IAIS

INTERNATIONAL ASSOCIATION OF
INSURANCE SUPERVISORS

Public

Draft Application Paper on Supervision of Insurer Cybersecurity

29 June 2018

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for Members to share their experiences and understanding of insurance supervision and insurance markets.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), member of the Standards Advisory Council of the International Accounting Standards Board (IASB), and partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

Application Papers provide additional material related to one or more ICPs, ComFrame or G-SII policy measures, including actual examples or case studies that help practical application of supervisory material. Application Papers could be provided in circumstances where the practical application of principles and standards may vary or where their interpretation and implementation may pose challenges. Application Papers can provide further advice, illustrations, recommendations or examples of good practice to supervisors on how supervisory material may be implemented.

International Association of Insurance Supervisors
c/o Bank for International Settlements
CH-4002 Basel
Switzerland
Tel: +41 61 280 8090
Fax: +41 61 280 9151
www.iaisweb.org

This document was prepared by Financial Crime Task Force in consultation with IAIS Members.

This document is available on the IAIS website (www.iaisweb.org).

Contents

1.0 Introduction and Background

1.1 Purpose of this Paper

1. In January 2018, the World Economic Forum noted that: "Cybersecurity risks are growing, both in their prevalence and in their disruptive potential, accompanied by rising financial impact." [1] Insurers, both as underwriters of cyber insurance, and as participants in the financial sector, are not immune to either the disruptive potential or the financial impact of cybersecurity incidents.[2]

2. As stated in the IAIS Issues Paper on Cyber Risk to the Insurance Sector, developed by the Financial Crime Task Force and published in August 2016, [3] "for insurers, cybersecurity incidents can harm the ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector."

3. Among its conclusions, the Issues Paper stated:

   "Cyber risk presents a growing challenge for the insurance sector, and one which, under the [Insurance Core Principles], supervisors are obliged to address. Insurers collect, store, and manage substantial volumes of confidential personal and commercial information. Because of these reservoirs of data, insurers are prime targets for cyber criminals who seek information that later can be used for financial gain through extortion, identity theft, or other criminal activities. In addition, because insurers are significant contributors to the global financial sector, interruptions of insurers' systems due to cybersecurity incidents may have far-reaching implications."

4. Importantly, while recognizing the "diversity of sophistication on cyber-related issues among IAIS Members," in the Issues Paper the IAIS observed that: "Because of the growing frequency and severity of cybersecurity incidents on all commercial entities, cyber resilience must be achieved by all insurers, regardless of size, speciality, domicile, or geographic reach."

5. Additionally, the Issues Paper noted that the nature of cyber risk requires supervisors to exercise increased scrutiny of insurers, and in this regard concluded that the Insurance Core Principles (ICPs), through the principle statements and accompanying standards and guidance, encompass the issues presented by cyber risks, thereby providing a general basis for supervision of the insurance sector with respect to cybersecurity.

6. Finally, the Issues Paper recommended that the IAIS develop and publish one or more Application Papers further exploring cyber risk, cybersecurity, and cyber resilience and proposing supervisory practices for the insurance sector.

---

[1] World Economic Forum, *The Global Risks Report* (January 2018), available at http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[2] OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (December 2017), available at http://www.oecd.org/publications/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm. For discussion of cyber threats faced by consumers and commercial entities, see, for example, RMS *Cyber Risk Outlook* (2018), available at http://forms2.rms.com/CyberRiskLandscapeReport2018.html.

[3] IAIS, *Issues Paper on Cyber Risk to the Insurance Sector* (August 2016), available at https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector.

7. In view of the developing nature of cyber security frameworks and practices, this Application Paper is intended to provide further guidance to supervisors seeking to develop or enhance their approach to supervising the cyber risk, cybersecurity, and cyber resilience of insurers.[4] Insurers are invited to consider this Application Paper, to assist in developing and implementing good cybersecurity practices in their organisations.

8. Recognizing the continuously evolving nature of the threat,[5] as well as the potential benefits of regulatory convergence,[6] this paper is generally principles-based and builds on frameworks and guidance from multiple sources, including the *G7 Fundamental Elements of Cyber Security for the Financial Sector* (G7FE)[7], the related *G7 Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector* (G7FEA)*;* [8] and the *CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures* (CPMI-IOSCO Guidance). [9]

9. This paper focuses on supervision of insurers' cybersecurity[10]. As with the Issues Paper, it does not cover cyber insurance (insurers' selling or underwriting that type of insurance product and related market or prudential issues) nor the use of cyber insurance in the reduction of residual risks.[11]

[4] A survey conducted by IAIS in late 2016 demonstrated both that jurisdictional cybersecurity regulatory and supervisory regimes vary significantly among IAIS Members, and that Members supported development of further guidance in areas most relevant to insurer cyber risk.

