Luxembourg, March 06th, 2020

Response to the EU Commission consultation on Digital Operational Resilience Framework for Financial Services: Making the EU financial Sector more secure

Introduction

The Association of the Luxembourg Fund Industry (ALFI) represents the face and voice of the Luxembourg asset management and investment fund community. The Association is committed to the development of the Luxembourg fund industry by striving to create new business opportunities, and through the exchange of information and knowledge.

Created in 1988, the Association today represents over 1,500 Luxembourg domiciled investment funds, asset management companies and a wide range of business that serve the sector. These include depositary banks, fund administrators, transfer agents, distributors, legal firms, consultants, tax advisory firms, auditors and accountants, specialised IT and communication companies. Luxembourg is the largest fund domicile in Europe and a worldwide leader in cross-border distribution of funds. Luxembourg domiciled investment funds are distributed in more than 70 countries around the world.

We thank the European Commission for the opportunity to participate in this consultation on Digital Operational Resilience Framework for Financial Services

As permissible under the regulatory framework for the financial institution, we would strongly recommend an approach whereby "all financial institutions should comply with the provisions set out in the future guidelines in such a way that is proportionate to, and takes account of, 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.

Please kindly note that the answers / opinions expressed in this paper are the outcome of discussions in the ALFI Cybersecurity Working Group in relation to this consultation. These answers/opinions are not specific to any organizations, but are the thoughts and observations of the ALFI Cybersecurity Working Group in relation to the industry

Response to the consultation

1. *Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?*

   ✓ ☐ *Yes*

   ☐ ☐ *No*

   ☐ ☐ *Don't know/no opinion*

   ☐ *To the extent you deem it necessary, please explain your reasoning. [Insert text box]*

2. *Where in the context of the risk management cycle has your organisation until now faced most difficulties, gaps and flaws in relation to its ICT resilience and preparedness? Please rate each proposal from 1 to 5, 1 standing for 'not problematic' and 5 for 'highly problematic').*

Stage in the risk management cycle (or any other relevant related element)	*1*	*2*	*3*	*4*	*5*	*Don't know/not applicable*
Identification					✓	
Detection				✓		
Ability to protect					✓	
Respond				✓		
Recovery					✓	
Learning and evolving				✓		
Information sharing with other financial actors on threat intelligence					✓	
Internal coordination (within the organisation)				✓		
				✓		
Other (please specify)						

All of the above vary from one organization to the other. Although there are more focus and developments, these items are still challenging.

3. *What level of involvement and/or what type of support/ measure has the Board (or more generally the senior management within your organisation) offered or put in place/provided for, in order to allow the relevant ICT teams to effectively manage the ICT and security risk? Please rate each proposal from 1 to 5, 1 standing for 'no support/ no measure' and 5 for 'high support/very comprehensive measures').*

Type of involvement, support or measure	*1*	*2*	*3*	*4*	*5*	*Don't know/not applicable*
Appropriate allocation of human and financial resources		✓				
Appropriate investment policy in relation to the ICT and security risks		✓				
Approval by the Board of an ICT strategy (that also deals with ICT security aspects)			✓			
Active role of the Board (or the senior management) when your organisation faces major cyber incidents or, as the case may be, role of the Board in the ICT business continuity policy		✓				

Top leadership and guidance received in relation to ICT security and ICT risks		✓				
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning and emphasize in addition any type of support and measure that you consider that you consider the Board and senior management should provide. [Insert text box]

4. *How is the ICT risk management function implemented in your organisation?*

   To the extent you deem it necessary, please explain your reasoning. [Insert text box]

5. *Which main arrangements, policies or measures you have in place to identify and detect ICT risks?*

Type of arrangement, policy, measure	*Yes*	*No*	*Don't know/not applicable*
Do you establish and maintain updated a mapping of your organisation's business functions, roles and supporting processes?	✓		
Do you have an up-to-date registry/inventory of supporting ICT assets (e.g. ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes)?	✓		
Do you classify the identified business functions, supporting processes and information assets based on their criticality?	✓		
Do you map all access rights and credentials and do you use a strict role-based access policy?		✓	
Do you conduct a risk assessment before deploying new ICT technologies / models?	✓		
Other (please specify)			

