Commission de Surveillance
du Secteur Financier

Circular CSSF 25/881

amending Circular CSSF 20/750

on requirements regarding information and communication technology (ICT) and security risk management

Circular CSSF 25/881

amending Circular CSSF 20/750

on requirements regarding information and communication technology (ICT) and security risk management

To all credit institutions and to all professionals of the financial sector within the meaning of the Law of 5 April 1993 on the financial sector (LFS).
To POST Luxembourg governed by the Law of 15 December 2000 on postal financial services1.
To all payment institutions and to all electronic money institutions within the meaning of the Law of 10 November 2009 on payment services (LPS).

Luxembourg, 9 April 2025

Ladies and Gentlemen,

As of 17 January 2025, the provisions of the Digital Operational Resilience Act[2] ("DORA") are applicable to the financial entities as defined in DORA and supervised by the CSSF. DORA has introduced, inter alia, harmonised requirements for information and communication technology (ICT) risk management framework.

In view of reducing the overlap with the DORA regulation, the European Banking Authority ("EBA") reviewed its existing Guidelines on ICT and security risk management EBA/GL/2019/04 (the "EBA Guidelines"), which were built on the provisions of Article 74 of Directive 2013/36/EU (CRD)[3] and Article 95(3) of Directive (EU) 2015/2366 (Payment Services Directive 2, "PSD2")[4]. The EBA Guidelines are implemented in Luxembourg by way of Circular CSSF 20/750 on ICT and security risk management.

The EBA arrived at the view that the entities subject to the EBA Guidelines should be narrowed down and the scope of the Guidelines reduced to Guideline 3.8 on relationship management of the payment service users in relation to the provision of payment services. To do so, the EBA issued EBA GL 2025/02 amending EBA GL/2019/04 on ICT and security risk management ("new EBA Guidelines"). The EBA further explained that National Competent Authorities have the possibility to subject Payment Service Providers (PSPs) that are not covered by DORA to national requirements irrespective of the existence or not of EBA Guidelines[5].

[1] For the sake of clarity, the wording "postal financial services" has the meaning provided for in Article 1 of the Law of 15 December 2000, as amended.

[2] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 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

[3] https://eur-lex.europa.eu/eli/dir/2013/36/oj/eng

[4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35–127)

[5] EBA/GL/2025/02 and corresponding press release

Consequently, to provide legal clarity to the market and clarify its expectations, the CSSF is taking two steps:

1. amend Circular CSSF 20/750 on requirements regarding ICT and security risk management:
   - **to reduce the scope to "non-DORA entities", i.e. the entities that are subject to CSSF supervision but are not financial entities as defined in Article 2 of DORA** and therefore not subject to DORA requirements. The amended Circular CSSF 20/750 also remains applicable to entities which are not in the scope of DORA, when providing payment services, such as POST Luxembourg and branches in Luxembourg of PSP incorporated in a third country[6]. In fact, the CSSF considers that financial entities subject to the supervision of the CSSF falling under Circular CSSF 20/750 but not falling under DORA shall continue to fulfil its expectations with regard to the ICT and security risk management by complying with this circular;
   - **to remove the specific elements <u>only</u> applicable to PSPs** (whether they are also in scope of DORA or not) which are regrouped in a new dedicated circular (see point 2 below), i.e. Guideline 3.8. on relationship management of the payment service users and section 4 of the circular related to PSP ICT assessment; and
   - to remove a few other obsolete sections and provisions of the circular.

2. issue a new circular, Circular CSSF 25/880 on relationship management of payment service users and PSP ICT assessment, **applicable to all PSPs** within the scope of LPS and supervised by the CSSF, including branches in Luxembourg of PSPs incorporated in a third country, and POST Luxembourg which:
   - **implements the EBA Guidelines 2025/02** amending EBA GL/2019/04 on ICT and security risk management. i.e. the contents of Guideline 3.8 referred to above;
   - **integrates** the existing additional national requirement for annual reporting of the risk assessment related to payment services (**PSP ICT assessment**), which was previously part of Circular CSSF 20/750.

