FINANCE & TECHNOLOGY LUXEMBOURG

ICT AND SECURITY REQUIREMENTS FOR REGULATED ENTITIES

25 September 2020

Welcome address

Jean-François Terminaux, Chairman, FTL

&

Jean Hilger, Head, ABBL Digital Banking and FinTech Innovation Cluster

Digital Banking and FinTech Innovation Cluster Luxembourg

an ABBL cluster

FINANCE & TECHNOLOGY LUXEMBOURG

Jean HILGER

Chair

ABBL's Digital Banking and FinTech Innovation Cluster (DBFI)

FINANCE & TECHNOLOGY LUXEMBOURG

EBA Guidelines ICT & Security risk management

Florian Bewig, IT Regulatory Leader, PwC

EBA Guidelines on ICT & Security risk management

By Florian Bewig

LinkedIn profile

pwc

Transposition of EBA ICT Guidelines by circular CSSF 20/750

Background

- Based on **EBA guidelines on security measures for operational and security risks of payment services (EBA/GL/2017/17)**, which only applied to Payment Service Providers (PSP) and are now repealed
- CSSF 20/750 transposes **EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)**

Main objectives

- **Address the risks and adverse impacts** on the supervised entities' operations caused by increased complexity of ICT & Security risks as well as the interconnectedness with third parties
- Provide details on **how supervised entities should manage and mitigate** ICT & Security risks they are exposed to
- Provide a **better understanding of CSSF's expectations** on the management of ICT & Security risks

Scope of application
(25 August 2020)

Entities governed by LSF* 1993, including:

- Credit institutions
- Investment firms
- **Specialized PSFs**
- **Support PSFs**

Entities governed by LSP 2009**, including:

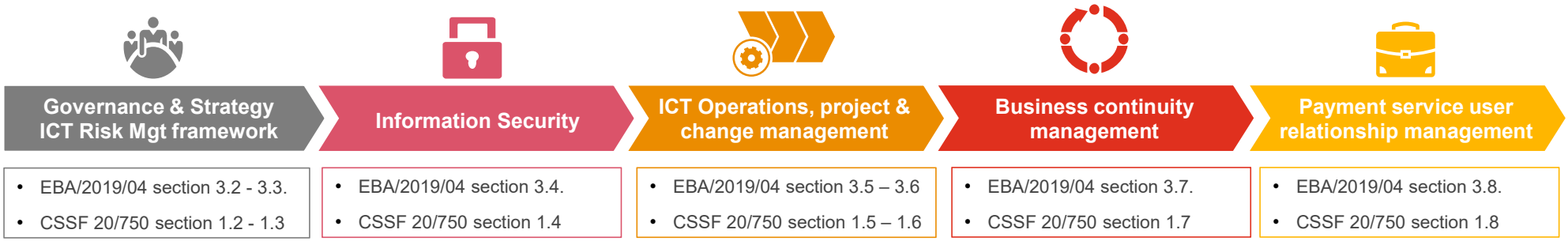
- E-money institutions
- Payment institutions

Main changes to the existing regulation

- **Repeals Circular CSSF 19/713** on security measures for operational and security risks of payment services under PSD2;
- **Updates Circular CSSF 12/552** on Central administration, internal governance and risk management, notably the requirements related to the IT function (section 5.2.3) and the role of IT function in the 3 lines of defence model (Part II Chapter 2);
- **Additional CSSF Risk Reporting obligations for payment service providers (PSP)**:
  - Credit institution: as soon as possible **after the closure of the financial year** and no **later than 30 April** of each calendar year;
  - E-money & Payment institutions: no later than **the last day of the third month after the closure of the financial year**;
  - Post Luxembourg: no later than one month after the AGM approving the accounts

**LSF: The Luxembourg Law dated 5 April 1993 on financial sector*
***LSP: The Luxembourg Law dated 10 November 2009 on payment services*

Clustering the main provisions



When complying with the provisions, **the "Principle of proportionality" (Section 3.1)** should be applied by taking into account the following characteristics:

- the **financial institutions' size**;
- their **internal organization**, and
- the **nature, scope, complexity and riskiness of the services and products** that the financial institutions provide or intend to provide.