Most of the above are work in progress for many organisations and the oganisations' answers to the above depend on the regulations, their licences, the type of firms, their business and risk profile and resources,

6. *Have you experienced cyber-attacks with serious repercussions for your clients or counterparties?*

   Yes

   ✓ *No*

   Don't know/Not applicable

To the best of our knowledge, Luxembourg industry has not experience major cyber attacks with serious repercussions for the clients and counterparties. Also, the industry needs better collaboration and cooperation in relation to sharing the cyber incidents in an anonymous way.

7. *How many cyber-attacks does your organisation face on average every year? How many of these have/are likely to create disruptions of the critical operations or services of your organisation?*

   Please explain your reasoning. [Insert text box]

8. *Do you consider that your ICT systems and tools are appropriate, regularly updated, tested and reviewed to withstand cyber-attacks or ICT disruptions and to assure their operational resilience? Which difference do you observe in this regard between in-house and outsourced ICT systems and tools?*

   Yes

   ✓ *No*

   Don't know/Not applicable

   Some companies do not have robust processes about outsourcing oversight. This varies from one company to the other.

9. *Has your organisation developed and established a cloud strategy?*

   ✓ *Yes*

   No

   Don't know/no opinion

10. *If the answer to the previous question (no. 9) is yes, please explain which of the following aspects are covered and how.*

	Yes	*No*	*Don't know/not applicable*
Do you use on-premise cloud technology?	✓		
Do you use off-premise cloud technology	✓		
Does this strategy contribute to managing and mitigating ICT risks?	✓		
Do you use multiple cloud service infrastructure providers? How many?	✓		
Did your Board and senior management establish a competence center for cloud in your organisation?	✓		

Most of the above are in place in the organisations in Luxembourg further to the CSSF Cloud Circular.

11. *Do you have legacy ICT systems that you would need to reconsider for enhanced ICT security requirements? What would be the level of investments needed (in relative or absolute terms)?*

✓ *Yes*

No

Don't know/Not applicable

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

12. *What in your view are possible causes of difficulties you experienced in a cyber-attack/ ICT operational resilience incident? Please rate each answer from 1 to 5, 1 standing for 'not problematic' and 5 for 'highly problematic').*

Causes of difficulties	*1*	*2*	*3*	*4*	*5*	*Don't know/not applicable*
ICT environmental complexity				✓		
Issues with legacy systems					✓	
Lack of analysis tools				✓		
Lack of skilled staff				✓		
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

13. *Do you consider that your organisation has implemented high standards of encryption?*

✓ *Yes*

No

Don't know/Not Applicable

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

14. *Do you have a structured policy for ICT change management and regular patching and a detailed backup policy?*

✓ *Yes*

No

Don't know/not Applicable

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

15. *Do you consider that your organisation has established and implemented security measures to manage and mitigate ICT and security risks (e.g. organisation and governance, logical security, physical security, ICT operations security, security monitoring, information security reviews, assessment and testing, and/or information security training and awareness measures)?*

✓ *Yes*

No

Don't know/Not applicable

There might be inconsistencies in standards and controls. The above is a generic answer.

16. *On average, how quickly do you restore systems after ICT incidents, in particular after a serious/major cyber-attack? Are there any differences in that respect based on where the impact was (impact on the availability, confidentiality or rather the integrity of data)?*

    To the extent you deem it necessary, please specify and explain. [Insert text box]

    Most organisation will categorise the classification on the cyberattack to assess the impact to their organisation in order to assess the remedial solution and extent of impact.