[5] For example, see CISCO, *2018 Annual Cybersecurity Report*, available at https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?.

[6] Financial Stability Board, "Summary of FSB Workshop on Cybersecurity," in *Summary Report of Financial Sector Cybersecurity Regulations, Guidance, and Supervisory Practices* (October 2017), at Section 3, available at http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/.

[7] *G7 Fundamental Elements of Cybersecurity for the Financial Sector* (October 2016), available at https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5.

[8] *G7 Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector* (October 2017), available at http://www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf.

[9] CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market Infrastructures* (29 June 2016), available at https://www.bis.org/cpmi/publ/d146.pdf.

[10] It is acknowledged that supervisory authorities themselves are subject to cyber risks. The G7 Fundamental Elements of Cybersecurity for the Financial Sector, for example, addresses public entities as well as private ones ("To address these risks, the below non-binding, high-level fundamental elements are designed for financial sector private and public entities to tailor to their specific operational and threat landscape, role in the sector, and legal and regulatory requirements."). This aspect, however, is outside the scope of this Application Paper.

[11] On the use of cyber insurance as a risk-mitigant for financial institutions, see, for example, "Cyber Insurance and its Potential Role in Risk Management Programs," U.S. Federal Financial Institutions Examination Council (Joint Statement 10 April 2018), available at https://www.ffiec.gov/press/pdf/FFIEC%20Joint%20Statement%20Cyber%20Insurance%20FINAL.pdf; European Insurance & Occupational Pensions Authority, *Cyber Risk: Some Strategic Issue* (2016), available at https://eiopa.europa.eu/Publications/Stakeholder%20Opinions/IRSG%20own%20initiative%20paper%20-

1.2 Terminology

10. In an October 2017 report, the Financial Stability Board (FSB) highlighted six different definitions of "cybersecurity" offered by FSB members.[12] Similarly, in 2015 the European Union Agency for Network and Information Security (ENISA) commented on the gaps and overlaps in cyber terminology usage among various stakeholders, noting that because of its "enveloping nature," the term "cybersecurity" needs a "contextual definition" that is relevant for particular organizations.[13]

11. As the FSB reported in March 2018,[14] based on its recommendation and in response to a suggestion from the G20 Finance Ministers and Central Bank Governors, an FSB working group expects to finalize a "cyber lexicon" for delivery at the November 2018 Buenos Aires G20 Summit. In general, the objective of the FSB in developing the lexicon is "to support the work of the FSB, standard-setting bodies, authorities and private sector participants ... to address cyber security and cyber resilience in the financial sector."[15]

NOTE – The Task Force expects to make additional and conforming definitional edits prior to final publication of this Application Paper, based in part on the FSB cyber lexicon work.

12. For purposes of this Application Paper reference is made to the Glossary of Terms in Annex II of the 2016 Issues Paper,[16] which in turn was primarily based on work of the Federal Financial Institutions Examination Council (FFIEC); the CRO Forum; the Cyber Resilience Working Group of the Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO); and the National Institute of Standards and Technology (NIST, U.S. Department of Commerce).

13. Accordingly, in the context of this paper, "cyber risk" means: "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage

%20Cyber%20risk.pdf. (prepared by EIOPA Insurance & Reinsurance Stakeholder Group); and Geneva Association, *Cyber Insurance as a Risk Mitigation Strategy* (April 2018), available at https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy.

[12] Box 1 – "What are Cybersecurity and Cyber Resilience," FSB *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*, at page 5 (October 2017), available at http://www.fsb.org/wp-content/uploads/P131017-2.pdf.

[13] ENISA, *Definition of Cybersecurity – Gaps and Overlaps in Standardisation* (offers multiple definitions for consideration by Standards Development Organizations and other organizations) (December 2015), available at https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

[14] Financial Stability Board, "Progress Update on Cyber Lexicon" (March 20, 2018); available at http://www.fsb.org/2018/03/progress-update-on-cyber-lexicon/ (and linked file: with more detail at http://www.fsb.org/wp-content/uploads/P200318.pdf).

[15] The IAIS is participating in the FSB cyber lexicon working group.