Governance & Risk management

Governance & Strategy ICT Risk Mgt framework | **Information Security** | **ICT Operations, project & change management** | **Business continuity management** | **Payment service user relationship management**

Main considerations

- Management to set clear **roles & responsibilities** for ICT function, Information Security Risk Management and BCM
- Ensure adequate **skills** of staff & allocate appropriate **budget**
- Annual **training for all staff** on ICT and security risks
- **Align IT strategy with the overall business strategy** and measure level of achievement
- Ensure adequate oversight over **outsourced** functions and risk coverage in SLAs (EBA/GL/2019/02)
- Assign ICT risk management to **independent control function** segregated from IT Operations
- Establish and regularly review a fully integrated **ICT Risk Management framework** including regular management **reporting**, subject to regular independent **audits**

Governance & Strategy:

- IT strategy
- IT organizational chart and job descriptions
- Staff training plan
- Contracts with service providers

Risk management:

- ICT & Security risk management framework
- Risk report to Management
- Audit Plan and reports

Main findings of CSSF On-site inspections in 2019

Lack of IT strategy

Insufficient monitoring of IT activities

Lack of policies & procedures

Low coverage of ICT risks by the 2rd line of defense

Low coverage of IT activities in internal audit plan and lack of relevant ICT skills

Inadequate SLAs and oversight, often caused by over-reliance on the Parent company

Information Security

Main considerations

- Establish an **Information Security Policy** approved by Management to ensure the confidentiality, integrity and availability of assets and data
- **Implement security measures,** including
  - **Logical security** (i.e. access management / recertification / authentication / PAM / logging)
  - **Physical security (**i.e. protect premises, data centres and sensitive areas / protect from environmental hazards)
  - **ICT operations security** (i.e. security patching / configuration baselines / endpoint security / data encryption)
  - **Security monitoring** (i.e. detect anomalous activities/ physical or logical intrusion / information leakages, malicious code)
  - **Information security review, assessment & testing** (i.e. testing framework to cover vulnerability scans and penetration tests; testing for critical ICT systems (on annual basis) / non-critical ICT systems (every 3 years)
  - **Information security training & awareness** for all staff and contractors (at least annually)

Key documents

- Information Security Policy;
- Access management procedure
- ICT operations procedure
- Security monitoring procedure
- Information security testing framework
- Results of testing activities
- Annual training program

Main findings of CSSF On-site inspections in 2019

Management of cyber threats and remediation of critical vulnerabilities

Management of the privileged access rights (PAM)

ICT Ops - PM - Change management

Main considerations

ICT operations management

- Maintain up-to-date ICT **asset inventory** (including location, security classification and ownership) and manage their lifecycle
- **Log** and monitor critical ICT operations
- Implement **capacity planning** to prevent performance issues
- Ensure data and systems **backups** and restoration tests
- Establish an **incident management** process (classify / root cause analysis / internal & external communication)

ICT project & change management

- Implement an ICT **project management policy** to monitor **portfolio** of ICT projects and govern acquisition, development and maintenance of ICT systems; regular **management reporting**
- Ensure that **information security requirements** are analysed by an independent function
- Provide for dedicated **test** environments
- Identify and maintain **EUC** register
- Implement change management process including **emergency changes**

Key documents

ICT operations management

- ICT asset inventory
- Logging & monitoring and backup procedures
- Incident management procedure

ICT project & change management

- ICT PM policy
- ICT project plans
- ICT Project reporting to Management
- Evidences of formal approval of business requirements
- Test documentation & formal release approvals
- User & system documentation
- EUC register

Main findings of CSSF On-site inspections in 2019

Weak controls environments with regards to the security of new IT development practices such as Agile / DevOps

Business Continuity Management

Governance & Strategy ICT Risk Mgt framework | Information Security | ICT Operations, project & change management | **Business continuity management** | Payment service user relationship management

Main considerations

- Perform **Business Impact analysis (BIA),** linked to results of risk assessments (CIA) of business functions
- **Align the design of ICT systems & ICT services** with the Business Impact Analysis (e.g. redundancy of critical components)
- Establish documented **Business Continuity Plans (BCPs)** based on BIA results to be approved by Management. BCP should cover **different scenarios** including cyber-attacks or failure of third party providers
- Specify **RTO and RPO objectives**
- Develop **response and recovery plans** which consider both short-term and long-term recovery options
- **Annual testing and update** for critical functions, assessing plausible scenarios, switch-over to DR site, governance & communication and response measures
- Have effective **crisis communication measures**