17. *Which issues you struggle most with, when trying to ensure a quick restoration of systems and the need to maintain continuity in the delivery of your (critical) business functions?*

Issues	*Yes*	*No*	*Don't know/not applicable*
Lack of comprehensive business continuity policy and/or recovery plans		✓	
Difficulties to keep critical/ core business operations running and avoid shutting down completely		✓	
Internal coordination issues (i.e. within your organisation) in the effective deployment of business continuity and recovery measures	✓		
Lack of common contingency, response, resumption/recovery plans for cyber security scenarios - when more financial actors in your particular ecosystem are impacted	✓		
No ex-ante determination of the precise required capacities allowing the continuous availability of the system		✓	
Difficulties of the response teams to effectively engage with all relevant (i.e. business lines) teams in your organization to perform any needed mitigation and recovery actions	✓		
Difficulty to isolate and disable affected information systems	✓		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

18. *What are your views on having in the legislation a specific duration for the Recovery Time Objective (RTO) and having references to a Recovery Point Objective (RPO)?*

    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Due to the complexity of the impact it would be inappropriate to apply a generic recovery time. It is essential that an organisation has the ability to begin to immediately assess the impact the consequences and to prudently establish and invoke a recovery plan.

19. *Through which activities or measures do you incorporate lessons post-incidents and how do you enhance the cyber security awareness within your organisation?*

	Yes	*No*	*Don't know/not applicable*
Do you promote staff education on ICT and security risk through regular information sessions and/or trainings for employees?	✓		
Do you regularly organize dedicated trainings for the Board members and senior management?		✓	
Do you receive from the Board all the support you need for implementing effective cyber incident response and recovery improvement programs?		✓	
Do you make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents? Do you conduct ex post root cause analysis of cybersecurity incidents?	✓		
Other (please specify)			

Some of the answers in relation to the Boards depends on the issue and it is not always consistent. This was the reason for the "No" answers.

20. *Is your organisation currently subject to ICT and security incident reporting requirements?*

✓ *Yes*

No
Don't know/Not applicable

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

21. *Do you agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities?*

✓ *Yes*

No

Don't know/Not applicable

To the extent you deem it necessary To the extent you deem it necessary, please explain your reasoning. [Insert text box]

22. *If the answer to the previous question (no. 21) is yes, please explain which of the following elements should be harmonised?*

Elements to be harmonised in the EU-wide system of ICT incident reporting	*Yes*	*No*	*Don't know/not applicable*
Taxonomy of reportable incidents	✓		
Reporting templates	✓		
Reporting timeframe	✓		
Materiality thresholds		✓	
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

23. *What level of detail would be required for the ICT and security incident reporting? Please elaborate on the information you find useful to report on, and what may be considered as unnecessary.*

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

24. *Should all incidents be within the scope of reporting, or should materiality thresholds be considered, whereby minor incidents would have to be logged and addressed by the entity but still remain unreported to the competent authority?*

✓ *Yes*

No

Don't know/Not applicable

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

25. *Which governance elements around ICT and security incident reporting would be needed? To which national competent authorities should ICT and security incidents be reported or should there be one single authority acting as an EU central hub/database?*

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

26. *Should a standing mechanism to exchange incident reports among national competent authorities be set up?*

✓ *Yes*

No

Don't know/Not applicable

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

27. *What factors or requirements may currently hinder cross-border cooperation and information exchange on ICT and security incidents?*

To the extent you deem it necessary, please explain your reasoning and provide concrete examples. [Insert text box]

28. *Is your organisation currently subject to any ICT and security testing requirements?*

✓ *Yes*

No

Don't know/Not applicable

If the answer is yes:

	Yes	*No*	*Don't know/ not applicable*
Do you face any issues with overlapping or diverging obligations?	✓		
Do you practice ICT and security testing on a voluntary basis?	✓		

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

29. *Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools? What could its different elements be?*

Different elements of a baseline testing/assessment framework	*Yes*	*No*	*Don't know/ not applicable*
Gap analyses?	✓		
Compliance reviews?	✓		
Vulnerability scans?	✓		
Physical security reviews?	✓		
Source code reviews?	✓		
Others (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

30. *For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be designated by competent authorities) as "significant" on the basis of a combination of criteria such as:*

