies) to launch a coordinated attack. In a DFS environment, a successful DoS or DDoS attack could result in the inability of users or financial institutions to complete a digital transaction due to a service outage or to suffer from transaction failures due to high technical delays.

In such scenarios, attackers exploit network failures and traffic monitoring vulnerabilities to shut down the service and cause temporary or permanent disruption.

Controls and procedures mitigating the risk a DFS actor can put in place involve high network availability solutions, technical capacity periodic tests, network admission techniques, and ad-hoc firewall rules.

Insider Attacks

An insider attack is widely acknowledged as one of the most subtle and disruptive cyber incidents targeting an organisation because it may involve disgruntled employees, entity officials, or blackmailed individuals who are already fully integrated within the company. For example, insider threats in a DFS ecosystem may include laid-off employees or management officials seeking financial revenues. Additionally, an insider attack involves data exposure and integrity risks, as the threat actor may have access to privileged folders or servers with confidential data that can be leaked or modified to pursue personal objectives.

An insider threat would customarily exploit vulnerabilities related to privileged access management, insufficient internal controls, and lack of data input checks. Capitalising on their role within the company, an insider attack would also leverage clock synchronisation, the absence of logging/captive portals, or the possibility of altering logs to manipulate data or leak it for foreign and domestic use. Additionally, insider attackers may conduct one-off operations for financial purposes or find themselves blackmailed and forced to comply for other reasons. Regardless of the justification behind the attack, an insider attack may be less visible and detectable due to employees' privileged position within an organisation.

For a DFS actor, controls and procedures mitigating the risk include segregation of duties, physical access controls, input validation controls, and robust logging mechanisms. Given the surge in the cases of insider threats, companies and organisations are traditionally advised to adopt a zero-trust mechanism, strengthen internal defences, and limit lateral movement.

Social Engineering Attacks

A social engineering attack is an easily customisable and common attack targeting various parts of today's society. In such scenarios, hackers lure victims into willingly providing credentials or data

access by pretending to be someone else. For example, more specifically in the DFS ecosystem, a hacker may target an end user pretending to be a financial institution and requesting the input of login credentials through a weaponised captive portal. Also prevalent is the instance of threat actors using watering holes to lure people into believing that a web page is legitimate, encouraging them to give up personal data[75] (such as personally identifiable information, geo-localisation, and social media activity) and potential credit card details.

In this scenario, an MNO, a Third-party Provider, and a Mobile User may face multiple risks, including data exposure and modification, unauthorised access to user data, and user impersonation. The hackers may also capitalise on weak defence mechanisms to perform user account takeovers, identity theft, and unauthorised financial transactions. Beyond the evident financial repercussions of a social engineering attack, a DFS actor may incur reputational damage and the loss of trust from its clients.

To successfully complete the attack, threat actors exploit vulnerabilities related to unprotected credentials, unverified or unsigned applications and inputs, weak encryption mechanisms, misconfigurations of accounts, and poor management of certificates or keys. Social engineering attacks vary in nature, and their magnitude may differ depending on their ultimate objective. For instance, a threat actor may capitalise on a social engineering scheme to leak data but may also decide to encrypt the information or maintain persistence and act as a fifth column for a hostile government agency. As in other instances, DFS actors, given their role in a country's critical national infrastructure (CNI), are particularly exposed to social engineering schemes.

DFS actors must strengthen user awareness, ensure robust authentication mechanisms, and fortify encryption algorithms to protect themselves and mitigate the risks.

DFS Infrastructure Attacks

Due to their importance in the economic posture of a country, hackers may decide to compromise the physical and logical infrastructure of DFS actors to disrupt services. In such scenarios, DFS providers and Third-party Providers face the risk of infrastructure and data compromise for political, personal, or social objectives. The disruptions include service outages, the inability to complete financial transactions, and data exfiltration and modification. Hackers likely want to compromise transaction integrity and cause operational inefficiency through service interruption. Beyond the most traditional cyber incursions, hacktivist groups often conduct these operations to bring radical political and social changes. Hacktivists and other threat actors may leverage vulnerabilities related to inadequate access controls on user accounts, untested restoration practices, and scarce data controls to infiltrate the network.

Attackers may also capitalise on weak defence mechanisms (e.g., loose cybersecurity policies and inadequate defence procedures) to conduct Supervisory Control and Data Acquisition (SCADA) attacks or compromise Distributed Control Systems (DCS). SCADA and DCS attacks, potentially targeting aggregating systems in telecommunication organisations or financial institutions, could facilitate more significant and disruptive operations, potentially bringing to a halt or disrupting critical operations in national and/or international infrastructures. While the direct consequences of such operations can vary greatly and go beyond the scope of this document, attackers could also capitalise on inadequate defence mechanisms to compromise data integrity and leverage over-reliance on external trust anchors to pursue their malicious intents.

To mitigate the risks, DFS actors must adopt MFA or multi-model authentication processes to access DFS accounts, ensure the removal of default accounts, and include backups and digital signature controls.

SIM Attacks

[75] Committee on Payments and Market Infrastructures and World Bank Group. (2016). *Payment aspects of financial inclusion. Bank for International Settlements and World Bank Group*. https://www.bis.org/cpmi/publ/d144.pdf

During a Subscriber Identity Module (SIM) attack, a DFS Provider and MNO face the risk of account takeover and unauthorised financial transactions. In such a scenario, financial institutions risk losing access to user accounts and potentially witness reputational damage and loss of business as clients grow unsatisfied with the entity's security processes and migrate to another provider[76].

To compromise a SIM card, attackers exploit vulnerabilities related to inadequate user identification controls and lack of transparency in the verification before SIM swap and SIM recycling. In doing so, attackers may be able to briefly impersonate users, compromise their accounts, and act as real users in their DFS operations.

To avoid such scenarios, DFS must ensure an identity verification process is in place before SIM swaps. Identity should be verified using a combination of something users are, have, or know. For example, identity theft risk can be mitigated by presenting a valid ID, biometric verification, and knowledge about the DFS account details before a SIM swap/SIM replacement. Moreover, DFS and Payment Service Providers must put in place systems to promptly detect potential SIM swaps or replacements and perform further verification before any high-value transaction or account changes are authorised with a new SIM. Such mechanisms should include ways for the DFS provider to block the account until the identity of the new person holding the SIM card is verified.

To perform this swap security controls, DFS providers must ensure they have procedures to check if the International Mobile Subscriber Identity (IMSI) associated with the phone number has changed. If so, this could be a direct sign of a SIM swap. In this case, DFS providers are encouraged to check the International Mobile Equipment Identity (IMEI) of the phone holding the SIM. If the IMEI has also changed, there is a high probability of a SIM swap. In that case, the DFS provider must block the account until performing account verification procedures to mitigate the risk of a SIM attack.

DFS Services Attacks

When a DFS service is compromised, a DFS Provider faces the risk of service failure and data compromise. When targeting a DFS service, attackers exploit vulnerabilities related to unauthorised changes to system configurations and data/file logs. Additionally, hackers may leverage inadequate user access or input validation to penetrate the network.

DFS actors must protect their networks against external tempering, allowing only online transactions and establishing robust MFA processes for users and third-party access to mitigate these risks. Furthermore, DFS actors must check incoming data against expected values in Application Programming Interface (API)-related data schema for Unstructured Supplementary Service Data (USSD), perform eXtensible Markup Language (XML), validation of XML over HyperText Transfer Protocol over Secure Socket Layer (HTTPs) requests, and use analytics systems to check user transactions details, including user activity's velocity, access time, and authorisation validation.

DFS Data Attacks

In the event of unauthorised data access, threat actors may manipulate, intercept, or leak data pertaining to DFS users or entities. In this scenario, attackers would exploit vulnerabilities such as weaknesses in the user account access control mechanisms, inherent Signaling System 7 (SS7) security flaws, or weak encryption practices. Furthermore, hackers may attempt to access data by leveraging unprotected sensitive traffic, intercepting MO-USSD transactions, or capitalising on the inadequate protection of DFS customer registration data, which may sometimes be stored in unprotected servers or unnecessarily exposed to external activities. Threat actors may capitalise on unmonitored wireless networks to infiltrate the DFS infrastructure and reach compromised servers. Similarly, entities are strongly recommended to enhance robust third-party data protection policies, including data destruction and erasing procedure, to limit the risk of data appropriation and dumpster diving events.

[76] Committee on Payments and Market Infrastructures and World Bank Group. (2016). *Payment aspects of financial inclusion. Bank for International Settlements and World Bank Group*. §1.4.6. https://www.bis.org/cpmi/publ/d144.pdf

To mitigate the risk of unauthorised data access, DFS actors must strengthen policies related to the PIN and Personal Unblocking Key (PUK) and establish multi-factor authentication methods to block potential identity theft attempts. Furthermore, DFS actors must use firewalls to detect and limit attacks based on SS7 security flaws, deploying SS7 and diameter signalling security controls. Moreover, it is strongly recommended that DFS entities monitor that the IMEI of the device performing the transaction matches the registered IMEI of the account holder's phone and mandate the use of a two-way secure One Time Password (OTP). Furthermore, entities are recommended to implement other defence mechanisms, such as robust cryptography practices, policies limiting the number of sessions per user, and strong encryption standards (e.g., TLS encryption v1.2 and higher) for API communications.

Finally, DFS actors must monitor user IP, device, and login time authentication for all privileged users, agents, and merchants connecting to the DFS system.

Malware Attacks

If compromised with malicious software (also known as malware), a DFS Provider, an MNO, Third Parties, and mobile users face the risk of service disruption and data leaks. In addition, a malware attack may comprise at the same time multiple software acting differently; therefore, if a threat actor compromises the network or a DFS device with malicious software, hackers may be able to perform various activities remotely. These include causing a service outage, accessing unauthorised data, downloading more invasive programs, and exfiltrating confidential information belonging to a user or an entity. Therefore, hackers can conduct a wider range of offensive cyber operations through a malware attack than a single user account compromise.

To deliver the malware, attackers may exploit a diverse range of vulnerabilities, such as outdated anti-malware or anti-virus software. Similarly, an inadequate collaboration with the mobile solution provider, including the lack of regular meetings on cybersecurity dynamics and/or the lack of transparency/communication in case of an attack, may facilitate the successful completion of a cyber event. Finally, an open/unpatched system may expose the network to outside attacks, with hackers leveraging obsolete software programs or a user device's physical tempering and rooting to conduct privilege escalation and execute arbitrary codes (Remote Code Execution, or RCE).

For the DFS ecosystem to mitigate the risk of malware compromise, DFS entities must deploy robust security software products on all corporate mobile devices, mandate a strong antivirus program, and use antispyware software. This is also recommended, though not mandatory, for all personal devices to mitigate the risk of lateral movement and/or the harvesting of corporate credentials stored in personal assets.

Additionally, the DFS ecosystem is strongly encouraged to deploy software authentication products to protect systems from current and evolving malicious software threats, disable unnecessary device functions and recommend installing only trusted software to users.

DFS applications should be subjected to regular security penetration scans and Penetration Testing activities. In addition, a consistent patching life cycle should be defined to mitigate the risk of malicious intrusions.

Zero-Day Attacks

A zero-day attack is acknowledged as a malicious operation targeting previously unknown vulnerabilities, for which security specialists had "zero days" to operate. Zero-day exposures are widely considered one of the most severe and aggressive menaces facing the current cybersecurity threat landscape and traditionally require a high level of technical expertise. Through a zero-day attack, DFS providers, MNOs, or Third Parties face the risk of unauthorised access to and unauthorised modification of confidential user data. Furthermore, DFS actors may be subject to fraud schemes and data alteration. Successful zero-day exploitations may allow threat actors to access confidential servers and modify their data.

When exploiting a zero-day vulnerability, attackers capitalise on undetected flaws to penetrate the system and deploy malicious software, exfiltrating data of interest or maintaining persistence in the targeted network.

Zero-day attacks are hard to detect and challenging to prevent. However, to mitigate the risk, DFS actors must ensure a consistent patching system of all their critical and non-critical software and hardware, designate periodic backups, and define potential contingency plans in case of an incident. In addition, DFS actors are strongly encouraged to have ad-hoc agreements with vendors to quickly acquire patches and system remediation if a zero-day attack is identified.

Mobile Devices Attacks

A DFS Provider faces the risk of fraudulent impersonation, data loss, or deceitful financial transactions through unauthorised access to a mobile device. Furthermore, a targeted mobile user may see their account being takeover and/or their transactions being denied.

Threat actors may decide to exploit multiple vulnerabilities to compromise a mobile device and gain unauthorised access. These include inadequate user authentication on the devices, outdated application software versions making devices susceptible to malware, and overly permissive access to the DFS infrastructure. In addition, a weaker transaction verification process may also facilitate malicious intrusions and help the threat actor achieve their malevolent intents.

DFS users and actors must use strong PINs, set up remote data wipes, arrange a PIN lock, and establish biometric authentication when applicable to prevent this threat and mitigate the risk of a device being compromised. Moreover, before authenticating DFS users, DFS entities are advised to validate the device's IMSI location and IP address to prevent unauthorised access to the network infrastructure.

Personal Information Attacks

Finally, the last identified DFS-centred threat is the unintended disclosure of personal information. In this scenario, a threat actor, or a staff member, may accidentally expose the client's Personally Identifiable Information (PII) and /or sensitive data. This could be caused by erroneous API use, insufficient data protection controls, and inadequate oversight and controls in test environments. However, notwithstanding the motive behind the leak, unintended information disclosure would have the same result as a traditional attack: data loss, reputational damage, and loss of trust in present and future clients.

DFS actors must ensure that customer data is not used in test environments unless anonymised according to best practices to mitigate the risk of unintended PII disclosure. Furthermore, they must ensure that customer-sensitive data is removed from trace logs and sensitive environments. Finally, third-party providers must restrict the sharing of information with other parties, including payment service providers and DFS providers, to the minimum required to assure the integrity of the transaction.

3.3 Main Considerations on Mapping the DFS Infrastructure

Mapping the DFS actors and most relevant attacks serves a twofold purpose. First, it provides the needed understanding for the reader to comprehend the stakeholders and related cyber-enabled threats in any DFS cyber environment. The nature of the architecture of such ecosystems may change depending on the digital maturity of a country. In a more advanced economy, the DFS ecosystem is likely to be more structured and may comprise a higher number of actors than in emerging markets. Nonetheless, this report defines the minimum required actors in any DFS transaction (i.e., a user, a mobile network architecture, and a financial institution or entity) and lists some of the most common security risks in emerging economies' DFS infrastructures.

Second, this section aims to standardise a cyber taxonomy (See Preliminary Elements, Taxonomy and Terminology), which is key to increasing cyber resilience and collaboration. As explicated in an IMF report published in 2021[77], the current fragmentation among DFS stakeholders and initiatives is one of the reasons behind the volatile DFS security environment and the difficulties in deterring malicious activities. A shared understanding of the ecosystem and current threats will facilitate knowledge transfer, the definition of information-sharing techniques to strengthen the DFS ecosystem's cyber resilience, and the conceptual understanding of the methodological framework presented in the next section of this report (Section 4.0, Establishing a Methodology).

The methodology presented in the next section will include methods to evaluate the cyber resilience level of the DFS actors and overall infrastructure. By understanding the degree of cyber resilience and their preparedness, the methodology will facilitate threat identification, Containment, and Eradication to conduct a holistic cyber resilience-centred self-assessment and prioritise potential gaps to bridge.

Maurer, T. et al. (2021). *The Global Cyber Threat*. The International Monetary Fund. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

4 Establishing a Methodology

Following the mapping of the DFS ecosystem, this report presents a comprehensive and holistic methodology that created the theoretical foundation to define the Cyber Resilience Toolkit. The methodology focuses on characteristics specific to developing areas (e.g., the diversity of infrastructure and cybersecurity maturity across DFSs in different countries) to ensure its applicability across all emerging economies.

Therefore, as a first methodological step, organisations must identify the scope of the evaluation – including the infrastructure, systems, and assets – and the relevant stakeholders to engage when assessing cyber resilience (Section 2.2, Critical Entity Information Matrix). More specifically, correctly identifying external stakeholders is critical in mapping potential dependencies on third-party systems, which could expose the entity and the overall architecture to misuse and compromise. These external stakeholders are here acknowledged as DFS actors external to the leading company, such as cloud infrastructure or digital supply chains. Given their role in the DFS infrastructure and the close relationship with the leading DFS actors, they can represent an additional access point for malicious intrusions and, if not secured and monitored, they can represent a way to access hackers' ultimate victims laterally. Further information on risks related to third-parties can be found in a later section (Section 4.1.4, Third Parties Risk Management).

Provided that the identification of the stakeholders and infrastructure is completed, the methodology considers whether the entity is considered critical or non-critical. For this evaluation to be fulfilled, this document provides a matrix that cross-references the entity's ownership and the estimated impact of a cybersecurity attack on the broader population (Section 2.3, Structure of the Cyber Resilience Assessment Toolkit). Based on these conditions, the methodology and toolkit qualify questions targeting telco entities and financial institutions. These questions address technical aspects of the infrastructure and may therefore require the direct input of the entity's management board. This is critical as regulators may not be able to autonomously answer technical questions, given that, in specific environments, they do not directly own the critical infrastructure. Finally, this report pays particular attention to the close network of interconnections among individual actors and the trickle-down effect of a cyberattack on the entire system.

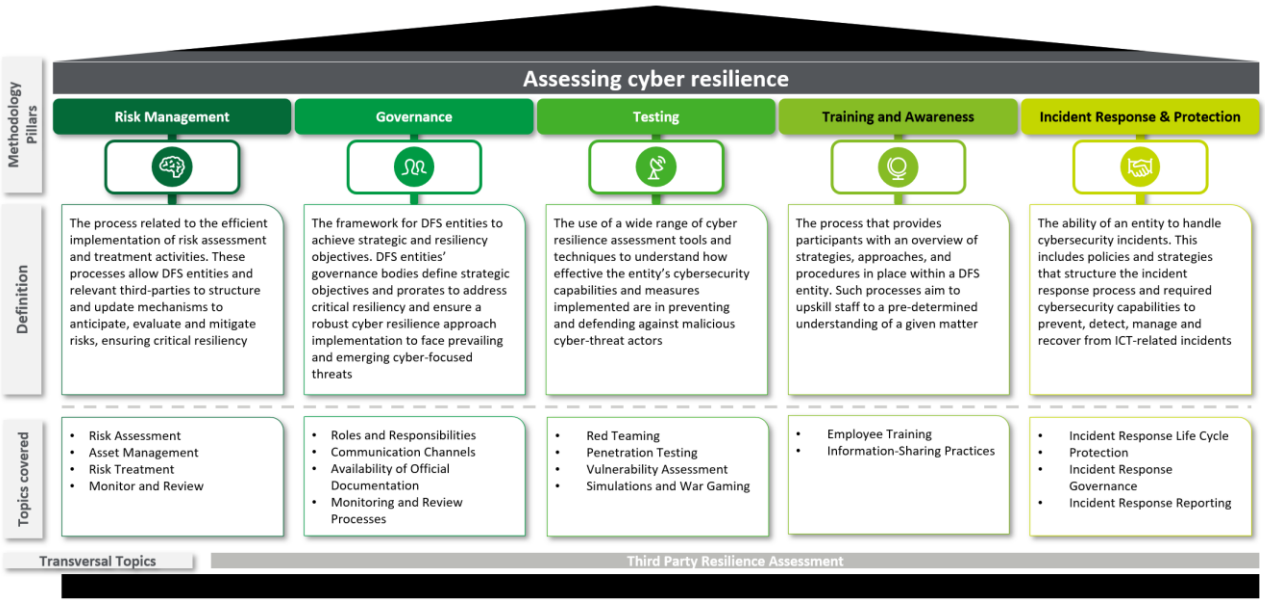

Figure 4: Methodology's pillars

Through an analysis of internationally-recognised cybersecurity standards and national best practices (i.e., NIST standards, DORA, TIBER-EU, ISO/IEC 27000-series), this report identifies five pillars that need to be investigated to assess cyber resilience:

1. Risk Management (Section 4.1, Risk Management - A process related to the correct and functioning implementation of risk treatment and assessment procedures).
2. Governance (Section 4.2, Governance - The principles and most important aspects needed to deliver key objectives and strengthen DFS entities and regulators' cyber resiliency posture).
3. Testing (Section 4.3, Testing - A set of activities dedicated to the testing of processes, systems, and procedures relating to the entity's and country's physical and non-physical infrastructure).
4. Training and Awareness (Section 4.4, Training and Awareness - Processes related to activities and campaigns for employees and stakeholders, aimed to increase their knowledge of cybersecurity operations and overview of implanted cyber resilience strategies, objectives, and procedures).
5. Incident Response (Section 4.5, Incident Response - Processes subsequent to the identification of a malicious/unplanned event and aimed at the prompt return to a business-as-usual status. Following international standards and frameworks, such as NIST, the Incident Response Pillar will include multiple domains, including Protection. The latter provides guidelines for securing the entity's data, systems, networks, and applications)

Therefore, DFS regulators and entities in EMDEs must develop and/or enhance the capabilities of each of the abovementioned areas to strengthen their cyber resilience.

These cybersecurity standards and national best practices were selected based on their relevance to DFS ecosystems in emerging economies and their alignment with previously-published ITU documentation and guidelines. More specifically, the main inspiration for this methodology was taken from the ISO/IEC 27000-series, European Union (EU) regulations (such as DORA[78] and TIBER EU[79]), applicable NIST Standards, PCI DSS[80], PA DSS[81] and reports on financial inclusion[82], such as the World bank's report "*Payment aspects of financial inclusion*". Indeed, the ISO/IEC 27000-series[83] confirms itself to be the core documentation to establish controls and thresholds for cybersecurity while ensuring wide applicability of its guidelines to critical infrastructure and DFS regulators/entities. The adaptability of the ISO series to a wide variety of situations and contexts is consistent with the primary objective of this report's methodology: to make sure that the Toolkit applies to the widest audience of DFS actors and ecosystems. Along these lines, the EU's DORA and TIBER were selected as they represent a cutting-edge effort to regulate and secure the DFS local and continental ecosystems in a region experiencing increased cybersecurity volatility. Similarly, NIST standards[84] were incorporated in the analysis to account for their technically-enhanced security

[78] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554
[79] European Central Bank. (2018). *Tiber-EU Framework*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
[80] PCI Security Standards Council (2022). *Data Security Standard.* https://www.pcisecuritystandards.org/document_library/
[81] PCI Security Standards Council (2013). *Payment Application Data Security Standard*. https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf
[82] Committee on Payments and Market Infrastructures and World Bank Group. (2016). *Payment aspects of financial inclusion.* Bank for International Settlements and World Bank Group. https://www.bis.org/cpmi/publ/d144.pdf
[83] International Organization for Standardization. (2022). *Information security, cybersecurity, and privacy protection — Information security management systems* — Requirements. ISO/IEC Standard No. 27001:2022. https://www.iso.org/standard/82875.html
[84] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (v.1.1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
For a complete list of NIST standards, please refer to the References section

controls and their prominent focus on critical national infrastructures. Finally, to ensure a deeper assessment of DFS cyber resilience and to account for a trusted environment for financial inclusion in emerging economies, security controls were also developed based on protection standards and guidelines, namely PCI DSS, PA DSS, and industry reports on financial inclusion.