Key documents

- Results of Business Impact Analysis
- Business continuity & Disaster recovery plans (BCP/DRP) including RTO & RPO objectives
- Continuity test reports & actions plans and evidence of follow-up based on identified weaknesses

Main findings of CSSF On-site inspections in 2019

Lack of governance

Inadequate BCPs & Testing

PSU Relationship management

Main considerations

- **Payment service providers (PSPs)** to establish processes, assistance and guidance to **enhance Payment service users (PSU) awareness of the security risks** linked to the payment services
- Guidance to PSU to be updated in case of **new threats and vulnerabilities**
- Allow PSUs to **disable specific payment functionalities** (if possible);
- Provide to PSUs **the option**
  - **to adjust spending limits** up to the maximum agreed limit;
  - **to receive alerts** on initiated/failed attempts to initiate payment transactions;
- PSP to inform PSU about **updates in security procedures**
- **PSP to assist PSU with security matters,** i.e. questions, support requests, reporting of anomalies

Key documents

- **Formal guidance and communication to PSUs** (incl. new threats and vulnerabilities and changes relating to security risks, assistance processes, updates in the security procedures)

Contact

Florian Bewig
Managing Director

pwc

2, rue Gerhard Mercator
L-1014 Luxembourg

Telephone: +352 49 48 48 4169
E-mail: florian.bewig@pwc.com

Thank you

www.pwc.lu

© 2020 PricewaterhouseCoopers, Société coopérative. All rights reserved.

In this document, “PwC” or “PwC Luxembourg” refers to PricewaterhouseCoopers, Société coopérative which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. PwC IL cannot be held liable in any way for the acts or omissions of its member firms.

EBA Guidelines in ICT and security risk management: Luxembourg' perspective

Cécile Gellenoncourt, Head of department, Supervision of Information Systems and Support PFS, CSSF

EBA Guidelines on ICT and security risk management

Luxembourg's perspective

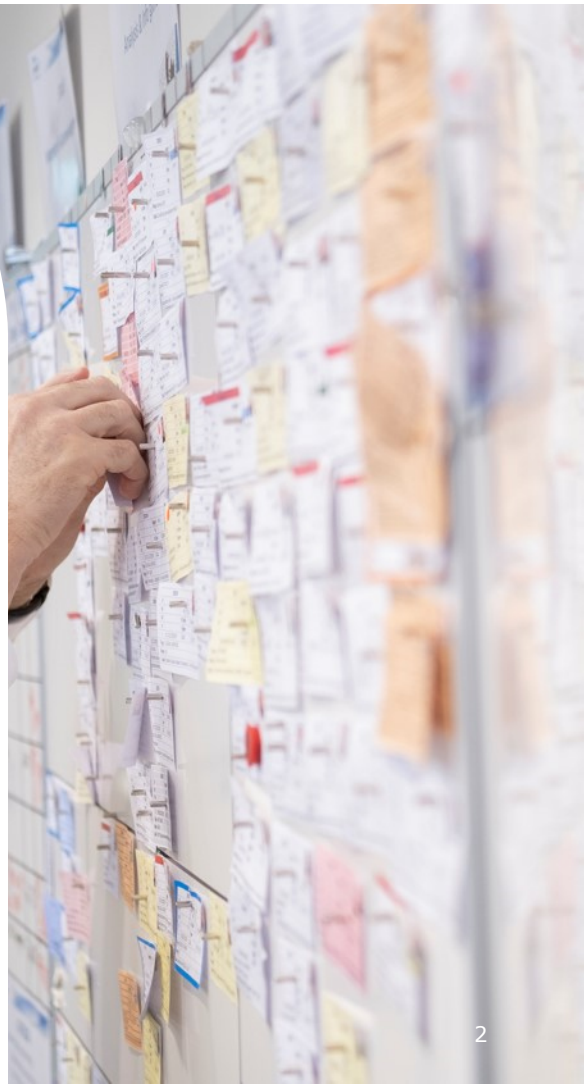
25 September 2020

cssf
Commission de Surveillance du Secteur Financier

Cécile Gellenoncourt
Supervision of information systems and Support PFS

Agenda

- **Why these guidelines?**
- More to come…
- Luxembourg implementation



Because ICT is important!

