JC 2019 26

10 April 2019

Joint Advice of the European Supervisory Authorities

To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector

Introduction

1. On 8 March 2018, the European Commission (EC) published its FinTech Action Plan.[1] In the Action Plan, the Commission

   "invites the ESAs to map, by Q1 2019, the existing supervisory practices across financial sectors around ICT security and governance requirements, and where appropriate: a) to consider issuing guidelines aimed at supervisory convergence and enforcement of ICT[2] risk management and mitigation requirements in the EU financial sector and, b) if necessary, provide the Commission with technical advice on the need for legislative improvements."

2. The European Banking Authority (EBA) competence to deliver an opinion is based on Article 56 in the context of its tasks in Chapter II and more in particular of Article 34(1) of Regulation (EU) No 1093/2010[3] as cyber-resilience in the EU financial sector relates to the EBA's area of competence.

3. The European Insurance and Occupational Pensions Authority (EIOPA) competence to deliver an opinion is based on Article 56 in the context of its tasks in Chapter II and more in particular of Article 34(1) of Regulation (EU) No 1094/2010[4] as cyber-resilience in the EU financial sector relates to the EIOPA's area of competence.

4. The European Securities and Markets Authority (ESMA) competence to deliver an opinion is based on Article 56 in the context of its tasks in Chapter II and more in particular of Article 34(1) of Regulation (EU) No 1095/2010[5] as cyber-resilience in the EU financial sector relates to the ESMA's area of competence.

[1] Communication from the Commission to the European Parliament, the council, the European Central Bank, The European Economic and Social Committee and the Committee of the Regions FinTech Action plan: For a more competitive and innovative European financial sector. COM/2018/0109 final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109

[2] The term ICT stands for 'information and communication technology'.

[3] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12)

[4] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48)

[5] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84)

General comments

5. The three ESAs welcome the opportunity to provide the Commission with technical advice on the need for legislative improvements in this context. As noted in the EC FinTech Action Plan, ICT risks, including cybersecurity risks, undermine confidence and represent a threat to the stability of the financial system. Furthermore, cyber-attacks are a growing concern because of their increasing frequency and potential impact. The ESAs believe that legislative improvements can support good and consistent risk management across the financial sector in relation to ICT security. This will in turn help ensure effective delivery of financial services across the EU while supporting consumer and market trust. The ESAs believe that every relevant entity should effectively manage ICT risk, including cybersecurity risk, with appropriate governance, operational and control measures in place.[6] This Joint Advice highlights areas of regulation where the ESAs have identified scope for improving certain legislative provisions related to ICT risk management, including the important area of cybersecurity. A related overarching objective that has guided the work of the ESAs in this area is the harmonisation of relevant requirements and terminology.

6. The ESAs are publishing these findings through their Joint Committee, reflecting the fact that many aspects of ICT risk and cybersecurity are cross-sectoral.

7. Ensuring appropriate ICT governance and security is key to proper ICT risk management. Section 1.1 sets out analysis of the existing legislative requirements regarding ICT governance and security in the different sectors within the ESAs' remit. Detailed proposals based on this analysis are in sections 2.1 and 2.2. All relevant analysed legislation is referenced in the Annexes.

8. In carrying out their analysis of existing ICT governance and security measures, the ESAs identified two related areas that may benefit from further action at EU level: ICT incident reporting and an appropriate oversight framework for monitoring critical service providers to the extent that their activities may impact relevant entities.[7] These issues are covered in section 2.2, which includes detailed joint ESA proposals.

9. The analysis throughout this document is informed by research that the ESAs have carried out, including by mapping supervisory practices relating to ICT security and governance requirements, in line with the FinTech Action Plan. The ESAs believe that the legislative improvements identified will complement planned work on supervisory convergence in this area by promoting consistent supervisory expectations.

[6] For the purposes of this Opinion, references to 'relevant entities' include 'financial institutions' within the meaning of Article 4(1) of the EBA Regulation and insurance and reinsurance undertakings addressed by the EIOPA Regulation as well as 'financial market participants' within the meaning of Article 4(1) of the ESMA Regulation.

[7] The scope of what such oversight would entail will be discussed by the ESAs following feedback to this proposal from the EC. The ESAs do not propose full supervision of these entities.

10. Additionally, alongside this Advice, the ESAs have published Advice to the Commission on a coherent cyber resilience testing framework for the EU financial sector.[8] The legislative improvements identified below will help ensure that entities take specific action to manage and mitigate ICT risks – a necessary foundation for any cyber resilience testing framework.

Joint ESAs Advice

11. The ESAs have identified scope to promote effective ICT risk management and greater harmonisation through common, targeted minimum requirements for ICT risk management. As set out in detail in the rest of this document and as informed by the analysis of legislation set out in the Annexes, the ESAs' proposals relate to the following areas:

ICT governance and security

- The ESAs have centered their analysis of current legislation on overall operational resilience, including ICT and cyber governance and security. While operational risk requirements are generally in place in the sectoral legislation, there is typically a lack of explicit references to ICT and cybersecurity risk. As such the ESAs believe that, across their respective sectors, it should be articulated clearly that every relevant entity should be subject to general requirements on governance of ICT, including cybersecurity, to ensure safe provision of regulated services. Such consistency will help set appropriate supervisory expectations, aid good governance and in turn promote greater ICT security and cybersecurity.

Related considerations

- The ESAs note that across the financial sector different and sometimes inconsistent terminology, templates and reporting timeframes are used for a variety of incident reporting frameworks which in some cases may conflate concepts relating to operational risk, IT risk, resilience, information security and cybersecurity risk. Although these incident reporting frameworks differ in scope, the ESAs consider that efforts should be made toward greater harmonisation.
- Third parties are themselves often a source of ICT/cybersecurity risk, and so appropriate management of third party risks is an important part of ICT risk management. Relatedly, the concentration risk associated with third parties in the financial sector is also a cause for concern in relation to financial stability. This concern is especially acute with regard to cloud services, as a few large providers service the majority of the EU financial sector and many other sectors. The ESAs therefore propose that the Commission consider the establishment of an appropriate oversight framework for monitoring critical service providers to the extent that their activities may impact relevant entities. Such a solution should recognise that third party providers operate across borders both within and outside the EU, and so international coordination is strongly desirable.

[8] Joint Advice of the European Supervisory Authorities to the European Commission on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector, 10 April 2019.

12. The detailed analysis and proposals in sections 1 and 2 below and the information contained in the Annexes further elaborate the above findings.

13. The ESAs remain at the disposal of the Commission, including for assistance on how to introduce the proposals into law and the production of any necessary guidance.

This opinion will be published on the ESAs websites.

Joint ESAs analysis and detailed proposals

Contents

1. Analysis

14. Across the financial sector, there is an increasing reliance on ICT in the provision of financial services and in entities' normal operational functioning. It is therefore important to ensure that relevant entities in the financial sector are adequately prepared to manage their ICT risks.

15. Management of ICT and cybersecurity risk requires adequate governance and security measures to be in place. Furthermore, having consistent requirements for relevant entities is necessary to ensure a level playing field and to avoid confusion in the market. The ESAs have analysed existing ICT governance and security requirements, as set out in the rest of this section. All relevant legislation analysed is referenced in the Annexes. Detailed proposals are set out in section 2.

1.1 Analysis of ICT governance and security requirements

1.1.1 Banking and payments

16. In conducting an analysis of the provisions in Level 1 legislation under the EBA's remit, the EBA identified various provisions that can be used to address ICT risks but also fragmentation in the level of detail and specificity of these provisions across the legislation which can affect financial institutions which are subject to more than one legislation. In particular:

- For credit institutions and investment firms the provisions in the Capital Requirements Directive [9] (CRD) and Capital Requirements Regulation [10] (CRR) are not explicit on requirements related to ICT, security of ICT systems and data, nor ICT risk management. The CRD requirements under Article 74 on internal governance require that institutions should have robust governance arrangements in place for the risks that they are exposed to. Whilst reference to ICT is not explicit here, given the reliance on ICT in all institutions, ICT and management of related risks is broadly expected to be covered within their internal governance arrangements. Furthermore, ICT risk management is implicitly addressed under Article 85 CRD on operational risk, pursuant to which institutions should implement policies and processes to evaluate and manage exposure to operational risk and have contingency and business continuity plans in place.

- The current provisions in the revised Payment Services Directive [11] (PSD2) are more explicit on ICT and security risk management measures. In particular, Article 5 (1) PSD2, which relates to the authorisation requirements for payment institutions (including, for these purposes, electronic money institutions), provides for some references related to ICT

[9] Directive 2013/36/EU

[10] Regulation (EU) 575/2013

[11] Directive 2015/2366

security. In particular Article 5 (1) (j) requires Payment Service Providers (PSPs) to submit and have a security policy document in place, including a description of security control and mitigation measures. As further specified in that Article, such a document shall indicate how those security control and mitigation measures ensure 'a high level of technical security and data protection for… software and IT systems…'. To complement these provisions the EBA published Guidelines on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers as mandated in Article 5 (5) PSD2 (EBA GL/2017/09) which elaborate provisions related to the security policy document that applicants must provide for authorisation. Furthermore, Article 95 PSD2 includes requirements for PSPs to have security measures for operational and security risks for the provision of payment services. Even though it is not explicit in that Article, it is understood that such security measures relate to the ICT risk measures, including security measures, given that the scope of application of PSD2 which specifically covers electronic payment services.