The results of this analysis will facilitate the identification of gaps, reviewing results against best practices. Once the gaps are identified, and vulnerabilities are observed, regulators and entities managing the CNI must cooperate in developing and implementing a cyber resilience remediation plan. This final step is fundamental to ensure that peripheral defences are strengthened, and defence-in-depth mechanisms are enforced. The methodology proposed in this report serves as a steppingstone for a hands-on toolkit to support the cyber resilience assessment. This toolkit will be based on a question library that will target DFS actors, including but not limited to the financial sector, the tech sector, and end users.

Cybersecurity and cyber resilience best practices derived from regional and international organisations create the preliminary methodological framework needed to assess the current resilience status and define the measures to mitigate cyberattack risks. Incorporating such practices is the first step to define the tailored DFS toolkit and identify the consequent levels needed for DFS entities or regulators to strengthen their resilience. Of such sources, this report acknowledges the following to provide critical conceptual insights into the proposed cyber resilience assessment process:

- The International Organisation for Standardization (ISO) 27005 standard provides a structured approach and security controls on risk management practices, which is at the core of this methodology.
- The Threat Intelligence-based Ethical Red Teaming (TIBER)-European Union (EU) framework provides best practices for security testing specifically addressed to financial entities. This framework was developed in consultation with the industry, thus providing an added-value to its principles.
- The EU's Digital Operational Resilience Act (DORA) provides enhanced directions on cybersecurity requirements and mandates information security measures specific to financial entities. The broad applicability of this legislation ensures that mechanisms put forward are implementable by different countries, hence resulting valuable to the scope presented in this report.
- The G7 documentation provides cybersecurity best practices developed and agreed upon by states exploring all the pillars' themes.

The sections below will outline the main elements of each Pillar included in this methodology. Since third-party discussions are considered transversal to all pillars, each section will include a specific section on third-party implications.

4.1 Risk Management

This report refers to pillar 1, Risk Management (RM), as the process related to the efficient implementation of risk assessment and treatment activities. These processes will allow DFS entities and concerned relevant third-parties to structure and update mechanisms to anticipate, evaluate and mitigate risks, ensuring critical resiliency. In this section, the report will analyse the different phases of a Risk Management cycle, which include risk assessment (1), risk treatment (2), and monitoring and review (3). Given the interconnected nature of the DFS ecosystem and the consequent intertwined shape of a Risk Management process applied to any digital financial architecture, this report will conclude the RM section with an overview of risks related to third-parties. The section will highlight the importance of monitoring third-party agreements, and data flows as they represent potential threat sources. A growing number of threat actors capitalise on external partners to compromise a CNI infrastructure and move laterally within the DFS sector.

4.1.1 Risk Assessment

This report defines risk assessment as identifying, estimating, and prioritising risks related to multiple diverse actors and processes. These include but are not limited to organisational operations, individuals, assets, and external institutions, which are interconnected due to the operational necessities of an information system[85]. A robust risk assessment will enable DFS entities to comprehend their risk profile and efficiently deploy risk management strategies and resources. The risk assessment process encompasses asset management, risk identification, risk analysis, and risk evaluation.

Asset Management

The asset management process represents a preliminary step not only to perform a precise and relevant risk assessment but also to facilitate the conduction of all the other functions (i.e., governance, testing, Training and Awareness, and incident response) necessary to achieve cyber resilience. Asset management refers to identifying, managing, and monitoring critical and non-critical assets within an entity, including essential functions of operating and services, system, and network infrastructure (e.g., hardware, software), end-users, and employees.

DFS entities should identify any critical assets vital for the entity's proper functioning and the delivery of its services. Furthermore, to ensure a comprehensive asset management procedure, entities should also identify assets representing a potential target that, if compromised, could significantly disrupt its operations. Entities should further ensure that they include any critical asset partly or fully managed by external interconnections (e.g., third-party providers)[86].

Once all critical assets are identified, they should be closely monitored and managed. This encompasses a constant prioritisation process to ensure that strong cybersecurity measures protect the most valuable and sensitive assets. Entities should also record the addition of new assets and any changes in their configurations and values compared to the asset's baseline reports. The conduction and continuous update of an asset inventory and prioritisation process informs the risk identification, analysis, evaluation, and treatment. Additionally, it will facilitate the proper implementation of adequate security mechanisms to prevent and respond to ICT-related incidents.

Risk Identification

The risk identification process's elements are finding, recognising, and characterising risks[87]. Identifying risks is a fundamental feature of an effective risk management process and contributes directly to enhancing the cyber resilience capabilities of an entity. Its goal is to detect a potential cybersecurity incident's causes, place, and time[88]. To ensure a broad understanding of risk identification, the input data should include identifying assets, threats, existing controls, and vulnerabilities while considering internal and external factors to the entity. In this context, risk outside the entity's control should also be included in the identification process[89] to mitigate the possibility of unexpected incidents.

Risk Analysis

---

[85] Grassi, P. et al. (2017). *Digital Identity Guidelines (SP 800-63-3).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[86] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[87] Ross, R. et al. (2022). *Engineering Trustworthy Secure Systems (SP 800-160 Vol.1 Rev.1).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

[88] International Organisation for Standardization. (2011). *Information technology – Security techniques – Information security risk management. ISO/IEC Standard No. 27005:2011*. §8.2

[89] International Organisation for Standardization. (2011). *Information technology – Security techniques – Information security risk management. ISO/IEC Standard No. 27005:2011*. §8.2

Once a risk is identified, the DFS entity must analyse it to gather additional information. This data-harvesting process will facilitate the needed risk categorisation process, which will be based on the estimated impact and likelihood of the assessed incident. This method is leveraged by appointed individuals in the company who require comprehensive and appropriate methodological tools.[90] Although approaches for risk analysis may vary significantly depending on sectors, entities, and risk themselves, methodologies are typically one of the two: a qualitative or quantitative analysis.

The qualitative analysis consists in evaluating risks based on their inherent attributes. Although the level of accuracy may be reduced compared to quantitative studies, it is a methodology needed to perform first-risk assessments and analyse unquantifiable data. This methodology entails defining a set of risk levels (such as low, medium, and high) referring to the expected impact and likelihood of risk occurrence[91]. This evaluation will enable specialists to prioritise risks and distribute them on a scale based on assigned attributes[92].

Quantitative analysis, instead, consists in assigning numerical values to risks' estimated impacts and the likelihood of occurrence. This methodology facilitates a more thorough analysis of risks compared to the quantitative analysis methodology, although it requires more effort to assess the risks and the related information. Still, international guidelines warn against a frequent and excessive utilisation of quantitative analysis, as it may give a false perception of high accuracy during risk assessment in case the initial evaluation and information gathered were insufficient to elaborate required measurements[93]. This significant shortfall may lead to inaccurate quantitative evaluations, depicting a fallacious image of the analysed risk.

Qualitative and quantitative assessments both provide robust approaches for risk analysis. However, these must be leveraged consistently within a DFS entity's scheme toward risk management and chosen appropriately depending on the nature of the assessed risk.

Whether an entity decides to perform qualitative or quantitative assessments to analyse risks, Business Impact Analysis (BIA) is a particularly useful method to assess cybersecurity incidents' consequences. The BIA is the process which analyses an entity's operational functions and the potential effects that a disruption may have on them[94]. One key parameter for a structured BIA is the asset valuation, which aims at classifying entity's assets according to their criticality in fulfilling business objectives[95]. This should be coupled with the definition of the entity's Recovery Point Objective (RPO) and of the Recovery Time Objective (RTO). The former calculates the point in time to which data must be recovered following a cybersecurity incident or outage[96]. On the other hand, the RTO indicates the duration of time the entity's systems and networks can take to recover before negatively impacting the entity and its business objectives[97]. For example, the Bank for International

[90] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 21.1. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554
[91] International Organisation for Standardization. (2011). *Information technology – Security techniques – Information security risk management. ISO/IEC Standard No. 27005:2011*. §8.3.1
[92] International Organisation for Standardization. (2011). *Information technology – Security techniques – Information security risk management. ISO/IEC Standard No. 27005:2011*. §8.3.1a
[93] International Organisation for Standardization. (2011). *Information technology – Security techniques – Information security risk management. ISO/IEC Standard No. 27005:2011*. §8.3.1b
[94] NIST. (2010). *NIST.SP.800-34 Rev.1. Contingency Planning Guide for Federal Information Systems*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
[95] International Organisation for Standardization. (2011). *Information technology – Security techniques – Information security risk management. ISO/IEC Standard No. 27005:2011*. §8.3.2
[96] NIST. (2010). *NIST.SP.800-34 Rev.1. Contingency Planning Guide for Federal Information Systems*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
[97] NIST. (2010). *NIST.SP.800-34 Rev.1. Contingency Planning Guide for Federal Information Systems*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Settlements recommends financial entities to set the RTO for the recovery of its systems and processes at two hours[98] to limit data loss and reputational damage.

Risk analysis requires further steps, namely risk evaluation and risk treatment. The two will support the analysis of the information gathered in the risk analysis step and facilitate the definition of mitigation measures to contain, treat, and eradicate the threat.

Risk Evaluation

The risk evaluation step entails comparing risk analysis findings with risk criteria to evaluate whether the risk and its level are acceptable[99]. This process entails the design of the Risk Appetite Framework (RAF)[100]. The RAF defines the overall approach and consideration of both material risks for the DFS entity and reputational risks towards, for instance, investors[101], customers and third-parties[102]. The RAF, defined as the frame of reference for determining the significance of risk, is based on organisational objectives and internal and external context, and is derived from laws, policies, qualitative and quantitative statements[103] or other relevant documents[104]. As detailed information about the entity risks is available at the current stage, the decisions, context definition, and the resulting risk criteria should be revised and updated if necessary.

Risk evaluation decisions depend on the entity's risk tolerance or appetite. For a comprehensive risk evaluation, the DFS entities should take into consideration internal information security properties (e.g., if one asset is deemed not critical by the entity, all risks affecting it may not be prioritised) as well as the significance of the business process or operation supported by a single or set of assets[105].

The risk evaluation phase entails defining a prioritised list of risks based on risk evaluation criteria in relation to the threat scenarios considered. The results of this valuation enable decision-making on future actions, comprising the decision on whether an operation should be performed. Finally, a robust risk evaluation process facilitates prioritising risk treatment based on the calculated risk levels[106].

Risk evaluation results should be communicated to the appropriate managers to ensure that the criteria utilised are aligned with business strategies and targets (e.g., by continuously analysing the legal and competition context and the internal risk criteria) and that no risk or risk element is underestimated[107]. This risk communication mechanism ensures compliance with local and international security standards, and bolsters transparency and trust among all relevant stakeholders.

Best Practices

- Establish a vulnerability log (NIST SP 800-53).
- Conduct risk assessments to evaluate the most relevant risks (NIST SP 800-53).

---

[98] Committee On Payments and Market Infrastructures and Board of the International Organization of Security Commissions. (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures*. Bank for International Settlements. https://www.bis.org/cpmi/publ/d146.pdf

[99] Ross, R. et al. (2022). *Engineering Trustworthy Secure Systems (SP 800-160 Vol.1 Rev.1)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

[100] Financial Stability Board (2013). *Principles for an Effective Risk Appetite Framework*. https://www.fsb.org/wp-content/uploads/r_131118.pdf

[101] Committee on Payments and Market Infrastructures and World Bank Group. (2016). Payment aspects of financial inclusion. Bank for International Settlements and World Bank Group. § 3.1.2.3 https://www.bis.org/cpmi/publ/d144.pdf

[102] Committee on Payments and Market Infrastructures and World Bank Group. (2016). Payment aspects of financial inclusion. Bank for International Settlements and World Bank Group. § 1.4.6 https://www.bis.org/cpmi/publ/d144.pdf

[103] Financial Stability Board (2013). *Principles for an Effective Risk Appetite Framework*. https://www.fsb.org/wp-content/uploads/r_131118.pdf

[104] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §8.4

[105] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §8.4

[106] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §8.4

[107] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §12.2

- Include all relevant assets in the cybersecurity framework (DORA).
- Define an acceptable level of risk tolerance (DORA).
- Establish or outsource threat analysis capabilities (DORA).
- Establish and continuously update audit logs to monitor activities and mitigate unauthorised intrusions (NIST SP 800-53).
- Prioritise critical assets and conduct resilience tests on them (NIST SP 800-53).
- Comply with industry, local, national, or international regulations related to risk management and data handling (NIST SP 800-53).
- Perform network security audits on telco entities (NIST SP 800-53).
- Regularly perform asset inventories and asset management procedures (NIST SP 800-53).
- Conduct screening and background tests on employees and staff (NIST SP 800-53).
- Establish an asset management process to be frequently updated (NIST SP 800-53).

4.1.2 Risk Treatment

Risk treatment refers to security controls implemented to reduce, retain, avoid, or share the risks identified during the risk assessment. The list of security controls should then be tailored to the definition of a risk treatment plan[108]. International standards on risk management detail four main risk treatment options, namely (a) risk modification; (b) risk retention; (c) risk avoidance; and (d) risk sharing. Entities may decide to implement one risk treatment option or combine multiple ones, depending on their strategic objectives and infrastructure. Generally, the decision to opt for a risk treatment option (or multiple ones) is influenced by the following criteria: (1) the outcome of the risk assessment; (2) the expected costs of mitigation measures' implementation; and (3) the expected benefits of the risk treatment option(s)[109].

An effective risk treatment plan should include selected risk treatments, prioritisation metrics, and planned and expected timeframes for each risk treatment. The prioritisation process of relevant and specific risk treatments is the responsibility of the organisation's leadership. It is generally established through different techniques; the most popular ones are risk ranking, cost-benefit analysis, and identifying existing controls to evaluate their effectiveness vis-à-vis the risks identified[110]. The latter will help assess whether existing controls have become redundant and/or unnecessary to then remove them accordingly.

Following the definition of a risk treatment plan, the entity should identify residual risks, usually through the risk assessment process. Unlike the previous risk assessment stage, this reiteration should specifically account for the defined risk treatment plan and its expected effects[111]. This activity ensures that residual risks meet the entity's risk acceptance criteria. Should this not happen, the entity must repeat the process until risk acceptance criteria match the identified residual risks[112].

The following sub-sections first outline the advantages and risks of each individual risk treatment option, namely risk modification, retention, risk avoidance and sharing. Then, they explore how, following the definition of a risk treatment plan, residual risks fit into the entity's risk appetite.

Risk Modification

[108] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.1
[109] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.1
[110] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.1
[111] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.1
[112] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.1

Risk modification entails managing the risk level by introducing, removing, or altering controls. This ensures that the level of residual risk is assessed as acceptable according to the organisation's risk acceptance criteria[113].

Controls represent an effective way to protect the organisation's infrastructure. In particular, they provide various types of protection, such as "*Correction, Elimination, Prevention, Impact Minimization, Deterrence, Detection, Recovery, Monitoring, and Awareness*"[114].

The organisation should select appropriate and justified controls that meet the requirements set out by the risk assessment outcome and the objectives of the risk treatment process. The controls' selection procedure should account for (a) the entity's established risk appetite; (b) legal, regulatory, and contractual requirements; (c) implementation costs and timeframe; (d) technical, environmental, and cultural implications; and (e) specialised skills needed for definition and implementation of controls[115].

Entities should be aware that controls present various constraints to be considered during the selection and implementation. The organisation's leadership should account for this to ensure that risk modification controls meet the desired performance requirements while providing sufficient corporate security and network protection[116]. Global international standards offer a comprehensive list of the most common control constraints. Some notable examples include (i) technical constraints, such as performance requirements and compatibility issues with devices, networks, and systems in use; (ii) time constraints; (iii) financial constraints; (iv) personnel constraints; (v) ethical constraints; and (vi) legal constraints[117].

Risk Retention

Risk retention entails the decision to retain identified risks without any further action. Such a decision should be based on the outcomes of the risk evaluation and the entity's risk acceptance criteria. Indeed, risk retention is usually employed when the level of risk matches the risk acceptance criteria. In that case, modifying existing controls or implementing new ones is unnecessary; in such a scenario, organisations are likely to retain the risk as it is[118].

Risk Avoidance

Risk avoidance entails identifying the conditions that generate the risk in question and the subsequent avoidance of such activities. This option is usually considered when the risk is considered too high or other risk treatment options are deemed, for instance, too expensive or against ethical/technical constraints and are therefore not matching the company's risk appetite for the benefits they provide. Risk avoidance is performed by quitting existing or planned activities or altering the conditions that affect them[119].

Risk Sharing

[113] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.2
[114] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.2
[115] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.2
[116] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.2
[117] The full list can be found in International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.2
[118] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.3
[119] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.4

Risk sharing entails sharing the risk with one or more external parties, which are usually better prepared to manage said risk. This consideration depends on the outcomes of the risk evaluation process. Risk sharing is traditionally performed through insurance agreements, signed to mitigate the risk's potential consequences.

Entities should know that the risk sharing option can modify or create new risks, as it increases interdependency over external parties. For example, an entity deciding to share its risk with a cybersecurity provider needs to account for potential vulnerabilities deriving from the third-party itself, such as third-party access to the entity's networks. Because of this, following the decision to opt for risk sharing, entities should perform an additional risk treatment to account for new or modified risks[120].

Risk Acceptance and Identification of Residual Risks

Once the entity has selected the risk treatment method(s) and defined a comprehensive risk treatment plan, it should assess residual risks and formally approve it.

Such approval and decision should be formally recorded and may include risk acceptance, avoidance, or sharing[121]. The organisation's leadership completes the formal review and approval of the proposed risk treatment plan and any identified residual risks. This should include a standard recording of any defined conditions associated with the approval.

Certain residual risks may exceed the entity's risk appetite. Consequently, depending on various circumstances, the entity may be forced to accept residual risks exceeding its risk acceptance criteria. In such a scenario, the organisation's leadership should create a justification for any accepted risk that does not meet the pre-established risk parameters[122]. Such justification will allow the entity to suspend the normal risk acceptance criteria and accept exceeding residual risks.

Best Practices

- Establish a plan to counteract power shutdowns and outages (NIST SP 800-53).
- Develop metrics to determine the current level of resiliency and security measures (NIST SP 800-53).
- Set up a CCTV infrastructure on server rooms and smart locks (NIST SP 800-53).
- Set up physical security measures for the DFS entity (NIST SP 800-53).
- Include the mapping of corporate assets in the cybersecurity framework (DORA).
- Develop information asset backup and recovery policies (DORA).
- Establish a cyber risk management framework to include both management of cyber risk and the protection physical infrastructures and components (DORA; PAFI).
- Track software installations on the devices (NIST SP 800-53).
- Implement least-privilege mechanisms (NIST SP 800-53).
- Define CTI preventative and responsive mechanisms (DORA).

4.1.3 Monitor and Review

Cyber events have the unique capacity to replicate and spread across the financial system, and they may extend across industries and beyond geographical boundaries[123]. As a result, threats, vulnerabilities, and their relative likelihood to occur might alter unexpectedly. Detecting these changes requires constant monitoring. In this context, a constantly-updated risk management process

[120] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §9.5
[121] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §10
[122] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §10
[123] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 79. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

can create a more secure and profitable organisational ecosystem. This also includes continuously monitoring the entity's threat landscape and related risk factors to appropriately review the aforementioned processes and facilitate risk identification and prompt treatment[124].

Risks and associated features (e.g., impact, likelihood) should be monitored to detect early changes in the organisation's environment and maintain a complete understanding of endogenous and exogenous risk factors. This can also be supported by external intelligence-gathering services that provide information about new threats or vulnerabilities. In addition, the results of risk monitoring operations may be used to inform additional risk-review actions. Therefore, all risks should be reviewed regularly, including when significant changes occur. Furthermore, risk management must constantly align with the organisation's business goals and risk appetite[125].

DFS entities are strongly encouraged also to ensure the establishment of robust monitoring and review mechanisms of the risk management process and procedures. This guarantees that the outcomes of the risk assessment and risk treatment activities, as well as the risk management strategies, stay relevant, updated, and suitable to current cybersecurity dynamics[126].

Best Practices

- Periodically review and update inventories in case of IT or network infrastructure changes (DORA).
- Implement measures to capture and analyse anomalous behaviour (DORA; BIS Cyber resilience for FMIs).
- Periodically review risk management process to account for developments in the threat landscape and organisational changes (NIST SP 800-53).
- Comply with applicable regulatory requirements on frequency of periodic reviews (DORA).
- Comply with applicable regulatory requirements on content of periodic reviews (DORA).

4.1.4 Third-Parties' Risk Management

Despite robust internal risk management processes, risks may reside in the external organisations that the DFS entity is dependent on, or to which it has significant logical or physical connections.

Therefore, to ensure that the risk management processes are efficiently and comprehensively performed, the analysis should take into consideration all DFS entity's activities' inherent risks. This entails analysing internal operations and including critical relationships with third-parties in the risk evaluation procedure[127].