In line with step 1 above, this circular amends Circular CSSF 20/750 by specifying the following:

1. the scope of application of Circular CSSF 20/750 has been modified to consider the entry into application of DORA. The scope is now described in Chapter 1:

   a. For financial entities as defined in Article 2 of DORA and supervised by the CSSF, Circular CSSF 20/750 no longer applies. They have been removed from the scope;

   b. For entities falling under Circular CSSF 20/750 but not falling under DORA, Circular CSSF 20/750 continues to apply in full.

2. Section 1 on "Requirements regarding information and communication technology (ICT) and security risk management", Section 2 on "Amendment of Circular CSSF 12/552", Section 3 on "Repeal and replacement of Circular CSSF 19/713" and Section 4 on "Additional requirement for payment service providers (PSPs)" have been removed.

3. The requirements that were listed in EBA Guidelines EBA/GL/2019/04 have been introduced directly in Circular CSSF 20/750 as follows:

[6] This is the reason why references to elements of compliance with the Law of 10 November 2009 on payment services (LPS) which apply to POST Luxembourg and branches in Luxembourg of PSP incorporated in a third country are retained in this circular.

a. The text of the EBA Guidelines in the section "Definitions" can now be found in Chapter 2;

b. The text of the EBA Guidelines in the section "Guidelines on ICT and security risk management" can now be found in Chapter 3.

The amendments to the EBA Guidelines, which are now in Chapters 2 and 3 are shown in track changes. They relate to requirements or references which were primarily relevant for entities which are now out of scope of this circular. In addition, some definitions were modified to align them with recent definitions in this area.

This circular shall apply with immediate effect.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex Circular CSSF 20/750 as amended by Circular CSSF 25/881

Commission de Surveillance
du Secteur Financier

Circular CSSF 20/750

as amended by Circular CSSF 25/881

on requirements regarding information and communication technology (ICT) and security risk management

Circular CSSF 20/750

as amended by Circular CSSF 25/881

on requirements regarding information and communication technology (ICT) and security risk management

To support PFS and specialised PFS within the meaning of the Law of 5 April 1993 on the financial sector (LFS), POST Luxembourg governed by the Law of 15 December 2000 on postal financial services[1], as well as to all branches in Luxembourg of credit institutions, investment firms, payment institutions and e-money institutions incorporated in a third country

Luxembourg, 25 August 2020

Ladies and Gentlemen,

This circular reflects the expectations of the CSSF as regards the risk management measures and control and security arrangements as referred to in Articles 17(1a) and 36(1) of the Law of 5 April 1993 on the financial sector ("LFS") and in Article 105-1 (1) of the Law of 10 November 2009 on payment services ("LPS").

This circular is divided in four Chapters:

- Chapter 1 indicates the scope of this circular
- Chapter 2 provides definitions and clarifications with regards to the terms used in this circular
- Chapter 3 lists the requirements regarding to ICT and security risk management
- Chapter 4 indicates the entry into force of this circular

[1] *For the sake of clarity, the wording "postal financial services" has the meaning provided for in Article 1 of the Law of 15 December 2000 as amended.*

TABLE OF CONTENTS

Chapter 1. Entities in Scope

This circular is applicable in full to all the following entities:

a) All support PFS within the meaning of the Law of 5 April 1993 on the financial sector (LFS)

b) All specialised PSF within the meaning of the Law of 5 April 1993 on the financial sector (LFS)

c) POST Luxembourg governed by the Law of 15 December 2000 on postal financial services[2] and as Payment Service Provider as referred to in Article 1(37)(iii) of the LPS

d) All branches in Luxembourg of credit institutions incorporated in a third country

e) All branches in Luxembourg of investment firms incorporated in a third country

f) All branches in Luxembourg of payment institutions and electronic money institutions incorporated in a third country