- The provisions of Article 95 PSD2 apply to PSPs - which may include credit institutions when providing payment services. With respect to payment services, credit institutions have some specific ICT security requirements stated explicitly in the legislation, whereas this is not the case for the provision of other services (i.e. the CRD has no explicit requirements related to ICT for the provision of the activities other than payment services listed in Annex I to the Directive).

- The Directive on security of network and information systems [12] (NISD) which does not fall under the remit of the EBA, applies to some credit institutions, when designated as operators of essential services. This Directive sets out some provisions for security requirements and incident notification (Article 14 NISD) but with limited application.

17. The summary above indicates that, in general, there is an absence of explicit provisions on ICT risk management and ICT security. This is combined with fragmentation of requirements across CRD, PSD2 and NISD, which overlap in their addressees. Given the increasing use of ICT across the finance sector which carries with it additional risks, specifically ICT security, including cyber-attacks, there is a need to ensure that there is full clarity about a common minimum level of ICT, specifically ICT security and ICT risk, management.

1.1.2 Insurance and re-insurance

18. Solvency II Directive (Article 41 and Article 44 of Directive 2009/138/EC) addresses the system of governance and the need for insurance and reinsurance undertakings to manage their business in a sound and prudent manner. The risk management system should cover risks, at an individual and at an aggregated level, to which undertakings are or could be exposed, and their interdependencies. This definition includes 'operational risk', where ICT risk (including cyber) should be classified.

[12] Directive 2016/1148

19. The reference in Article 41 (4) to business continuity and contingency plans should also be considered in this context as EIOPA agrees that operational resilience goes beyond effective risk management, as ICT failures, or breaches, caused by people or processes are inevitable and it aims to ensure the financial insurance and reinsurance undertakings preparedness to ensure they are able to continue services through disruptions and to minimise the impact on others.

20. Under Solvency II the Own Risk and Solvency Assessment (ORSA) at Article 45 plays an important role. The role of the ORSA in the assessment by the undertaking of the material risks it is exposed to, is crucial for any risk but particularly for ICT risks (including cybersecurity risk) as part of the undertaking's operational risk. In fact, it is known that the standard formula for operational risk calculation is not as sensitive to the risks as the other risk modules. As such, under the ORSA it is expected that undertakings assess if the standard formula reflects its operational risk profile. It is also expected that considering the global consensus in identifying ICT risk as possibly one of the top emergent risks for the insurance market that the ORSA of each undertakings shall include an assessment of these risks, if these are assessed as material by the undertaking.

21. The Commission Delegated Regulation 2015/35 (Article 258) addresses the establishment of information systems which produce complete, reliable, clear, consistent, timely and relevant information concerning the business activities. These requirements refer to the information systems used (letter h), and require undertakings to maintain adequate and orderly records of the undertaking's business and internal organisation (letter i) and safeguard the security, integrity and confidentiality of information (letter j) as well as establishing, implanting and maintaining a business continuity policy (paragraph 3).

22. The analysis of the current 'EIOPA Guidelines on System of Governance' and taking the analysis of the performed survey into account, it appears that the above mentioned Guidelines do not cover ICT security and governance requirements in detail and that, from a 'local' perspective, the regulatory landscape appears fragmented throughout Europe.

23. These Guidelines do not properly reflect the importance of taking care of ICT risks (including cybersecurity risks) as stressed e.g. by the FinTech Action plan. There is no guidance regarding vital elements that are generally acknowledge as being part of proper ICT security and governance requirements. To better reflect these elements and to achieve convergence within the EEA, EIOPA proposes to develop Guidelines regarding ICT security and governance requirements. In Annex B1 an overview of ruling may be found.

24. 22 out of the 28 countries that have submitted the EIOPA survey on current ruling (see annex B) have defined local rules for ICT-security and governance requirements. Even if those requirements are quite similar, this still leads to a scattered picture. In addition, the supervisory practices vary from 'no specific supervision' to 'strong supervision' (including 'off-site-inspections' and 'on-site inspections'). In Annex B3 overall results of the stock take exercise may be found.

25. This fragmented regulatory and supervisory landscape regarding ICT security and governance requirements could lead to non-convergent practices across Europe and endanger the level-playing field and the EU single market for insurance.[13]

26. Furthermore EIOPA emphasizes the specificities of ICT risks (including cybersecurity risks) as part of the reinsurance or insurance undertaking's risk profile.

27. This specific risk is basically any threat to information, information systems and business processes and addresses safeguarding 'confidentiality'; 'integrity' and 'availability' of information, information systems and business processes involved. Although every financial undertaking is vulnerable to these risks, there are certain differences depending on the business model / operating model and the underlying processes between the different entities in the financial sector. In comparison with, for instance, credit institutions or other financial institutions, (re)insurance undertakings, especially life and health insurers, are by nature (based on their current business model and underlying processes) less vulnerable to disruptive attacks / business interruptions.

28. However, undertakings (and the large amount of liaised agents, intermediaries and other affiliated companies with often their own access to the data) are very attractive to cyber criminals because of their large data repositories with sensitive personal information such as information on health, housing and mobility and other proprietary data related to business secrets. In the near future these data repositories will probably grow by the expected use of data from Internet of Things (IOT), like data gathered by smart cars, smart homes and some health apps used for insurance purposes.

29. Furthermore, undertakings are going to be even more vulnerable to attacks by the increasing use of IOT-tools, the use of platforms and other forms of cooperation (e.g. distributed ledger technologies such as blockchain). In Annex B2 a complete description of the risk profile may be found.

1.1.3 Securities markets

30. Among the areas of sectoral legislation most relevant to ESMA's remit, ICT risk management is covered only to the extent that the legislation contains broad requirements concerning operational risk. Overarching requirements on operational risk also vary with respect to how applicable they are to ICT governance and security requirements. For example, Credit Rating Agencies Regulation (CRAR) contains no specific provision regarding operational risk, while at the other end of the spectrum, Central Securities Deposit Regulation (CSDR) explicitly states that its overarching requirement on operational risk applies to 'deficiencies in information systems'.

31. However, cybersecurity requirements are more specific than ICT governance and security requirements. As noted in the Introduction and in the FinTech Action Plan, cybersecurity risk in

[13] Supervisory Convergence Plan: https://eiopa.europa.eu/Publications/Reports/Supervisory%20Convergence%20Plan%202018-2019.pdf

particular is an area of increasing importance within operational risk management. Among the areas of legislation examined, bespoke cybersecurity requirements are present only in MiFID II, EMIR and CSDR. In the case of CRAR, therefore, the lack of specific cybersecurity requirements couples with an absence of ICT governance and security requirements more broadly.

32. Terminology relevant to cybersecurity is present in all the areas of legislation examined, with terminology specific to cybersecurity present in Directive 2014/65/EU and Regulation (EU) 600/2014 on Markets in Financial Instruments (MiFID II / MiFIR), Regulation (EC) 648/2012 on European Market Infrastructure (EMIR), Regulation (EC) 909/2014 on Central Securities Depositories (CSDR) and Regulation (EC) 1060/2009 on Credit Rating Agencies (CRAR). In some cases, terminology is inconsistent. A notable example is that MiFID II, EMIR, CSDR and CRAR respectively refer to 'information systems', 'information technology systems' and 'information processing systems'.

33. Across the areas of legislation, governance and strategy requirements apply to ICT and cybersecurity risk, but an explicit link is not stated.

34. In addition to differences across areas of legislation, the work ESMA has carried out with its National Competent Authorities (NCAs) to map supervisory practices indicates significant heterogeneity in national cybersecurity rules and guidance, in several respects. The extent to which national rules cover different types of entities within ESMA's remit varies. In some countries where guidance on cybersecurity risk management has been issued the provisions are mandatory, while in other cases some or all provisions are voluntary.

35. The mapping exercise also revealed significant variation between Member States in how cybersecurity risk management is supervised in sectors within ESMA's remit. Most NCAs do cover cyber issues as part of their supervision work, often basing their practices on international standards. However, many different such standards are used. ESMA plans to facilitate further supervisory convergence among the relevant NCAs as regards cybersecurity risk.

2. Proposals

36. The ESAs believe that every relevant entity should effectively manage ICT risk, including cybersecurity risk, with appropriate governance, operational and control measures in place. Relevant entities should be subject to clear and consistent requirements that support this objective.

37. Section 2.1 sets out sectoral proposals from each of the ESAs. These proposals reflect the fact that existing legislation introduces relevant requirements in different ways, with varying levels of detail. While the sectoral proposals from each of the ESAs are designed to address the needs of relevant entities within their respective remits, where relevant, the proposals reflect cross-sectoral considerations. The sectoral proposals in section 2.1 aim to enhance ICT risk management, security and governance across the financial sector.