[16] Annex II - IAIS, *Issues Paper on Cyber Risk to the Insurance Sector* (August 2016).

that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information − be it related to individuals, companies, or governments."

14. "Cybersecurity," in turn, "refers to strategies, policies, and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities, and policies regarding the security of an insurer's operations."

15. As in the Issues Paper, "cybersecurity incident" is used generally to include both "cyber attacks" and "cyber incidents."

1.3 Proportionality

16. Cybersecurity is both a collective and an individual undertaking. Supervisors should recognize, moreover, that while cybersecurity is necessary for all insurers, there is no one-size-fits-all prescription for insurers or for supervisors. Nothing in this Application Paper is intended to derogate from the general description in the ICPs that while they are applicable to insurance supervision in all jurisdictions, regardless of the sophistication of its insurance markets and the type of products / services under supervision, nevertheless:

"[S]upervisory measures should be appropriate to attain the supervisory objectives of a jurisdiction and should not go beyond what is necessary to achieve those objectives. It is recognised that supervisors need to tailor certain supervisory requirements and actions in accordance with the nature, size, complexity, risk profile, and culture of individual insurers. In this regard, supervisors should have the flexibility to tailor supervisory requirements and actions so that they are commensurate with the risks posed by individual insurers as well as the potential risks posed by insurers to the insurance sector or the financial system as a whole."[17]

1.4 Nature of This Paper

17. This paper provides guidance for insurance supervisors (and may also useful to insurers), but it is not intended to be exhaustive or prescriptive.

18. Under IAIS procedures an Application Paper can provide additional material related to one or more ICPs that help with practical application of ICPs, but an Application Paper is not binding and does not establish standards. Application Papers can provide examples of good practices, as well as further advice and recommendations on how ICPs may be implemented.[18]

19. Supervisors should also consider this Application Paper with respect to cybersecurity of insurance intermediaries that are subject to their supervision.[19]

[17] ICP, Introduction - Scope and coverage of the Insurance Core Principles.

[18] Policy for Consultation of Stakeholders at 2 and Annex 1 (February 2015), available at https://www.iaisweb.org/page/about-the-iais/policies-and-procedures/file/47624/policy-for-consultation-of-stakeholders.

[19] ICP 18 (Intermediaries).

2.0 International, National, and Industry Cybersecurity Standards and Guidance

20. Multiple international, national and industry organizations, both public and private sector, have developed cybersecurity frameworks and guidance that have relevance to insurance supervision.[20]

2.1 Frameworks

21. In response to increasing concerns over cyber risk, various cybersecurity frameworks have been developed by public and private entities to provide a foundation for improving the ability of institutions to prevent, protect, and respond to cybersecurity incidents. Widely accepted cybersecurity frameworks include:

(a) Information Systems Audit and Control Association (ISACA) – COBIT

22. COBIT ("Control Objectives for Information and Related Technologies")[21] is an IT management and IT governance practices framework created by ISACA. COBIT provides an implementable set of controls over information technology and organizes them around a logical framework of IT-related processes and enablers.[22]

23. The framework (first released in 1996) defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures, and a maturity model. COBIT also provides a set of practices for governance and control process of information systems and technology with the goal of aligning IT with business. COBIT is used to implement, test, and audit controls over IT processes and related information security.

(b) International Organization for Standardization (ISO)[23]

24. ISO is an international (non-governmental) organization composed of representatives from over 160 national standards organizations, which seeks to develop and promote common standards. ISO and the International Electrotechnical Commission (IEC) offer recommendations on information security management and programme elements for the financial sector. ISO defines the broadest structure of an effective overall programme, supporting information security as a systems issue that includes technology, practice, and people, and describes the need for a formal security programme. ISO has

[20] Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices* (October 2017), pages 32-43 (compiling guidance and other work of international bodies), available at http://www.fsb.org/wp-content/uploads/P131017-2.pdf.

[21] ISACA, formerly known as the Information Systems Audit and Control Association, is an independent, nonprofit, global association, engaged in development of practices for information systems. http://www.isaca.org/about-isaca/Pages/default.aspx.

[22] ISACA also developed the *Cybersecurity Nexus (CSX)* particularly focusing on the mitigation of cybersecurity risks. It is also based on COBIT and available at https://cybersecurity.isaca.org/csx-nexus.