Internationally-recognised best practices, such as standards issued by the Basel Committee on banking supervision[128], highlight the necessity for intended entities to manage their dependencies. This includes the relationship with third-parties for the delivery of critical operations[129]. Accordingly, DFS entities must identify and address critical ICT and non-ICT-related partnerships with external suppliers; such collaborations are categorised based on the relevance of the relationship, the nature

[124] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §12.1
[125] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §12.1
[126] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §12.2
[127] International Organisation for Standardization. (2011). Information technology – Security techniques – Information security risk management. *ISO/IEC Standard No. 27005:2011*. §7.2.3
[128] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf
[129] Basel Committee on Banking Supervision. (2005). *The Joint Forum. Outsourcing in Financial Services.* Bank for International Settlements. https://www.bis.org/publ/joint12.pdf

of externalised activities[130], and the prioritisation of suppliers and third-parties within the supply chain[131].

Entities should assess risks and vulnerabilities inherent to critical third-parties and ICT suppliers. For this reason, before entering the relationship, organisations must conduct targeted due diligence activities to review existing third-party risk management approaches[132] and mitigate the risk of cyber incidents. When conducting background checks, organisations are advised to consider supported business operations, level of access, connection methods, and the sensibility/criticality of data managed by third-party.

DFS entities must perform a risk assessment and due diligence to ensure supplier and third-party risk management policies and operational resilience approaches are consistent with the DFS intended levels[133]. This risk management review must be carried out by DFS entities on third parties priorly to establishing the relationship and for the lifespan of their agreement with external entities. By doing so, organisations would ensure that the third party's risk approach is consistent with the DFS entity's control environment[134].

The results of this analysis lead to the development of appropriate business continuity plans and more comprehensive incident response schemes, including events such as failure or disruption at a critical third-party operation, the assessment of substitutability, and alternatives to outsourcing services to external operators[135].

In these regards, DFS entities are recommended to adopt exit strategies if contemplating and/or already experiencing external outsourcing arrangements. Exit strategies are mitigation measures against the unexpected termination of services, may that be the consequence of a cyberattack or not. For example, exit strategies in the context of a Cloud Service Provider (CSP) may take into account potential service disruptions caused by hardware failure, termination of outsourcing arrangements, or deterioration of the functions' quality[136]. Regardless of the reasons behind the service disruption, such occurrences may cause severe reputational, financial, or operational damage to the company. Exit strategies limit these risks and those associated with unexpected service terminations; they should, therefore, be constantly monitored and tested. Their costs vary and depend highly on the entity's risk appetite.

Best Practices

- Establish business continuity plans considering third-party interdependencies (NIST SP 800-53; PAFI).
- Plan cross-checks with external vendors and suppliers to identify and mitigate potential entry points (NIST SP 800-53; PAFI).

---

[130] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 26.5. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[131] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §IDSC-2. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[132] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[133] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[134] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[135] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[136] European Banking Federation, *Cloud exit strategy – testing of exit plans*, EBF https://www.ebf.eu/wp-content/uploads/2020/09/Cloud-exit-strategy-Testing-of-exit-plans.pdf

- Establish communication channels with stakeholders on the impact of security events (NIST SP 800-53).
- Perform due diligence background checks on external third-party services (DORA).
- Establish and implement an ICT Third-Party Risk Management framework (DORA).
- Implement mechanisms to withstand and account for network outages caused by Internet Service Providers (DORA; PAFI).

4.2 Governance

This report defines the second pillar, Governance, as the framework for Digital Financial Services (DFS) entities to achieve strategic and resiliency objectives[137]. Its role and relevance can hardly be underestimated, as it is critical to ensure a robust cyber resilience approach implementation to face prevailing and emerging cyber-focused threats[138]. Indeed, DFS entities' governance bodies define strategic objectives and priorities to address critical resiliency. Within this section, this report will examine in more detail the duties assigned to these critical bodies and the interconnections that define a governance-centred policy in the digital financial ecosystems.

More specifically, a resilient internal governance structure refers to the definition of (1) roles and responsibilities, (2) the establishment of effective communication channels between responsible bodies and stakeholders, (3) the existence and availability of relevant documentation to inform interested parties, and (4) the correct implementation and review of internal processes. Moreover, (5) third-parties may also play a fundamental role depending on the extent and nature of their activities.

4.2.1 Roles and Responsibilities

To establish its resiliency objectives and approach, DFS entities' management should define their appointed bodies and officials responsible for implementing the entity's policy.

A Roles and Responsibilities (R&R) structure describes the network of relations within a given entity. For example, a financial institution's internal R&R architecture sees the interconnections and interactions among IT, financial, and telecommunication actors. In such a structure, the actors aim to support the successful completion of a DFS operation, protect its integrity, and timely respond to an incident or disruption of operation[139]. More specifically, this report presents R&R structures as a critical part of a DFS ecosystem's governance process. This mechanism provides the foundation to ensure efficient DFS operations, clarify duties within the entity, and anticipate potential threats to the ecosystem.

The R&R domain identifies the relevant bodies and officers responsible for specific functions within the DFS entity, providing a high-level overview of the entity's governance approach toward operations, communication, and internal coordination[140]. Top management must ensure that responsibilities and authorities communicate with the relevant internal and external stakeholders. This

[137] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[138] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures.* International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[139] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[140] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5C. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

entails the distribution of responsibilities and the identification of the entity's hierarchic architecture[141].

A structured chain of command ensures the most efficient and reliable assignment of executive decision functions within the entities, supporting their "*overall operational resilience approach*"[142] and their response to ICT incidents. Indeed, DFS entity management is to be considered responsible for effectively communicating resilience objectives, framework, and governance arrangements to third-parties and relevant stakeholders[143].

Best Practices

- Develop and implement a clear internal structure for cyber defence to ensure accountability and chain of command (NIST SP 800-53).
- Identify and assign roles and responsibilities for cyber defence, including IT/OT, crisis management (NIST SP 800-53; DORA).
- Ensure leadership's involvement, accountability and awareness for cybersecurity policies and cybersecurity incident impact evaluation (DORA; BIS Cyber resilience for FMIs).
- Determine the role of the entity and its criticality to the stability of the DFS environment (NIST 800-53).
- Once the chain of command and internal hierarchical structure is identified, communicate it with all relevant internal and external stakeholders to ensure transparency.

4.2.2 Communication Channels

R&R structure provides a clear overview of appointed officers and bodies within a DFS entity. In a traditional DFS architecture, the actors must communicate through dedicated channels, which is crucial in information-sharing, and facilitate internal and external coordination. Identifying such communication channels allows DFS entities to strengthen the information flow and ensure efficient internal and external reporting. In turn, these enable entities to be duly informed on ongoing activities and operations and promptly identify a service disruption/incident, activating a smooth and effective response.

A timely and accurate communication process is necessary for entities to efficiently anticipate, manage and recover from operational disruptions. The entity's leadership should plan communication by priorly identifying content, timing, recipients, and forms of communication[144]. In particular, the management should ensure that appropriate reporting systems are established at all the relevant organisation levels, from the board of directors to business unit levels[145]. This entails transparency within the organisation and effective communication with all relevant stakeholders. Failing to do so would harm the entity's cyber resilience and potentially weaken its defensive cyber-oriented processes.

Moreover, since DFS entities mainly rely on trust as a core part of their business, appointed bodies and officers must establish functioning communication channels and ensure their messages are disseminated efficiently and effectively. This process significantly supports the entity's resilience

---

[141] International Organisation for Standardization. (2022). Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. *ISO/IEC Standard No. 27001:2022*. §5.3 https://www.iso.org/standard/82875.html

[142] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[143] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1.* Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[144]International Organisation for Standardization. (2022). Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. *ISO/IEC Standard No. 27001:2022*. §7.4 https://www.iso.org/standard/82875.html

[145] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

objectives and facilitates cyber awareness for officers, employees, customers, supervisors, and the general public[146].

Best Practices

- Define and implement a process for data in transit and ingoing and outgoing communication (NIST SP 800-53).
- Monitor communication channels and consistently check for potential MITM attacks (NIST SP 800-53).
- Establish and implement a Security Operation Centre (SOC) (NIST SP 800-53).
- Define, implement, and communicate designated communication channels for internal use in case of detection of anomalies (NIST SP 800-53; DORA).
- Define, implement, and communicate designated communication channels for partners, external stakeholders, suppliers, and end-users (NIST SP 800-53; DORA).

4.2.3 Availability of Official Documentation

Tightly bound to the need for effective communication, this report identifies the need to ensure that DFS entities can deliver key documentation. Due to the nature of the DFS operations and its interconnections with external actors and third-parties, DFS entities must maintain high availability of specific documentation. This is a pre-requisite to ensure that DFS organisations can translate mandatory requirements, legal obligations, and international best practices into standardised internal documentation.

International guidelines (e.g., ISO series) already highlight the importance of formalising entities' internal documented information. These documents concern a wide range of critical data, such as information security policies[147], business continuity plans[148], and Information and Communication Technologies (ICT) policies[149].

These documents must be formalised and reviewed cyclically to ensure that measures and information within them remain updated[150]. This entails ensuring, establishing, and providing availability to these documents and their correct and effective distribution, access, usage, and storage[151].

DFS organisations may be required to define and provide available relevant documentation depending on national requirements and other legal obligations. In addition, notwithstanding prior legal and mandatory obligations, while reinforcing cyber resilience, DFS entities may voluntarily adhere to international shared best practices or standardised guidelines that require further obligations concerning documentation formalisation and availability.

Best Practices

- Define and implement a cybersecurity policy (NIST SP 800-53).

---

[146] G7 Cyber Expert Group. (2022). *G-7 Fundamental Elements of Ransomware Resilience For The Financial Sector.* United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134062/2022-10-13-g7-fundamental-elements-ransomware-data.pdf

[147] International Organisation for Standardization. (2022). Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. *ISO/IEC Standard No. 27001:2022*. §5.2 https://www.iso.org/standard/82875.html

[148] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[149] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[150] International Organisation for Standardization. (2022). Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. *ISO/IEC Standard No. 27001:2022*. §7.5.3 https://www.iso.org/standard/82875.html

[151] International Organisation for Standardization. (2022). Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. *ISO/IEC Standard No. 27001:2022*. §7.5.3 https://www.iso.org/standard/82875.html

- Designate a system development life cycle for software and hardware (NIST SP 800-53).
- Establish and implement mechanisms to record activities pertinent to the activation of emergency plans (e.g., business continuity plans, disaster recovery plans, incident response plans) (DORA; PAFI).
- Define and implement a cyber resilience strategy and framework (BIS Cyber resilience for FMIs).
- Establish and implement mechanisms to gather and record evidence pertinent to security events (e.g., business continuity plans, disaster recovery plans, incident response plans) (ISO 27001).
- Define, implement, and communicate cybersecurity operating procedures to internal personnel and relevant external stakeholders (ISO 27001).

4.2.4 Monitoring and Review Processes

The constant enhancement of defensive and cyber resilience-oriented governance will allow DFS entities to be better prepared to face the cyber-threat landscape.

Once the overall governance approach (including R&R, communication channels, and the high availability of documented information) has been designed and established, DFS entities should make sure it is constantly improved[152], allowing cyber resilience to be strengthened over time. This entails, for instance, verifying that the DFS entity is equipped with a governance mechanism to assess adjustments[153] in the entity's risk appetite and tolerance for service disruption[154]. Following cyclical assessments, the management should approve, oversee, and periodically review[155] the defined internal resilience approach, strategy, and critical documentation. This includes ICT policies, business continuity schemes, and recovery plans to bring corporate resiliency up to speed with fluctuating cyber-oriented threats and risks.

Best Practices

- Ensure compliance with local, national, and international regulations and norms (NIST SP 800-53).
- Assign and examine budget constraints impacting cybersecurity activities (DORA).
- Monitor technological developments and studies on ICT security (DORA).
- Implement mandated digital operational resilience requirements, if available (DORA).
- Define and implement process to identify and mitigate potential single points of failures (NIST SP 800-53).
- Define, implement, and review metrics to measure effectiveness of cyber resilience program (DORA).
- Ensure alignment of cybersecurity policies to national and international best practices (BIS Cyber resilience for FMIs).

[152] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures.* International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[153] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5.1. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[154] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[155] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

4.2.5 Third-Parties' Governance

While performing operations, DFS organisations often rely on external entities, whether for services or product provision for the final users. Therefore, when defining DFS governance, entities should consider internal functions and relationships with key external stakeholders, partners, providers, and suppliers.

While structuring and continuously improving DFS entities, management should develop a comprehensive internal third-party resiliency policy aligned to the entity's tailored commitments[156]. This involves a comprehensive analysis of roles and responsibilities, together with the appropriate internal and external communication channels, also with third-parties and relevant authorities[157]. In addition, a DFS entity should accurately document cross-entities governance resiliency processes and modifications and ensure that the appropriate documentation is stored, protected, and available to relevant stakeholders and third-parties for cyclical review.

To achieve this, organisations are recommended to regularly perform an inventory and risk assessment of third-party service providers, ensuring that critical activities and external entities-initiated operations are performed within the perimeter of the DFS entity resilience policy. This activity shall be performed via third-party self-assessment, DFS entity assessment of third-party resiliency approach, or external audit, such as certification of adherence to internationally-recognised standards[158].

In conclusion, the Governance pillar demonstrates the importance of providing DFS entities' management with the appropriate instruments and tools to structure the entity's resilience. These structures must be continuously assessed to ensure that measures undertaken are sufficient to achieve a resiliency level dictated by the entity. This entails performing regular testing activities on the established standards and tools within the DFS entity.

Best Practices

- Define a point of contact for suppliers and partners in case of emergency (NIST 800-53).
- Mandate minimum cybersecurity requirements for partners and suppliers (NIST SP 800-53).
- Define and implement security collaboration programs on response and recovery with suppliers and partners (NIST SP 800-53).
- Establish communication channels with relevant third-parties (DORA).
- Establish contractual agreements with third-parties to minimise impact of third-party interdependencies (DORA).

[156] G7 Cyber Expert Group. (2022). G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector. *United Kingdom (UK) Government.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[157] G7 Cyber Expert Group. (2022). G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector. *United Kingdom (UK) Government.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[158] G7 Cyber Expert Group. (2022). G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector. *United Kingdom (UK) Government.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

4.3 Testing

Pillar 3, Testing, encompasses assessing an organisation's cybersecurity capabilities and measures implemented to understand how effective they are in preventing and defending against malicious cyber-threat actors. The complex and diversified nature of the DFS ecosystem includes financial and telecommunication entities, requiring all participants to use a wide range of cyber resilience assessment tools and techniques to test their cyber resilience; these are customarily deployed to verify the efficacy of internal procedures and analyse defensive cyber capabilities[159].

Whether taken internally or by an independent party, testing practices should implement a risk-based approach to include, among others, risks deriving from the ICT landscape, the specificities of the entity, and the criticality of information assets and services provided[160]. Organisations can identify strengths, weaknesses, and gaps in their defensive posture by periodically comparing expected behaviour with those assessed to better handle cybersecurity incidents[161]. This process will identify, prioritise, and classify issues, allowing the entity to establish remediation policies and procedures to strengthen cybersecurity mechanisms, plans, and capabilities[162]. Testing is also beneficial to properly implementing pillar 4, Training and Awareness. More specifically, organisations can capitalise on the findings of testing mechanisms to hone the delivery of exercises to enhance the awareness and preparedness of internal staff, end-users, and external stakeholders[163].

As briefly mentioned, numerous testing methods exist to assess the efficacy and efficiency of an organisation's cyber resilience capabilities. Some of the most-used ones include (1) Red Teaming; (2) Penetration Testing; (3) Vulnerability Scanning; and (4) Simulations and War Gaming. In addition, all entities need to account for vulnerabilities and risks deriving from (5) Third-Party dependencies and identify a remediation plan that encompasses connections with all external providers.

4.3.1 Red Teaming

Red Teaming (RT) is a testing method that mimics the behaviour of real-life threat actors who could represent a genuine threat to the entity. This is achieved with the help of threat intelligence focused on identifying the most likely potential malicious actors targeting the organisation and analysing previous malicious behaviours regarding tactics, techniques, and procedures (TTPs).

During an RT exercise, an internal or external team, designated as the "Red Team", simulates a realistic cyberattack against an entity, whether targeting vital operating functions, critical assets, its employees, or its end-users. Red Teaming exercises are beneficial to assess an organisation's protection, detection, and response capabilities. This is because only a limited number of people within the organisation know the exercise, ensuring that the cyber response team employs its capabilities to the most authentic effort[164].

---

[159] European Central Bank. (2018). *Tiber-EU Framework*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf. See Also G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Threat-LED Penetration Testing*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134064/2018-10-24-g7-fundamental-elements-led-penetration-testing-data.pdf

[160] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Official Journal of the European Union*. Article 24.3. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[161] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 24. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[162] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 24.5. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[163] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[164] European Central Bank. (2018). *Tiber-EU Framework*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

Financial entities are especially encouraged to perform intelligence-led Red Teaming testing as they represent a high-value target for malicious actors. Indeed, as shown in previous sections, its critical assets and systems are perceived as extremely valuable to all malicious actors, increasing the chance of the entity being targeted by common - and highly sophisticated - threats. Financial entities, thus, need to be protected and need to be able to respond to technically advanced, highly-resourced, and persistent malicious cyber campaigns, including Advanced Persistent Threats (APT). Implementing up-to-date, advanced, and targeted intelligence-led Red Teaming exercises can accurately identify vulnerabilities and simultaneously test incident response capabilities[165].

Best Practices

- Define and conduct threat-led Penetration Testing to subjects with highest level of independence (DORA).
- Conduct threat-led Penetration Testing on a regular basis and at least every three years (DORA).
- Conduct threat-led Penetration Testing to vital operating functions and critical assets to test their security measures (TIBER-EU).
- Tailor threat-led Penetration Testing to mimic attacks based on most common threats identified through CTI data-gathering (TIBER-EU).
- Tailor threat-led Penetration Testing to mimic behaviours of most common threat actors identified through CTI data-gathering (TIBER-EU).

4.3.2 Penetration Testing

Similar to Red Teaming, Penetration Testing (or "pentesting") is an exercise where testers simulate real-world cyberattacks to find ways to penetrate the victim organisation's applications, systems, and/or networks[166]. The testing is usually conducted using data and information gathered during threat intelligence activities to ensure it is as similar to potential threats as possible. This is referred to as "threat-led Penetration Testing".

Penetration Testing is widely acknowledged as a crucial preventive measure, providing entities with critical information on their systems' security posture and preparedness against potential malicious actors. Indeed, pentesting indicates the likely level of sophistication of potential threat actors and shows the extent to which the system tolerates real-life attacks. It further reveals possible countermeasures to mitigate the threat and facilitates testing the entity's ability to detect and respond to similar attacks[167]. In addition to this, it is a valuable exercise to identify vulnerabilities in the system and better understand its implications.

The need and frequency of pentesting depend on the entity's threat landscape and risk profile. Regulators can play a guiding role in advising which entities and how often they should perform Penetration Testing exercises. Key criteria include (1) impact-related factors, meaning the importance of the entity on the financial sector's service offering; (2) stability-related factors, meaning the impact a compromise of the entity could have on the stability of the financial sector at the national level; and (3) the specific risk profile and ICT infrastructure of the entity itself. In general, and particularly to achieve the latter, entities must identify their critical ICT systems, processes, and technologies that

[165] European Central Bank. (2018). *Tiber-EU Framework*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

[166] NIST. (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[167] NIST. (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

should be covered during pentesting. This will also allow them to determine the scope of the exercise[168].

Best Practices

- Define and conduct scenario-based Penetration Testing (DORA).
- Use a production environment to conduct scenario-based Penetration Testing (DORA).
- Integrate cyber-threat intelligence during the definition and conduction of Penetration Testing exercises (NIST SP 800-225).
- Incorporate findings of Penetration Testing to assess and update security measures associated to the tested resources (NIST SP 800-115).
- Determine the need and frequency of Penetration Testing on the basis of the organisation's threat landscape and risk profile (DORA).

4.3.3 Vulnerability Scanning

Vulnerability Scanning (VS) is a testing method that examines the exploit points of an entity's devices, systems, and networks. As a result, VS identifies security gaps and potential access points for malicious actors, providing a vital baseline to establish mitigation measures. Indeed, Vulnerability Scanning helps detect outdated or unpatched systems and applications and potentially critical misconfigurations. As was the case for Red Teaming, the results are then checked against expected outcomes derived from compliance with the organisation's or provider's security policies to determine the presence of any criticalities[169].

Vulnerabilities can be identified either in isolation or in aggregation. In the former case, the scan aims at rapidly and easily identifying "surface vulnerabilities", where the exploit point is isolated and independent from other systems' weaknesses. In the latter, the exercise aims to determine how a malicious actor can exploit various vulnerabilities to compromise the target. In these circumstances, Vulnerability Scanning is usually performed in the context of Penetration Testing[170].

According to international best practices, financial entities should conduct vulnerability scans following "any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions of the financial entity". Additionally, the risk level deriving from the scanning should be verified by testers to ensure that each vulnerability is granted the appropriate risk level vis-à-vis the specific characteristics of the entity in question.

Best Practices

- Define and implement a vulnerability management plan (NIST SP 800-53).
- Conduct regular Vulnerability Scanning and vulnerability assessments (NIST SP 800-53; DORA).
- Test and update vulnerability detection processes (NIST SP 800-53).
- Conduct Vulnerability Scanning to identify potential entry points (NIST SP 800-53).
- Conduct Vulnerability Scanning on both DFS critical and non-critical assets (NIST SP 800-53).

[168] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 26. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[169] NIST. (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[170] NIST. (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

4.3.4 Simulations and War Gaming

Simulations and War Gaming test an organisation's preparedness for a cyber crisis. Using various methodological tools, ranging from collective scenario-based Simulations to individual role-playing, these exercises often include different cyber scenarios of disruptive incidents to test out the ability of the organisation to implement emergency plans (e.g., business continuity plans, disaster recovery plans, incident response policies) and the efficacy of established security policies and procedures[171]. Simulations and War Gaming are flexible in nature, allowing organisations to tailor them to specific requirements and include multiple internal and external stakeholders. Collaboration with other functions and external suppliers is recommended to ensure that internal connections and external interdependencies are accounted for (e.g., testing out internal reporting to various business units, such as legal or Public Relations (PR), or testing out external communication plans when notifying an incident to authorities or end-users)[172].

Implementing Simulations and War Gaming exercises provides numerous advantages to a financial entity. Indeed, it (1) allows the organisation to identify critical operations and understand how malicious actors could exploit them; (2) verifies the efficiency of incident response plans, procedures, and capabilities; (3) contributes to the improvement of incident response and recovery processes and capabilities; and if regularly performed (4) shows improvements across time[173].