38. In addition to ensuring that relevant entities are subject to appropriate requirements on ICT security, governance and risk management, the ESAs highlight the importance of ensuring that the incident reporting framework to which relevant entities are subject allows them to report accurate and timely information efficiently and supports competent authorities in monitoring ICT risks. To this end, in section 2.2 the ESAs set out a joint proposal that existing incident reporting requirements should be streamlined. Furthermore, the ESAs recognise the increasing role played by third party providers of ICT services providing critical services to relevant entities. Section 2.2 includes a joint proposal that the Commission consider a legislative solution for an appropriate oversight framework for monitoring the activities of third party providers when they are critical service providers to relevant entities.

2.1 Sectoral proposals

39. In making the following detailed proposals for legislative change in their respective sectors, the ESAs believe it is important to harmonise requirements on governance of ICT and cyber security for all relevant entities, where possible. Such harmonisation will promote convergence of supervisory expectations towards ICT-security and governance requirements and supervisory practices to enforce ICT risk management and mitigation.

2.1.1 Banking and payments

40. The EBA considers that there is a need for improving the sectoral legislation on ICT security and governance[14] and to establish absolute clarity about the minimum requirements for all financial institutions on ICT risk and ICT security. The objective of such improvements would be to enhance ICT security and governance across all regulated institutions and address the need for cyber resilience as well as contingency planning and business continuity planning. These elements are consistent with the need to strengthen a financial institution's operational resilience. Operational resilience goes beyond effective risk management, as ICT failures or breaches caused by people or processes are inevitable, and it aims to ensure the financial institution's preparedness to ensure they are able to continue services through disruptions and to minimise the impact on others.

41. There is also a need for legislative improvements to clarify the requirements given the fragmentation which is evident for credit institutions. The EBA considers that legislative improvements covering operational resilience will serve to bridge the gap on the different aspects that contribute to sound ICT risk management and sound ICT security issues like internal governance and risk management whilst also ensuring 'security by design'.

42. The EBA therefore proposes the following legislative changes:

a. **new articles in CRD and PSD2 on operational resilience as a requirement relating to governance**. The concept of operational resilience would serve to address the global interconnectedness, interdependence and reliance on technology in the financial sector which can make disruption to operations more impactful and it would incorporate aspects of contingency planning and business continuity planning. The EBA's view is consistent with the evolving work at the Basel Committee on operational resilience and any future legislative changes should take heed of Basel work on this topic. The proposed new articles should be principles-based and, focused on governance and internal controls. Such wording should also be considered in the finalisation of the forthcoming investment firms framework.

[14] Parallel proposals on ICT risk management from an operational risk perspective will be made through the answer of the EBA to the "*Call for advice to the EBA for the purposes of revising the own fund requirements for credit, operational, market and credit valuation adjustment risk*" by mid-2019

b. Within this new proposed article in CRD on operational resilience, **the EBA proposes to include an explicit mandate for the EBA to draft guidelines on operational resilience and ICT and security risk management for institutions**. This would allow the EBA to elaborate more detailed provisions on operational resilience, ICT risk management and security, strengthening the basis for the EBA guidelines on ICT and security risk management[15]. This mandate should additionally reflect the wording in Article 95 (4) of PSD2, which allows for the EBA to develop draft regulatory technical standards, where requested to do so by the Commission, on this topic. This would facilitate consistency of the nature of the requirements for all institutions covered by the scope of application of the Guidelines on ICT and security risk management.

43. The EBA considers that having a high degree of security requirements for network and information security is necessary for all institutions in the banking market. With reference to the provisions in NISD, which could apply to some credit institutions designated as operators of essential services, enacting the proposals referred to in paragraph 36 would result in the combined reading of those with Recital 9 and Article 1 (7) of NISD so as to render it unequivocally clear that the EU banking legislation constitutes *lex specialis* vis-a-vis NISD also for these institutions that are operators of essential services. This would mean that, with regard to these institutions, the more specific provisions in CRD and PSD2 should have precedence over the general provisions of NISD when it comes to defining finance sector requirements on ICT risk management and security, covering governance and security.

2.1.2 Insurance and re-insurance

44. EIOPA believes that the establishment of a baseline towards ICT-security (including cyber resilience) across the EEA is a priority for the insurance sector. EIOPA believes that the requirements reflected in both Solvency II Directive and the Delegated Regulation are consistent with CRD and provide a sound legislative baseline. However, if a **new article on operational resilience as a requirement relating to governance is added to CRD, a similar provision for Solvency II Directive should be considered as well, considering the level of detail of similar provisions in Solvency II Directive.**

45. Considering that this baseline should also consider the specific ICT security risks in the risk profile of (re-)insurance undertakings, **EIOPA proposes to start developing Guidelines** during 2019, according to Article 16 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council (hereafter EIOPA Regulation). EIOPA will address these Guidelines to national competent authorities.

46. These Guidelines will further define supervisors' expectations on how Articles 44 of Solvency II Directive and Article 258 of Commission Delegated Regulation (EU) 2015/35 should be implemented by insurance and reinsurance undertakings in the context of ICT-security and governance requirements. Guidelines offer the flexibility to take into account that the

[15] Consultation Paper on guidelines on ICT and Security risk management EBA/CP/2018/15

environment of ICT security is still evolving and it is expected that lessons learned and better practices will emerge in the sector in future. In addition to allowing such flexibility, the Guidelines will also allow NCAs to consider the broader context of ICT-security and governance requirements at national level, e.g. how NISD has been implemented in different member states.

47. The proposed Guidelines will be based on existing legislation, guidelines and commonly used standards / frameworks across the financial sector, i.e. G7-principles[16] on ICT security, IAIS[17]-documentation, [18] FSB Cyber Lexicon [19], draft EBA Guidelines on ICT and security risk management[20] and COBIT (Control Objectives for Information and Related Technologies)[21] and ISO/IEC 2700X [22] (International Organization for Standardization) as most common standards/frameworks in the area of ICT security.

48. To align supervisory practices and to encourage convergence, **following publication of the proposed Guidelines EIOPA proposes to develop a chapter for the Supervisory Handbook** on how to supervise ICT security and governance requirements, also including good supervisory practices. This work would be carried out in cooperation with the EIOPA Members.

2.1.3 Securities markets

49. Based on ESMA's assessment of each of the relevant areas of legislation, ESMA sees a need for legislative improvements to streamline and harmonise regulatory requirements and definitions regarding ICT and cybersecurity risk. Harmonisation in legislation is all the more important given the existing heterogeneity in rules, guidance and supervisory practices at national level. **ESMA proposes that the Commission should consider introducing specific references to cybersecurity in those areas of legislation currently absent such references**, as identified in Table C1 of Annex C. ESMA further proposes that an integral part of making legislative improvements of this kind is to use consistent terminology in all new provisions.

50. References to cybersecurity should take account of the fact that internationally accepted information security and cybersecurity frameworks (such as NIST[23] and COBIT) exist and that these are often adopted by larger entities and used as a reference point for supervision. It should

[16] *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, available at: http://www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf

[17] IAIS is the International Association of Insurance Supervisors

[18] https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

[19] http://www.fsb.org/wp-content/uploads/P121118-1.pdf

[20] https://eba.europa.eu/documents/10180/2522896/EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf

[21] http://www.isaca.org/Knowledge-Center/cobit/Pages/Products.aspx

[22] https://www.iso.org/isoiec-27001-information-security.html

[23] NIST is the National Institute for Standards and Technology. The NIST Cybersecurity Framework is available at: https://www.nist.gov/cyberframework

be clear from legislation that explicit new requirements to address cybersecurity should not inhibit relevant entities from adopting successful such frameworks, nor inhibit their use by NCAs for supervisory purposes.

51. Further to this, **ESMA proposes that incident reporting requirements be introduced** in those areas of legislation examined in Table C1 of Annex C for entities not currently subject to such incident reporting requirements. Requirements should take into consideration suitable criteria for incidents to be reported, in addition to specifying the content and recipients of incident reports.

52. In considering the above proposals, ESMA's analysis was focused on the sectoral EU legislation most relevant to its remit. ESMA recognises that other legislation, both national and at EU level, may impose upon entities relevant ICT risk management requirements. ESMA recommends that the Commission take into account such issues of scope when considering legislative changes, to avoid duplication of requirements and inconsistent standards being mandated.

53. Finally, ESMA believes that the legislative improvements it has identified will help set appropriate supervisory expectations for relevant entities in those cases where national guidance may not suffice. ESMA believes that the legislative improvements will thereby complement and support supervisory convergence of ICT risk management and mitigation requirements. ESMA has communicated to the Commission that a majority of NCAs want to see work develop in this area through ESMA-level cooperation. ESMA will continue to facilitate coordination between NCAs on these issues.

2.2 Cross-sectoral proposals

54. In reviewing relevant legislation, the ESAs concluded that further work at EU level may be beneficial on ICT incident reporting and an appropriate oversight framework for monitoring the activities of critical third party providers to the extent that they affect relevant entities.

2.2.1 Joint ESAs proposals on existing incident reporting requirements

55. Incident reporting is highly relevant to ICT risk management and allows relevant entities and authorities to log, monitor, analyse and respond to ICT operational, ICT security and fraud incidents. There many different incident reporting schemes at EU and national level, differing in scope, addressees and requirements.