Chapter 2. Definitions

Financial Institution	Throughout this document this term refers to the supervised entities in scope of this circular as defined in Chapter 1.
Payment Service Provider (PSP)	Throughout this document this term refers to POST Luxembourg and branches in Luxembourg of credit institutions, payment institutions and electronic money institutions incorporated in a third country, when they provide payment services as defined in Article 1(38) of the LPS.
ICT and security risk	Risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility)[3]. This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security.
Management body	~~(a) For credit institutions and investment firms, this term has the same meaning as the definition in point (7) of Article 3(1) of Directive 2013/36/EU.~~ ~~(b) For payment institutions or electronic money institutions, this term means directors or persons responsible for the management of the payment institutions and electronic money institutions and, where~~

[2] *For the sake of clarity, the wording "postal financial services" has the meaning provided for in Article 1 of the Law of 15 December 2000 as amended.*

~~[3] Definition from the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process of 19 December 2014 (EBA/GL/2014/13), amended by EBA/GL/2018/03.~~

	~~relevant, persons responsible for the management of the payment services activities of the payment institutions and electronic money institutions.~~ ~~(c) For PSPs referred to in points (c), (e) and (f) of Article 1(1) of Directive (EU) 2015/2366, this term has the meaning conferred on it by the applicable EU or national law.~~A Financial Institution's body or bodies, which are appointed in accordance with national law, which are empowered to set the Financial Institution's strategy, objectives and overall direction, and which oversee and monitor management decision-making and include the persons who effectively direct the business of the Financial Institution and the directors and persons responsible for the management of the Financial Institution. In accordance with relevant circulars CSSF as applicable, the term management body encompasses the notions of authorised management, board of directors/or board of managers and/or supervisory board and executive board.
Operational or security incident	A singular event or a series of linked events unplanned by the financial institution that has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of services.
~~**Senior management**~~	~~(a) For credit institutions and investment firms, this term has the same meaning as the definition in point (9) of Article 3(1) of Directive 2013/36/EU.~~ ~~(b) For payment institutions and electronic money institutions, this term means natural persons who exercise executive functions within an institution and who are responsible, and accountable to the management body, for the day-to-day management of the institution.~~ ~~(c) For PSPs referred to in points (c), (e) and (f) of Article 1(1) of Directive (EU) 2015/2366, this term has the meaning conferred on it by the applicable EU or national law.~~
Risk appetite	The aggregate level and types of risk that the PSPs and institutions are willing to assume within their risk capacity, in line with their business model, to achieve their strategic objectives.
~~**Audit function**~~	~~(a) For credit institutions and investment firms, the audit function is as referred to in Section 22 of the EBA guidelines on internal governance (EBA/GL/2017/11).~~

	~~(b) For PSPs other than credit institutions, the audit function must be independent within or from the PSP and may be an internal and/or an external audit function.~~
ICT projects	Any project, or part thereof, where ICT systems and services are changed, replaced, dismissed or implemented. ICT projects can be part of wider ICT or business transformation programmes.
Third party	An organisation that has entered into business relationships or contracts with an entity to provide a product or service[4].
Information asset	A collection of information, either tangible or intangible, that is worth protecting.
ICT asset	An asset of either software or hardware that is found in the business environment.
ICT systems[5]	ICT set-up as part of a mechanism or an interconnecting network that supports the operations of a financial institution.
ICT services[6]	~~Services provided by ICT systems to one or more internal or external users. Examples include data entry, data storage, data processing and reporting services, but also monitoring, and business and decision support services.~~means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services. [7]

Chapter 3. Guidelines on ICT and security risk management

3.1. Proportionality

1. All financial institutions should comply with the provisions set out in these guidelines in such a way that is proportionate to, and takes account of, the financial institutions' size, their internal

~~[4] Definition from G7 fundamental elements for third party cyber risk management in the financial sector.~~

~~[5] Definition from Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/ 2017/05).~~

~~[6] ibid.~~

[7] Definition from Article 3(21) of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 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 ("DORA")

organisation, and the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide.