Simulations and War Gaming are instrumental when organised consistently and regularly. With a staged approach, such exercises can continuously enhance cyber capabilities and facilitate a holistic understanding of the entity's priorities, threats, and risks. In addition, regular Simulations allow financial entities to define improved key risk indicators and identify improvements for the internal incident handling process. For example, as internationally-recognised best practices suggest, establishing a multi-year exercise planning facilitates integrating lessons learned from real and simulated incidents into the exercise program to ensure that scenarios are always up-to-date and accurate[174].

Best Practices

- Implement testing sessions to measure digital resilience and test preparedness and response during an emergency (NIST SP 800-53; DORA; PAFI).
- Develop, document and test cybersecurity policies including (DORA; PAFI):
    - Backup policies.
    - Cyber risk management protocols.
    - Recovery and restoration of ICT systems procedures.
    - Business continuity plans.
- Develop a testing program that includes development of scenarios, frequency of testing, number of business services to be tested, availability of supporting assets, communication plans (DORA).

---

[171] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[172] G7 Cyber Expert Group. (2020). *G-7 Fundamental Elements of Cyber Exercise Programmes*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948042/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf

[173] G7 Cyber Expert Group. (2020). *G-7 Fundamental Elements of Cyber Exercise Programmes*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948042/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf

[174] G7 Cyber Expert Group. (2020). *G-7 Fundamental Elements of Cyber Exercise Programmes*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948042/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf; Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

- Incorporate lessons learned from previous ICT incidents in the testing program to verify mitigation measures implemented (DORA).
- Conduct tests to assess staff's understanding of emergency processes (NIST SP 800-53; PAFI).
- Design and conduct tests to assess and time the recovery of accurate data following an ICT breach (BIS Cyber resilience for FMIs).

4.3.5 Third-Parties' Testing

As briefly mentioned above, testing exercises are fully effective when they account for interdependencies and interconnections with external parties to the entity. This includes relationships with intragroup entities, sister agencies, and third-party providers[175].

When adding third-party providers to the scope of testing, financial entities should first map their ecosystem to identify relevant stakeholders on which they are operationally dependent[176]. Secondly, the entity should indicate any discovered vulnerability external to the organisation[177] to facilitate the identification of any potential entry points for malicious actors. Finally, the approach and granularity level of the mapping exercise should also include external critical functions, which are dependent on the services of the entity in question. For example, a telecommunication provider performing ecosystem scanning should consist of all external critical functions (e.g., banks) to which the telecommunication provider provides services[178].

Testing matters should be discussed in contractual agreements between entities and third-party providers. Specific reference to supporting mechanisms should be integrated regarding cyber risk management deriving from contracting or sub-contracting external companies[179]. In addition to this, the terms and conditions of the agreement should include "scope of the relationship, performance standards, access, information and audit rights for the entity and its relevant authorities, reporting provisions, requirements about frequency and types of cyber resilience tests (e.g., penetration tests, threat-led Penetration Testing)"[180]. A reference should also be made to data location conditions, storage and disposal provisions, and ICT supply chain implications[181].

---

[175] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[176] G7 Cyber Expert Group. (2020). *G-7 Fundamental Elements of Cyber Exercise Programmes*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948042/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf; Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[177] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[178] The European Parliament and Council. (2022) *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 26. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[179] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[180] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[181] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

Following the third-party mapping, financial entities should take appropriate steps to encourage and support the participation of third-party providers in testing exercises[182]. This includes testing any interdependency the two or more organisations share. Indeed, best practices presented in the EU directive Digital Operational Resilience Act (DORA)[183] encourage the organisation of pooled testing, which includes multiple financial entities and the ICT third-party service provider that provides ICT services to all the interested financial entities[184]. All entities in the scope are subject to a pooled threat-led Penetration Testing exercise covering all essential or critical functions contracted to the external provider[185]. This would allow financial entities to identify weaknesses in their interdependencies and simulate a more sophisticated cyberattack targeting the sector as a whole.

In addition to conducting testing exercises with external stakeholders, entities should also ensure that third-parties periodically test out the defensive and cybersecurity measures to ensure that their networks and entities are adequately protected and potential spill over effects generated by an attack are mitigated and accounted for. This is predominantly achieved by incorporating obligations on auditing and cyber risk assessments for the third-party provider[186]. Such practices ensure that entities are aware of potential risks and vulnerabilities derived from the third party or ICT supply chain and are proactive in establishing protective measures. Testing obligations for third-parties should be set and carried out prior to entering the agreement with the external organisation and periodically for the duration of the contract engagement[187].

Best Practices

- Extend the scope of testing activities to critical services of third-party providers (DORA).
- Include all third-party interdependencies during testing activities (DORA).
- Include third-party capabilities during testing activities (DORA).
- Stress-test third-party systems and network interconnections (DORA; G7 Fundamental elements for threat-led Penetration Testing).
- Organise joint testing campaigns with third-parties (DORA; G7 Fundamental elements for threat-led Penetration Testing) and update relevant internal and external stakeholders of findings and results.

[182] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 26. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[183] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[184] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 26. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[185] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 26. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[186] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[187] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

4.4 Training and Awareness

This document's fourth domain (Training and Awareness) defines the process that provides participants with an overview of strategies, approaches, and procedures in place within a DFS entity. Such processes aim to upskill staff to a pre-determined understanding of a given matter[188]. Explicitly referring to the DFS cyber resiliency, this process may occur at various levels inside and outside an entity to provide relevant personnel with the knowledge and skills necessary to perform their activities safely and support established procedures[189].

Leadership's support in establishing training practices is vital. Management must maintain Training and Awareness programs to minimise the risk of cyber incidents and capitalise on economic and human investments[190].

Training and Awareness campaigns must be focused ad provide knowledge and skills to various actors, such as employees, stakeholders[191], and third parties.

4.4.1 Employee Training

Employees and staff members of DFS entities are the first implementers of the entity's resilience policies and processes. Therefore, their knowledge of existing threats and safety measures in place must be known at all levels of seniority within the entity.

This entails that management[192], employee-level staff[193], relevant stakeholders, and end-users[194] must be updated with sufficient knowledge to understand existing risks, assess the impact on operations, and implement established practices to avoid, mitigate and respond to existing threats[195]. Therefore, Training and Awareness progress should present diversified content to provide adequate and commensurate knowledge and skills, depending on the recipients[196].

---

[188] G7 Cyber Expert Group. (2020). *G-7 Fundamental Elements of Cyber Exercise Programmes*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948042/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf
U.S. Department of Homeland Security. (2020). *Exercise and Evaluation Program (HSEEP)* https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf)

[189] Carnegie Mellon University. (2016). *Volume 9 Training and Awareness v1.1 – CRR supplemental resource Guide* https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-TA.pdf

[190] Adapted from EU. (2023). *The EU Cybersecurity Skills Academy Factsheet. EU Digital Strategy*. https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-skills-academy-factsheet

[191] Cicchitto, N. (2020). *Winning the Cybersecurity Race is a team sport: How to engage your stakeholders*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/09/28/winning-the-cybersecurity-race-is-a-team-sport-how-to-engage-your-stakeholders/?sh=136e341b6667

[192] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5.4. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[193] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 6. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[194] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 7. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554. See also, Committee on Payments and Market Infrastructures and World Bank Group. (2016). Payment aspects of financial inclusion. Bank for International Settlements and World Bank Group. https://www.bis.org/cpmi/publ/d144.pdf

[195] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[196] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 7. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

Education programs, reflecting the role and responsibilities of the individuals for whom it is intended, should provide employees with continuous training to instil risk awareness, reinforce codes of conduct, and select tools to enhance their ability to adapt and respond to incidents[197].

In terms of the knowledge and skills that employees must be kept up-to-date with, DFS entities must ensure that the content of training campaigns considers overall existing risks and mitigation measures[198]. Similarly, they must include dedicated training to enhance employees' awareness of specific ICT resilience tools and security[199].

Best Practices

- Train staff and personnel for risks connected to the internet including fraud and social engineering tactics (NIST SP 800-53; PAFI).
- Inform management of internal cybersecurity procedures and its role in the identification, coordination, and response to cyber incidents (NIST SP 800-53).
- Define and promote cyber risk and cyber hygiene awareness campaigns (DORA).
- Train staff and leadership to continuously update and uplift cybersecurity skills (DORA).
- Conduct training sessions on cyber threat capabilities (DORA).
- Conduct specific physical security training to staff handling telco communications and dependencies (NIST SP 800-53).
- Train staff and personnel on risks and threats specific to the DFS environment (NIST SP 800-53).
- Train staff and personnel on mechanisms to mitigate the impact of a potential cyber incident targeting its telco provider (DORA).
- Organise joint training sessions between financial and telecommunication entities (DORA).
- Organize and encourage pentesting awareness and practical training to bolster internal and external defence mechanisms. (DORA).
- Train relevant staff and personnel charged with vulnerability disclosures (BIS Cyber resilience for FMIs).

4.4.2 Information-Sharing Practices

Preventive education and awareness campaigns prepare employees and stakeholders to face existing risks and threats, enhancing cyber resilience. However, keeping training programs up-to-date with the rapid technological penetration and the development of new technologies may become difficult as threats evolve and are sometimes not easily detected.

For this reason, more advanced content of Training and Awareness programs must be updated regularly with data on newly identified threats[200]. These information-gathering activities mandate a structured information-sharing process among DFS entities and national agencies to cross-reference internal resilience mechanisms, inform on occurred incidents, and define incoming threats[201].

---

[197] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[198] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 7. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[199] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5G.4. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[200] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 13. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[201] CISA. (2023). *Partnerships and collaboration | Cybersecurity and Infrastructure Security Agency*. CISA. https://www.cisa.gov/topics/partnerships-and-collaboration

Information-sharing activities leverage private and public coordination to strengthen awareness and knowledge. Additionally, they recognise that cybersecurity threats are not constrained by sector or geographical boundaries and require cooperative efforts to be counteracted. In these regards, best practices already share the common necessity to integrate national intelligence agencies from different countries and regions to jointly elevate resilience and security measures[202]. Establishing these "joint taskforces" requires DFS entities and national agencies to promote collaborative information, incidents, and best practices, sharing mechanisms internally, nationally [203], and globally[204].

The entity should periodically communicate with end-users to notify any incidents, active malicious cyber campaigns, or any defensive action they should undertake to protect their interests and relevant data[205].

Information-sharing processes may be implemented differently, depending on the information and entity. For instance, depending on the jurisdiction, these processes may be voluntary[206] or mandated by government agencies[207]. Voluntary information-sharing may consider the collaboration among entities toward building ordinary intelligence and information-sharing networks, ensuring more efficiency than national-guided information-sharing processes[208].

Best Practices

- Establish communication mechanisms with end-users to communicate cyber campaigns (DORA).
- Share training material and practices with staff and external partners (DORA).
- Promote and participate in information sharing practices within the sector/community (DORA; BIS Cyber resilience for FMIs; PAFI).
- Promote and participate in information sharing practices between technical teams across the sector/community (NIST SP 800-53; PAFI).
- Define and implement responsible vulnerability disclosure policies (BIS Cyber resilience for FMIs).

[202] Interpol. (2023). *AFJOC - African Joint Operation Against Cybercrime*. INTERPOL. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

[203] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.2. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[204] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements of ransomware resilience for the financial sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134062/2022-10-13-g7-fundamental-elements-ransomware-data.pdf

Interpol. (2023). *AFJOC - African Joint Operation Against Cybercrime*. INTERPOL. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

[205] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.3. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554 . See also, Committee on Payments and Market Infrastructures and World Bank Group. (2016). Payment aspects of financial inclusion. Bank for International Settlements and World Bank Group. § 2.3. https://www.bis.org/cpmi/publ/d144.pdf

[206] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1).* National Institute of Standards and Technology. §RS.CO-5. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[207] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 13.6. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[208] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements of ransomware resilience for the financial sector*. United Kingdom (UK) Government

4.4.3 Third-Parties' Training and Awareness

Third parties may be invited or required to participate in DFS-initiated training campaigns, depending on the dependency grade and the relationship's criticality.

Extending training programs outside the perimeter of DFS entities is essential to ensure that mandatory and required resiliency measures are understood, shared, and implemented at all DFS entity service levels.

Specifically, DFS entities, while relying on external partners to provide services or products subject to training and knowledge requirements, must ensure that third-party employees and stakeholders remain up-to-date; this would facilitate implementing the DFS entity's resilience mechanisms. Training programs with third-parties entails extending the perimeter of education and awareness campaign accordingly to comprehend all relevant personnel, whether DFS entity or third-party employees[209].

Best Practices

- Implement mechanisms to determine third-party staff cybersecurity skills and competences (DORA).
- Coordinate with external stakeholders on third-party-led cybersecurity awareness campaigns (DORA).
- Promote the upskilling of third-party cybersecurity capabilities (DORA).
- Expand information-gathering cyber-threat intelligence capabilities to include threats derived from external sources and interdependencies (BIS Cyber resilience for FMIs).
- Establish responsible vulnerability disclosure policies with third-party providers (BIS Cyber resilience for FMIs).
- Encourage training for third-parties, or mandate training sessions, on social engineering schemes and supply chain attacks to mitigate the risk of lateral movement. (DORA).

[209] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 30.2.i. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

4.5 Incident Response

Pillar 5, Incident Response, refers to the ability of an organisation to handle cybersecurity incidents. This includes policies and strategies that structure the incident response process and required cybersecurity capabilities to detect, manage, and recover from ICT-related incidents[210]. The Incident Response Pillar includes the Protection domain, which is here categorised under Incident Response Life Cycle cluster. Protection, which is in the Toolkit singled out as a separate and unique domain, encompasses measures recommended to strengthen cyber resilience, such as the adoption of Multi-Factor Authentication (MFA).

Financial institutions are expected to develop and implement incident response and recovery procedures to handle all cyber-related incidents impacting their operativity and delivery of critical functions[211]. For incident management plans to be efficient, DFS entities should accurately implement Asset Management practices (Section 4.1.1, Risk Assessment) to ensure that all critical assets that malicious actors could potentially target are identified and adequately protected. This includes identifying critical roles, responsibilities, data assets, and external interconnections[212]. Once critical assets have been specified, documented procedures will facilitate the restoration of compromised assets and operativity during disruptions[213]. In addition, such plans should undergo continuous revision and improvement by incorporating internationally-recognised best practices and lessons learned from past incidents and reflecting changes in the regulatory environment, supply chain considerations, and the entity's business strategy[214]. This will ensure that the incident handling procedures are always up-to-date and relevant.

Incident handling and response plans must cover all ICT-related incidents, including those deriving from dependencies, such as third-party vulnerabilities or the supply chain[215]. Indeed, past incidents have shown that the ICT supply chain represents a cyber risk for both individual entities and the digital financial sector as a whole. Third-party and ICT supply chain vulnerabilities can interrupt business operations, unauthorised customer/corporate data access, or destabilise financial markets[216]. Accounting for third-party dependencies and vulnerabilities enables entities to mitigate cyber risks more comprehensively.

4.5.1 Incident Response Life Cycle

The incident response life cycle refers to a series of steps an entity needs to perform when handling a cybersecurity incident. Divided into four main stages, they define the standard procedure that technical teams (e.g., incident responders, incident commanders), management (e.g., Chief

---

[210] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 17. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[211] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf; Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[212] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[213] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[214] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[215] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[216] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

Information Security Officer, CISO, or Chief Executive Officer, CEO), and other relevant business units (e.g., business continuity functions, legal functions, public relations functions) need to follow to detect and respond to a cyber event[217]. While each entity can have an incident response life cycle tailored to its specific needs and requirements, it usually resembles the one provided by the U.S. National Institute of Standards and Technology (NIST). The model includes the four following steps: (1) Protection; (2) Detection and Analysis; (3) Containment, Eradication, and Recovery; and (4) Post-Incident Activity[218].

Protection

Protection provides guidelines for securing the entity's data, systems, networks, and applications. Furthermore, it assesses how to establish an incident response capability to prepare the organisation for malicious cyber events[219].

Security controls need to be implemented to ensure that the entity's critical assets are protected and can act as a first barrier against malicious behaviour. In addition, a robust peripheral defence mechanism prevents the incident response team from being overwhelmed[220]. To achieve this, international best practices[221] suggest the implementation of risk assessments, host and network security, malware prevention, and user/employee Training and Awareness practices. This will increase the protection level of the entity's data, systems, networks, and applications.

Protection measures extend beyond the adoption of standard security mechanisms, such as implementing multi-factor authentication, antiviruses and antimalware, patching policies, and cyber-threat intelligence programs. Indeed, entities must also implement data, network, and account protection measures to mitigate the risk of cyber intrusions.

On data protection, organisations must primarily implement a comprehensive data backup policy, including minimum frequency requirements[222] and regular incremental backup procedures, to mitigate the risk of data corruption and loss in the unfortunate event of, for instance, a ransomware attack. Incremental and/or differential backup policies should be accompanied by adopting data loss prevention strategies to classify confidential or sensitive information and restrict its exfiltration[223]. In addition, organisation-wide encryption tools can be useful tools to guarantee the confidentiality and integrity of the entity's data and information, whether at rest or in transit[224].

Network protection, instead, aims to prevent unauthorised access, misuse or theft of the entity's network and its underlying infrastructure[225]. This can be achieved by implementing security mechanisms such as traffic filtering, network saturation mitigations, and network intrusion prevention tools. Considering the criticality of entities operating within the DFS ecosystem, network

---

[217] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[218] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[219] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[220] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[221] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[222] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.22. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[223] MITRE ATT&CK. *Entreprise Mitigations.* Mitigations-Entreprise | MITRE ATT&CK. https://attack.mitre.org/mitigations/enterprise/

[224] MITRE ATT&CK. *Entreprise Mitigations.* Mitigations-Entreprise | MITRE ATT&CK. https://attack.mitre.org/mitigations/enterprise/

[225] CISCO. *What is Network Security?* CISCO. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

segmentation is pivotal in ensuring that sensitive systems, functions, and resources are isolated from the main network and that, in the event of a compromise, threat actors can move freely and laterally in the architecture[226].

Account protection, finally, ensures that user accounts are properly managed and protected, including both general users accounts and administrator accounts with privileged access. This includes, among others, the definition of comprehensive password policies and logic attempts thresholds. Additionally, entities should ensure the adoption of credential access prevention processes to mitigate the risk of credential dumping. Finally, privileges should be appropriately protected, managed, and monitored to ensure integrity[227].

Incident response teams must be prepared to manage cybersecurity incidents when prevention fails. This is facilitated by practices and behaviours allowing the cybersecurity team to access all necessary information immediately. One of the key priorities for the financial entity is to create and constantly update the inventory of internal and third-party resources; this will ensure a prompt response and recovery[228].

Just as important, the protection phase requires organisations to account for potential disruptions caused by an incident and, thus, implement alternative solutions aligned with the incident response process. This includes, for example, the development of multiple and separate communication and coordination mechanisms (e.g., smartphones, encryption software, secure storage facility) to be activated in case the main one fails[229]. These failover mechanisms can facilitate crisis management and incident response in case of emergency.

Incident responders should also have access to hardware and software that enables and facilitates incident analysis, including removable media, packet sniffers, protocol analysers, portable printers, and digital forensic software programs[230]. This should be coupled with appropriate incident analysis resources like port lists, relevant documentation, and network diagrams[231].

Another key feature of the protection phase is incorporating cyber-threat intelligence into daily tasks[232]. Similar to the testing phase, threat intelligence provides the financial entity with significant insights into exposed critical functions and malicious cyber behaviours. Thus, integrating cyber-threat intelligence into the organisation's daily activities can facilitate the proactive identification of attacks before they are launched. The same advantages can be derived by establishing intra-sector and cross-sector information-sharing practices on cyber incidents[233].

Considering the critical importance of the Protection phase to secure the entities' systems and assets and prevent ICT-related incidents, the proposed Cyber Resilience Toolkit (Section 2, Cyber Resilience Toolkit) separates Protection from Incident Response. This will ensure a more precise

---

[226] MITRE ATT&CK. *Entreprise Mitigations.* Mitigations-Entreprise | MITRE ATT&CK. https://attack.mitre.org/mitigations/enterprise/

[227] MITRE ATT&CK. *Entreprise Mitigations.* Mitigations-Entreprise | MITRE ATT&CK. https://attack.mitre.org/mitigations/enterprise/

[228] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf; Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[229] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[230] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[231] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[232] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.18 https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[233] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.18 https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

definition of cyber resilience maturity gaps for entities and facilitate the definition, development, and implementation of remedial plans.

Best Practices

- Track software installations, especially in case of a hybrid BYOD policy (NIST SP 800-53).
- Set timeouts and auto-logout user sessions on DFS applications (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Establish password complexity, set maximum unsuccessful login attempts, password history and reuse periods, and account lock-out periods (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Require user identify validation for dormant DFS accounts (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Limit access to DFS services based on user location (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Implement client-side authentication or authorisation token (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Store DFS passwords using robust salted cryptographic hashing algorithms (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Add session timeouts for USSD, SMS, application, and web access to DFS services (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Encrypt DFS user passwords (PCI DSS, PA DSS, ITU DFS security assessment framework)
- Require the use of long and complex PINs (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Do not allow mobile users to trust individual binary-based SMS messages (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Use Network Address Translation to limit external exposure of DFS IP address and routing information (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Set up and use DMZ to isolate DFS systems and filter incoming traffic (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Remove customer sensitive data from trace logs (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Restrict information sharing of transactions with third-parties and service providers (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Monitor APIs and encrypt all data shared with third-parties (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Implement security measures to protect the network (e.g., firewall, traffic filters (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Use database fingerprinting/digital signatures to detect data tampering and modification (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Encrypt algorithms and data on all DFS sensitive information and infrastructure (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Require user authentication and authorisation for high-risk account changes and transactions, including MFA (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Implement technical controls to ensure an effective management during system downtime with related service providers (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Perform end-to-end tests after changes to the DFS, MNO, SP, and other third-party systems (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Implement standard ACID (Atomicity, Consistency, Isolation, Durability) functionality of the database (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Implement mechanisms to detect in real-time cases of SIM swapping, recycling, or replacing (PCI DSS, PA DSS, ITU DFS security assessment framework).