56. Incident reporting is governed to varying degrees by sectoral legislation, but also by cross sectoral legislation, notably including NISD and GDPR.[24] This multitude of incident reporting frameworks sometimes use different terminology, different timeframes and involve different authorities as recipients of the reported information. Nonetheless, the frameworks can overlap for some incidents. In some cases this is because despite differences in scope, incidents may

[24] Annexes A, B and C summarise the extent to which incident reporting is covered by different areas of legislation within the remit of the ESAs. In the case of legislation most relevant to ESMA's remit, no specific cyber incident reporting requirements are in place, though a general requirement is in place in CDSR.

involve different aspects of the incident (e.g. one incident of fraud may also impact personal data). An additional source of complication stems from differences in reporting templates. Complications of this kind can become burdensome, especially in time-critical environments where an entity's resources may be stretched.

57. The ESAs propose that efforts should be made to streamline incident reporting to reduce the burdens mentioned above. However, it is important to recognise that reporting adds value both in the short and the long term, and that different reporting schemes have different purposes. As a result, no incident reporting requirements should be removed. Instead, and in addition to the sectoral proposal from ESMA above in section 2.1.3, the ESAs propose that **existing incident reporting requirements should be streamlined** by clarifying any overlapping provisions and standardising reporting templates, taxonomy and timeframes where possible. Streamlined incident reporting would facilitate better operational resilience and business continuity, as it would aid smooth and efficient interactions between authorities and computer security incident response teams (CSIRTS). These efforts would also help avoid inconsistencies in the reported information.

58. To this end, **the Commission could consider facilitating the development of harmonised templates and a uniform taxonomy of commonly used terms** amongst these different schemes. One further option to be explored should be how to coordinate and make available (while respecting confidentiality requirements) the results of existing incident reporting among relevant authorities in the financial sector, to avoid overlaps.

2.2.2 Joint ESAs proposals on an appropriate oversight framework for monitoring the activities of critical third party providers affecting relevant entities

59. Another area relevant to ICT risk management and ICT security in the financial sector that could benefit from further review by the Commission relates to third party providers. Relevant entities are increasingly making use of third party providers, particularly for ICT services, to remain competitive and to respond to consumer demand.[25]

60. The presence of third party providers in financial services can lead to concerns about their operational resilience including the cyber vulnerabilities to which relevant entities are exposed through these providers. Concerns about cyber vulnerabilities were reflected in the G7 Cyber Expert Group 'Fundamental Elements for Third Party cybersecurity risk management in the financial sector' published in November 2018. Operational resilience incidents resulting from third party vulnerabilities can lead to fraud, disruption of services or access to sensitive customer or corporate information.

61. One type of ICT services provider that is increasingly used in the EU financial sector is cloud services providers (CSPs). A limited number of big players dominate cloud services for the financial sector and there are concerns that their interconnectedness in the financial system could be a single point of failure if one were to be subject to a serious breach. Furthermore, with

[25] ICT services in this respect includes for example data providers, which may be critical for certain entities.

the increased use of outsourced or third party services such as CSPs, concentration is becoming more relevant from the financial stability perspective and such providers might become 'critical service providers' and therefore a single point of failure.

62. Within the sectoral Level 1 legislation most relevant to the respective remits of the ESAs, as summarised in the Annexes, at present there are no legal provisions that specifically address third-party concentration risk.[26] [27] An oversight framework could provide a useful template for the way forward regarding monitoring the risks stemming from third party providers.[28] [29] This should not detract from the responsibilities of micro prudential requirements of relevant entities to monitor the risks to which they are exposed.

63. Taking into account the potential systemic risks that may result from outsourcing or third party concentration risks, **the ESAs propose that Commission could consider a legislative solution for an appropriate oversight framework for monitoring the activities of third party providers when they are critical service providers to relevant entities**.[30] This will be particularly relevant in the near term for cloud service providers. Such a legal framework should define the criteria for considering when a third party provider is 'critical', establish the extent of the activities subject to the framework and designate the authority or authorities responsible at national and/or EU level. It should also be designed not to duplicate any obligations arising from existing legislation.

64. The ESAs stand ready to contribute to the preparation of such an oversight framework by providing additional technical input. The ESAs also recognise that efforts in this respect need to be made at global level and therefore foresee cooperation with international bodies.

[26] In ESMA's case, each area of legislation considered in Annex C contains a general requirement only, with the exception of EMIR where no such requirement is applicable at all.

[27] The EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) addresses outsourcing concentration risk. They specify that competent authorities should identify and monitor risk concentration at single service providers and assess whether or not these could pose a risk to the stability of the financial system.

[28] In the banking sector, critical service providers (e.g. SWIFT) are subject to central bank oversight (as provided by the standards of the Committee on Payment and Settlement Systems of the G10 central banks, 2005). BIS-IOSCO has an assessment methodology for the oversight expectations applicable to critical service providers of Financial Market Infrastructures (FMIs).

[29] In the insurance sector, outsourcing of critical or important operational functions or activities shall not be undertaken in certain circumstances specified in the Directive, they need to be notified to the supervisory authorities prior to the outsourcing as well as notification of any subsequent material developments with respect to those functions or activities (Article 49 of Solvency II Directive). Additional requirements are set out in Article 274 of the Delegated Regulation, among others supervisory authority shall have effective access to all information relating to the outsourced functions and activities including carrying out on-site inspections of the business premises of the service provider.

[30] This could be particularly relevant in the near term for cloud service providers.

Annex A: background material to analysis of banking and payments legislation

Relevant legislation

65. To identify whether there is a need for improvements in the legislative provisions relating to ICT risk management security and governance, the EBA has reviewed the legislative texts under its remit specifically the requirements under

    - Regulation (EU) No 575/2013 (Capital Requirements Regulation, hereafter 'CRR')
    - Directive 2013/36/EU (Capital Requirements Directive, hereafter 'CRD');
    - Directive (EU) 2015/2366 (the revised Payment Services Directive, hereafter 'PSD2');

    as well as

    - the proposed text for a prudential framework for investment firms published by the Commission on 20 December 2017, which is currently being elaborated in the course of the EU institutions' trilogue negotiations;
    - Directive (EU) 2016/1148 (the security of network and information systems Directive for operators of essential services);

66. The scope of addressees of these regulations covers credit institutions, investment firms – under the CRD and CRR - and PSPs under PSD2. As credit institutions can also be PSPs, for their payment services the requirements in the PSD2 apply.

67. Furthermore, the EBA conducted an assessment of the current supervisory practices regarding cybersecurity in the EU in 2017 and also consulted its members and observers through various subgroups on internal governance, IT risk supervision, operational risk and payment services to gauge supervisory views on the current legislative landscape regarding ICT risk.

68. The relevant sections of the legislation in questions are set out below.

Regulation (EU) No 575/2013 (CRR)	
Articles 288, 368:	*The integrity of the management information system is required to be annually reviewed, as part of the regular internal auditing process, for the purposes of credit and market risk under the Internal Models method.*
Article 320:	*Criteria for the Standardised Approach (for Operational Risk)*
Articles 321-322:	*Qualitative and Quantitative standards for Advanced measurement approaches (for Operational Risk)*
Directive 2013/36/EU (CRD IV)	
Article 74:	*(1) Institutions shall have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks they are or might be exposed to, adequate internal control mechanisms, including sound administration and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management. (2) The arrangements, processes and mechanisms referred to in paragraph 1 shall be comprehensive and proportionate to the nature, scale and complexity of the risks inherent in the business model and the institution's activities. The technical criteria established in Articles 76 to 95 shall be taken into account. (3) EBA shall issue guidelines on the arrangements, processes and mechanisms referred to in paragraph 1, in accordance with paragraph 2.*
Article 85:	*(1) Competent authorities shall ensure that institutions implement policies and processes to evaluate and manage the exposure to operational risk, including model risk, and to cover low-frequency high-severity events. Institutions shall articulate what constitutes operational risk for the purposes of those policies and procedures. (2) Competent authorities shall ensure that contingency and business continuity plans are in place to ensure an institution's ability to operate on an ongoing basis and limit losses in the event of severe business disruption.*
Directive (EU) 2015/2366 (PSD2)	
Article 5	***Applications for authorisation*** *1. For authorisation as a payment institution, an application shall be submitted to the competent authorities of the home Member State, together with the following:* *(b) a business plan including a forecast budget calculation for the first 3 financial years which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;* *(d) for the payment institutions referred to in Article 10(1), a description of the measures taken for safeguarding payment service users' funds in accordance with Article 10;*

