

CSSF Circular 20/750

How does it affect your organisation?

Webinar 29 October 2020

Jean-Hubert Antoine



Introduction



1. The CSSF aligns with the EBA for ICT/Secu risk management
EBA/GL/2019/04 (29/11/2019) - apply from 30 June 2020.
2. PSP additional requirement:
PSPs are obliged to provide the CSSF with an up-to-date and comprehensive risk assessment

EBA/GL/2019/04



Modifying CSSF 12/552, Replace 19/713 – apply from 25 August 2020

Executive Summary



This circular, entirely based on EBA Guidelines is a combination of ICT, Security and Business Continuity best practices.

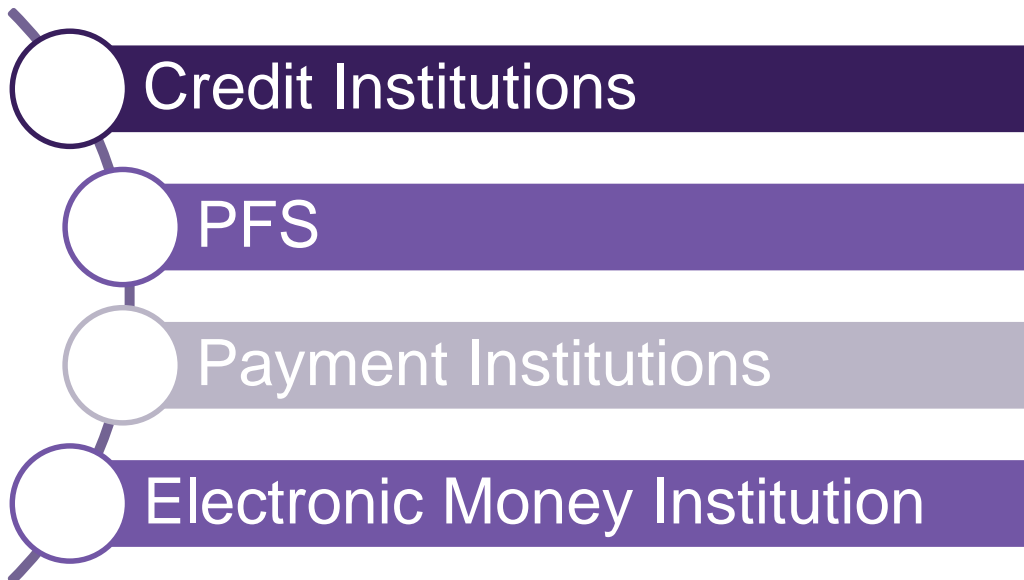
There are similarities or alignments with:

- ISO27005 (Risk Management)
- ISO27002 (Security Measures)
- ITIL (ICT operations)
- ISO22301 (Business Continuity)



Scope

Financial Sector and Payment Services - LFS, LPS



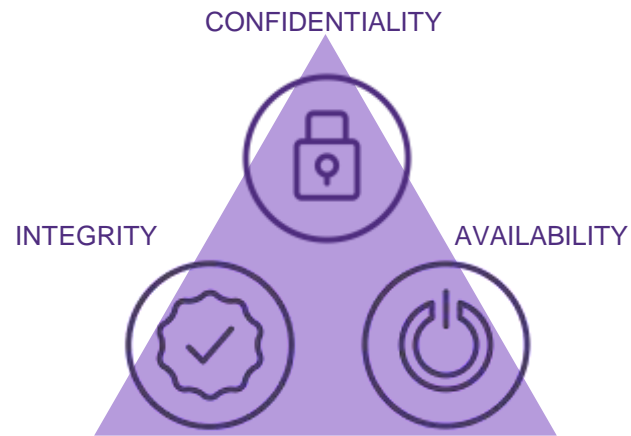
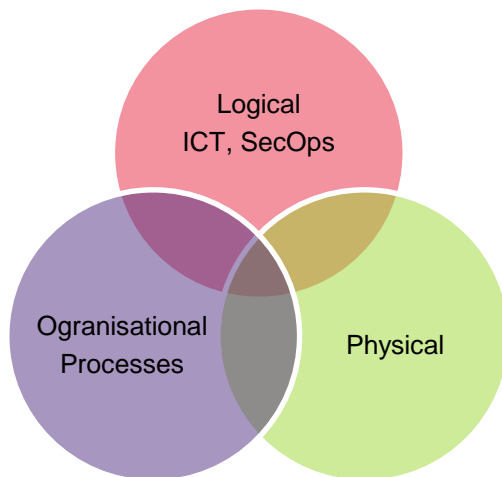
ICT and security risks



Risk of loss due to breach of Confidentiality, Integrity and Availability.