- Mask the Primary Number Account (PNA) according to local or national payment policies and regulations (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Enforce the use of Secure OTP to verify the transaction's legitimacy (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Limit the lifetime of TLS certificates (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Deploy and regularly update security software products on all devices (PCI DSS, PA DSS, ITU DFS security assessment framework).
- Monitor asset's lifecycles and implement patching mechanisms to close vulnerabilities to the network (DORA).

Detection & Analysis

The Detection & Analysis phase aims to detect a cyber event, identify its severity, and classify it according to its characteristics (e.g., type, magnitude of impact, and extent). This process will facilitate incident prioritisation and response.

The first step is identifying parameters to determine what constitutes an incident compared to a cybersecurity event. This document defines a *cyber event* as a change that could impact the organisation's operations, missions, or reputation[234]. Similarly, a cybersecurity incident is here intended as an action taken through an information system or network that adversely affects a targeted digital environment[235]. The United States Government goes a step forward. It indicates with *severe cyber incidents* any incidents (or group thereof) that can disrupt the national security interest severely impact U.S. foreign relations, economy, civil liberties, public confidence, or safety[236]. Understanding the differences between these three definitions will ensure that cybersecurity incidents are accurately detected, categorised, and prioritised, triggering the incident management and response procedures[237]. Such processes should clearly outline how to identify, track, and categorise cybersecurity incidents[238].

Establishing signs of incidents, assets, and system monitoring facilitates the detection of an incident. Signs of incidents, divided between precursors and indicators, enable the entity to understand whether there is a potential or concrete compromise. Indeed, precursors refer to signs indicating that an incident may occur in the future, thus allowing incident responders to attempt to prevent the attack. At the same time, indicators show that an incident has occurred or is occurring[239]. Signs of incidents can be derived from, for example, antivirus and antispam software programs, network device logs, publicly available information on new vulnerabilities and exploits, and people internal or external to the organisation[240]. In addition to this, the continuous monitoring of the information system and assets

[234] Ross, R. (2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
[235] Ross, R. (2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
[236] CISA. (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf
[237] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf
[238] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 17.3b. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554
[239] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2).* National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2
[240] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2).* National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

of the entity ensures that incident responders adopt a proactive approach to the detection of cybersecurity incidents whilst assessing the effectiveness of protective and defensive mechanisms[241].

Once an anomalous activity is detected and categorised as a cybersecurity incident, the following step determines its impact on the system[242]. One of the goals of the incident analysis phase is, based on predefined criteria, to determine the incident severity, appropriately prioritise it, and allocate adequate resources for the incident response and Recovery[243]. The criteria to determine the severity of an incident vary across organisations. The most common ones[244] are:

1. The criticality of the services at risk.
2. The number and/or importance of customers or stakeholders targeted.
3. The extent of the areas targeted.
4. The functional impact.
5. The information impact.
6. The recoverability efforts.

Containment, Eradication & Recovery

The Containment, Eradication, and Recovery section refers to all activities undertaken to minimise the impact of a cybersecurity incident by avoiding the spread of the incident, deleting its components from the victim's networks and systems, and resolving the malicious event[245].

Firstly, looking at Containment, this phase is fundamental to ensure the incident is contained and isolated before it further damages the target or overwhelms its responsive resources. It also constitutes an effective strategy to buy time for the organisation when analysing the incident to identify tailored remediation measures. Financial entities should be aware that Containment strategies change according to the incident type, making it difficult to prepare standardised measures. Nevertheless, incident responders are encouraged to develop and test Containment strategies for the main incidents they could confront. This will facilitate decision-making, save time, and mitigate potential effects[246].

The NIST Incident Handling Guide[247] provides valuable guidance on choosing proper Containment strategies. Indeed, the standardised procedure includes a list of criteria that can help determine which Containment strategy to use: (a) potential damage; (b) evidence preservation obligations; (c) availability of services (e.g., network connectivity); (d) logistical requirements for the strategy implementation (e.g., time, resources); (e) strategy effectiveness (i.e., partial or full Containment); and (f) duration of the strategy (e.g., the solution to be removed in two hours or two weeks)[248].

---

[241] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §DE.CM, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[242] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §DE.AE. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[243] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf; Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1.* Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[244] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2; The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 18.2. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[245] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §RS.MI, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[246] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[247] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[248] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

As part of the response process, Eradication is needed to ensure that the threat is no longer active and that all its components are erased from the entities' networks, systems, and devices[249]. One essential Eradication step is determining all hosts affected by the incident to guarantee that Eradication measures thoroughly remediate the malicious behaviour's impact. Entities should be aware that Eradication is always needed and can only be performed at a later time if the circumstances of the incident allow it[250]. To ensure its effectiveness, response procedures should constantly be updated and monitored[251]. Examples of Eradication activities include the identification and mitigation of exploited vulnerabilities, as well as the deletion of malware and disabling of compromised user accounts[252].

Finally, Recovery refers to procedures executed to guide the restoration of all systems and assets that were impacted during the incident[253]. At this stage, administrators are charged with returning systems and networks to their pre-incident state, ensuring everything is operating normally, and, if necessary, fixing vulnerabilities to prevent future occurrences[254]. Recovery activities often require the joint participation of internal and external stakeholders, such as an Internet Service Provider (ISP), third-party service providers, end-users, authorities, and other Computer Security Incident Response Teams (CSIRTs)[255]. Typical recovery activities include employing backed-up data, rebuilding systems, replacing compromised files, installing patches, replacing passwords, and updating firewall rulesets[256].

Post-Incident Activity

The last phase of the Incident Response Life Cycle is the post-incident activity, where all relevant stakeholders gather to assess what occurred, what measures were implemented, and how to prevent future incidents from taking place[257]. This can be done through lessons learned documentation and the consequent incorporation of major findings into established processes and procedures, promoting constant improvement. This mechanism should include lessons learned related to recovery planning and processes[258], organisational response activities[259], incident management programs for both internal and external incidents[260], and contingency and resumption plans[261].

---

[249] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[250] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[251] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §RS.SP. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[252] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[253] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §RC.RP. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[254] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[255] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §RC.CO and RS.CO. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[256] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[257] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[258] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §RC.IM. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[259] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §RC.IM. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[260] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[261] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures.* International Telecommunication Union. §5.15. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

In addition, the post-incident activity should also cover the root cause analysis of the incident, aimed at understanding how to prevent, or minimise, the chance of a similar incident recurring in the future[262]. Just as was the case for the lessons learned, the root cause analysis findings should be incorporated into the organisations' detection, response, and recovery plans and procedures[263].

Best Practices

- Segregate the network, implement VLANs, and implement defensive security measures (NIST SP 800-53).
- Establish a threat categorisation and prioritisation process for cybersecurity events (NIST SP 800-53).
- Establish encryption techniques for data-at-rest (NIST SP 800-53).
- Establish security mechanisms for data-in-transit (NIST SP 800-53).
- Ensure data and server availability (NIST SP 800-53).
- Regularly implement security patches of software external to the organisation (NIST SP 800-53).
- Set up incremental and differential backups (NIST SP 800-53).
- Implement load balancing and/or failover mechanisms (NIST SP 800-53).
- Develop detection capabilities to identify malicious codes/behaviour and anomalies (NIST SP 800-53; BIS Cyber resilience for FMIs; PAFI).
- Develop analysis capabilities to assess detected cybersecurity events (NIST SP 800-53).
- Develop capabilities and metrics to assess the internal and external impact of a cybersecurity incident (DORA).
- Establish mechanisms to implement lessons learned from previous cybersecurity incidents (NIST SP 800-53).
- Periodically define a Business Impact Analysis (BIA) and the maximum tolerable duration of business interruptions (DORA).
- Record information on cyber vulnerabilities, threats, and cybersecurity incidents (DORA).
- Conduct post-incident analysis to identify the root cause of the incident (DORA).

4.5.2 Incident Response Governance

Incident Response Governance adapts its main guiding principles to incident response based upon the Governance Pillar. Indeed, Incident Response Governance refers to strategic, organisational, and oversight measures specific to the incident response process that entities should implement[264].

All entities should first define and assign incident response-related roles and responsibilities to their staff and external parties[265]. This includes clear communication of such functions and responsibilities to ensure that all interested parties are aware of what they must do in case of an incident and are ready

[262] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[263] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.10. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[264] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 5. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[265] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 17.3c. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554; Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.3. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

at all times to activate related plans and procedures correctly. Roles and responsibilities may vary according to the entity's incident type. Internal staff and external stakeholders should also be aware of such differences[266]. Provisions should ensure that incident response-related roles and associated responsibilities are also assigned for secondary or deputy positions. This is especially important when resources assigned as primary roles are unavailable or unreachable.

Entities should guarantee that the incident response team has the knowledge to detect, respond to, and recover from cybersecurity incidents[267]. This includes, for example, skills related to system administration, network administration, programming, intrusion detection, and technical support[268]. Management should also ensure that relevant staff receives training to remain up-to-date with the latest developments, skills, and information[269].

Entities should further ensure that incident response and recovery plans are periodically reviewed and updated to reflect changes in the DFS ecosystem, including the cyber-threat landscape, new technological advancements, and lessons learned from past internal and external cybersecurity incidents[270]. Processes and procedures should also be regularly tested[271], including communication plans[272].

Best Practices

- Develop and periodically update cyber-related emergency plans and procedures according to changes in the cybersecurity landscape and/or any changes to the organisation, including (NIST SP 800-53; DORA):
    - Incident response plans.
    - Disaster recovery plans.
    - Technical guidelines to response and recover from malicious activity.
    - Business continuity plans.
- Define roles and responsibilities in the company and ensure that the hierarchical structure of incident response teams is constantly monitored and updated to reflect internal corporate changes (DORA; BIS Cyber resilience for FMIs).
- Align cyber-related emergency plans to national and international best practices (NIST SP 800-53).
- Determine frequency metrics to review and update cyber-related emergency plans (NIST SP 800-53).
- Clearly outline any connection between incident response, business continuity and disaster recovery procedures (DORA).

---

[266] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 17.3c. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[267] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.6. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[268] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[269] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.6. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[270] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf; Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.3. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[271] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (v.1.1)*. National Institute of Standards and Technology. §DE.DP. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[272] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

4.5.3 Incident Response Reporting

Incident Response Reporting refers to developing communication mechanisms and provisions to notify and report cybersecurity incidents, as required or needed, to all relevant stakeholders in a timely manner[273]. This includes internal and external parties depending on the incident and its implications[274]. Generally, the incident response plan should consist of indications on the type of reporting (e.g., status update, incident report, incident update)[275], to whom the report will be provided (e.g., a specific person within the organisation, the whole organisation, specific business unit, third-party provider)[276] and when (e.g., after detection, during the incident, during the post-incident)[277].

The entity should ensure that the incident response and related communication plans account for multiple communication methods, including standardised and out-of-band channels. Examples of such communication methods are (a) emails; (b) websites; (c) telephone; (d) in-person or virtual meetings; (e) separate, dedicated voice mailbox; and (f) paper[278].

Internal Reporting

Incident responders should notify the detection of a cybersecurity incident and relevant information stakeholders internal to the entity. For example, this includes senior managers, employees, and specific business units[279]. The notification may include explanations of the impact of the incident, its risk category, the response measures in place, and additional controls to resolve the incident[280].

Provisions on internal incident reporting vary from entity to entity, especially concerning the type of reporting, the time requirements, and the type of content to add. Generally, incident response procedures include three main types of reporting: (1) initial notification; (2) intermediate report; and (3) final report. The initial notification is usually performed right after the detection of the incident and results in a brief preliminary analysis that facilitates the identification of the incident severity and subsequent prioritisation. The initial notification tends to contain less information than the intermediate and final reports. The former usually indicates a change of incident status or the discovery of new information, and its frequency is established according to the availability of relevant status updates or as decided by higher management[281]. The final report is issued when the root cause

---

[273] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.40. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[274] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Risk Management V.2*. Hong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-1.pdf; Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[275] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[276] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 17.3d. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[277] Hong Kong Monetary Authority. (2022). *Supervisory Policy Manual – Operational Resilience V.1. H*ong Kong Monetary Authority. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf

[278] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[279] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[280] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures.* International Telecommunication Union. §5.39. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf; The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 17.3e. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[281] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.4. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

analysis is completed and should detail how the relevant teams handled the incident (e.g., detection, Containment, Eradication, and mitigation measures implemented)[282].

Following a cybersecurity event, internal stakeholders to whom notify the incident may include the Chief Information Officer (CIO), the Information Security team (InfoSec team, both organization-wide and local, if applicable), other internal emergency teams (e.g., business continuity team, disaster recovery team, crisis management team), internal system owners, and other relevant business units (e.g., legal, public affairs, public relations, human resources)[283].

External Reporting

Depending on local or national regulatory obligations, organisation policies, and/or contractual agreements, organisations may sometimes be forced or recommended to notify external stakeholders of cybersecurity incidents. External stakeholders may include external incident response teams (e.g., in case of outsourcing incident response obligations), external system owners, end-users (e.g., clients), national or industry CERTs; law enforcement; third-party service providers, media outlets, information-sharing networks (e.g., Information-Sharing and Analysis Centres)[284].

A financial entity should notify cybersecurity incidents or significant cybersecurity threats deemed of relevance to their sector, service users, or clients to competent authorities (e.g., regulators)[285]. The notification can either be mandated by local, national, or industry-wide regulatory obligations, or performed voluntarily, depending on the entity's specific circumstances[286]. The initial notification to the competent authority generally includes any relevant information needed to assess the significance and severity of the incident and to determine its potential impact on a geographical area (e.g., local impact, national impact, transnational impact) or an industry (e.g., one or more entities affected within the same sector, cross-industry implications)[287]. Based on this information, the competent authority should suggest or mandate specific mitigation measures when appropriate[288].

Similarly, according to local, national, or industry legislative obligations, or voluntarily, entities should notify end-users when an incident impacts clients' financial interests. The notification should include both measures being implemented by the organisation to mitigate the incident's impact and, when appropriate, any protective action suggested to, or required for, end-users[289].

---

[282] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.4. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554; Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[283] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[284] Cichonski, P., et al. (2012). *Computer Security Incident Handling Guide (SP 800-61 rev.2)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-61r2; G7 Cyber Expert Group. (2022). *G7 Fundamental Elements of ransomware resilience for the financial sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134062/2022-10-13-g7-fundamental-elements-ransomware-data.pdf

[285] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.2. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[286] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.2. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[287] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.1. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[288] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.7. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[289] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.3. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

Regulators are encouraged to develop and implement guiding documents on incident reporting mechanisms for financial and telecommunication entities. These should include, at minimum, which incidents to report, time requirements for the first notification, the content of incident reports, and the frequency of reporting after the first notification. In addition, according to international best practices, entities should report to relevant regulators the following incidents:

- Ransomware attacks[290].
- Significant cyber incident, or group of related cybersecurity incidents, likely to cause demonstrable harm to national security interests, foreign relations, the economy of the host country, or to the public confidence, civil liberties, or public health and safety of the host country[291].
- Cybersecurity breaches of applicable local, national, industry, or transnational regulations[292].

Best Practices

- Establish mechanisms to share information on cybersecurity events or incidents with clients and partners (NIST SP 800-53).
- Establish coordination mechanisms on incident response practices with relevant stakeholders (NIST SP 800-53).
- Establish communication mechanisms to share information on recovery measures with relevant stakeholders (NIST SP 800-53).
- Implement internal communication plans on cybersecurity incidents (DORA)
- Comply with local, national, and international regulations on incident reporting requirements to authorities (NIST SP 800-53).

4.5.4 Third-Parties' Incident Response

The incident response process should account for the increasing reliance of organisations on the ICT supply chain, including third-party providers. This is particularly important when third-parties provide critical services to the organisation, or the entity outsources its incident response obligations and responsibilities[293].

To achieve this, organisations should collaborate with interconnected entities, industries, and other external stakeholders to enhance their incident response plans and procedures[294]. In particular, the incident response plan should include provisions to detect cybersecurity incidents involving third-parties and mechanisms to gather information on them. To guarantee the effectiveness of developed procedures, entities are encouraged to test plans and processes with all relevant stakeholders, including third-parties and other appropriate partners[295]. In addition to this, the post-activity phase

[290] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements of ransomware resilience for the financial sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134062/2022-10-13-g7-fundamental-elements-ransomware-data.pdf

[291] Greene, A., et al. (2022). *Cyber incident reporting. New rules, new timelines*. Crowe. https://www.crowe.com/cybersecurity-watch/cyber-incident-reporting-new-rules-new-timelines

[292] ENISA. *Incident Reporting.* enisa.europa.eu. https://www.enisa.europa.eu/topics/incident-reporting

[293] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

[294] Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[295] G7 Cyber Expert Group. (2022). *G7 Fundamental Elements for Third Party Cyber Risk Management For The Financial Sector*. United Kingdom (UK) Government.

should leverage the lessons learned from previous incidents experienced by third parties, especially those with which the entity in question shares an interconnection or interdependency[296].

Finally, third-parties' role in incident response is particularly relevant regarding reporting mechanisms. Indeed, the entity should establish communication channels and provisions to ensure that third-parties (e.g., relevant authorities, end-users) are contacted when a cyber incident targets the organisation. The organisation should also put in place contractual reporting obligations to ensure that third-party providers (e.g., software providers) notify and keep the entity informed in case of a cyber incident[297].

Best Practices

- Establish mechanisms to raise awareness of third-party remote access (NIST SP 800-53).
- Issue best practices for information sharing with external stakeholders (NIST SP 800-53).
- Issue best practices on forensics checks and compromised systems to external stakeholders and partners (NIST SP 800-53).
- Develop and implement data sharing agreements on cybersecurity incidents with third-parties to facilitate recovery (BIS Cyber resilience for FMIs).
- Establish communication obligations for third-parties to adhere to in case they are hit by a cyberattack (DORA).

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134063/2022-10-13-g7-fundamental-elements-third-party-risk.pdf; Financial Inclusion Global Initiative. (2019). *Cyber Resilience for Financial Market Infrastructures*. International Telecommunication Union. §5.19. https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[296] Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

[297] The European Parliament and Council. (2022). *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. Article 19.5. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

Conclusion

The digitalisation of emerging economies' financial services has both positive and negative repercussions. While sustaining economic growth, an unprotected DFS ecosystem exposes critical national infrastructure to threat actors and malicious cyber behaviour. This is especially significant for emerging economies that might suffer from less robust regulations than advanced DFS ecosystems. Therefore, to mitigate the risk of disruptive attacks, DFS actors should improve their cybersecurity measures and cyber-preparedness.

To achieve this, regulators and entities in EMDEs need first to assess their current cyber resilience and, based on the aggregated results, create national cyber resilience roadmaps for the short-, medium-, and long-term.

The DFS Cyber Resilience Toolkit and its methodology were developed upon five main pillars (i.e., Risk Management, Governance, Testing, Training and Awareness, and Incident Response) derived from the analysis of internationally-recognised cybersecurity standards, frameworks, and best practices. These standards include, but are not limited to, the ISO series, DORA, the World Bank and Bank for International Settlements report on Payment Aspect for Financial Inclusion (PAFI), and multiple national methodological frameworks that define risks, vulnerabilities, and mitigation measures. The frameworks analysed include standards from a wide range of international organisations with the clear purpose of creating a hybrid methodology that covers all the most relevant cyber resilience domains. In doing so, this report provides the foundation to align emerging economies with the journey already started by mature countries on cyber resilience and the needed awareness to increase their levels of external/internal cooperation, transparency, and proactivity.

In conclusion, the report defines a comprehensive methodology and a tailored toolkit identifying guidelines and specific recommendations for DFS regulators and operators dealing with critical national infrastructure in emerging economies. However, the toolkit should be considered as a starting point, and not a solution to achieve a higher cyber resilience; it will enable DFS regulators and DFS entities to understand their current state, define strategies to address gaps, and delineate roadmaps to improve the cyber security posture.