	(e) a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures, which demonstrates that those governance arrangements, control mechanisms and procedures are proportionate, appropriate, sound and adequate; *(f) a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incidents reporting mechanism which takes account of the notification obligations of the payment institution laid down in Article 96;* *(g) a description of the process in place to file, monitor, track and restrict access to sensitive payment data;* *(h) a description of business continuity arrangements including a clear identification of the critical operations, effective contingency plans and a procedure to regularly test and review the adequacy and efficiency of such plans;* *(j) a security policy document, including a detailed risk assessment in relation to its payment services and a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud and illegal use of sensitive and personal data;* *(l) a description of the applicant's structural organisation, including, where applicable, a description of the intended use of agents and branches and of the off-site and on-site checks that the applicant undertakes to perform on them at least annually, as well as a description of outsourcing arrangements, and of its participation in a national or international payment system;* *For the purposes of points (d), (e) (f) and (l) of the first subparagraph, the applicant shall provide a description of its audit arrangements and the organisational arrangements it has set up with a view to taking all reasonable steps to protect the interests of its users and to ensure continuity and reliability in the performance of payment services.* *The security control and mitigation measures referred to in point (j) of the first subparagraph shall indicate how they ensure a high level of technical security and data protection, including for the software and IT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations. Those measures shall also include the security measures laid down in Article 95(1). Those measures shall take into account EBA's guidelines on security measures as referred to in Article 95(3) when in place*
Article 19:	*Use of agents, branches or entities to which activities are outsourced – […] (6) Where a payment institution intends to outsource operational functions of payment services, it shall inform the competent authorities of its home Member State accordingly. Outsourcing of important operational functions, including IT systems, shall not be undertaken in such way as to impair materially the quality of the payment institution's internal control and the ability of the competent authorities to monitor and retrace the payment institution's compliance with all of*

	the obligations laid down in this Directive. For the purposes of the second subparagraph, an operational function shall be regarded as important if a defect or failure in its performance would materially impair the continuing compliance of a payment institution with the requirements of its authorisation requested pursuant to this Title, its other obligations under this Directive, its financial performance, or the soundness or the continuity of its payment services. Member States shall ensure that when payment institutions outsource important operational functions, the payment institutions meet the following conditions: […]. (8) Payment institutions shall communicate to the competent authorities of their home Member State without undue delay any change regarding the use of entities to which activities are outsourced […].
Article 20:	***Liability** - (1) Member States shall ensure that, where payment institutions rely on third parties for the performance of operational functions, those payment institutions take reasonable steps to ensure that the requirements of this Directive are complied with. (2) Member States shall require that payment institutions remain fully liable for any acts of their employees, or any agent, branch or entity to which activities are outsourced.*
Article 95	*Management of operational and security risks - (1) Member States shall ensure that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents. (2) Member States shall ensure that payment service providers provide to the competent authority on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks. (3) By 13 July 2017, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant. EBA shall, in close cooperation with the ECB, review the guidelines referred to in the first subparagraph on a regular basis and in any event at least every 2 years. (4) Taking into account experience acquired in the application of the guidelines referred to in paragraph 3, EBA shall, where requested to do so by the Commission as appropriate, develop draft regulatory technical standards on the criteria and on the conditions for establishment, and monitoring, of security measures.*
Article 96:	***Incident reporting** - (1) In the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment service provider. Where the*

	incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.[…] (6) Member States shall ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide EBA and the ECB with such data in an aggregated form.
Directive (EU) 2016/1148 (NISD)	
Recital 56	*This Directive should not preclude Member States from adopting national measures requiring public-sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public-sector body concerned and not to the cloud computing service provider.)*
Article 13:	***International cooperation*** *The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.*
Article 14	*Security requirements and incident notification -1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.* *2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.* *3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.* *4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account: (a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident.* *5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other*

affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification. Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.

6. After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

7. Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.

Table A1: A non-exhaustive list of incident reporting schemes

Subjects	Article	Notification	Recipient and Timeframe
PSPs	Art 96 (1) and (2) PSD2 + GL on major incident reporting	Notification of major operational and security incidents in the provision of payment services	To competent authorities within 4 hours. CAs to EBA & ECB
PSPs	Art 96 (6) PSD2 + GL on fraud reporting requirements	Collect and report data on payment transactions and fraudulent payment transactions	To CAs every 6 months. CAs to EBA & ECB
Data controllers (organisations deciding on the purpose and means of the personal data processing)	Art 33 GDPR	(i) Notification of a personal data breach to the data protection authority within 72 hours after becoming "aware" of it, and (ii) communicate the personal data breach to the data subject without undue delay.	(i) Data protection authority within 72 hours
Operators of essential services (where applicable, credit institutions and FMIs)	Art 16 (5) NISD	Notification of significant impact on continuity of the essential services due to an incident affecting the digital service provider. *NB recital 13 NISD specifies that where there are incident reporting in supervisory manuals then they should be considered lex specialis. Also note that NISD is a min harmonisation directive and should be transpose by MS.*	To competent authorities or CSIRT (computer security incident response team)
Significant institutions	SSM	Significant cyber-incidents to be reported. Reporting template.	To SSM as soon as detected
ALSO: National schemes, eIDas and TARGET2			

Annex B: background material to analysis of (re)insurance legislation

B1. Relevant legislation

69. To answer the Commission question posed in the FinTech action plan, EIOPA's ha performed a gap-analysis with reference to the mandated legislation and guidance regarding Information and Communications Technology (ICT) security and governance requirements (including cyber security) issued by the Commission or by EIOPA:

- Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)
- Commission Delegated Regulation (EU) 2015/35 of 10 October 2014
- EIOPA Guidelines on System of Governance, EIOPA-BoS-14/259[31]
- EIOPA Guidelines on Own Risk and Solvency Assessment, EIOPA-BoS-14/259

70. EIOPA identified the gaps in Solvency II framework, in particular regarding the system of governance requirements, and assessed the current practices in supervision of ICT security and governance requirements.

Analysis of the legal framework in place

71. The rest of this section of Annex B gives an overview of current legal framework applicable to ICT security and governance requirements (including cyber security). The assessment of mandated current legislation and guidelines resulted in the following findings:

Solvency II Directive (Articles 41 and 44)

72. Solvency II Directive (Article 41 and Article 44 of Directive 2009/138/EC) addresses the system of governance and the need for insurance and reinsurance undertakings to manage their business in a sound and prudent manner. The risk management system should cover risks, at an individual and at an aggregated level, to which undertakings are or could be exposed, and their interdependencies. This definition includes 'operational risk', where ICT security risk (including cybersecurity risk) should be classified.

[31] These Guidelines are based on Articles 40 to 49, Article 93, Article 132 and Article 246 of Solvency II and on Articles 258 to Article 275 of Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC ("Commission Delegated Regulation 2015/35")

73. The reference in Article 41 (4) to business continuity and contingency plans should also be considered in this context.

74. Under Solvency II the ORSA (Article 45) plays an important role. The role of the ORSA in the assessment by the undertaking of the material risks it is exposed to, is crucial for any risk but particularly for ICT risks (including cybersecurity risk) as part of the undertaking's operational risk. In fact, it is known that the standard formula for operational risk calculation is not as sensitive to the risks as the other risk modules. As such, under the ORSA it is expected that undertakings assess if the standard formula reflects its operational risk profile. It is also expected that considering the global consensus in identifying ICT risk as possibly one of the top emergent risks for the insurance market that the ORSA of each undertakings shall include an assessment of these risks, if these are assessed as material by the undertaking.

Article 41 (extract)
General governance requirements
1. Member States shall require all insurance and reinsurance undertakings to have in place an effective system of governance which provides for sound and prudent management of the business.
4. Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, the undertaking shall employ appropriate and proportionate systems, resources and procedures.

Article 44 (extract)
Risk management
1. Insurance and reinsurance undertakings shall have in place an effective risk-management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies.
2. The risk-management system shall cover the risks to be included in the calculation of the Solvency Capital Requirement as set out in Article 101(4) as well as the risks which are not or not fully included in the calculation thereof.
The risk-management system shall cover at least the following areas:
(a) underwriting and reserving;
(b) asset–liability management;
(c) investment, in particular derivatives and similar commitments;
(d) liquidity and concentration risk management;
(e) operational risk management;
(f) reinsurance and other risk-mitigation techniques.

Article 45 (extract)
Own risk and solvency assessment
1. As part of its risk-management system every insurance undertaking and reinsurance undertaking shall conduct its own risk and solvency assessment. That assessment shall include at least the following:
(a) the overall solvency needs taking into account the specific risk profile, approved risk tolerance limits and the business strategy of the undertaking;

Delegated Regulation 2015/35/EC (Article 258)

75. The Delegated Regulation supplementing the Solvency II Directive details the general governance requirements specified above (System of Governance, section 1, Elements of the system of governance, Article 258, General governance requirements). These requirements refer to the information systems used (letter h), and require undertakings to maintain adequate and orderly records of the undertaking's business and internal organisation (letter i) and safeguard the security, integrity and confidentiality of information (letter j) as well as establishing, implanting and maintaining a business continuity policy (paragraph 3).

Article 258 (extract)
General governance requirements

1. Insurance and reinsurance undertakings shall fulfil all of the following requirements:
(a) establish, implement and maintain effective cooperation, internal reporting and communication of information at all relevant levels of the undertaking;
(..) ….
(h) establish information systems which produce complete, reliable, clear, consistent, timely and relevant information concerning the business activities, the commitments assumed and the risks to which the undertaking is exposed;
(i) maintain adequate and orderly records of the undertaking's business and internal organisation;
(j) safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question;
3. Insurance and reinsurance undertakings shall establish, implement and maintain a business continuity policy aimed at ensuring, in the case of an interruption to their systems and procedures, the preservation of essential data and functions and the maintenance of insurance and reinsurance activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of their insurance or reinsurance activities.