3.2. Governance and strategy

3.2.1. Governance

2. The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees.

3. The management body should ensure that the quantity and skills of financial institutions' staff is adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the allocated budget is appropriate to fulfil the above. Furthermore, financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required (see also Section 3.4.7.)

4. The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.

3.2.2. Strategy

5. The ICT strategy should be aligned with financial institutions' overall business strategy and should define:

    a. How financial institutions' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;
    b. The planned strategy and evolution of the architecture of ICT, including third-party dependencies;
    c. Clear information security objectives, focusing on ICT systems and ICT services, staff and processes

6. Financial institutions should establish sets of action plans that contain measures to be taken to achieve the objective of the ICT strategy. These should be communicated to all relevant staff (including contractors and third-party providers where applicable and relevant). The action plans should be periodically reviewed to ensure their relevance and appropriateness. Financial institutions should also establish processes to monitor and measure the effectiveness of the implementation of their ICT strategy.

3.2.3. Use of third-party providers

7. Without prejudice to Circular CSSF 22/806 ~~the EBA Guidelines~~ on outsourcing arrangements ~~(EBA/GL/2019/02)and article 19 of PSD2~~, financial institutions should ensure the effectiveness

of the risk-mitigating measures as defined by their risk management framework, including the measures set out in these guidelines, when operational functions of payment services and/or ICT services and ICT systems of any activity are outsourced, including to group entities, or when using third parties.

8. To ensure continuity of ICT services and ICT systems, financial institutions should ensure that contracts and service level agreements (both for normal circumstances as well as in the event of service disruption- see also section 3.7.2.) with providers (outsourcing providers, group entities, or third-party providers) include the following:

    a. Appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements; specifications of the financial institution's data life cycle; any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres;
    b. Operational and security incident handling procedures including escalation and reporting.

9. Financial institutions should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets of the financial institution.

3.3. ICT and security risk management framework

3.3.1. Organisation and objectives

10. Financial institutions should identify and manage their ICT and security risks. The ICT function(s) in charge of ICT systems, processes and security operations should have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the financial institution's risk appetite and that the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.

11. Financial institutions should assign the responsibility for managing and overseeing ICT and security risks to a control function~~, adhering to the requirements of Section 19 of the EBa/GL/2017/11~~. Financial institutions should ensure the independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function should be directly accountable to the management body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Financial institutions should ensure that this control function is not responsible for any internal audit.

    The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of a financial institutions with the financial institution's policies and procedures and with external requirements~~, adhering to the requirements of section 22 of the EBA GL on internal governance(EBA/GL/2017/11)~~.

12. Financial institutions should define and assign key roles and responsibilities, and relevant reporting lines, for the ICT and security risk management framework to be effective. This framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes.

13. The ICT and security risk management framework should include processes in place to:

    a. Determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the financial institution;
    b. Identify and assess the ICT and security risks to which a financial institution is exposed;
    c. Define mitigation measures, including controls, to mitigate ICT and security risks;
    d. Monitor the effectiveness of these measures as well as the number of reported incidents, including for PSPs the incidents reported in accordance with Article 105-2 of LPS~~96 of PSD2~~ affecting the ICT-related activities, and take action to correct the measures where necessary;
    e. Report to the management body on the ICT and security risks and controls;
    f. Identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or security incident.

14. Financial institutions should ensure that the ICT and security risk management framework is documented, and continuously improved, based on "lessons learned" during its implementation and monitoring. The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body.

3.3.2. Identification of functions, processes and assets

15. Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.

16. In addition, financial institutions should identify, establish and maintain updated mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.

3.3.3. Classification and risk assessment

17. Financial institutions should classify the identified business functions, supporting processes and information assets referred to in paragraphs 15 and 16 in terms of criticality.

18. To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity and availability requirements. There should be clearly assigned accountability and responsibility for the information assets.

19. Financial institutions should review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed.

20. Financial institutions should identify the ICT and security risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality. This risk assessment should be carried out and documented annually or at shorter intervals if required. Such risk assessments should also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.