Appendix A – DFS Cyber Resilience Assessment Toolkit Questions

Domains	Questions
Risk Management	71
Monitor and Review	5
Risk Assessment	30
Risk Treatment	20
Third-Parties	16
Governance	57
Availability of Official Documentation	9
Communication Channels	9
Monitoring and Review Process	11
Roles and Responsibilities	16
Third-Parties	12
Testing	42
Penetration Testing	3
Red Teaming	3
Simulations and War Gaming	21
Third-Parties	5
Vulnerability Scanning	10
Training & Awareness	42
Employee Training	24
Information-Sharing Practices	10
Third-Parties	8
Protection	79
Enterprise Policy	23
Filter Network Traffic	13
Privileged Account Management	3
Multi-Factor Authentication	11
Encrypt Sensitive Information	14
Exploit Protection	9
Data Loss Prevention	2
Security Updates	2
SSL-TLS Inspection	2
Incident Response	75
Third-Parties	4
Incident Response Reporting	8
Incident Response Life Cycle	49
Incident Response Governance	14
Total Questions	**366**

Risk Management Pillar

Domain	ID	Applicability	Question	Informative Reference
Third-Parties	RM.01	FS Entity / Telco Entity	Is the entity reliant on a specific supplier? Does it have a business continuity plan in place in case suppliers or other linked services are unavailable?	NIST SP 800-53 Rev. 4[298]
Third-Parties	RM.02	FS Regulator / Telco Regulator	Does the national or international regulator mandate requirements concerning third-parties related risk assessments within the DFS entity's business continuity plan?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.03	FS Entity / Telco Entity	Does the entity have in place a plan to counteract power shutdowns, whether involuntary or resulting from a cyber-attack? For example, is it prepared to withstand extended delivery outages?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.04	FS Regulator / Telco Regulator	Do national regulations mandate appropriate measures against power shutdowns and extended delivery outages for DFS entities?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.05	FS Entity / Telco Entity	Does the entity have a vulnerability log, and has it reported all the vulnerabilities observed during the latest test?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.06	FS Regulator / Telco Regulator	Do regulators mandate the establishment of vulnerability logs and reporting mechanisms for DFS entities?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.07	FS Entity / Telco Entity	Does the board of directors/management of the entity/agency know the threats, vulnerabilities, and likelihoods connected to the risks to critical assets?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.08	FS Entity / Telco Entity	Has the entity conducted a risk assessment and evaluated the most relevant risks connected to the entity?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.09	FS Entity / Telco Entity	If completed, has the entity's risk assessment been appropriately addressed at all levels?	NIST SP 800-53 Rev. 4
Monitor and Review	RM.10	FS Entity / Telco Entity	Does the entity have a risk management process in place? Is it being revised according to the latest threats?	NIST SP 800-53 Rev. 4
Monitor and Review	RM.11	FS Regulator / Telco Regulator	Does the regulator mandate the consistent revision of the DFS risk management process?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.12	FS Entity / Telco Entity	How aware is the entity of its current status within the DFS ecosystem? If the entity manages critical assets within the infrastructure, is it planning extra security measures to ensure high availability?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.13	FS Regulator / Telco Regulator	Are entities within the national scope of DFS activities aware of their current resiliency and security measures level?	NIST SP 800-53 Rev. 4
Third-Parties	RM.14	FS Entity / Telco Entity	Besides an internal risk management process, has the entity planned a cross-check with external vendors and suppliers to ensure potential entry points into its networks are secured?	NIST SP 800-53 Rev. 4

[298] Joint Task Force (2020). *Security and Privacy Controls for Information Systems and Organizations (NIST.SP.800-53 Rev.5)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Domain	ID	Applicability	Question	Informative Reference
Third-Parties	RM.15	FS Regulator / Telco Regulator	Does the regulator mandate regular cross-checks among entities and external partners to ensure the patching and monitoring of potential vulnerabilities and entry points?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.16	FS Entity / Telco Entity	Does the entity have in place any CCTV infrastructure on server rooms and smart locks to ensure that only authorised personnel can enter confidential premises?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.17	FS Entity / Telco Entity	Is the entity's personnel monitored on the premises to ensure that suspicious activity is flagged to security and IT professionals?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.18	FS Regulator / Telco Regulator	Are regulations mandating DFS entities' physical security measures, including monitoring employees and visitors on-premises?	NIST SP 800-53 Rev. 4
Third-Parties	RM.19	FS Entity / Telco Entity	Does the entity understand an event's impact on its network and on third-parties potentially linked to its network infrastructure? Does it communicate with stakeholders in these regards regularly?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.20	FS Regulator / Telco Regulator	Does the national regulator clearly understand the impact of a given cyber-attack on a specific DFS Critical National Infrastructure?	NIST SP 800-53 Rev. 4
Third-Parties	RM.21	FS Regulator / Telco Regulator	Does the national regulator communicate regularly with DFS stakeholders and partners to monitor and mitigate the risk of cyber intrusions?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.22	FS Entity / Telco Entity	Does the entity have a clear baseline for accepted risk? Is the risk acceptance level clear to the management, and has it been approved?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.23	FS Entity / Telco Entity	Has the entity included all relevant assets in its cybersecurity frameworks and corporate approaches?	DORA
Risk Assessment	RM.24	FS Regulator / Telco Regulator	Does the regulator describe the assets that must be mandatorily included within DFS entities' cybersecurity frameworks and approaches?	DORA
Risk Treatment	RM.25	FS Entity / Telco Entity	Has the entity adopted measures to monitor and internally respond to cyber risks and menaces?	DORA
Risk Assessment	RM.26	FS Entity / Telco Entity	Does the DFS entity define an acceptable level of risk tolerance, considering internal objectives, Key Performance Indicators (KPI), and assets?	DORA
Risk Assessment	RM.27	FS Entity / Telco Entity	Does the entity's present cyber resilience strategy include direct objectives in terms of ICT security, cyber baseline parameters, and risk management measures?	DORA
Risk Treatment	RM.28	FS Entity / Telco Entity	Does the entity's internal cybersecurity framework include mapping corporate assets and, eventually, the necessary changes to achieve commercial objectives?	DORA
Third-Parties	RM.29	FS Regulator / Telco Regulator	Do local and federal regulations mandate Due Diligence background checks on external third-party services?	DORA
Third-Parties	RM.30	FS Entity / Telco Entity	Has the entity completed the necessary Due Diligence checks to guarantee cyber resilience and trustworthiness for all systems, protocols, and external ICT tools provided by third-parties?	DORA
Monitor and Review	RM.31	FS Entity / Telco Entity	Does the entity periodically review and update the inventories in case of major IT and network system infrastructure changes?	DORA
Monitor and Review	RM.32	FS Regulator / Telco Regulator	Are there any regulatory requirements mandating the frequency and content of periodic reviews and updates of DFS entities' IT and network infrastructure?	DORA

Domain	ID	Applicability	Question	Informative Reference
Risk Treatment	RM.33	FS Entity / Telco Entity	Do the entity's information asset backup and recovery policies include the following conditions? 1) backup systems that ensure the security of computer and network systems, availability, authenticity, integrity, and confidentiality of data; 2) physically and logically segregated ICT systems from the source ICT system to restore backup data; 3) adequate resources and backup and recovery equipment to offer and maintain services at all times.	DORA
Risk Treatment	RM.34	FS Entity / Telco Entity	Does the entity have in place a robust and documented Cyber Risk Management Framework that defines the mechanisms and measures aimed at rapid, efficient, and organic management of cyber risks and protects physical infrastructure and components?	DORA
Risk Treatment	RM.35	FS Entity / Telco Entity	Is there a national guideline or content baseline defining the content of DFS entities' Cyber Risk Management Framework?	DORA
Risk Assessment	RM.36	FS Entity / Telco Entity	Is the provider of the threat analysis an external party to the financial entity?	DORA
Third-Parties	RM.37	FS Entity / Telco Entity	Does the entity have an ICT Third-Party Risk Management framework in place?	DORA
Third-Parties	RM.38	FS Entity / Telco Entity	How often does the entity conduct risk assessment activities (including security risk) related to ICT services provided by third-parties for essential or critical functions?	DORA
Third-Parties	RM.39	FS Entity / Telco Entity	Does the entity have in place, as part of its Cyber Risk Management Framework, arrangements for maintaining a register of information on all contractual arrangements for using ICT services provided by third-parties?	DORA
Third-Parties	RM.40	FS Entity / Telco Entity	Does the entity consider, at the pre-contract stage, whether the agreement will provide for the outsourcing of any essential or critical functions?	DORA
Third-Parties	RM.41	FS Entity / Telco Entity	Does the national or international regulator mandate specific content levels and efficiency of business continuity, contingency, and exit strategies for DFS entities?	DORA
Third-Parties	RM.42	FS Entity / Telco Entity	Does the entity have adequate business continuity, contingency, and exit strategies in place to protect its operational resiliency in the event of third-party supplier failures or outages that impact critical operations?	DORA
Risk Assessment	RM.43	FS Entity / Telco Entity	Does the entity keep audit logs to document system activities and mitigate the risk of unauthorised intrusions?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.44	FS Regulator / Telco Regulator	Does the regulator mandate entities to periodically conduct business impact analysis (BIA) and risk assessments?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.45	FS Entity / Telco Entity	Has the entity completed a business impact analysis (BIA) and risk assessment over the past six months? Is it updated regularly?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.46	FS Entity / Telco Entity	Does the entity sanitise outdated hardware? Does it dispose of it in a coherent way?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.47	FS Entity / Telco Entity	Has the entity tracked software installations into its devices and set up a thorough check of staff's personal devices in case of a hybrid Bring-your-own-device (BYOD) policy?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.48	FS Entity / Telco Entity	Has the entity prioritised the most critical assets and ensured their cyber resilience in case of cyber-attacks?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.49	FS Regulator / Telco Regulator	Does the regulator mandate the regular prioritisation of critical assets and ensure that specific resilience tests are conducted to withstand disruptive cyber-attacks?	NIST SP 800-53 Rev. 4

Domain	ID	Applicability	Question	Informative Reference
Risk Treatment	RM.50	FS Entity / Telco Entity	Is the entity implementing a physical Access Control List (ACL) to monitor corporate premises visitors, employees, and staff?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.51	FS Entity / Telco Entity	Does the entity implement a least-privilege people management mechanism to separate work duties and define network access levels? Is it aware of breaches to this mechanism with employees accessing confidential folders or servers without authorisation?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.52	FS Entity / Telco Entity	Does the entity comply with industry, national, and/or federal data collection, storing, and destruction regulations?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.53	FS Regulator / Telco Regulator	Does the entity comply with national and federal data collection, storage, and destruction regulations?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.54	FS Entity / Telco Entity	Has the entity defined internal cyber-threat intelligence (CTI) preventive and responsive mechanisms?	DORA
Risk Treatment	RM.55	FS Regulator / Telco Regulator	Does the regulator mandate the adoption of cyber-threat intelligence (CTI) preventive and responsive mechanisms?	DORA
Risk Treatment	RM.56	FS Entity / Telco Entity	Has the entity defined appropriate cyber-threat intelligence (CTI) preventive and responsive capabilities?	DORA
Risk Assessment	RM.57	Telco Regulator	Does the regulator mandate network security audits to telcos entities?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.58	FS Regulator	Does the regulator mandate network security audits for financial entities?	DORA
Third-Parties	RM.59	FS Entity / Telco Entity	What mechanisms are in place to withstand network outages caused by Internet Service Providers (ISP)?	DORA
Third-Parties	RM.60	FS Regulator / Telco Regulator	Does the regulator mandate security mechanisms that entities need to implement to mitigate the risk of network saturation?	NIST SP 800-53 Rev. 4
Risk Treatment	RM.61	FS Entity / Telco Entity	Does the entity implement mechanisms to account for and mitigate network saturation?	DORA
Risk Treatment	RM.62	FS Entity / Telco Entity	Which of the following mechanisms is implemented to mitigate the risk of network saturation/power outages? 1) fault tolerance 2) clustering 3) network filtering 4) redundancy 5) high availability mechanisms	NIST SP 800-53 Rev. 4
Risk Assessment	RM.63	FS Regulator / Telco Regulator	Does the national/federal regulator mandate regular asset inventories?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.64	FS Regulator / Telco Regulator	Does the regulator mandate a structured process to identify data in transit and to ensure data confidentiality, integrity, and availability?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.65	FS Entity / Telco Entity	Has the entity conducted an asset inventory? Is it being consistently reviewed?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.66	FS Entity / Telco Entity	Does the entity conduct screening/background checks on new employees and staff terminating employment or changing responsibilities to mitigate insider threats? Are similar assessments conducted on all staff at regular intervals throughout their career, commensurate with staff's access to critical systems?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.67	FS Regulator / Telco Regulator	Does the regulator mandate asset management procedure also for DFS critical third-party services and entities?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.68	FS Regulator / Telco Regulator	Does the regulator mandate the definition of an asset management process?	NIST SP 800-53 Rev. 4

Domain	ID	Applicability	Question	Informative Reference
Risk Assessment	RM.69	FS Entity / Telco Entity	How often does the entity update the asset management process?	NIST SP 800-53 Rev. 4
Risk Assessment	RM.70	FS Entity / Telco Entity	Does the entity ensure that the asset management process and risk prioritisation process are aligned?	BIS Report Guidance for cyber resilience for FMIs[299]
Monitor and Review	RM.71	FS Entity / Telco Entity	Has the entity implemented measures to capture and analyse anomalous behaviour by persons accessing its systems (monitoring anomalies)?	BIS Report Guidance for cyber resilience for FMIs

[299] Committee On Payments and Market Infrastructures and Board of the International Organization of Security Commissions (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures.* Bank for International Settlements. Guidance on cyber resilience for financial market infrastructures (bis.org)

Governance Pillar

Domain	ID	Applicability	Question	Informative Reference
Communication Channels	GO.01	FS Entity / Telco Entity	Do you have a structured process to identify data in transit and detect incoming and outgoing communication?	NIST SP 800-53 Rev. 4
Third-Parties	GO.02	FS Entity / Telco Entity	Do you have a structured process for communicating with third-parties and suppliers? For example, do you conduct regular Due Diligence checks?	NIST SP 800-53 Rev. 4
Third-Parties	GO.03	FS Regulator / Telco Regulator	Are there mandatory processes for DFS entities to communicate with third-parties and establish external partnerships/relationships?	NIST SP 800-53 Rev. 4
Roles and Responsibilities	GO.04	FS Regulator / Telco Regulator	Do you have a clear internal structure and roles for the cyber defence to ensure accountability and a robust chain of command?	NIST SP 800-53 Rev. 4
Roles and Responsibilities	GO.05	FS Regulator / Telco Regulator	Does the regulator provide DFS entities with guidelines or requirements for establishing internal structure and roles and responsibilities allocation?	NIST SP 800-53 Rev. 4
Third-Parties	GO.06	FS Entity / Telco Entity	Do you know how your entity links with other suppliers to ensure cyber resilience in case of malicious lateral movement?	NIST SP 800-53 Rev. 4
Availability of Official Documentation	GO.07	FS Entity / Telco Entity	Does your entity have a cybersecurity policy?	NIST SP 800-53 Rev. 4
Availability of Official Documentation	GO.08	FS Regulator / Telco Regulator	Are DFS entities required to provide a cybersecurity policy?	NIST SP 800-53 Rev. 4
Roles and Responsibilities	GO.09	FS Entity / Telco Entity	Do you have clear IT/OT cybersecurity roles in your organisational chart?	NIST SP 800-53 Rev. 4
Monitoring and Review Process	GO.10	FS Entity / Telco Entity	Are you compliant with the local cybersecurity regulations and norms? Are you updated with the latest security directives, and do you constantly monitor ongoing legal changes?	NIST SP 800-53 Rev. 4
Monitoring and Review Process	GO.11	FS Entity / Telco Entity	Is there clear communication among DFS entities regarding cybersecurity regulations, norms, and directives?	NIST SP 800-53 Rev. 4
Third-Parties	GO.12	FS Entity / Telco Entity	Have you shared your cyber security policies and mandated minimum cyber requirements with your corporate partners and suppliers? Are you constantly in contact with them to discuss the latest cybersecurity developments?	NIST SP 800-53 Rev. 4
Third-Parties	GO.13	FS Entity / Telco Entity	Is there a mechanism to monitor the extent of DFS entities' network of suppliers to ensure effective communication of regulatory changes in mandated minimum cyber requirements?	NIST SP 800-53 Rev. 4
Third-Parties	GO.14	FS Regulator / Telco Regulator	Do you have a security collaboration program regarding your response and recovery planning activities with suppliers and partners? Do you regularly review this scheme?	NIST SP 800-53 Rev. 4
Roles and Responsibilities	GO.15	FS Regulator / Telco Regulator	Have you established a structured Identification Management (IM) mechanism to ensure accountability and mitigate the risk of unauthorised access?	NIST SP 800-53 Rev. 4

Domain	ID	Applicability	Question	Informative Reference
Availability of Official Documentation	GO.16	FS Entity / Telco Entity	Have you designed a system development life cycle for all your software programs and hardware devices? If yes, has it been shared with the IT and InfoSec teams?	NIST SP 800-53 Rev. 4
Monitoring and Review Process	GO.17	FS Entity / Telco Entity	Do you have a transparent process for repairing and maintaining organisational assets, including hardware and software? Do you require remote access from third-parties, or can you complete all maintenance cycles internally within the entity?	NIST SP 800-53 Rev. 4
Communication Channels	GO.18	FS Regulator / Telco Regulator	Do you have a designated Security Operation Centre (SOC) in place to monitor events and report issues of interest? Do you foster collaboration between the IT and InfoSec teams?	NIST SP 800-53 Rev. 4
Communication Channels	GO.19	FS Entity / Telco Entity	Do you communicate anomalies through direct and official channels? For example, is there direct, open, and clear communication between management and staff?	NIST SP 800-53 Rev. 4
Monitoring and Review Process	GO.20	FS Entity / Telco Entity	Does the entity assign and periodically examine budget constraints to ensure the functioning of all cybersecurity activities?	DORA
Roles and Responsibilities	GO.21	FS Regulator / Telco Regulator	Is the entity leadership involved in the definition and approval of a cyber resilience strategy?	DORA
Communication Channels	GO.22	FS Regulator / Telco Regulator	Does the entity guarantee information sharing with all stakeholders with regard to internal strategies and cyber resilience objectives?	DORA
Communication Channels	GO.23	FS Regulator / Telco Regulator	Does the entity communicate auditing plans to internal stakeholders?	DORA
Third-Parties	GO.24	FS Regulator / Telco Regulator	Are there mandatory requirements for third-parties and stakeholders' communication of audit activities?	DORA
Third-Parties	GO.25	FS Entity / Telco Entity	Does the entity establish and monitor communication channels with third-parties and suppliers?	DORA
Third-Parties	GO.26	FS Entity / Telco Entity	Is the entity's leadership constantly updated on changes to the agreements with third-parties and suppliers?	DORA
Third-Parties	GO.27	FS Entity / Telco Entity	If so, is the entity's leadership aware of such changes' impact?	DORA
Roles and Responsibilities	GO.28	FS Entity / Telco Entity	Is the entity's leadership aware of disruptive cyber-attacks to evaluate the impact of the incident, its responses, and future mitigation measures?	DORA
Communication Channels	GO.29	FS Entity / Telco Entity	Does the entity ensure alignment among all cyber resilience strategies and cybersecurity frameworks?	DORA
Communication Channels	GO.30	FS Entity / Telco Entity	Does the regulator ensure alignment among all cyber resilience regulations and frameworks? Does it provide instruments to simplify applicable regulation to DFs entities?	DORA
Roles and Responsibilities	GO.31	FS Entity / Telco Entity	Does the entity have an inventory of ICT-supported business functions with details of (i) roles and responsibilities, (ii) information assets and supporting ICT resources, (iii) roles and dependencies concerning IT risks?	DORA
Roles and Responsibilities	GO.32	FS Regulator / Telco Regulator	Are the national regulations mandating or providing elements for the establishment of (i) roles and responsibilities, (ii) information assets and supporting ICT resources, and (iii) roles and dependencies concerning IT risks?	DORA
Communication Channels	GO.33	FS Entity / Telco Entity	Does the entity have structured mechanisms and procedures in place for staff and contractors to report anomalies?	DORA

Domain	ID	Applicability	Question	Informative Reference
Roles and Responsibilities	GO.34	FS Entity / Telco Entity	Do the entity's functions include a profile responsible for crisis management?	DORA
Availability of Official Documentation	GO.35	FS Regulator / Telco Regulator	Does the entity have a mechanism in place to record the activities carried out while activating ICT-related "business continuity plans" and "response and recovery plans" that allow their accessibility to third-parties, if necessary?	DORA
Availability of Official Documentation	GO.36	FS Regulator / Telco Regulator	Do you mandate entities to implement an activity log after activating ICT-related business continuity and response and recovery plans?	DORA
Roles and Responsibilities	GO.37	FS Regulator / Telco Regulator	Do you know the role your entity places in the DFS environment and how critical its functions are to a successful DFS operation?	NIST SP 800-53 Rev. 4
Roles and Responsibilities	GO.38	FS Entity / Telco Entity	Are your suppliers and partners aware of the chain of command in your entity, and do they have a designated point of contact in case of emergency?	NIST SP 800-53 Rev. 4
Roles and Responsibilities	GO.39	FS Regulator / Telco Regulator	Are DFS entities mandated to provide third-parties with a designated point of contact in an emergency?	NIST SP 800-53 Rev. 4
Monitoring and Review Process	GO.40	FS Entity / Telco Entity	Does the entity consider continuously monitoring technological developments and studies to understand the potential impacts of deploying emerging technologies on ICT security and digital operational resilience requirements?	DORA
Monitoring and Review Process	GO.41	FS Regulator / Telco Regulator	Do regulators mandate digital operational resilience requirements? If so, are these requirements updated by continuously monitoring technological developments and the impact of emerging technologies?	DORA
Third-Parties	GO.42	FS Regulator / Telco Regulator	Does the regulator mandate entities establish contractual agreements with providers to minimise the impact of network outages caused by third-party interdependencies?	DORA
Third-Parties	GO.43	FS Entity / Telco Entity	Do you have contractual agreements in place with third-parties to minimise the impact of network outages caused by interdependencies?	DORA
Monitoring and Review Process	GO.44	FS Entity / Telco Entity	Does the entity have a process for identifying and mitigating potential single points of failure in its technology infrastructure, particularly in the telco and DFS sectors?	NIST SP 800-53 Rev. 4
Monitoring and Review Process	GO.45	FS Regulator / Telco Regulator	Does the regulator mandate a process to identify single points of failure and mitigate the risk of a disruptive incident?	NIST SP 800-53 Rev. 4
Monitoring and Review Process	GO.46	FS Entity / Telco Entity	Does the entity measure the success and effectiveness of its cyber resilience program, and are these metrics used to drive continuous improvement and inform decision-making?	DORA
Monitoring and Review Process	GO.47	FS Regulator / Telco Regulator	Has the regulator identified common Key Performance Metrics (KPI) to assess the DFS entities' cyber resilience programs?	DORA
Availability of Official Documentation	GO.48	FS Entity / Telco Entity	Has the DFS entity's board designed and applied a Cyber Resilience strategy?	BIS Report Guidance for cyber resilience for FMIs
Availability of Official Documentation	GO.49	FS Entity / Telco Entity	Has the DFS entity's board designed and applied a Cyber Resilience Framework?	BIS Report Guidance for cyber resilience for FMIs

Domain	ID	Applicability	Question	Informative Reference
Monitoring and Review Process	GO.50	FS Entity / Telco Entity	Are the DFS entity's cybersecurity policies aligned with national and international standards?	BIS Report Guidance for cyber resilience for FMIs
Roles and Responsibilities	GO.51	FS Entity / Telco Entity	Is the DFS entity's management and board members, as ultimately responsible for the effectiveness of the entity's cyber resilience measures, aware of existing threats, risk management measures, and implementation of the entity's mitigation measures?	BIS Report Guidance for cyber resilience for FMIs
Communication Channels	GO.52	FS Entity / Telco Entity	Is the DFS entity's management committed to promoting strong cybersecurity culture within the entity?	BIS Report Guidance for cyber resilience for FMIs
Roles and Responsibilities	GO.53	FS Entity / Telco Entity	Is the DFS entity ensuring that the board and senior management members possess the appropriate skills and knowledge to understand and manage the risks posed by cyber threats common to the DFS environment?	BIS Report Guidance for cyber resilience for FMIs
Roles and Responsibilities	GO.54	FS Entity / Telco Entity	Has the DFS entity established a process to designate a senior executive responsible and accountable for the internal cyber resilience framework?	BIS Report Guidance for cyber resilience for FMIs
Roles and Responsibilities	GO.55	FS Regulator / Telco Regulator	Does the Regulator mandate establishing a process to designate a senior executive to be responsible and accountable for the cyber resilience framework within the DFS entity?	BIS Report Guidance for cyber resilience for FMIs
Availability of Official Documentation	GO.56	FS Entity / Telco Entity	Does the DFS entity implement procedures for identifying, collecting, acquiring, and preserving evidence related to information security events?	ISO 2022:27001
Availability of Official Documentation	GO.57	FS Entity / Telco Entity	Does the management ensure that internal cybersecurity operating procedures are documented and available to internal personnel and external stakeholders?	ISO 2022:27001