Criteria	*Yes*	*No*	*Don't know/ not applicable*
Proportionality–related factors (i.e. size, type, profile, business model)?	✓		
Impact – related factor (criticality of services provided)?	✓		
Financial stability concerns (Systemic importance for the EU)?	✓		

Other appropriate qualitative or quantitative criteria and thresholds (please specify)?			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

31. *In case of more advanced testing (e.g. TLPT), should the following apply?*

	Yes	*No*	*Don't know/ not applicable*
Should it be run on all functions?		✓	
Should it be focused on live production systems?		✓	
To deal with the issue of concentration of expertise in case of testing experts, should financial entities employ their own (internal) experts that are operationally independent in respect of the tested functions?	✓		
Should testers be certified, based on recognised international standards?	✓		
Should tests run outside the Union be recognised as equivalent if using the same parameters (and thus be held valid for EU regulatory purposes)?	✓		
Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model?	✓		
Should the ESAs be directly involved in developing a harmonised testing framework (e.g. by issuing guidelines, ensuring coordination)? Do you see a role for other EU bodies such as the ECB/SSM, ENISA or ESRB?	✓		
Should more advanced testing (e.g. threat led penetration testing) be compulsory?		✓	

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

32. *What would be the most efficient frequency of running such more advanced testing given their time and resource implications?*

Every six months

Every year

Once every three years

Other

It depends on type and significance and criticalness to the organisation to define the frequency of testing. Note most organisation have developed and incorporated this time of testing framework into the overall testing and recovery plans.

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

33. *The updates that financial entities make based on the results of the digital operational testing can act as a catalyst for more cyber resilience and thus contribute to overall financial stability. Which of the following elements could have a prudential impact?*

	Yes	*No*	*Don't know/ not applicable*
The baseline testing/assessment tools (see question 29)?	✓		
More advanced testing (e.g. TLPT)?		✓	
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

34. *What are the most prominent categories of ICT third party providers which your organisation uses?*

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

35. *Have you experienced difficulties during contractual negotiations between your organisation and any ICT third party providers, specifically with regard to establishing arrangements reflecting the outsourcing requirements of supervisory/regulatory authorities?*

✓ *Yes*

No

Don't know/not applicable

To the extent you deem it necessary, please explain your reasoning, elaborating on which specific outsourcing requirements were difficult to get reflected in the contract(s). [Insert text box]

36. *As part of the Commission's work on Standard Contractual Clauses for cloud arrangements with financial sector entities, which outsourcing requirements best lend themselves for standardisation in voluntary contract clauses between financial entities and ICT third party service providers (e.g. cloud)?*

To the extent you deem it necessary, please explain your reasoning [Insert text box]

37. *What is your view on the possibility to introduce an oversight framework for ICT third party providers?*

	Yes	*No*	*Don't know/not applicable*
Should an oversight framework be established?	✓		
Should it focus on critical ICT third party providers?	✓		

Should "criticality" be based on a set of both qualitative and quantitative thresholds (e.g. concentration, number of customers, size, interconnectedness, substitutability, complexity, etc.)?	✓		
Should proportionality play a role in the identification of critical ICT third party providers?	✓		
Should other related aspects (e.g. data portability, exit strategies and related market practices, fair contractual practices, environmental performance, etc.) be included in the oversight framework?	✓		
Should EU and national competent authorities responsible for the prudential or organisational supervision of financial entities carry out the oversight?	✓		
Should a collaboration mechanism be established (e.g. within colleges of supervisors where one national competent authority assumes the lead in overseeing a relevant ICT service provider to an entity under its supervision - see e.g. CRD model)?	✓		
Should the oversight tools be limited to non-binding tools (e.g. recommendations, cross-border cooperation via joint inspections and exchanges of information, onsite reviews, etc.)?		✓	
Should it also include binding tools (such as sanctions or other enforcement actions)?	✓		

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

38. *What solutions do you consider most appropriate and effective to address concentration risk among ICT third party service providers?*