Resulting from internal processes failure, Cyber-Attack, or Physical security problem:

- Organisational
- Technical
- Physical



Governance and Strategy



Proportionality (adequate governance)

Governance aspects:

- Secu and ICT Strategy
(Align with Business, with Objectives, Plans)
- R&R
- Skills/training/Awareness (annual or more)
- Management Review
- Risk Management
- Third Party Mgt



Governance and Strategy



Third Party Management

SLA, Contracts includes:

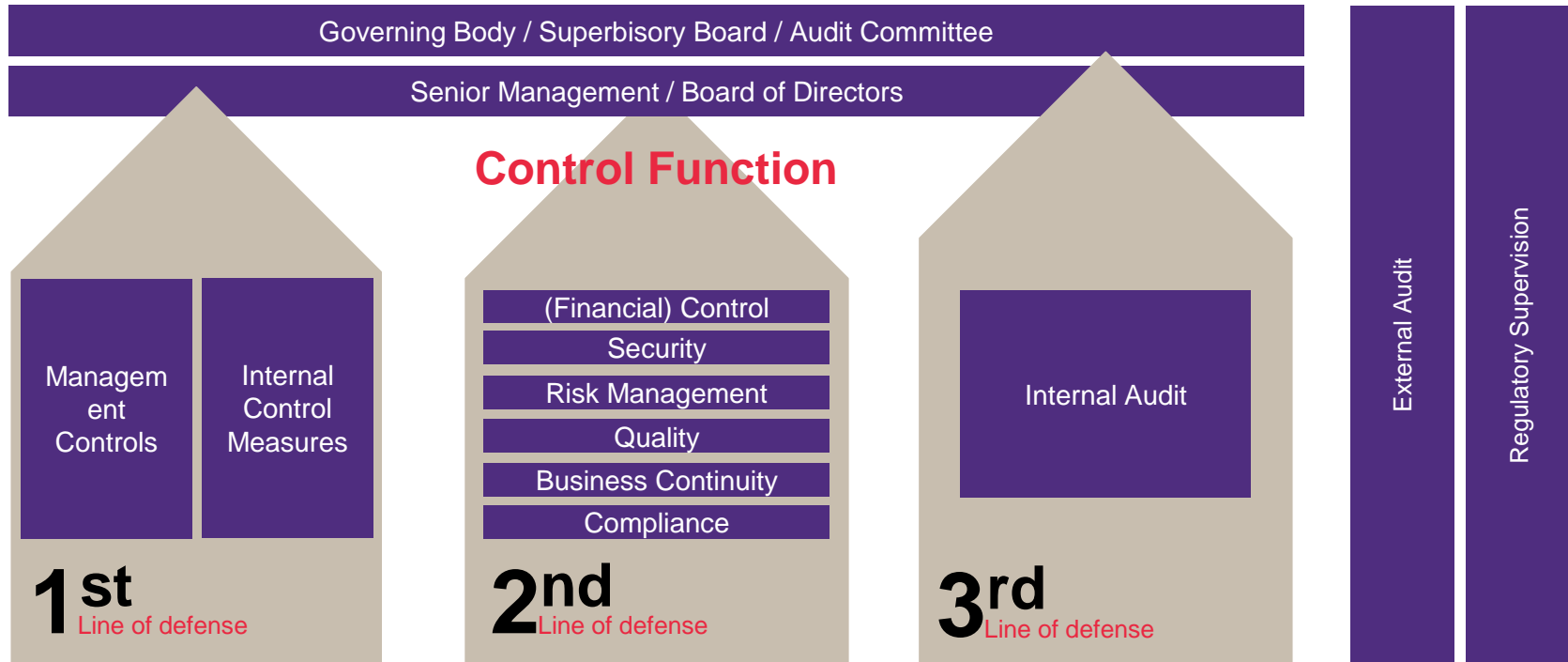
- Security objectives and measures
- Incident Handling
 - Risk Assessment and Mitigating Measures
 - Monitor Compliance



Governance – Control Function



Control Function, independant and objective (different from Internal Audit)



ICT and Risk Management Framework



Risk Management **Controls and processes** to ensure a proper risk management

Framework – (in line with ISO27005):

- Set of processes to ensure ICT/Security Management
- R&R defined
- Should be integrated into overall risk management processes.
- Continuous Improvement
- Management Review