YEARS AGO…

NOW

- ICT systems:
  - **Support** and develop services to implement **the Bank's strategy**
  - **Automatize** and support all **internal control** frameworks
  - Improve **efficiency**
- ICT innovation is a source for **competitive advantages**
- Technology opens **new business opportunities**

Because ICT is important!

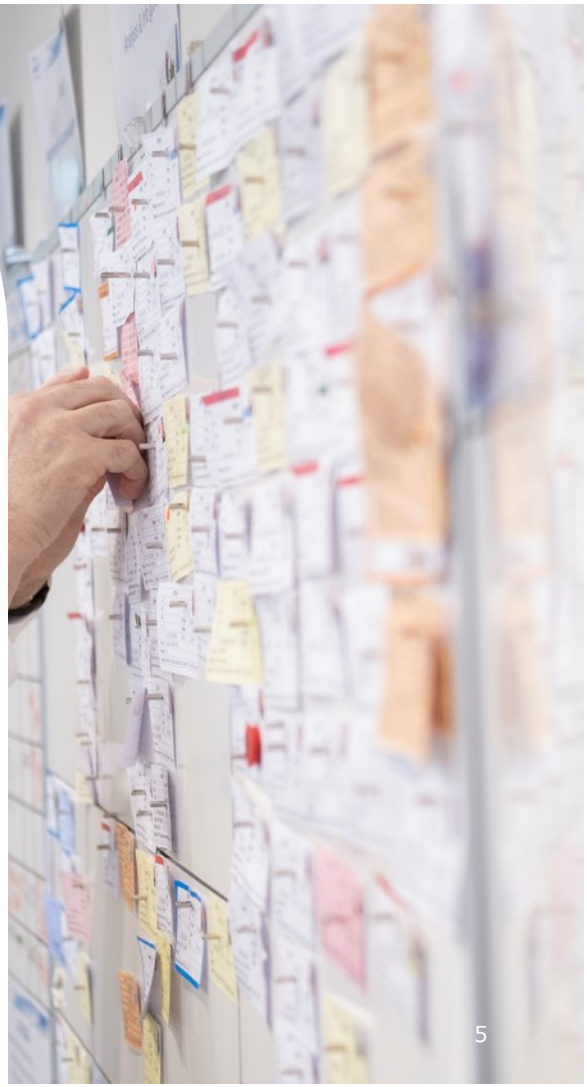
- BUT…
  - (Almost) total **dependency** on technology
  - Represents **significant costs**
  - Increasing level of ICT systems **complexity**
  - Everything is **interconnected** and **mobile**
  - Technology evolves at a **very fast pace**
  - **New competitors** appear
  - **Attackers** are using more and more sophisticated means

- LEADING TO…
  - **Operational risks** increase
  - Incidents revealed in real-time and spread very quickly, increasing **reputational risk**
  - Potential **financial impacts for FI** (market position, liquidity and cash flow, …) and **economic impacts** (very hard to quantify ex-ante)

➢ **Need for** sound ICT and security **risk management**

Agenda

- Why these guidelines?
- **More to come…**
- Luxembourg implementation



A logical continuation of EU texts…

- How banking supervisors should cover ICT and security risks within supervision?
  - EBA GL on ICT risk assessment under SREP (EBA/GL/2017/05)
  - But only for bank supervision and not addressed to entities

- What is expected from entities to manage their ICT and security risks?
  - EBA GL on security measures for operational and security risks under the PSD2 (EBA/GL/2017/17) adopted via Circular CSSF 19/713.
    - But addressed to PSPs only for payment services.
  - EBA GL on outsourcing (EBA/GL/2019/02)
    - Addressed to all entities under EBA's remit (B, IF, PI, EMI)
    - Adoption through a CSSF circular ongoing
    - But cover only (IT) outsourcing risk management

- EBA GL on ICT and security risk management
- Adressed to all entities under EBA's remit
- All ICT and security risks to which the entity is exposed

But above all an element of a broader plan: the DORA

- Following a joint advice from the 3 European Supervisory Authorities (EBA, ESMA, EIOPA)
- Objective: to develop a single regulatory and supervisory rulebook for ICT operational resilience in the financial sector
- Legislative proposal published on 24/09/2020
- Final voted text….End of Q1 / Q2 2022?