	Yes	*No*	*Don't know/not applicable*
Diversification strategies, including a potential mandatory or voluntary rotation mechanism with associated rules to ensure portability (e.g. auditing model)	✓		
Mandatory multi-provider approach		✓	

Should limits be set by the legislator or supervisors to tackle the excessive exposure of a financial institution to one or more ICT third party providers?		✓	

Other (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

39. *Do you agree that the EU should have a role in supporting and promoting the voluntary exchanges of such information between financial institutions?*

✓ *Yes*

No

Don't know/not applicable

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

40. *Is your organisation currently part of such information-sharing arrangements?*

✓ *Yes*

No

Don't know/not applicable

To the extent you deem it necessary, please explain your reasoning. If you have answered yes to the question, please explain how these arrangements are organised and with which financial counterparts you exchange this information. Please specify the type of information exchanged and the frequency of exchange. [Insert text box]

41. *Do you see any particular challenges associated with the sharing of information on cyber threats and incidents with your peer financial institutions?*

✓ *Yes*

No

Don't know/not applicable

To the extent you deem it necessary, please explain your reasoning. If you answered yes, please explain which are the challenges and why, by giving concrete examples. [Insert text box]

42. *Do you consider you need more information sharing across different jurisdictions within the EU?*

✓ *Yes*

No

Don't know/not applicable

To the extent you deem it necessary, please explain your reasoning and clarify which type of information is needed and why its sharing is beneficial. [Insert text box]

43. *Does your organisation currently have a form of cyber insurance or risk transfer policy?*

Yes

✓ *No*

Don't know/not applicable

If you answered yes, please specify which form of cyber insurance and whether it comes as a stand-alone cyber risk insurance policy or is offered bundled with other more traditional insurance products. [Insert text box]

44. *What types of cyber insurance or risk transfer products would your organisation buy or see a need for?*

To the extent you deem it necessary, please specify and explain whether they should cover rather first or third-party liability or a combination of both? [Insert text box]

45. *Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any?*

Issues	*Yes*	*No*	*Don't know/ not*
Lack of a common taxonomy on cyber incidents	✓		
Lack of available data on cyber incidents	✓		
Lack of awareness on the importance of cyber/ICT security	✓		
Difficulties in estimating pricing or risk exposures	✓		
Legal uncertainties around the contractual terms and coverage	✓		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning, by also specifying to the extent possible how such issues or lacks could be addressed. [Insert text box]

46. *Should the EU provide any kind of support to develop EU or national initiatives to promote developments in this area? If so, please provide examples.*
    - ✓ *Yes*

    No

    Don't know/not applicable

    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

47. *Does your organisation fall under the scope of application of the NIS Directive as transposed in your Member State?*
    - ✓ *Yes*

    No

    Don't know/not applicable

    To the extent you deem it necessary, please explain your situation in this respect. If you answered yes to the question, please specify the requirements you are subject to, indicating the financial sector you are operating in. [Insert text box]

48. *How would you asses the effects of the NIS Directive for your specific financial organisation? How would you assess the impact of the NIS Directive on your financial sector - taking into account the 3 specific financial sectors in its scope (credit institutions, trading venues and central clearing parties), the designation of operators of essential services and the lex specialis clause?*

    No Opinion
    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

49. *Are you covered by more specific requirements as compared to the NIS Directive requirements and if so, do they originate from EU level financial services legislation or do they come from national law?*

    No Opinion
    To the extent you deem it necessary, please explain your reasoning and provide details. [Insert text box]

50. *Did you encounter difficulties based on the fact that in the Member State where you are established the NIS competent authority is not the same as your own financial supervisory authority?*

    No Opinion
    Please provide details on your experience. [Insert text box]

51. *How do you cooperate with the NIS competent authority in the Member State where you are established? Do you have agreements for cooperation/MoUs?*

    No Opinion
    Please provide details on your experience. [Insert text box]

52. *Do you receive NIS relevant information in relation to a financial entity under your remit?*

    No Opinion

Please detail your experience, specifying how this information is shared (e.g. ad hoc, upon request, regularly) and providing any information that may be disclosed and you consider to be relevant. [Insert text box]

53. *Would you see merit in establishing at EU level a rule confirming that the supervision of relevant ICT and security risk requirements - which a regulated financial institution needs to comply with - should be entrusted with the relevant European and national financial supervisor (i.e. prudential, market conduct, other etc.)?*

    Yes, there would be merit is having a consistent approach and interpretation of policies and application.