ICT and Risk Management Framework



Risk Identification

- Assets and processes mapping
- Classification with C,I,A at minimum

Risk Assessment – yearly or more

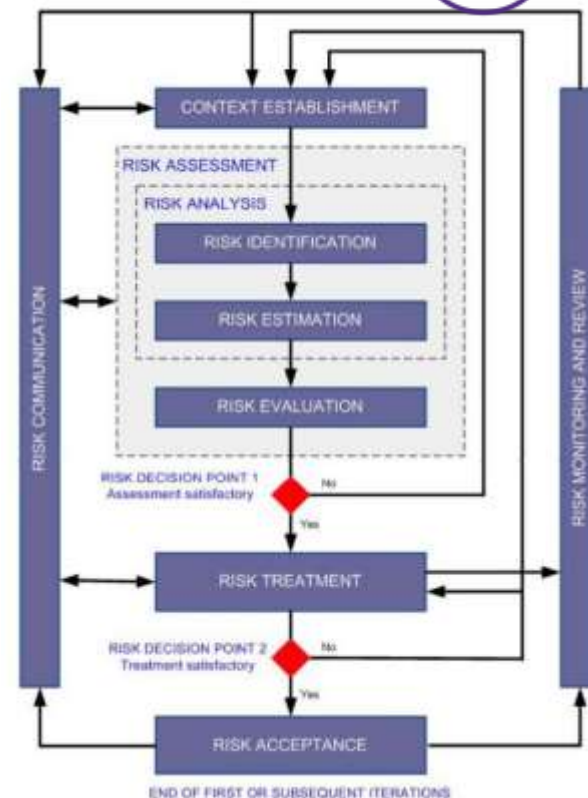
Threat and Vulnerability Monitoring, Risk review

Risk Mitigation

- Select and implement mitigation measures

Reporting

Audit



Information Security



Information Security Policy (CIA, Objectives, approval, R&R)

Security Measures (according to risks)

a) Organisation and governance

b) Logical security (IAM, PAM)

c) Physical security

d) ICT operations security

e) Security monitoring

f) Information security reviews, assessment and testing

g) Information security training and awareness

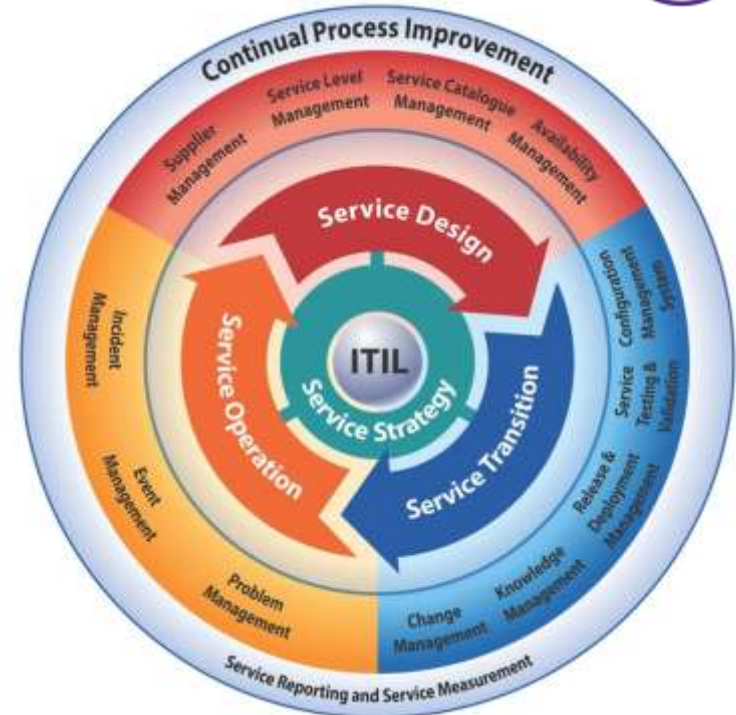
- Vulnerability and Patch Mgt
- Secure Configurations
- Network Security
- DLP
- Endpoint Security
- Encryption
- ...

ICT Operations Management



1. Processes and procedures
2. Inventory
3. Performance Mgt of operations
4. Logging and monitoring
5. Configuration Management
6. ICT lifecycle Management
7. Performance and Capacity Planning
8. Backup/Restore

Incident and Problem Management



ICT Project and Change Management



- Project Management Governance
- ICT Acquisition and Development
- ICT Change Management (incl. Security and Risk Management)

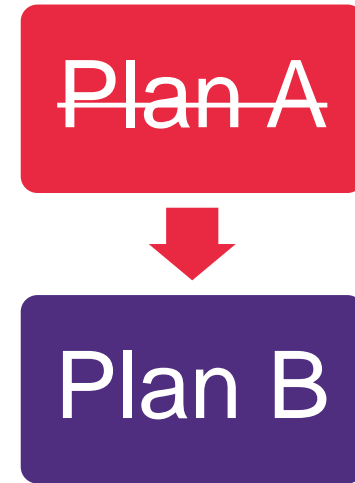


Business Continuity



In line with ISO22301

- BIA (on C,I,A)
- BIA quantitatively and qualitatively
- Designs aligned with BIA
- Business Continuity Planning
- Response and Recovery Plans
- Testing
- Crisis Communication