Digital

Operational

Resilience

for financial services

Act

But above all an element of a broader plan: the DORA

- Four main areas expected to be covered in Level 1 texts:
  - Requirements on **ICT and security risk management** in the legislative acquis applicable to the financial sector,
  - Incident reporting requirements
  - Digital operational resilience testing framework and,
  - Oversight of ICT third party providers to the financial institutions.
- Mandates to ESAs to specify further in guidelines and/or regulatory technical standards (RTS)

Digital

Operational

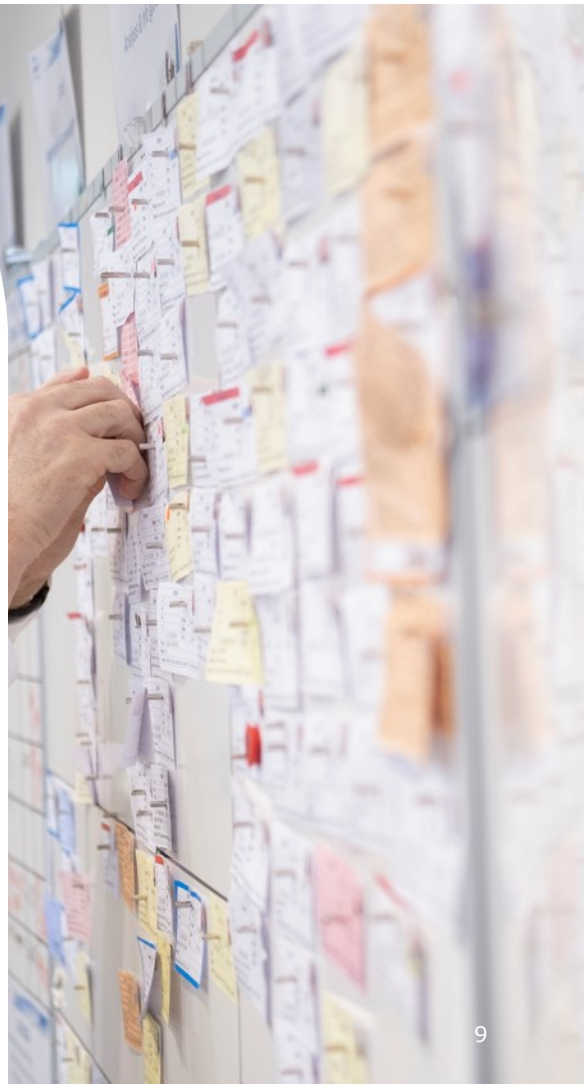
Resilience

for financial services

Act

Agenda

- Why these guidelines?
- More to come…
- **Luxembourg implementation**



CSSF circular 20/750

- Adopt the guidelines without modification
- Extend the scope to Specialised PFS and to Support PFS
  - Rely also on IT
  - Are exposed to IT risks too
  - Can bring risks to partners
- Proportionality principle
  - Upwards or downwards
  - E.g. expected upwards for Operator of essential services (OSE) under NIS law

Changes to CSSF circular 12/552

- Consequence
  - Identification of ICT provisions in other circulars (apart from IT outsourcing related ones) => only 12/552 impacted
  - Comparison / compatibility with the circular 20/750 and the ICT and security risk management guidelines
  - Decision to delete ICT provisions of circular 12/552 already covered in 20/750 and insertion of a cross-reference to CSSF circular 20/750

- Principle = all ICT risk related provisions in one single text

Changes to CSSF circular 12/552

- The organisation of the IT function and internal control?
  - Section 3.2 Governance and strategy
  - Section 3.3.1. Organisation and objectives
- The monitoring process (including patch management)
  - Section 3.4.4. ICT operations security (para. 36)
  - Para. 25 for audit requirement
- The need for back-up
  - Para. 57

- Deletion of passages that are also covered in the new circular (see e.g. some references to the new circular (para. of the EBA GL))

Changes to CSSF circular 12/552

- The appointment of an "IT officer" and a "CISO"
  - Para. 2 and 11
- No "CISO" title but a "control function"
  - No prescriptive positioning in the organizational chart but:
    - independence and objectivity must be ensured
    - by appropriately segregating it from ICT operations processes
  - Principle of proportionality applies as for the whole circular