    Please explain your reasoning [Insert text box]

54. *Did you encounter any issue in getting access to relevant information, the reporting of which originates from the NIS requirements (i.e. incident reporting by a financial entity under your remit/supervision)?*
    - ✓ *Yes*
    - *No*
    - *Don't know/not applicable*

    If you answered yes, please explain those particular issues. [Insert text box]

55. *Have you encountered any issues in matters involving cross-border coordination?*
    - ✓ *Yes*
    - *No*
    - *Don't know/not applicable*

    If you answered yes, please explain which issues. [Insert text box]

56. *What is your experience with the concrete application of the lex specialis clause in NIS?*

    The NIS has been transposed into the Luxembourg Law of 28 May 2019. It delegates the supervision of the financial sector's compliance to the CSSF. As firms operating in the financial sector in Luxembourg are already subject to the lex specialis, it would make sense not to duplicate or contradict these provisions with other cyber specific regulations. To this end, the technical specifications, guidelines and Q & A assist firms to more clearly identify their cyber-resiliency requirements.

    Please explain by providing, whenever possible, concrete cases where you either found the application of the lex specialis helpful, or otherwise where you encountered difficulties or faced doubts with the application or interpretation of specific requirements and the triggering of the lex specialis. [Insert text box]

57. *To the extent possible and based on the information provided for in the different building blocks above, which possible impacts and effects (i.e. economic, social, corporate, business development perspective etc.) could you foresee, both in the short and the long term?*

All the above scenario and the effects as stated could have a short and long term impact. Prevention measures, ability to assess the criticalness of the impact and the prudency and as tunes to implement remediation are essential for the well-being and viability of a firm, industry and society. Consistently in applying these measures noted throughout this document is the first line of defence.

Please provide details. [Insert text box]

58. *Which of the specific measures set out in the building blocks (as detailed above) would bring most benefit and value for your specific organisation and your financial sector? Do you also have an estimation of benefits and the one-off and/or recurring costs of these specific measures?*

    No Opinion
    Please provide details. [Insert text box]

59. *Which of these specific measures would be completely new for your organisation and potentially require more steps/gradual approach in their implementation?*

    No Opinion
    Please provide details. [Insert text box]

60. *Where exactly do you expect your company to put most efforts in order to comply with future enhanced ICT risk management measures and with increased safeguards in the digital environment? For instance, in respect to your current ICT security baseline, do you foresee a focus on investing more in upgrading technologies, introducing a corporate discipline, ensuring compliance with new provisions such as testing requirements, etc.?*

    Most organisation are continually increasing the business and IT budgets in areas of technology, educational training, board governance in all lines of defence.

    Please provide details. [Insert text box]

61. *Which administrative formalities or requirements in respect to the ICT risks are today the most burdensome, human-resource intensive or cost-inefficient from an economic perspective? And how would you suggest they should be addressed?*

    As cyber security impacts the entire organization, i.e. all lines of defence. The financial impact in prevention and monitoring outside of the IT budget is embedded in the on-going budgets of many departments and similar other business continuity approach.

    Please provide details. [Insert text box]

62. *Do you have an estimation of the costs (immediate and subsequent) that your company incurred because of ICT incidents and in particular cyber-attacks? If yes, to the extent possible, please provide any useful information (in relative or absolute) terms that you may disclose.*

    The cost of measuring cyber-attacks depends on the significance of the attack is measure from an internal expense and external from a revenue and reputational impact.
    Please provide details. [Insert text box]