Testing Pillar

Domain	ID	Applicability	Question	Informative Reference
Vulnerability Scanning	TE.01	FS Entity / Telco Entity	Have you ever conducted a vulnerability assessment and have a vulnerability management plan in place?	NIST SP 800-53 Rev. 4
Vulnerability Scanning	TE.02	FS Regulator / Telco Regulator	Do you mandate vulnerability assessments on all DFS critical and non-critical entities?	NIST SP 800-53 Rev. 4
Vulnerability Scanning	TE.03	FS Entity / Telco Entity	Have you ever performed vulnerability scans and pentesting to ensure you monitor and know all potential entry points?	NIST SP 800-53 Rev. 4
Vulnerability Scanning	TE.04	FS Regulator / Telco Regulator	Do you mandate that entities regularly test their vulnerability detection processes?	NIST SP 800-53 Rev. 4
Vulnerability Scanning	TE.05	FS Entity / Telco Entity	Do you test your vulnerability detection processes and ensure a regular update of all your asset's life cycles?	NIST SP 800-53 Rev. 4
Vulnerability Scanning	TE.06	FS Entity / Telco Entity	Are detection processes updated and improved on a regular basis?	NIST SP 800-53 Rev. 4
Simulations and War Gaming	TE.07	FS Entity / Telco Entity	Do you complete mock response tests to ensure preparedness and a swift response during an emergency?	NIST SP 800-53 Rev. 4
Simulations and War Gaming	TE.08	FS Entity / Telco Entity	Do you implement testing sessions to measure the digital resilience of your entity? If so, are these included in your entity's strategy?	DORA
Simulations and War Gaming	TE.09	FS Regulator / Telco Regulator	Do you mandate testing sessions for DFS critical and non-critical entities?	DORA
Simulations and War Gaming	TE.10	FS Entity / Telco Entity	Does the entity's cyber strategy include testing sessions to measure corporate digital resilience?	DORA
Simulations and War Gaming	TE.11	FS Regulator / Telco Regulator	Do you mandate entities to develop, document, and periodically test backup policies and procedures, as well as procedures and mechanisms for recovery and restoration of ICT-related systems?	DORA
Simulations and War Gaming	TE.12	FS Entity / Telco Entity	Does the entity have in place the development, documentation, and periodic testing of "backup policies and procedures" and "recovery and restoration procedures and methods" for ICT-related systems?	DORA
Simulations and War Gaming	TE.13	FS Entity / Telco Entity	Do you periodically test your ICT systems, protocols, tools, cyber risk management framework, business continuity plans and related response and recovery measures? Are these formalised in a testing plan?	DORA

Domain	ID	Applicability	Question	Informative Reference
Simulations and War Gaming	TE.14	FS Entity / Telco Entity	Does the entity have a periodic testing plan for ICT systems, protocols, tools, a Cyber Risk Management Framework, business continuity plans, and related response and recovery measures?	DORA
Simulations and War Gaming	TE.15	FS Entity / Telco Entity	Does the entity's testing program specify the following elements? a. Scenarios considered b. Scenarios for which it is expected to remain within impact tolerance levels c. Frequency of testing d. The number of important business services tested e. Availability and integrity of supporting assets f. Communication plans in case of disruption	DORA
Simulations and War Gaming	TE.16	FS Entity / Telco Entity	When changes are made to critical business services and/or associated impact tolerance levels, does the entity conduct testing?	DORA
Red Teaming	TE.17	FS Entity / Telco Entity	Does the entity assign threat-based Penetration Testing to subjects with the highest level of independence?	DORA
Simulations and War Gaming	TE.18	FS Regulator / Telco Regulator	Do you mandate implementing a structured process to incorporate lessons learned from previous ICT-related incidents to improve the recovery and response mechanisms of the entities?	DORA
Simulations and War Gaming	TE.19	FS Entity / Telco Entity	Does the entity have a structured process for improving the recovery and response processes in case of a disruption based on the lessons learned from testing?	DORA
Penetration Testing	TE.20	FS Regulator / Telco Regulator	Do you mandate the conduction of scenario-based Penetration Testing?	DORA
Penetration Testing	TE.21	FS Entity / Telco Entity	Does the entity ever conduct scenario-based Penetration Testing in a production environment?	DORA
Simulations and War Gaming	TE.22	FS Entity / Telco Entity	Do the scenarios tested by the entity include at least the following? - Corruption/deletion/manipulation of critical data for essential business services - Unavailability of critical buildings/staff - Unavailability of critical third-party services for critical business services - Disruption to other market operators - Loss or reduction in the supply of underlying technology for critical business services	DORA
Vulnerability Scanning	TE.23	FS Regulator / Telco Regulator	Do you mandate the conduction of vulnerability assessments before releasing new or existing ICT products and services into the market?	DORA
Vulnerability Scanning	TE.24	FS Entity / Telco Entity	Does the entity conduct vulnerability assessments before releasing new or existing applications, infrastructure components, and ICT services that support essential or critical functions?	DORA
Red Teaming	TE.25	FS Regulator / Telco Regulator	Do you mandate Threat Led Penetration Testing (Red Teaming) exercises?	DORA
Red Teaming	TE.26	FS Entity / Telco Entity	Has the entity conducted Threat Led Penetration Testing (Red Teaming) in the last three years?	DORA

Domain	ID	Applicability	Question	Informative Reference
Simulations and War Gaming	TE.27	FS Regulator / Telco Regulator	Do you mandate entities to review and test business continuity and recovery plans periodically?	DORA
Simulations and War Gaming	TE.28	FS Entity / Telco Entity	Are the business continuity and recovery plans subject to periodic review and testing?	BIS Report Guidance for cyber resilience for FMIs
Simulations and War Gaming	TE.29	FS Regulator / Telco Regulator	Do you mandate business continuity and recovery plan testing to address potential risks or disaster scenarios?	DORA
Simulations and War Gaming	TE.30	FS Entity / Telco Entity	Do the business continuity and recovery plans test address different potential risks/disaster scenarios, including Simulation of cyber-attacks/disasters, and designed to assess the defined RTOs and RPOs, resumption and recovery practices, including governance arrangements and communication plans?	BIS Report Guidance for cyber resilience for FMIs
Simulations and War Gaming	TE.31	FS Regulator / Telco Regulator	Do you mandate entities to organise tests that assess staff's understanding of emergency processes and procedures?	NIST SP 800-53 Rev. 4
Simulations and War Gaming	TE.32	FS Entity / Telco Entity	Do the test exercises also assess the ability of staff and processes to respond to unfamiliar scenarios to achieve stronger operational resilience?	BIS Report Guidance for cyber resilience for FMIs
Vulnerability Scanning	TE.33	FS Regulator / Telco Regulator	Do you mandate the incorporation of cyber threat intelligence in the design of tests and scenarios?	NIST SP 800-53 Rev. 4
Vulnerability Scanning	TE.34	FS Entity / Telco Entity	Does the entity make use of the cyber intelligence threat process to design its tests and plausible scenarios?	BIS Report Guidance for cyber resilience for FMIs
Simulations and War Gaming	TE.35	FS Regulator / Telco Regulator	Do you mandate entities to design and test their systems and processes to ensure the timely recovery of accurate data in case of an ICT-related breach?	BIS Report Guidance for cyber resilience for FMIs
Simulations and War Gaming	TE.36	FS Entity / Telco Entity	Has the entity designed and tested its systems and processes to provide the recovery of accurate data following a breach?	NIST SP 800-53 Rev. 4
Third-Parties	TE.37	FS Entity / Telco Entity	Do the scenarios tested specifically address third-parties related capabilities, such as: - Unavailability of critical third-party services for critical business services - Disruption to other market operators - Loss or reduction in the supply of underlying technology for critical business services	DORA
Third-Parties	TE.38	FS Entity / Telco Entity	Does the entity extend the scope of testing activities to critical services third-party providers?	DORA
Third-Parties	TE.39	FS Regulator / Telco Regulator	Does the regulator mandate testing of all third-party interdependencies?	DORA

Domain	ID	Applicability	Question	Informative Reference
Third-Parties	TE.40	FS Entity / Telco Entity	Does the entity organise joint testing campaigns with third-parties?	DORA G-7 Fundamental elements for threat-led penetration testing
Penetration Testing	TE.41	FS Entity / Telco Entity	Does the entity integrate cyber-threat intelligence within Penetration Testing exercises?	NIST SP 800-115[300]
Third-Parties	TE.42	FS Entity / Telco Entity	Does the entity stress-test third-party systems and network interconnections?	DORA G-7 Fundamental elements for threat-led penetration testing

[300] NIST. (2008). *Technical Guide to Information Security Testing and Assessment (NIST.SP-115)*. National Institute of Standards and Technology. Technical guide to information security testing and assessment (nist.gov)

Training and Awareness Pillar

Domain	ID	Applicability	Question	Informative Reference
Employee Training	TA.01	FS Entity / Telco Entity	Are your personnel and staff properly trained in the risks connected to the internet? These include phishing, fraud, malware characteristics, and other social engineering schemes.	NIST SP 800-53 Rev. 4
Employee Training	TA.02	FS Regulator / Telco Regulator	Do you mandate the training of personnel and staff in internet-related risks?	NIST SP 800-53 Rev. 4
Employee Training	TA.03	FS Entity / Telco Entity	Are employees with privileged access to the network aware of their roles within the entity and the risks connected to them?	NIST SP 800-53 Rev. 4
Employee Training	TA.04	FS Entity / Telco Entity	Is your corporate management aware of internal cybersecurity procedures and their roles in identifying, coordinating, and responding to cyber incidents?	NIST SP 800-53 Rev. 4
Employee Training	TA.05	FS Regulator / Telco Regulator	Do you mandate the promotion of cyber risks awareness campaigns and cyber hygiene practices at all levels of the DFS ecosystem?	DORA
Employee Training	TA.06	FS Entity / Telco Entity	Does the leadership actively promote a strong awareness of cyber risks and commitment to adhere to cyber hygiene practices at every level of the entity and among all employees?	DORA
Employee Training	TA.07	FS Entity / Telco Entity	Does the entity's leadership have a high degree of cybersecurity understanding and knowledge?	DORA
Employee Training	TA.08	FS Entity / Telco Entity	Do members of the entity's leadership maintain their competencies on cybersecurity and cyber resilience constantly up to date?	DORA
Employee Training	TA.09	FS Regulator / Telco Regulator	Do you mandate staff training to ensure that cybersecurity skills are constantly updated and uplifted?	DORA
Employee Training	TA.10	FS Entity / Telco Entity	Does the entity ensure that staff's cybersecurity skills and competencies are constantly updated and /or uplifted?	DORA
Information-Sharing Practices	TA.11	FS Entity / Telco Entity	Does your entity manage external communication to end-users about ongoing malicious cyber campaigns targeting the DFS?	DORA
Employee Training	TA.12	FS Entity / Telco Entity	Has the entity implemented the necessary training for the person responsible for the corporate cyber threat intelligence capabilities?	DORA
Employee Training	TA.13	FS Entity / Telco Entity	Has the entity defined training sessions on cyber-threat capabilities for staff and corporate management?	DORA
Information-Sharing Practices	TA.14	FS Entity / Telco Entity	To ensure full transparency, do you continuously share training material and practices with internal staff and external partners?	DORA
Information-Sharing Practices	TA.15	FS Regulator / Telco Regulator	Do you have mechanisms in place to promote information-sharing practices within your sector/community?	DORA

Domain	ID	Applicability	Question	Informative Reference
Information-Sharing Practices	TA.16	FS Entity / Telco Entity	Has the entity established functional intelligence-gathering cyber threat intelligence capabilities, including information sharing and scenario prevention?	DORA
Third-Parties	TA.17	FS Entity / Telco Entity	Is there a mechanism to assess whether third-party staff has been properly trained on cybersecurity skills and competencies?	DORA
Third-Parties	TA.18	FS Regulator / Telco Regulator	Do you mandate entities to coordinate with relevant external stakeholders on third-party-led cybersecurity awareness campaigns?	DORA
Third-Parties	TA.19	FS Entity / Telco Entity	Does the entity coordinate externally on third-party-led awareness campaigns?	DORA
Third-Parties	TA.20	FS Entity / Telco Entity	Do you implement mechanisms to promote the upskilling of third-party cybersecurity capabilities?	DORA
Third-Parties	TA.21	FS Regulator / Telco Regulator	Does the entity promote the upskilling of third-party cybersecurity capabilities?	DORA
Information-Sharing Practices	TA.22	FS Regulator / Telco Regulator	Do you support the implementation of industry-wide information-sharing practices among cybersecurity teams?	NIST SP 800-53 Rev. 4
Information-Sharing Practices	TA.23	FS Entity / Telco Entity	Do you ensure information sharing and regularly meet with cybersecurity teams from partner companies?	NIST SP 800-53 Rev. 4
Employee Training	TA.24	FS Regulator / Telco Regulator	Has the regulator mandated specialised training to recognise phishing activities?	NIST SP 800-53 Rev. 4
Employee Training	TA.25	FS Entity / Telco Entity	Has your staff been trained to recognise phishing activities?	NIST SP 800-53 Rev. 4
Employee Training	TA.26	FS Regulator	Do you mandate entities to provide specific physical security training to staff handling telco communications and dependencies?	NIST SP 800-53 Rev. 4
Employee Training	TA.27	FS Entity	Do you organise specific training on physical security (e.g., USB compromise, cutting network cabling) for staff handling telco communications and dependencies?	NIST SP 800-53 Rev. 4
Information-Sharing Practices	TA.28	FS Entity / Telco Entity	Do you participate in information-sharing groups, including cross-industry, cross-government, and cross-border groups, to gather, distribute and assess information about cyber threats and early warning indicators?	BIS Report Guidance for cyber resilience for FMIs
Employee Training	TA.29	FS Regulator / Telco Regulator	Does the regulator issue mandatory training on threats and risks specific to the DFS environment?	NIST SP 800-53 Rev. 4
Employee Training	TA.30	FS Entity / Telco Entity	Does the entity facilitate staff training on risks and threats specific to the DFS environment?	NIST SP 800-53 Rev. 4
Employee Training	TA.31	FS Entity / Telco Entity	Does the entity include information and/or inputs specific to the DFS environment in its training sessions?	NIST SP 800-53 Rev. 4
Information-Sharing Practices	TA.32	FS Entity / Telco Entity	Do you have information-sharing plans established to communicate timely information that could facilitate the detection, response, resumption, and recovery of your systems in a cyber incident?	BIS Report Guidance for cyber resilience for FMIs

Domain	ID	Applicability	Question	Informative Reference
Third-Parties	TA.33	FS Entity / Telco Entity	Do your information-gathering cyber threat intelligence capabilities include scenarios with DFS threats derived from external sources, especially third-party interdependencies?	BIS Report Guidance for cyber resilience for FMIs
Employee Training	TA.34	FS Entity	Has the entity defined training sessions to mitigate the potential impact of a cyber incident targeting its telco provider on its own systems and networks?	DORA
Employee Training	TA.35	Telco Entity	Do you organise training sessions with FS customers to ensure staff on both entities is able to mitigate the potential impact of a cyber incident targeting your entity?	DORA
Employee Training	TA.36	FS Regulator / Telco Regulator	Do you mandate FS and Telco entities to organise joint training sessions to inform and prepare staff to deal with cyber incident targeting either or both entities?	DORA
Information-Sharing Practices	TA.37	FS Entity / Telco Entity	Have you established responsible disclosure policies to share potential vulnerabilities with the industry community and/or relevant regulators to ensure the stability of the DFS ecosystem?	BIS Report Guidance for cyber resilience for FMIs
Information-Sharing Practices	TA.38	FS Regulator / Telco Regulator	Do you implement an industry-wide responsible disclosure policy for entities to share potential vulnerabilities identified to ensure the stability of the DFS ecosystem? If so, are entities mandated to share relevant findings with regulators as well?	BIS Report Guidance for cyber resilience for FMIs
Third-Parties	TA.39	FS Entity / Telco Entity	Have you established responsible disclosure policies with your third-party providers? If so, do these define notification and collaboration timelines to activate when shared vulnerabilities are identified?	BIS Report Guidance for cyber resilience for FMIs
Third-Parties	TA.40	FS Regulator / Telco Regulator	Do you mandate entities to include responsible disclosure policies and data-sharing agreements with their third-party providers? If so, do you provide specific guidance or minimum thresholds to support entities in establishing such policies?	BIS Report Guidance for cyber resilience for FMIs
Employee Training	TA.41	FS Entity / Telco Entity	Do you provide training sessions to staff responsible for handling vulnerability disclosures?	BIS Report Guidance for cyber resilience for FMIs
Employee Training	TA.42	FS Regulator / Telco Regulator	Do you mandate entities to provide training sessions for staff responsible for handling vulnerability disclosures to the wider community?	BIS Report Guidance for cyber resilience for FMIs

Protection Pillar

Domain	ID	Applicability	Question	Informative Reference
Enterprise Policy	PR.01	FS Entity / Telco Entity	Have you tracked software installations into your devices, and have you set up a thorough check of staff's personal devices in case of a hybrid Bring-your-own-device (BYOD) policy?	NIST SP 800-53 Rev. 4
Filter Network Traffic	PR.02	FS Entity / Telco Entity	Do you issue a process model to identify data in transit and detect incoming and outgoing communication?	NIST SP 800-53 Rev. 4
Filter Network Traffic	PR.03	FS Entity / Telco Entity	Do you have a structured process to identify data in transit and detect incoming and outgoing communication?	NIST SP 800-53 Rev. 4
Enterprise Policy	PR.04	FS Entity	Does your entity set timeouts and auto-logout user sessions on DFS applications (logical sessions)? Within the application, do you ensure support for password complexity (enforced by the server), set maximum unsuccessful login attempts, password history and reuse periods, and account lock-out periods to a reasonably minimal value?	PCI DSS[301] PA DSS[302] ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.05	FS Entity	Does your entity require user identity validation for dormant DFS account users before re-activating accounts?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.06	FS Entity	Does your entity limit access to DFS services based on user locations (for example, disable access to DFS USSD codes while roaming, STK and SMS for merchants and agents) where possible, restrict access by region for DFS agents, where possible, check that agent and number performing a deposit or withdrawals are within the same serving area?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Privileged Account Management	PR.07	FS Entity	Does your entity restrict DFS services by communication channels (during registration, customers should optionally choose service access channel, USSD only, STK only, app only, or a combination) attempted DFS access through channels other than opted should be blocked and red-flagged?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.08	FS Regulator	Do you mandate the implementation of any client-side authentication or authorisation token?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

[301] PCI Security Standards Council (2022). *Data Security Standard.* https://www.pcisecuritystandards.org/document_library/
[302] PCI Security Standards Council (2013). *Payment Application Data Security Standard*. https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf

Domain	ID	Applicability	Question	Informative Reference
Multi-Factor Authentication	PR.09	FS Entity	Does the DFS system trust any client-side authentication or authorisation tokens? Is the validation of access tokens performed on the server side?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.10	FS Entity	Does your entity store DFS passwords using robust salted cryptographic hashing algorithms?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.11	FS Entity / Telco Entity	Does your entity add session timeouts for USSD, SMS, application, and web access to DFS services?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.12	FS Entity	Does your entity allow to set DFS users with their own passwords at registration, encrypted throughout the transmission to the DFS system? Where first-time credentials are sent to the users, ensure DFS application credentials are sent to users directly without third-parties/agents. Users should then be required to set new passwords after the first-time login.	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.13	FS Entity / Telco Entity	Does your entity require the use of longer and not easily guessed PINs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.14	FS Entity / Telco Entity	Are the DFS applications designed to verify the server's name they are connecting to?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.15	FS Regulator / Telco Regulator	Do you enforce processes and mechanisms to limit the number of attempted logins or unauthorised access?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.16	FS Entity / Telco Entity	Does your entity enforce a maximum number of login attempts to DFS accounts for back-end users, merchants, agents and DFS customers on DFS systems (database, OS, application)?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Filter Network Traffic	PR.17	FS Entity	Does your entity allow mobile users to trust or distrust individual binary-based SMS messages?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.18	FS Entity / Telco Entity	Does your entity securely transmit DFS providers' user authentication credentials over a different channel (out of band)?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.19	FS Entity / Telco Entity	Does your entity use Network Address Translation to limit external exposure of DFS IP address and routing information?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.20	FS Regulator / Telco Regulator	Does the regulator enforce the use of Demilitarized Zones (DMZs) or other mechanisms to filter incoming network traffic?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.21	FS Entity / Telco Entity	Does your entity avoid direct access by external systems to the DFS backend systems by setting up a DMZ that logically separates the DFS system from all other internal and external systems?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.22	FS Entity / Telco Entity	Does your entity ensure that security libraries offered by the operating system are correctly designed and implemented and that the cypher suites they support are sufficiently strong?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.23	FS Entity / Telco Entity	Do you ensure that all sensitive consumer data, such as PINs and passwords, are encrypted when traversing the network and while the data is at rest?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.24	FS Entity / Telco Entity	Does your entity remove customer-sensitive data from trace logs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Enterprise Policy	PR.25	FS Entity / Telco Entity	Do you restrict the sharing of information to be only the minimum amount required for transactions with third-parties and service providers?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.26	FS Entity / Telco Entity	Does your entity monitor APIs and encrypt all data shared with third-parties? Additionally, do you implement data management procedures and controls, such as signed non-disclosure agreements with payment service providers, to avoid information/data leakage?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.27	FS Entity / Telco Entity	Does your entity protect its network against attacks using firewalls and traffic filters, and protect against DFS infrastructure threats by challenging suspicious traffic through network admission techniques and mechanisms such as CAPTCHAs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.28	FS Entity / Telco Entity	Does your entity limit inbound internet traffic and continuously monitor it?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.29	FS Regulator / Telco Regulator	Do you issue restrictive firewall rules by default? If so, how detailed are they?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.30	FS Entity / Telco Entity	Does your entity set restrictive firewall rules by default? For example, does it use port whitelisting, packet filters, and continuously monitor access to whitelisted/permitted ports and IPs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Privileged Account Management	PR.31	FS Entity / Telco Entity	Where possible, does your entity limit critical changes using the Segregation of Duties principle for critical actions, including (but not limited to) an administrator creating, modifying, or deleting another administrator account, changing, attaching, and detaching of DFS account from mobile number/user ID, and transaction reversal?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.32	FS Entity / Telco Entity	Does your entity have robust input validation routines on external-facing services by checking out-of-range values and unpermitted characters in fields and constraining and sanitising input? Additionally, does your organisation block, log and review all requests that violate the Web Services Description Language (WSDL) and schemas?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Encrypt Sensitive Information	PR.33	FS Entity / Telco Entity	Does your entity use database fingerprinting/digital signatures to detect tampering and modification of data after storing it?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.34	FS Entity / Telco Entity	Does your entity assure clock accuracy synchronisation on all systems connected to the DFS system?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.35	FS Entity / Telco Entity	Do you mask user passwords and PINs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.36	FS Regulator / Telco Regulator	Do you enforce robust cryptographic algorithms on all DFS sensitive information and infrastructure?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.37	FS Entity / Telco Entity	Do you still use A5/0, A5/1, and A5/2 GSM encryption cyphers? Do you have a deployment strategy ready for these newer cyphers?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.38	FS Entity	Do you perform CLI analysis for calls/SMS to detect calls and SMS that may be spoofed to appear as DFS provider calls?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.39	FS Regulator / Telco Regulator	Do you mandate entities to implement user authentication and authorisation for high-risk account changes and transactions?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.40	FS Entity / Telco Entity	Does your entity require user authentication and authorisation for high-risk account changes and transactions and deny performing transactions even when the device is logged in until knowledge of PIN or password has been demonstrated?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Enterprise Policy	PR.41	FS Entity / Telco Entity	Does your entity have in place procedural and technical controls for effective management during system downtime with related service providers? For example, set controls to manage offline transactions (e.g., SIM swaps) when access to the DFS system is intermittent. Have additional checks for remittances and third-party payments when the DFS system or 3rd party system access is intermittent.	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.42	FS Entity / Telco Entity	Does your entity use multi-factor or multi-model authentication for access to DFS accounts?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.43	FS Entity / Telco Entity	Does your entity deactivate and remove default accounts and credentials from databases, applications, operating systems, and other access interfaces that interact with the production DFS system?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Data Loss Prevention	PR.44	FS Entity / Telco Entity	Do you perform end-to-end tests after any changes to the DFS, MNO, SP, and third-party systems, including regression and capacity tests in the acceptance tests? Also, do you have a fall-back/blackout plan?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Data Loss Prevention	PR.45	FS Entity / Telco Entity	Do you use standard ACID (Atomicity, Consistency, Isolation, Durability) functionality of the databases to ensure transaction integrity?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.46	Telco Entity	Does your entity ensure an identity verification process is in place before SIM swaps are performed?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.47	Telco Entity	Is your entity able to detect in real-time whenever a SIM card with DFS services has been swapped or replaced? For example, before any high-value transactions or account changes are authorised with a new SIM, do you verify further?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.48	Telco Entity	Do you safeguard and securely store SIM data like IMSI and SIM secret key values (KI values)?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Multi-Factor Authentication	PR.49	Telco Entity	When a SIM is recycled, the mobile operator will report a new IMSI of the related account phone number. Do you block the account until the identity of the new person holding the SIM card is verified as the account holder?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.50	Telco Entity	Does your entity have procedures to detect and avert suspicious SIM swaps and recycling?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.51	FS Entity / Telco Entity	Does your entity protect its systems against tampering and allow only online transactions?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.52	FS Entity	Do you check incoming data against expected values in the API-related data schema for USSD and perform XML validation of XML over HTTP requests?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.53	FS Entity	Do you have analytics systems in place to check user velocity between transactions, transaction time of day access tracking for additional authorisation validation checks?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.54	FS Entity / Telco Entity	Regardless of the method used for producing receipts (e.g., e-mail, SMS, or attached printer), do you mask the Primary Account Number (PAN) in support of applicable laws, regulations, and payment-card policies?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.55	FS Entity	Do you enforce the use of Secure OTP to the original phone number to verify the transaction's legitimacy?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Filter Network Traffic	PR.56	FS Entity	Do you limit the number of DFS sessions per user?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Security Updates	PR.57	FS Entity / Telco Entity	Do you use firewalls to detect and limit attacks based on SS7 security flaws? For example, does your organisation deploy SS7 and diameter signalling security controls specified by the GSMA (FS.11, FS.07, IR.82, and IR.88) to limit threats due to SS7 attacks?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
SSL-TLS Inspection	PR.58	FS Entity / Telco Entity	Do you use strong encryption standards like TLS encryption v1.2 and higher for API communication? Does your organisation extend threat detection to explicitly incorporate threats associated with APIs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.59	FS Entity / Telco Entity	Do you limit remote login access and minimise privileges to remote login sessions to backend DFS systems?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
SSL-TLS Inspection	PR.60	FS Entity / Telco Entity	Do you limit the lifetime of TLS certificates?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Privileged Account Management	PR.61	FS Entity / Telco Entity	Do you authenticate user IP, device, and login time for all privileged users, agents, and merchants connecting to the DFS system?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Security Updates	PR.62	FS Entity / Telco Entity	Does your entity deploy and regularly update security software products on all devices, including antivirus, antispyware, and software authentication, to protect systems from current and evolving malicious software threats?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.63	FS Entity / Telco Entity	Do you implement a formalised process to monitor assets' life cycles?	DORA
Enterprise Policy	PR.64	FS Regulator / Telco Regulator	Do you mandate a formalised process to monitor assets' life cycles?	DORA
Enterprise Policy	PR.65	FS Entity / Telco Entity	Does your entity set timeouts and auto-logout user sessions on DFS applications (logical sessions)? Then, within the application, does the entity ensure support for password complexity (enforced by the server), set maximum unsuccessful login attempts, password history and reuse periods, and account lock-out periods to a reasonably minimal value?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Encrypt Sensitive Information	PR.66	FS Regulator / Telco Regulator	Do you mandate storing DFS passwords using robust salted cryptographic hashing algorithms?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.67	FS Regulator / Telco Regulator	Do you mandate strong security measures to assure authenticity, such as policies on passwords, credentials, and PINs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.68	FS Regulator / Telco Regulator	Do you mandate entities to remove customer-sensitive data from trace logs?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Encrypt Sensitive Information	PR.69	FS Regulator / Telco Regulator	Do you mandate monitoring API's usage and implementing cryptographic measures to cover all data shared with third-parties? For example, are additional data management controls encouraged/mandated (e.g., NDAs) with payment service providers?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.70	FS Entity / Telco Entity	Do you implement procedural and technical controls for effective management during system downtime? For example, do you implement additional checks for remittances and third-party payments?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.71	FS Entity / Telco Entity	Does your entity have in place procedural and technical controls for effective management during system downtime with related service providers? For example, set controls to manage offline transactions (e.g., SIM swaps) when access to the DFS system is intermittent	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.72	FS Regulator / Telco Regulator	Do you mandate using multi-factor or multi-model authentication to access DFS accounts?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.73	Telco Regulator	Do you mandate measures to securely store SIM data and confidential information, including data encryption?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Domain	ID	Applicability	Question	Informative Reference
Enterprise Policy	PR.74	FS Regulator / Telco Regulator	Do you issue regulations/best practices on proper SIM and other hardware recycling or sanitisation?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.75	Telco Regulator	Do you mandate the implementation of plans and procedures to detect and avert suspicious SIM malicious abuse?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.76	FS Regulator / Telco Regulator	Do you mandate the definition of analytics systems to check transaction validation and the user's identity?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Multi-Factor Authentication	PR.77	FS Regulator	Do you mandate the implementation of secure One Time Passwords (OTP) to verify the transaction's legitimacy?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Enterprise Policy	PR.78	FS Regulator / Telco Regulator	Do you enforce a mechanism to limit the number of DFS sessions per user?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework
Exploit Protection	PR.79	FS Regulator / Telco Regulator	Do you mandate the regular update of software products on all devices, including antivirus, antispyware, and software authentication products?	PCI DSS PA DSS ITU Digital Financial Services security assurance framework

Incident Response Pillar

Domain	ID	Applicability	Question	Informative Reference
Incident Response Reporting	IR.01	FS Entity / Telco Entity	Do you have a mechanism in place to share information and data of attempted or successful cyber incidents with your clients, and partners?	NIST SP 800-53 Rev. 4
Incident Response Reporting	IR.02	FS Regulator / Telco Regulator	Do you mandate the implementation of mechanisms to share information and data of attempted or successful cyber incidents with the entity's relevant internal and external stakeholders?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.03	FS Regulator / Telco Regulator	Do you mandate a threat categorisation and prioritisation process to withstand cyber intrusions according to individual operational needs?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.04	FS Entity / Telco Entity	Have you gone through a threat categorisation process to prioritise incoming menaces and counteract them accordingly based on operational needs?	NIST SP 800-53 Rev. 4
Third-Parties	IR.05	FS Entity / Telco Entity	Are you aware of any remote access done by third-parties (e.g., Original Equipment Manufacturers (OEMs)) into your network, even if only for a remote software update?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.06	FS Entity / Telco Entity	Is your network segregated, and have you set up VLANS, firewalls, and authentication barriers to ensure defence-in-depth?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.07	FS Regulator / Telco Regulator	Do you have measures in place to mandate encryption techniques for data-at-rest?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.08	FS Entity / Telco Entity	Is your data-at-rest encrypted, and do you have extra mitigation measures for information stored in highly-classified/confidential servers?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.09	FS Regulator / Telco Regulator	Do you mandate security mechanisms to control data in transit? For example, do you mandate security provisions to limit access to harmful applications?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.10	FS Entity / Telco Entity	Do you control data in transit both within and external to the entity? Do you collaborate with your InfoSec team to restrict the use of potentially harmful applications, such as social media platforms or instant messaging?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.11	FS Entity / Telco Entity	Do you ensure data availability and high availability for your critical servers? Are you aware of instances in which a power supply outage interrupted the service for a long period?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.12	FS Entity / Telco Entity	Do you mandate the verification of software integrity and the regular implementation of security patches of software external to the entity?	NIST SP 800-53 Rev. 4

Domain	ID	Applicability	Question	Informative Reference
Incident Response Life Cycle	IR.13	FS Entity / Telco Entity	Do you verify software integrity and regularly update firmware programs to mitigate the risk of unpatched software exploitation?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.14	FS Entity / Telco Entity	Have incremental and differential back-ups been set up for data in line with the internal corporate strategy? How often do you complete backups?	NIST SP 800-53 Rev. 4
Incident Response Governance	IR.15	FS Regulator / Telco Regulator	Do you mandate the development of incident response plans and procedures for entities?	NIST SP 800-53 Rev. 4
Incident Response Governance	IR.16	FS Entity / Telco Entity	Do you have in place an incident response plan to protect assets and data?	NIST SP 800-53 Rev. 4
Incident Response Governance	IR.17	FS Regulator / Telco Regulator	Do you mandate the development of disaster recovery plans and procedures for entities? Are these plans periodically tested?	NIST SP 800-53 Rev. 4
Incident Response Governance	IR.18	FS Entity / Telco Entity	Do you have an approved Disaster Recovery Plan? Do you perform Disaster Recovery testing periodically?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.19	FS Entity / Telco Entity	Does your staff have access to USBs, and can your personnel bring any types of removable media into your entity and plug into corporate assets?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.20	FS Regulator / Telco Regulator	Do you mandate using and implementing load balancing or other failover mechanisms?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.21	FS Entity / Telco Entity	Do you have in place any load balancing or failover mechanisms?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.22	FS Entity / Telco Entity	Does to entity analyse logged events to understand potential attack targets and methods?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.23	Telco Regulator	Does the regulator mandate measures to collect and correlate data from multiple sources and sensors?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.24	Telco Entity	Does the entity collect and correlate data from multiple sources and sensors?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.25	FS Regulator / Telco Regulator	Do you mandate the implementation of peripheral defences, such as Intrusion Detection Systems (IDS)? Do you also mandate the implementation of Intrusion Prevention Systems (IPS)?	NIST SP 800-53 Rev. 4

Domain	ID	Applicability	Question	Informative Reference
Incident Response Life Cycle	IR.26	FS Entity / Telco Entity	Do your peripheral defences have any Intrusion Detection Systems? Do you plan to upscale the hardware to also include Intrusion Prevention Systems to react to potential intrusions?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.27	FS Entity / Telco Entity	Do you have the necessary software and hardware capabilities to detect malicious codes, even if embedded in potentially unharmful files?	NIST SP 800-53 Rev. 4
Incident Response Reporting	IR.28	FS Entity / Telco Entity	Do you implement coordination mechanisms with relevant stakeholders on incident response practices? If so, do you coordinate with both internal and external stakeholders?	NIST SP 800-53 Rev. 4
Incident Response Reporting	IR.29	FS Entity / Telco Entity	Do you coordinate with stakeholders on how to respond to a cyber-attack, and do you ensure transparency with local authorities and clients to mitigate the risk of reputational loss?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.30	FS Regulator / Telco Regulator	Do you issue detection and investigation best practices/regulations during the incident response process?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.31	FS Entity / Telco Entity	Do you investigate notifications from detection systems or potential issues connected to the network? Do you have a multi-step incident response in case of a false alarm?	NIST SP 800-53 Rev. 4
Third-Parties	IR.32	FS Regulator / Telco Regulator	Do you issue best practices on forensics checks, compromised systems, and data sharing with relevant internal and external stakeholders?	NIST SP 800-53 Rev. 4
Third-Parties	IR.33	FS Entity / Telco Entity	Do you perform forensics checks on compromised systems and share data with local authorities and partners?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.34	FS Entity / Telco Entity	Do you categorise and prioritise incidents based on the entity's scope, mission, objectives, and current status? Do you update this prioritisation regularly?	NIST SP 800-53 Rev. 4
Incident Response Governance	IR.35	FS Entity / Telco Entity	Do you implement measures to respond to and recover from malicious activity within your systems? Are such measures derived from international/national best practices?	NIST SP 800-53 Rev. 4
Incident Response Governance	IR.36	FS Regulator / Telco Regulator	Do you have technical guidelines on responding to and recovering from any malicious activity within your systems?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.37	FS Regulator / Telco Regulator	Do you periodically issue best practices to verify incident data and implement lessons learned?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.38	FS Entity / Telco Entity	Do you verify past incident data to ensure future risk mitigation and lessons learned?	NIST SP 800-53 Rev. 4

Domain	ID	Applicability	Question	Informative Reference
Incident Response Governance	IR.39	FS Entity / Telco Entity	If you have Response strategies in place, do you update them? How frequently?	NIST SP 800-53 Rev. 4
Incident Response Reporting	IR.40	FS Regulator / Telco Regulator	Do you issue communication mechanisms to encourage sharing recovery measures between relevant stakeholders and across industries?	NIST SP 800-53 Rev. 4
Incident Response Reporting	IR.41	FS Entity / Telco Entity	Once the threat is contained and eradicated, are recovery activities communicated to internal and external stakeholders? Are regular meetings scheduled with management to ensure information sharing?	NIST SP 800-53 Rev. 4
Incident Response Governance	IR.42	FS Entity / Telco Entity	Does the entity's cyber resilience framework include references to its incident management process?	DORA
Incident Response Life Cycle	IR.43	FS Regulator / Telco Regulator	Does the entity's existing cyber resilience strategy include references to past incidents, and does it consider metrics to show the efficacy of existing preventive measures?	DORA
Incident Response Life Cycle	IR.44	FS Entity / Telco Entity	If so, does the entity have an automated tool to detect and respond to ICT incidents in place?	DORA
Incident Response Governance	IR.45	FS Entity / Telco Entity	Do you implement ICT-related response and recovery plans? If so, how structured are they?	DORA
Incident Response Governance	IR.46	FS Regulator / Telco Regulator	Do you mandate entities have structured ICT-related response and recovery plans?	DORA
Incident Response Life Cycle	IR.47	FS Regulator / Telco Regulator	Do you mandate the periodic definition of a Business Impact Analysis (BIA)?	DORA
Incident Response Life Cycle	IR.48	FS Entity / Telco Entity	Does the entity's Business Impact Analysis (BIA) clearly define the maximum tolerable duration of business interruptions, taking into account their central roles, as well as established parameters such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?	DORA
Incident Response Life Cycle	IR.49	FS Entity / Telco Entity	Does the entity ensure capacity and redundancy criteria for ICT facility reliability?	DORA
Incident Response Life Cycle	IR.50	FS Entity / Telco Entity	Are information on cyber vulnerabilities, threats, and ICT-related incidents adequately recorded?	DORA
Incident Response Life Cycle	IR.51	FS Entity / Telco Entity	Does the entity correctly record information concerning cyber vulnerabilities, threats, and ICT-related incidents?	DORA

Domain	ID	Applicability	Question	Informative Reference
Incident Response Life Cycle	IR.52	FS Entity / Telco Entity	Following major ICT-related incidents, does the entity conduct a post-incident reassessment and Root Cause Analysis (RCA)?	DORA
Incident Response Life Cycle	IR.53	FS Regulator / Telco Regulator	Do you mandate implementing a structured process to collect and properly store Root Cause Analysis (RCA) findings and lessons learned?	DORA
Incident Response Life Cycle	IR.54	FS Regulator / Telco Regulator	Do you mandate the implementation of testing practices to determine the effectiveness of incident analysis procedures and best practices?	DORA
Incident Response Life Cycle	IR.55	FS Entity / Telco Entity	Does the entity use the findings of all incident analysis and digital operational resilience testing as input for continuous improvement of the Cyber Risk Management Framework?	DORA
Incident Response Life Cycle	IR.56	FS Entity / Telco Entity	Does the entity deploy ICT safeguards and tools that enable early detection of risk sources and anomalies in information systems and rapid handling of ICT-related incidents?	DORA
Incident Response Governance	IR.57	FS Entity / Telco Entity	Do you implement business continuity plans and response and recovery measures? Do they include backup and recovery measures?	DORA
Incident Response Governance	IR.58	FS Entity / Telco Entity	Does the entity have business continuity plans and response and recovery measures in place that, at a minimum, include backup and recovery measures and ensure continuity of essential or critical functions?	DORA
Incident Response Governance	IR.59	FS Entity / Telco Entity	If so, how often is the Incident Response Plan (IRP) updated?	DORA
Incident Response Governance	IR.60	FS Entity / Telco Entity	If so, is there any connection between Incident Management, Business Continuity, and Disaster Recovery procedures?	DORA
Incident Response Life Cycle	IR.61	FS Entity / Telco Entity	Does the entity's ICT-related incident management and monitoring process include early warning indicators?	DORA
Incident Response Reporting	IR.62	FS Entity / Telco Entity	Do you implement internal communication plans for ICT-related incidents?	DORA
Incident Response Reporting	IR.63	FS Regulator / Telco Regulator	Do you mandate entities to develop internal communication plans for ICT-related incidents?	DORA
Incident Response Life Cycle	IR.64	FS Entity / Telco Entity	Do you implement mechanisms to assess an ICT-related incident's internal and external impact?	DORA

Domain	ID	Applicability	Question	Informative Reference
Incident Response Life Cycle	IR.65	FS Regulator / Telco Regulator	Do you mandate the definition and implementation of specific mechanisms to assess a cybersecurity ICT incident's external and internal impact?	DORA
Incident Response Life Cycle	IR.66	FS Entity / Telco Entity	What is the entity's average detection and response time in case of an incident?	DORA
Incident Response Life Cycle	IR.67	FS Entity / Telco Entity	Does the entity classify ICT-related incidents according to the following requirements? 1) Number and/or significance of customers or business partners; 2) Duration of the incident; 3) Geographic range of the incident; 4) Data loss resulting from the incident; 5) Criticality of services affected 6) Economic impact of the incident.	DORA
Incident Response Life Cycle	IR.68	FS Regulator / Telco Regulator	Did you issue power outages/saturation regulations in the entity's Incident Response Plan (IRP)?	NIST SP 800-53 Rev. 4
Incident Response Life Cycle	IR.69	FS Entity / Telco Entity	Have you established capabilities to continuously monitor (in real time or near real time) and detect anomalous activities and events (i.e., Security Operations Centre)?	BIS Report Guidance for cyber resilience for FMIs
Incident Response Life Cycle	IR.70	FS Entity / Telco Entity	Are these capabilities tested and updated? What is the frequency of the tests?	BIS Report Guidance for cyber resilience for FMIs
Incident Response Life Cycle	IR.71	FS Entity / Telco Entity	Does the entity monitor relevant internal and external factors, including business line and administrative functions and transactions, to detect publicly known vulnerabilities and vulnerabilities that are not yet publicly known, such as so-called zero-day exploits, through a combination of signature monitoring for known vulnerabilities and behaviourally based detection mechanisms?	BIS Report Guidance for cyber resilience for FMIs
Incident Response Life Cycle	IR.72	FS Entity / Telco Entity	Do you account for network outages and/or saturation in your Incident Response Plan (IRP)?	NIST SP 800-53 Rev. 4
Third-Parties	IR.73	FS Entity / Telco Entity	Has the entity considered setting up data-sharing agreements with relevant third-parties or participants in advance in order to enable, in the case of a cyber-attack, such clean data to be received in a timely manner?	BIS Report Guidance for cyber resilience for FMIs
Incident Response Life Cycle	IR.74	FS Entity / Telco Entity	Does the entity's incident detection capabilities include detecting access misuse by service providers, cloud service providers, utility providers or other trusted agents, potential insider threats and other advanced threat activity?	BIS Report Guidance for cyber resilience for FMIs
Incident Response Life Cycle	IR.75	FS Entity / Telco Entity	Are the entity's incident detection processes integrated with a cyber threat intelligence programme?	BIS Report Guidance for cyber resilience for FMIs