- Deletion of passages that are also covered in the new circular (see e.g. some references to the new circular (para. of the EBA GL))

Thank you for your attention

cssf
Commission de Surveillance
du Secteur Financier

The role of PSF de support for ICT and security risk management in Luxembourg

Cédric Mauny, Cybersecurity Lead,
Proximus Luxembourg

The role of Support-PSFs for ICT and security risk management in Luxembourg

25 September 2020

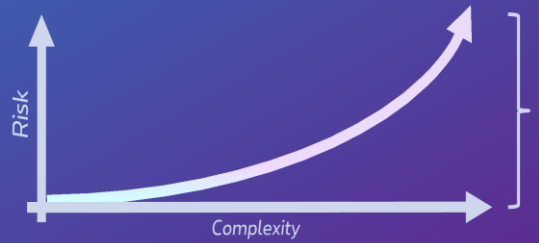
Cédric Mauny
Cybersecurity Lead
Proximus Luxembourg S.A.

proximus

Proximus Luxembourg S.A. – External Communication – restricted audience

ICT and security risk management become increasingly more important in today's interconnected world

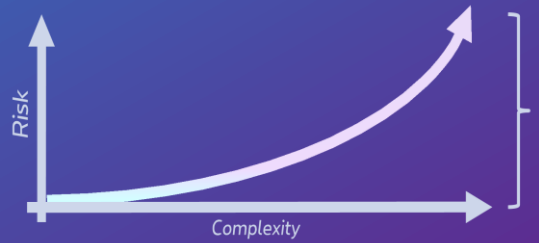
"The complexity of information and communication technology (ICT) and security risks is increasing and the frequency of ICT and security-related incidents (…) is rising, together with their potential significant adverse impact on _____ institutions' operational functioning. Moreover, due to the interconnectedness of _____ institutions, ICT and security-related incidents risk causing potential systemic impacts."



Year over year, the complexity of IT systems has been increasing, and the risk exposure rising accordingly

ICT and security risk management become increasingly more important in today's interconnected world

"The complexity of information and communication technology (ICT) and security risks is increasing and the frequency of ICT and security-related incidents (…) is rising, together with their potential significant adverse impact on financial institutions' operational functioning. Moreover, due to the interconnectedness of financial institutions, ICT and security-related incidents risk causing potential systemic impacts." EBA, Final draft Guidelines on ICT and security risk management, 2019



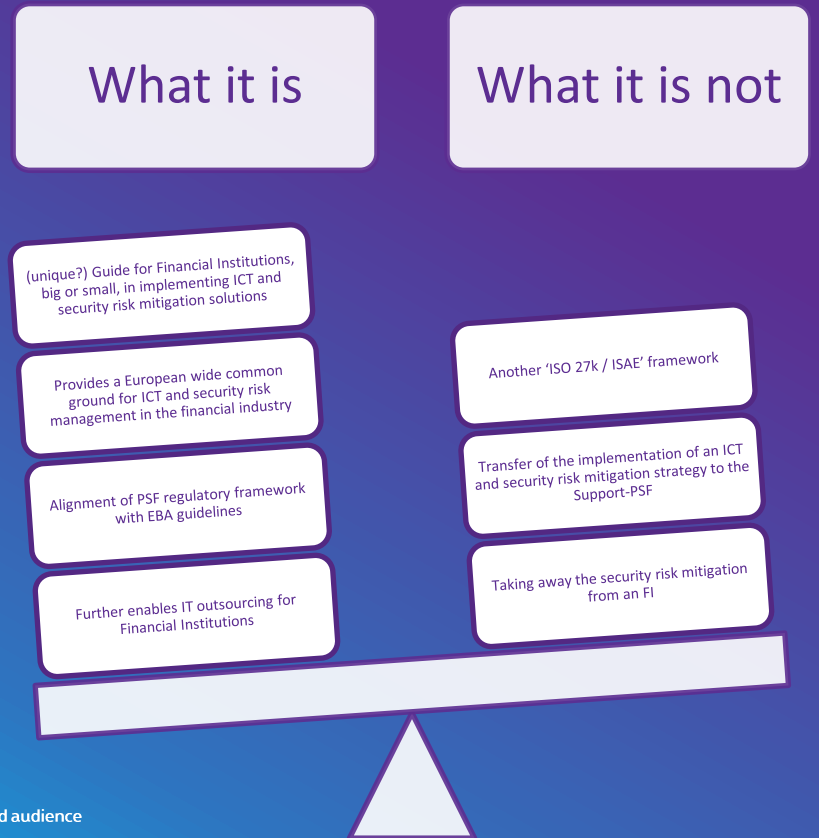
Year over year, the complexity of IT systems has been increasing, and the risk exposure rising accordingly