21. Financial institutions should ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and should regularly review the risk scenarios impacting them.

3.3.4. Risk mitigation

22. Based on the risk assessments, financial institutions should determine which measures are required to mitigate identified ICT and security risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, ICT systems and ICT services. A financial institution should consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and security risks to stay within the financial institution's ICT and security risk appetite.
23. Financial institutions should define and implement measures to mitigate identified ICT and security risks and to protect information assets in accordance with their classification.

3.3.5. Reporting

24. Financial institutions should report risk assessment results to the management body in a clear and timely manner. Such reporting is without prejudice to the obligation of PSPs to provide competent authorities with an updated and comprehensive risk assessment, as laid down in Article 105-1(2) of LPS.~~95(2) of Directive (EU) 2015/2366.~~

3.3.6. Audit

25. A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.
26. A financial institution's management body should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the financial institution and should be updated regularly.
27. A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings should be established.

3.4. Information security

3.4.1. Information security policy

28. Financial institutions should develop and document an information security policy that should define the high-level principles and rules to protect the confidentiality, integrity and availability of financial institutions' and their customers' data and information.~~ For PSPs this policy is identified in the security policy document to be adopted in accordance with Article 5(1)(j) of Directive (EU) 2015/2366.~~ The information security policy should be in line with the financial

institution's information security objectives and based on the relevant results of the risk assessment process. The policy should be approved by the management body.

29. The policy should include a description of the main roles and responsibilities of information security management, and it should set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring financial institutions' information security. The policy should ensure the confidentiality, integrity and availability of a financial institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated to all staff and contractors of the financial institution.

30. Based on the information security policy, financial institutions should establish and implement security measures to mitigate the ICT and security risks that they are exposed to. These measures should include:

    a. organisation and governance in accordance with paragraphs 10 and 11;
    b. logical security (Section 3.4.2);
    c. physical security (Section 3.4.3);
    d. ICT operations security (Section 3.4.4);
    e. security monitoring (Section 3.4.5);
    f. information security reviews, assessment and testing (Section 3.4.6);
    g. information security training and awareness (Section 3.4.7).

3.4.2. Logical security

31. Financial institutions should define, document and implement procedures for logical access control (identity and access management). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies. These procedures should, at a minimum, implement the following elements, where the term 'user' also includes technical users:

    a. **Need to know, least privilege and segregation of duties:** financial institutions should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').

    b. **User accountability:** financial institutions should limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.

    c. **Privileged access rights:** financial institutions should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.

d. **Logging of user activities:** at a minimum, all activities by privileged users should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with Section 3.3.3, without prejudice to the retention requirements set out in EU and national law. A financial institution should use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of services.

e. **Access management:** access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights should be promptly withdrawn.

f. **Access recertification:** access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn when no longer required.

g. **Authentication methods:** financial institutions should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or the process being accessed. This should, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.

32. Electronic access by applications to data and ICT systems should be limited to a minimum required to provide the relevant service.

3.4.3. Physical security

33. Financial institutions' physical security measures should be defined, documented and implemented to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

34. Physical access to ICT systems should be permitted to only authorised individuals. Authorisation should be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.

35. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

3.4.4. ICT operations security

36. Financial institutions should implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and should minimise their impact on ICT service delivery. These procedures should include the following measures:

a. identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by

financial institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;

b. implementation of secure configuration baselines of all network components;
c. implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);
d. implementation of protection of endpoints including servers, workstations and mobile devices; financial institutions should evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network;
e. ensuring that mechanisms are in place to verify the integrity of software, firmware and data;
f. encryption of data at rest and in transit (in accordance with the data classification).

37. Furthermore, on an ongoing basis, financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.

3.4.5. Security monitoring

38. Financial institutions should establish and implement policies and procedures to detect anomalous activities that may impact financial institutions' information security and to respond to these events appropriately. As part of this continuous monitoring, financial institutions should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection processes should cover:

a. relevant internal and external factors, including business and ICT administrative functions;
b. transactions to detect misuse of access by third parties or other entities and internal misuse of access;
c. potential internal and external threats.

39. Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Financial institutions should actively monitor technological developments to ensure that they are aware of security risks. Financial institutions should implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.

40. The security monitoring process should also help a financial institution to understand the nature of operational or security incidents, to identify trends and to support the organisation's investigations.

3.4.6. Information security reviews, assessment and testing

41. Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information

security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team exercises.

42. Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.

43. The information security testing framework should ensure that tests:

    a. are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures;
    b. include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.

44. Financial institutions should perform ongoing and repeated tests of the security measures. For all critical ICT systems (paragraph 17), these tests should be performed at least on an annual basis and, for PSPs, they will be part of the comprehensive assessment of the security risks related to the payment services they provide, in accordance with Article 105-1(2) of LPS~~95(2) of PSD2~~. Non-critical systems should be tested regularly using a risk-based approach, but at least every 3 years.

45. Financial institutions should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.

46. Financial institutions should monitor and evaluate the results of the security tests and update their security measures accordingly without undue delays in the case of critical ICT systems.

47. For PSPs, the testing framework should also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services, (2) payment terminals and devices used for authenticating the payment service users (PSU), and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

48. Based on the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.

3.4.7. Information security training and awareness

49. Financial institutions should establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks. Financial institutions should ensure that the training programme provides training for all staff members and contractors at least annually.

3.5. ICT operations management

50. Financial institutions should manage their ICT operations based on documented and implemented processes and procedures ~~(which, for PSPs, include the security policy document in accordance withArticle 5(1)(j) of PSD2)~~ that are approved by the management body[8]. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.

51. Financial institutions should ensure that performance of their ICT operations is aligned to their business requirements. Financial institutions should maintain and improve, when possible, efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.

52. Financial institutions should implement logging and monitoring procedures for critical ICT operations to allow the detection, analysis and correction of errors.

53. Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.

54. The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.

55. Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.

56. Financial institutions should implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.

57. Financial institutions should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set out in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.

58. Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.

3.5.1. ICT incident and problem management

59. Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial

[8] means "management body or authorised management as defined by the management body"

institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the 'Definitions' section of this circular~~these guidelines~~, as well as early warning indicators that should serve as alerts to enable early detection of these incidents. ~~Such criteria and thresholds, for PSPs, are without prejudice to the classification of major incidents in accordance with Article 96 of PSD2 and the Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10).~~

60. To minimise the impact of adverse events and enable timely recovery, financial institutions should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents. The incident and problem management process should establish:

    a. the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;
    b. the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);
    c. problem management procedures to identify, analyse and solve the root cause behind one or more incidents — a financial institution should analyse operational or security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organisation and should consider key lessons learned from these analyses and update the security measures accordingly;
    d. effective internal communication plans, including incident notification and escalation procedures — also covering security-related customer complaints — to ensure that:
        i. incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management[9] and ICT senior management[10];
        ii. the management body is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents.
    e. incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;
    f. specific external communication plans for critical business functions and processes in order to:
        i. collaborate with relevant stakeholders to effectively respond to and recover from the incident;
        ii. provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.

[9] means "management"

[10] means "management"

3.6. ICT project and change management

3.6.1. ICT project management

61. A financial institution should implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.

62. A financial institution should appropriately monitor and mitigate risks deriving from their portfolio of ICT projects (programme management), considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

63. A financial institution should establish and implement an ICT project management policy that includes as a minimum:

    a. project objectives;
    b. roles and responsibilities;
    c. a project risk assessment;
    d. a project plan, timeframe and steps;
    e. key milestones;
    f. change management requirements.

64. The ICT project management policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function.

65. A financial institution should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.

66. The establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Financial institutions should include project risk in their risk management framework.

3.6.2. ICT systems acquisition and development

67. Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach.