PSU relationship Management



- Awareness of risks
- Assistance
- Alerting/Communication



GT Advisory Tailored Services



Check Compliance Assessment

- High Level / Strategic
- Detailed / Tactical

Plan Remediation

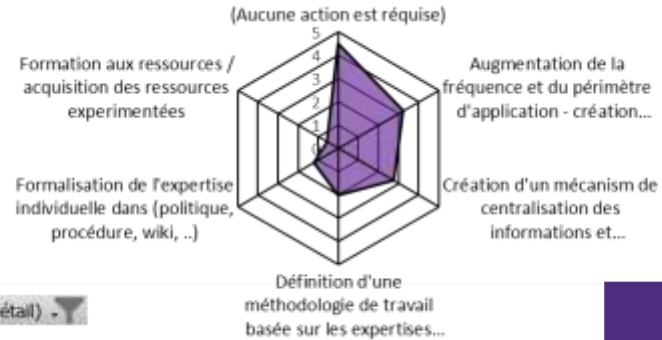
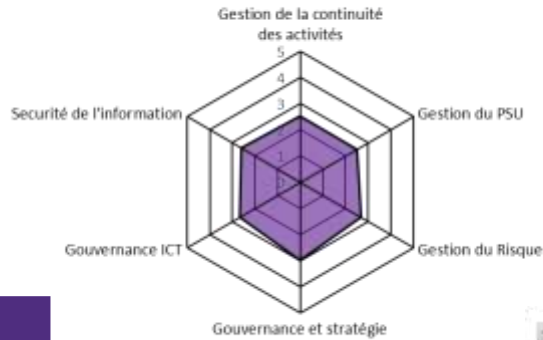
- Objectives and Strategy
- Actions
- Program Management
- Resources

DO Implement

- ICT Governance
- Security Governance
- Risk Management
- Business Continuity
- PSU/PSD2

Focus du plan d'action de la continuité des activités

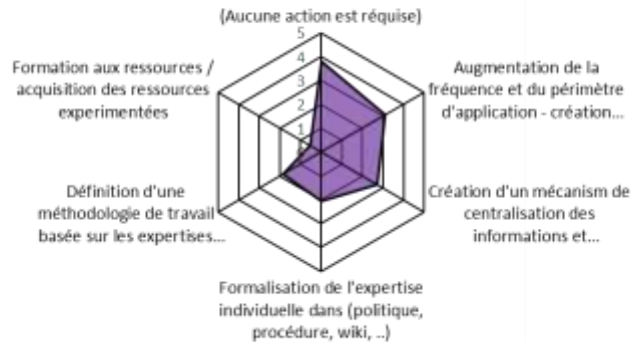
Maturite - Vue d'ensemble



Level 1

Level 2

Focus du plan d'action - Vue d'ensemble



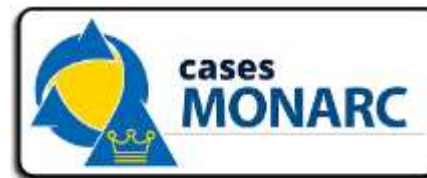
Focus du plan d'action de la continuité des activités



GRC Platforms



Excel	GRC Tool
Manual input Manual reporting Single User	<ul style="list-style-type: none">• Automation• Standard Frameworks• Collaboration• Reporting• Task Management• Efficient Data Mgt• Up-to-date



OneTrust GRC
INTEGRATED RISK MANAGEMENT

KnowBe4

KCM
Audits Done Half The Time.

Q&A session

Stay Tuned

Next Webinar:

**Sustainability: own your action;
be aware of your impact**

26th November 2020

Time: 11.00 am



SAVE THE DATE

Friday 4th December - 9:30 am

**IT Resilience
in the financial industry**

Phygital Workshop by LCL

 Jean-Francois BILLIN
Founder - LCL

 David HAGEN
Founder - Hagen Advisory

 Jean-Yves MATHIEU
ISO - Grant Thornton

The graphic features a background image of hands working on a laptop with a blue overlay. The text is centered and uses a mix of white and teal colors. Three circular headshots of the speakers are arranged horizontally at the bottom.

En partenariat avec:



Grant Thornton



Contact



Jean-Hubert Antoine

Senior Manager - Chief Information Security Officer (CISO)

T +352 45 38 78 525

M +352 621 385 710

E jean-hubert.antoine@lu.gt.com

© 2020 Grant Thornton Luxembourg. All rights reserved.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton Luxembourg and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.