Guidelines on system of governance (EIOPA-BoS-14/253 EN)

76. EIOPA Guidelines on system of governance refer to the operational risk and in Guideline 21 (b) specifically to IT-systems whereas Guideline 8 refers to contingency plans.

Guideline 8 - Contingency plans
The undertaking should identify material risks to be addressed by contingency plans covering the areas where it considers itself to be vulnerable, and it should review, update and test these contingency plans on a regular basis.

Guideline 21 – Operational risk management policy
In the risk management policy, the undertaking should cover at least the following with regard to operational risk:
a) identification of the operational risks it is or might be exposed to and assessment of the way to mitigate them;
b) activities and internal processes for managing operational risks, including the IT system supporting them;
c) risk tolerance limits with respect to the undertaking‘s main operational risk areas.

77. These Guidelines do not properly reflect the importance of taking care of ICT risks (including cybersecurity risks) as stressed e.g. by the FinTech Action plan. There is no guidance regarding vital elements that are generally acknowledged as being part of proper ICT security and governance requirements.

B2. ICT security risk profile of an insurance or reinsurance undertaking

Summary

78. EIOPA emphasises the specificities of ICT risks (including cybersecurity risks[32]) as part of the insurance and reinsurance undertaking's risk profile. These specificities need to be considered during the drafting process of the proposed Guidelines in order to target those guidelines to undertakings as much as possible (while making use of already existing legislation and guidance).

79. The risk profile as described in Article 295 and Article 309 of Delegated Regulation (EU) 2015/35 for purposes of public disclosure and regular supervisory reporting includes 'ICT-security risk' (including cybersecurity risk) as part of 'operational risk'. This specific risk is basically any threat to information, information systems and business processes and addresses safeguarding 'confidentiality'; 'integrity' and 'availability' of information, information systems and business processes involved. Although every financial undertaking (Article 13 paragraph 25 of Solvency II Directive) is vulnerable to these risks, there are certain differences depending on the business model / operating model[33] and the underlying processes between the different entities in the financial sector. In comparison with, for instance, credit institutions or other financial institutions, insurance undertakings[34], especially life and health insurers, are by nature (based on their current business model and underlying processes) less vulnerable to disruptive attacks / business interruptions. However, undertakings (and the large amount of liaised agents, intermediaries and other affiliated companies with often their own access to the data) are very attractive to cyber criminals because of their large data repositories with sensitive personal information such as information on health, housing and mobility and other proprietary data related to business secrets. In the near future these data repositories will probably grow by the expected use of data from Internet of Things (IOT), like data gathered by smart cars, smart homes and some health apps used for insurance purposes.

80. Furthermore, undertakings are going to be even more vulnerable to attacks by the increasing use of IOT-tools, the use of platforms and other forms of cooperation (e.g. distributed ledger technologies such as blockchain).

[32] Cyber Risk The combination of the probability of cyber events occurring and their consequences. Source: FSB Cyber Lexicon

[33] Also taking into account that insurance undertaking often have multiple (cyber) connection with agents, intermediaries and customers.

[34] For non-life insurers, one can imagine that business interruption could be a disruptive event, because possible clients would not be able to 'buy' their short term insurance immediately or get their claims settled.

Undertakings' business model

81. Insurance undertakings base their business models around assuming and diversifying risk. Their business model involves pooling risk from individual payers and redistributing it across a larger portfolio. Most of these undertakings generate revenue in two ways: charging premiums in exchange for insurance coverage, then reinvesting those premiums into other interest-generating assets.

82. Reinsurance undertakings provide insurance against loss for other insurance undertakings. Reinsurance undertakings target a very different customer base than insurance undertakings, and they tend to work in wider jurisdictions that involve different, or even competing, legal systems.

The value chain

83. The main elements of the value chain for (re) insurance undertakings are 'Product design and pricing'; 'Marketing'; 'Underwriting'; 'Distribution / sales'; 'Claims handling' and 'Service to customers'. This value chain is underpinned by e.g. technology, which is both diverse in design and interconnectivity. These diverse technology infrastructures are open to cybersecurity risk, which could undermine the confidentiality, integrity and availability of insurance business processes as well as of undertaking's data / information.

Data

84. Data is, nowadays, next to labour, administration and management one of the, perhaps even the most valuable, resource of the value chain described above. (Re) insurance undertakings are data owners and data processors of large data repositories. These data repositories could draw the attention of cyber criminals or 'interested third countries'. E.g., the personal data stored in these data repositories often have much more details about individual customers than the data held in other financial institutions. Undertakings' data can contain all aspects of an individual's private, social and commercial life.

Third Parties as a stakeholders of the value chain

85. Other stakeholders like brokers, (managing) agents, intermediaries and customers, communicate sometimes using the platform provided by (re)insurance undertakings and sometimes via their own platforms. This allows these stakeholders to have access to the (re)insurers undertakings' databases. This interconnectivity through third party telecommunications links can generate a possible contagious silent threat travelling to the company system through these communications channels.

86. Undertakings often make use of external service providers via outsourcing of various parts of the process. Undertakings often 'outsource' the complete IT-infrastructure and services. This brings an increase of cybersecurity risks and more complex risk mitigation is required.

87. Outsourcing and cloud commonly used by undertakings represent a threat because they are difficult to have oversight of for both the company and the supervisor. Outsourced third parties have heightened access to (re)insurance ICT systems with full administration rights that the (re)insurance companies themselves may not have. A lack of appropriate implementation of information security measures or contingency planning in the case of a failure of a third party could compromise the cyber-resilience and increase the severity of a cyber-incidence (increased risk that the 'weakest link' will have an impact on the entire value chain).

88. The combination of all of these elements and their interconnectedness can raise the likelihood of spread of a cyber-incident and its potential impact. It could affect both critical and non-critical functions. The supply of critical functions to a specific organisation may not in itself create systematic risk, whereas non-critical functions could provide "aggregated and compound risk".

Technology as a business enabler

89. Increasing use of technology and its affiliated data affects every part of the undertaking's value chain and, thanks to its capabilities, completely changes communications and interactions across the traditional business model:

- Products. Autonomous vehicles, connected homes and sharing economy is changing the underlying need for insurance;
- Marketing. Evolving consumer behaviour is creating a shift to personalized mobile and online channels;
- Pricing. The combination of rich customer data, telematics and enhanced computing power is opening the door to pricing policies that could reduce barriers to entry;
- Distribution. New consumer behaviours and entrants are threatening traditional distribution channels;
- Service. Consumers expect personalized, self-directed interactions with companies via any device at any hour, much as they do with leading online retail leaders.

90. As stated, data is a central resource to the value chain and information security and business processes can be categorized by a triad of confidentiality, integrity and availability.

Confidentiality

91. Data confidentiality is probably the highest risk to the value chain so preventing the disclosure of information to unauthorized individuals or systems is a top priority for the (re)insurance undertakings' business model. Researchers revealed that close to 95% of all enterprise networks have been compromised by external attackers and only 3% of organisations felt safe against insider threats. Hundreds of millions of consumers have had their identity information compromised. The financial and reputational losses to businesses and shareholders stretch into tens of billions of euros annually. Moreover, infrastructure and data storage outsourcing put undertakings' further at risk as unregulated cloud service providers have highly differentiated security mechanisms that may not address threats to their customers.

92. Innovative, global technologies are disrupting the traditional infrastructure of the insurance industry. Mobile, digital, analytics and payment platforms are accelerating rapidly. In this new complex environment any breach of trust in the customers-insurer relationship that dilutes the customer experience or, worse, causes a loss of data leads to legal disputes or regulatory fines. There is increasing pressure on insurance companies to ensure this trust is maintained at all times.

Integrity

93. Integrity is maintaining and ensuring the accuracy and consistency of systems and information over the entire life cycle, Integrity is a pre-requisite for ensuring confidentiality. Without it, encryption is obsolete, bringing a false sense of security that almost always leads to downfall. Integrity brings auditability and transparency

94. Data loss is a huge risk for undertakings. The need of an undertaking to protect their data and to avoid data loss comes from two points: the importance to be able to conserve data integrity for their own business and internal risk model and secondly to protect their consumer (people and organizations) from data breaches and their possible consequences such as reputational damage.

95. Also the protection of the "intellectual property" of undertakings is key. (Re)insurance undertakings for instance use algorithms for the calculation of premiums and claims as well as in the underwriting process. The integrity of these algorithms, which are critical to the business and are an integral support to the value chain, should be protected. Unauthorised manipulation of these modelling engines either internally or through a cyber-incident could have a large impact on the integrity not only of the data that is compromised but the entire business model they support.

Availability

96. In comparison with other financial sectors, (re)insurance undertakings processes are less time critical and therefore business interruption due to unavailability of technology services is not its highest priority. Without underestimating the problems this would cause for individual customers, there is no systemic risk if an undertaking is not able to pay out claims for one week. On the other hand, for an individual undertaking it might be a problem if the (re)insurer would not be able to accept new clients for a week due to system unavailability. The main area of high availability to support the critical business processes within undertakings is to have high availability payments providers, which are shared with all other parts of the financial sector.

B3. Overall results of the stock take exercise

97. To gain an overview about the existing local legislation and guidance as well as about the supervisory practices across financial sectors, especially regarding undertakings, around ICT security and governance requirements EIOPA has performed a survey.