The financial sector is the largest user of information and communications technology (ICT) in the world, accounting for about a fifth of all ICT expenditure

Source : Statista

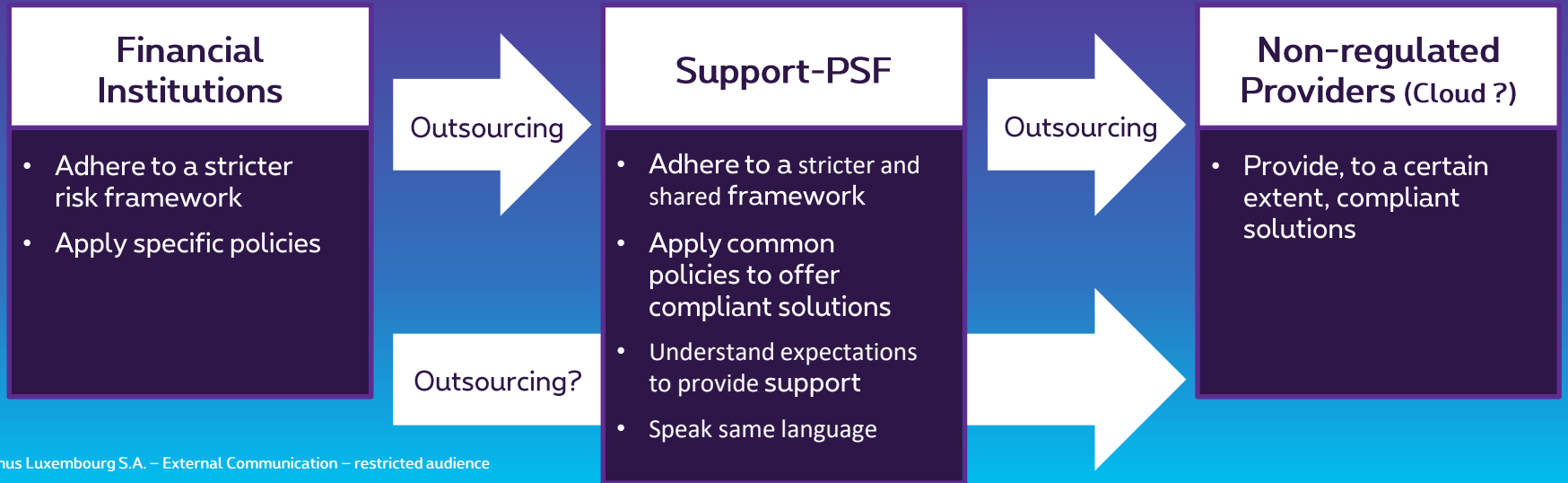
Key elements that paved the way for the Support-PSF to become the trusted advisor for regulated customers

CSSF circular 20/750, what it is but also what it isn't in regards to Support-PSF's offered solutions



The impact of CSSF circular 20/750 on outsourcing activities of regulated institutions and their partner ecosystem

- By nature, Support-PSFs are familiar with some (not all) requirements that apply to FI
- Defining more explicitly risk management in relation to ICT and security finally puts legal requirements on something that was known and applied by many
- For Support-PSFs, the applicability of this circular means that their internal IT but also their service portfolio and solutions must comply and provide compliant solutions
- These guidelines will ultimately enforces the Trust through the whole chain of outsourcing



Are Support-PSFs ready for this circular? What needs to be done?