68. A financial institution should ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.

69. A financial institution should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

70. Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. They should also use test environments that adequately reflect the production environment.

71. Financial institutions should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

72. A financial institution should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments. A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.

73. Financial institutions should implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation and/or configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.

74. A financial institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.

3.6.3. ICT change management

75. Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.

76. Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes should be in accordance with the financial institutions' formal change management process.

3.7. Business continuity management

77. Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption ~~in line with Article 85(2) of Directive 2013/36/EU and Title VI of the EBA Guidelines on internal governance (EBA/GL/2017/11)~~.

3.7.1. Business impact analysis

78. As part of sound business continuity management, financial institutions should conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third-party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario

analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies, in accordance with Section 3.3.3.

79. Financial institutions should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

3.7.2. Business continuity planning

80. Based on their BIAs, financial institutions should establish plans to ensure business continuity (business continuity plans, BCPs), which should be documented and approved by their management bodies. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.

81. Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, financial institutions should prioritise business continuity actions using risk-based approach, which can be based on the risk assessments carried out under Section 3.3.3. For PSPs this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.

82. A financial institution should consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have. Based on these scenarios, a financial institution should describe how the continuity of ICT systems and services, as well as the financial institution's information security, are ensured.

3.7.3. Response and recovery plans

83. Based on the BIAs (paragraph 78) and plausible scenarios (paragraph 82), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.

84. The response and recovery plans should consider both short-term and long-term recovery options. The plans should:

    a. focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial institutions and on the financial system, including on payment

systems and on payment service users, and to ensure execution of pending payment transactions;

b. be documented and made available to the business and support units and readily accessible in the event of an emergency;

c. be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

85. The plans should also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.

86. Furthermore, as part of the response and recovery plans, a financial institution should consider and implement continuity measures to mitigate failures of third-party providers, which are of key importance for a financial institution's ICT service continuity (in line with the provisions of the Circular CSSF 22/806 ~~EBA Guidelines~~ on outsourcing arrangements ~~(EBA/GL/2019/02)~~ regarding business continuity plans).

3.7.4. Testing of plans

87. Financial institutions should test their BCPs periodically. In particular, they should ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with paragraph 89.

88. BCPs should be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, should also be considered, where relevant, as a basis for updating the BCPs.

89. Financial institutions' testing of their BCPs should demonstrate that they are able to sustain the viability of their businesses until critical operations are re-established. In particular they should:

    a. include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as testing of services provided by third parties, where applicable); this should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;

    b. be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans; and

    c. include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the scenarios defined in paragraph 89(a).

90. Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.

3.7.5. Crisis communication

91. In the event of a disruption or emergency, and during the implementation of the BCPs, financial institutions should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authorities when

required by national regulations, and also relevant providers (outsourcing providers, group entities, or third-party providers) are informed in a timely and appropriate manner.

~~3.8. Payment service user relationship management~~

~~92. PSPs should establish and implement processes to enhance PSUs' awareness of the security risks linked to the payment services by providing PSUs with assistance and guidance.~~

~~93. The assistance and guidance offered to PSUs should be updated in the light of new threats and vulnerabilities, and changes should be communicated to the PSU.~~

~~94. Where product functionality permits, PSPs should allow PSUs to disable specific payment functionalities related to the payment services offered by the PSP to the PSU.~~

~~95. Where, in accordance with Article 68(1) of Directive (EU) 2015/2366, a PSP has agreed with the payer spending limits for payment transactions executed through specific payment instruments, the PSP should provide the payer with the option to adjust these limits up to the maximum agreed limit.~~

~~96. PSPs should provide PSUs with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their accounts.~~

~~97. PSPs should keep PSUs informed about updates in security procedures that affect PSUs regarding the provision of payment services.~~

~~98. PSPs should provide PSUs with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. PSUs should be appropriately informed about how such assistance can be obtained~~

Chapter 4. Date of application

~~99.~~92. This circular shall apply with immediate effect.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General