Stock take results

98. The survey was sent to all the EEA countries and the results were collected from 28 members, describing their current legislation as well as supervisory practices.

99. The outcome of the survey shows that the vast majority of countries, actually 22 of the 28 countries that replied to the questionnaire, have legislation and / or guidance about ICT security and governance (including cyber security) in force. In this respect, the survey revealed further that quality of legislations / guidance is heterogeneous, varying from brochures with guiding instructions to fixed legislation approved by Parliaments. Based on the answers collected, most of these regulations are guiding rules (9 countries) and the rest are either pure comply or a combination of comply and explain.

100. The vast majority of the legislation / guidance in place covers the following main areas of ICT security and governance: IT-Strategy, IT Risk and Security Management, IT Operations as well as Third Party Management. However, the level of detail and the aspects covered in each of these areas appears to be varying.

101. On the other hand, the survey revealed that in some areas such as IT governance, “malware, patch management and anti-virus management”, “security awareness and training”, reporting and personnel security (vetting, disciplinary actions) the coverage was slightly above 50 percent. One area, Cyber Resilience Benchmarking (use of metrics), was not covered by any legislation / guidance.

102. Regarding supervisory practices, the survey captured that although many NCAs have procedures to cope with this issue in place, not every country has specific expertise or an organisational structure addressing this. Overall the survey indicates a wide range of supervisory practices applied.

103. In relation to on-site supervision, the majority of the members that are active in supervising ICT security and governance do actively perform on-site assessments or are planning to do so in the near future, even though the procedure and the frequencies vary among them.

104. In addition, member states were asked to give their opinion about the priority of additional legislation: ten of the members replied “High priority / Priority”; seven members see a low priority and other members did not provide an answer.

105. EIOPA concludes from the survey that although the majority of countries are aware of the risks of ICT-security, there is little harmonisation of regulation and supervisory practice within

the member states. Because ICT-security is such a universal issue this area would greatly benefit from more harmonisation between the member states.

Table B1: Ruling concerning IT and cyber security for the (re)insurance sector

Ruling concerning IT and cyber security for the (re)insurance sector			
Yes	Austria Belgium Croatia Czech Republic Denmark Estonia Finland France Germany Greece Hungary Iceland Ireland Italy Latvia Liechtenstein Netherlands Norway Poland Spain Sweden UK	**No**	Bulgaria Cyprus Luxembourg Portugal Slovak Republic Slovenia

Annex C: background material to analysis of securities markets legislation

32. To identify whether there is a need for improvements in the legislative provisions relating to ICT risk management, security and governance, ESMA has reviewed the legislative texts under its remit, specifically:[35]

    - Regulation (EC) 1060/2009 on Credit Rating Agencies (CRAR)
    - Regulation (EU) 648/2012 on OTC derivatives, central counterparties and trade repositories (EMIR)
    - Regulation (EU) 909/2014 on Central Securities Depositories (CSDR)
    - Directive 2014/65/EU and Regulation (EU) 600/2014 on Markets in Financial Instruments (MiFID II / MiFIR)
    - Directive 2011/61/EU on Alternative Investment Fund Managers (AIFMD)
    - Directive 2009/65/EC of the European Parliament and of the Council on Undertakings for Collective Investment in Transferable Securities (UCITS)

33. These areas of legislation principally apply to the following groups of entities.

    - Credit Ratings Agencies (CRAs) [36] are subject to CRAR
    - Trade Repositories (TRs)[37] are subject to EMIR
    - Central Counterparties (CCPs) are subject to EMIR
    - Central Securities Depositories (CSDs) are subject to CSDR
    - Investment firms are subject to MiFID II / MiFIR
    - Trading venues are subject to MiFID II / MiFIR

[35] The detailed analysis presented in Table C1 focuses on Level 1 and Level 2 requirements. In some cases, Level 3 Guidelines may be relevant to the thematic questions considered. For example, CRAR contains no provision on incident reporting of cybersecurity incidents (see row E of Table C1) but the relevant Guidelines on Periodic information to be submitted to ESMA by CRAs [ESMA 33-9-295, published 5 February 2019] require CRAs to notify ESMA of "any IT or information security incidents that impact the operation of CRA's credit rating business under the CRA Regulation". ESMA's proposals set out in section 2.1 would ensure a clear, consistent basis for such reporting in Level 1 or Level 2.

[36] These entities are under ESMA's direct supervision mandate.

[37] These entities are under ESMA's direct supervision mandate.

- Data Reporting Service Providers (DRSPs) are subject to MiFID II / MiFIR

- Asset managers are subject to AIFMD / UCITS

34. Table C1 in Annex C sets out in detail the extent to which the current Level 1 and Level 2 legislative provisions most relevant to ESMA's remit contain the following:

    A. Specific cybersecurity requirements

    B. Terminology specific to cybersecurity

    C. Overarching requirements on operational risk that may cover ICT/cybersecurity risk

    D. Governance and strategy requirements of the legislation which may be applicable to ICT/cybersecurity governance

    E. Requirements for incident reporting to authorities that could cover cybersecurity incidents

    F. Requirements that may address third-party concentration risk so as to mitigate a source of ICT/cybersecurity risk

35. Thematic areas A-F form the rows of Table C1, with different regulations and directives forming the column headings.

Table C1: Content of different areas of legislation most relevant to ESMA's remit, with respect to thematic questions on ICT/cybersecurity risk

Thematic question	AIFMD	UCITS	MIFID investment firms	MIFID DRSPs	MIFID trading venues	CSDR CSDs	EMIR CCPs	EMIR TRs	CRAR CRAs
A. Are there specific cybersecurity requirements in the legislation?	No	No	No	Yes: A DRSP shall set up and maintain procedures and arrangements for physical and electronic security designed to: (a) protect its IT systems from misuse or unauthorised access; (b) minimise the risks of attacks against the information systems as defined in Art 2(a) Directive 2013/40/EU; (c) prevent unauthorised disclosure of confidential information; (d) ensure the security and integrity of the data.	Yes: Trading venues shall have in place procedures and arrangements for physical and electronic security designed to protect their systems from misuse or unauthorised access and to ensure the integrity of the data that is part of or passes through their systems, including arrangements that allow the prevention or minimisation of the risks of attacks against the information systems as defined in Art 2(a) of Directive 2013/40/EU (L2: Art 23 CDR 2017/584) "Resilience" – "Sufficient " e "Business Continuity"	Yes: A CSD's comprehensive risk management framework shall enable the CSD to protect the information at its disposal from unauthorised access or disclosure, ensure data accuracy and integrity and maintain availability of the CSD's services and shall include comprehensive framework for information security to manage the risks CSDs face from cyber-attacks. (L2: Art 70 CDR 2017/392) A CSD shall ensure that its information technology (IT) systems are well-documented and that they are	Yes: A CCP shall maintain a robust information security framework that appropriately manages its information security risk. The framework shall include appropriate mechanisms, policies and procedures to protect information from unauthorised disclosure, to ensure data accuracy and integrity and to guarantee the availability of the CCP's services. (L2: Art 9(3) CDR 153/2013)	No, however some EMIR requirements are relevant: L1: Art 79: "1. […] Such systems shall be reliable and secure and have adequate capacity to handle the information received." "2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan aiming at ensuring the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations. Such a plan shall at least	No, however some CRAR requirements are relevant: L1: Art 6(2), Annex I, Section A: "4. A credit rating agency shall have sound […] internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems." Art 6(2), Annex I, Section A: "8. A credit rating agency shall employ appropriate systems,

Thematic question	AIFMD	UCITS	MIFID investment firms	MIFID DRSPs	MIFID trading venues	CSDR CSDs	EMIR CCPs	EMIR TRs	CRAR CRAs
				A DRSP shall set up and maintain measures and arrangements to promptly identify and manage the risks identified above. Specific to Approved Reporting Mechanism (ARM), where an investment firm uses a third party to submit information to an ARM on its behalf, an ARM shall have procedures and arrangements in place to ensure that the submitting firm does not have access to any other information about or submitted by the reporting firm to the ARM which may have been sent by the reporting firm directly to the ARM or via	(L1: Art 48 Directive 2014/65/EU)	designed to cover the CSD's operational needs and the operational risks that the CSD faces. (L2: Art 75(1) CDR 2017/392) A CSD's information security framework shall outline the mechanisms that the CSD have in place to detect and prevent cyber-attacks. The framework shall also outline the CSD's plan in response to cyber-attacks. (L2: Art 75(5) CDR 2017/392)		provide for the establishment of backup facilities." Art 80(1): "A trade repository shall ensure the confidentiality, integrity and protection of the information received under Art 9."	resources and procedures to ensure continuity and regularity in the performance of its credit rating activities."