Effort to be compliant with CSSF circular 20/750 should be reasonable considering Support-PSFs are expected to already have suitable governance and risk mitigations in place for ICT & Security risks (application of frameworks or certifications on top of existing Circulars)

1st line of defense can be considered as the core-function of the Support-PSFs → should be under control + specific attention to additional guidelines (continuity, operations, change, backup, …)

Specific attention and efforts should be given to the 2nd and 3rd line of defense

- Risk management
- Internal Audit

- Do not underestimate the importance to give assurance that the service organisation has adequate internal controls
  - through Service Organization Control reports (ISAE 3402 / SOC report)

What added value does the circular bring to Support-PSFs and how can it secure the market?

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

Circular 20-750 defines minimum requirements to be met in regards to ICT security, allowing Support-PSFs to provide additional services to secure its customers and towards the ecosystem (we are all interconnected)

On top of a suitable strategy, governance, 2nd and 3rd LoD, business continuity, operations and change management) security measures should include:

	Preventive	Defensive	Detective	Reactive	Offensive	Predictive	CSIRT / CERT
1.4.2. Logical security	✓	✓	✓				
1.4.3. Physical security	✓						
1.4.4. ICT operations security	✓	✓	✓		✓	✓	✓
1.4.5. Security Monitoring	✓	✓	✓	✓	✓	✓	✓
1.4.6. Information security reviews, assessment and testing	✓	✓	✓		✓	✓	✓
1.4.7. Information security training and awareness	✓						

Compliance is nice, managing the effective exposure to the risk is better

> 41. [...] simulations de cyber-attaques avec équipe adverse (dite «rouge»).
> 48.Sur la base des menaces identifiées pour la sécurité et des changements apportés, des tests qui incluent des scénarios d'attaques potentielles pertinentes et connues devraient être réalisés.

In conclusion

EBA Guidelines on ICT and Security Risk Management recall a common sense when it comes to ICT and security risks and constitutes a logical extension of the current regulated outsourcing framework

Because it transforms the good practices that were already followed by the majority of regulated actors into binding rules, as a Support-PSF, this new Circular should be seen as an opportunity for our sector to give more confidence in the ecosystem, to their customers, to some extent to their Regulator, and maybe to other EU banking sector

It enables Support-PSFs with a stricter risk governance framework to better serve regulated and non-regulated industries, therefore it could also benefits all verticals, regulated and non-regulated, for a sustainable economy in an ever more complex world while preserving the principle of proportionality

As example, the CISO *function* should clearly be positioned as 2nd line of defense (?!)
This should made a reference for levelling up every economic sector to foster digital trust globally by addressing the ICT and security risks at the appropriate level of decision

It remains some open-points, such as how the CSSF will align the CSSF circulars to EBA Guidelines on Outsourcing (to which reference is made in the EBA guidelines on ICT and Security risks) but keeping in mind the principle of proportionality and looking for harmonisation with all the risk regulation frameworks?

Thank you

Proximus Luxembourg S.A.© 2020 - This presentation is for general information and discussions purposes only and the imbedded information are subject to change without further notice.
Statements, figures and images are only indicative. Proximus Luxembourg S.A. makes no representation or warranty regarding, and assumes no responsibility or liability for, the accuracy or completeness of, or any errors or omissions in, any information contained herein. It does not constitute an offer, commitment or contract. This presentation is also subject to intellectualproperty rights. No part of it should be reproduced, adapted or communicated without the written consent of Proximus Luxembourg SA.

The Proximus Group, a reference shareholder

4 core businesses

ICT services / Telephony
Connectivity / TV

+80 years
experience

The **incumbent**
Operator in Belgium

5 686 M€
Turnover in 2019

Proximus Luxembourg

tango

telindus

Guillaume Boutin,
CEO of Proximus Group

Gérard Hoffmann,
CEO of Proximus Luxembourg

12 931
employees worldwide

750
employees in Luxembourg

Our total Proximus ICT ecosystem today

proximus

FINANCE & TECHNOLOGY LUXEMBOURG

Panel discussion

***Moderator**: Laurent de la Vaissière, FTL - KPMG*

Cécile Gellenoncourt, CSSF

Nabil Meziani, Raiffeisen

Florian Bewig, PwC

Cédric Mauny, Proximus Luxembourg

Concluding remarks

Jean-François Terminaux, Chairman, FTL

FINANCE & TECHNOLOGY LUXEMBOURG

We thank you for your attention.

We remain at your disposal for any further question.