Thematic question	AIFMD	UCITS	MIFID investment firms	MIFID DRSPs	MIFID trading venues	CSDR CSDs	EMIR CCPs	EMIR TRs	CRAR CRAs
				another submitting firm. (L2: Art 9 (1) and (2) CDR 2017/571)					
B. Does the legislation contain terminology specific to cybersecurity?	Yes, although terminology is relevant but not specific: 'Information', 'Electronic data', 'business continuity'	Yes, although terminology is relevant but not specific: 'Information', 'Electronic data', 'business continuity'	Yes, although terminology is relevant but not specific: 'Critical or important operational functions', 'business continuity'	Yes: 'Information systems', 'attacks'	Yes: 'Information systems', 'attacks'	Yes: 'IT tools, controls and procedures', 'Information systems', 'Cyber-attacks'	Yes: 'Information technology systems'	Yes: 'Reliable and secure systems', 'business continuity policy', 'disaster recovery plan', 'confidentiality, integrity, protection of information'	Yes: 'Information processing systems', 'continuity', 'regularity'
C. Does the legislation contain overarching requirements on operational risk that may cover ICT/cybersecurity risk?	Yes, though the requirements are general. Requirement to have risk management policies and arrangements that identify all relevant risk, and to manage them. (L1: Art 15, 2011/61/EU) Effective internal operational risk management	Yes, though the requirements are general. Requirement to have risk management policies and arrangements that identify all relevant risk, including operational risks and to manage them L2: Art 38, 39 and 40	Yes, although the requirements are general and specificities relate only to outsourcing, critical functions. and ensuring outsourcing does not lead to undue operational risk L1: Art 16 (5), MIFID II. Business continuity is dealt with by L2 (Art 21 (3) of CDR 2017/565). See also outsourcing	Yes: Member states shall require the DRSP to have sound security mechanisms in place designed to guarantee the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access and to prevent information	Yes (L1: Art 48(1) MIFID II)	Yes: 'Operational risks comprise the risks caused by deficiencies in information systems' (L2: Art 66(1) CDR 2017/392)	Yes: A CCP shall have a sound framework for the comprehensive management of all material risks to which it is or may be exposed. (L2: Art 4 CDR 153/2013) 'A CCP shall maintain IT systems adequate to deal with the complexity, variety and type of services and activities performed so as to ensure high standards of security and the integrity and	Yes: L1: Art 79: "1. A trade repository shall identify sources of operational risk and minimise them through the development of appropriate systems, controls and procedures."	No, however CRAR has some organisational requirements relevant to operational risk. L1: Art 6(2), Annex I, Section A: "8. A credit rating agency shall employ appropriate systems, resources and procedures to ensure continuity and regularity in the performance of

Thematic question	AIFMD	UCITS	MIFID investment firms	MIFID DRSPs	MIFID trading venues	CSDR CSDs	EMIR CCPs	EMIR TRs	CRAR CRAs
	policies also required by L2: Art 13, Commission Delegated Regulation (EU) No [CDR] 231/2013 Note: some (but not all) AIF Managers are subject to CRD/CRR, which may pose additional requirements.	Please note that some (but not all) UCITS Managers are subject to CRD/CRR and there may be additional requirements from those pieces of legislation.	requirements on critical operational functions. Please note that investment firms generally are also subject to CRD/CRR and there may be additional requirements from those pieces of legislation.	leakage, maintaining the confidentiality of the data at all times. The home Member State shall require the DRSP to maintain adequate resources and have back-up facilities in place in order to offer and maintain its services at all times. (L1: Art 64(4), 65(5) and 66(3) of MiFID II for APA, CTP and ARM respectively).			confidentiality of the information maintained' (L1: Art 26 EMIR)		its credit rating activities."
D. What are the governance and strategy requirements of the legislation which may be applicable to ICT/cybersecurity governance?	Governance requirements are applicable to cyber / ICT, but not specific. Overarching requirement to act with due skill, care and diligence: L1: Art 12(1) 2011/61/EU	Governance requirements are applicable to cyber / ICT, but not specific. Overarching requirement to act with due skill, care and diligence: L1: Art 14(1) Directive 2009/65/EC	Requirements applicable to cyber / ICT governance are exhaustive but they are also general, not specific to the area, or indeed, granular. MiFID II organisational requirements apply to investment firms	L2: Art 9 of CDR 2017/571.	General requirements for governance and robust risk management framework for regulated markets are applicable, but not specific, to cyber/ICT. (L1: Art 47 MIFID II)	General requirements for governance and robust risk management framework are applicable, but not specific, to cyber/ICT. (L2: Art 49 CDR 2017/392, Art 70 CDR 2017/392)	General requirements for governance and robust risk management framework are applicable, but not specific, to cyber/ICT. (L1: Art 26(1) EMIR, L2: Art 9(3) CDR 153/ 2013)	Governance requirements are applicable to cyber / ICT, but not specific. L1: Art 78(1): "A trade repository shall have robust governance arrangements, which include a clear organisational structure with well defined,	CRAR has some organisational requirements which are applicable to cyber / ICT, but not specific. L1: Art 6(2), Annex I, Section A: "4. A credit rating agency shall have […] internal control mechanisms,

Thematic question	AIFMD	UCITS	MIFID investment firms	MIFID DRSPs	MIFID trading venues	CSDR CSDs	EMIR CCPs	EMIR TRs	CRAR CRAs
	There are overarching requirements for robust risk management frameworks L1: Art 15 2011/61/EU, L2: Chapter III, Section 3 Commission Delegated Regulation No (EU) 231/2013	There are overarching requirements for robust risk management frameworks Art 51 (1) 2009/65/EC, Commission Directive 2010/43/EU L2: Chapter VI Commission Directive 2010/43/EU	and credit institutions providing investment services and performing investment activities. MiFID II requires firms to establish, implement and maintain risk management policies, additionally imposing "quality requirement" on general basis (the risks management must be "adequate" and "effective"). L2: Delegated Regulation 2017/565, Art 23 and internal audit.					transparent and consistent lines of responsibility and adequate internal control mechanisms, including sound administrative and accounting procedures, which prevent any disclosure of confidential information"	effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems."
E. Does legislation contain a requirement for incident reporting to authorities that	No	No	No	Yes: DRSPs are required to notify their competent authority (in the case of ARMs the notification shall	No specific requirement, but could cover cybersecurity incidents. See Art 23(3) CDR 2017/584	No specific requirement, but could cover cybersecurity incidents: a CSD 'shall inform [authorities] without	No	No	No

Thematic question	AIFMD	UCITS	MIFID investment firms	MIFID DRSPs	MIFID trading venues	CSDR CSDs	EMIR CCPs	EMIR TRs	CRAR CRAs
could cover cybersecurity incidents?				include all other NCAs to whom the ARMs submit transaction reporting) and clients that have been affected by the breach. (Art 9(4) CDR 2017/571)		delay of any operational incidents resulting from such risks [that key participants, service and utility providers, other CSDs and market infrastructures might pose to its operations]' (Art 45(6) CSDR and Art 41 CDR 2017/392)			
F. Does legislation contain requirements which may address third-party concentration risk so as to mitigate a source of cyber / ICT risk?	Somewhat. There are specific rules on delegation of AIFM activities, (may be a limit to the extent AIFM activities are applicable to cybersecurity risk).). Delegation must be undertaken with due care and skill, and monitored effectively (L1: Art 20(1), 2011/61/EU)	Somewhat. Overarching requirement to act with due skill, care and diligence, which could reasonably capture managing third party risk: L1: Art 14/1 2009/65/EC Requirement to exercise due skill, care and diligence when entering into, managing or terminating	Yes: There are specific and extensive provisions on outsourcing critical or important operational functions: Directive 2014/65, art 16(5) and art 30, 31, 32 of Delegated Regulation 2017/565	There are provisions on outsourcing functions but no requirements with regard to "concentration risk". (Art 6 of CDR 2017/571)	There are provisions on outsourcing operational functions but no requirements with regard to "concentration risk". (Art 6 of CDR 2017/584)	Yes, though general: CSDs shall identify operational risks that may be posed by key participants, critical utilities and critical service providers, and by other CSDs or market infrastructures (Art 45(6) CSDR, Art 67, 68, 69 CDR 2017/392) In case of outsourcing, service providers must meet applicable EU standards for data	Yes, though general: A CCP shall develop appropriate risk management tools to be in a position to manage and report on all relevant risks. These shall include the identification and management of system, market or other interdependencies. (Art 4 CDR 153/2013) Business continuity policy to take into account external links and interdependencies	No	Yes: L1: Art 9: "Outsourcing of important operational functions shall not be undertaken in such a way as to impair materially the quality of the credit rating agency's internal control and the ability of ESMA to supervise the credit rating agency's compliance with obligations

Thematic question	AIFMD	UCITS	MIFID investment firms	MIFID DRSPs	MIFID trading venues	CSDR CSDs	EMIR CCPs	EMIR TRs	CRAR CRAs
		any arrangements with third parties in relation to the performance of risk management activities. However, note this relates to *risk management.* L2: Art 23 Commission Directive 2010/43/EU				protection (Art 30(1)(i) CSDR)	including TVs cleared by the CCP, SSS and payment systems and CIs used by the CCP or a linked CCP (Art 17 CDR 153/2013) Business impact analysis of critical business functions: take into account dependencies on external providers, including utilities services (Art 18 CDR 153/2013). CCPs to take action to manage such dependencies. In outsourcing requirements: service provider to implement equivalent business continuity requirements to those of the CCP under EMIR (Art 35 CDR 153/2013)		under this Regulation."