[23] ISO/IEC 27000 family - Information security management systems available at https://www.iso.org/isoiec-27001-information-security.html.

produced two families of standards largely used for the governance of information technology (ISO 38500) and the management of information security (ISO 27000).[24]

(c) NIST Cybersecurity Framework

25. The NIST Cybersecurity Framework,[25] released by the United States Commerce Department's National Institute of Standards and Technology (NIST) in 2014, following collaboration between the public and private sector, is a voluntary, risk-based set of industry standards and best practices to help organizations manage cybersecurity risks. Although originally developed for critical infrastructure, the Cybersecurity Framework "enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience." The Framework Core defines standardized cybersecurity activities, desired outcomes, and applicable references, and is organized by five continuous functions: Identify, Protect, Detect, Respond, and Recover. The Framework Core, in effect, describes the continuous cycle of business processes that constitute effective cybersecurity.

2.2 Guidance

26. The following paragraphs introduce several sets of financial sector guidance that have recently been published to assist institutions and supervisors in improving their approach to cybersecurity.

(a) FFIEC

27. In light of the increasing volume and sophistication of cyber threats, the U.S. Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment) to help institutions identify their risks and determine their cybersecurity preparedness.[26] The Assessment is intended to provide a repeatable and measurable process for financial institutions to track their cybersecurity preparedness over time. The Assessment consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. The Cybersecurity Maturity includes domains, assessment factors, components, and individual declarative statements across five maturity levels to identify specific controls and practices that are in place.

[24] See ISO 27032 Guidelines for Cybersecurity (specific for cyber) available at https://www.iso.org/standard/44375.html.

[25] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1 released on 16 April 2018), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[26] Federal Financial Institutions Examination Council (FFIEC), *Cybersecurity Assessment Tool* (Update May 2017), available at https://www.ffiec.gov/cyberassessmenttool.htm. The FFIEC is an inter-agency body responsible for developing uniform reporting systems for federally supervised financial institutions, their holding companies, and the nonfinancial institution subsidiaries of those institutions and holding companies. See https://www.ffiec.gov/about.htm.

(b) CPMI-IOSCO

28. In June 2016, the CPMI-IOSCO Working Group on Cyber Resilience (WGCR) released its CPMI-IOSCO Guidance.[27] The IAIS participated on the WGCR as an Observer Organization. Developed with the intention to "build resilience [that is] similar from one country to another,"[28] the CPMI-IOSCO Guidance has been described as "the first set of internationally agreed principles in the field of financial markets and institutions to support consistent and effective oversight and supervision in the area of cyber resilience."[29]

29. The CPMI-IOSCO Guidance focuses on cyber governance, response and recovery, threat intelligence, rigorous testing of systems and processes, cyber risk awareness, and continual improvement, and describes a systemic approach to cybersecurity.

30. The CPMI-IOSCO Guidance recognizes that governance is central to an institution's ability to build and maintain a cyber resilient organization.

31. Development of the CPMI-IOSCO Guidance was a key milestone of international cooperation on financial sector cybersecurity and, as further described below, the guidance offered in this Application Paper is informed by its proposals.

(c) G7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE)

32. The finance ministers and central governors of the G7 released the G7FE in 2016. Developed by a group of experts under the joint leadership of the United States Department of the Treasury and the Bank of England, the G7FE is a concise set of cybersecurity principles for public and private entities in the financial sector. While non-binding, the G7FE is intended to be useful both to firms and supervisors.

33. For firms, the elements "serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture," and can be used to re-evaluate the firm's cybersecurity programme "as the operational and threat environments evolves."[30]

34. For supervisors, the G7FE explains that: "Public authorities within and across jurisdictions can use the elements as well to guide their public policy, regulatory, and supervisory efforts."[31]

35. The G7FE identifies eight "high-level" fundamental elements of cybersecurity: (1) Cybersecurity Strategy and Framework; (2) Governance; (3) Risk and Control

[27] CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market Infrastructures* (June 2016), available at https://www.bis.org/cpmi/publ/d146.pdf.

[28] "CPMI-IOSCO release guidance on cyber resilience for financial market infrastructures," BIS Press Release (29 June 2016), available at https://www.bis.org/press/p160629.htm.

[29] Speech by Benoît Cœuré, European Central Bank Executive Board (13 January 2016), available at https://www.ecb.europa.eu/press/key/date/2016/html/sp160113_1.en.html.

[30] G7FE page 1, front matter.

[31] G7FE page 1, front matter.

Assessment; (4) Monitoring; (5) Response; (6) Recovery; (7) Information Sharing; and (8) Continuous Learning.[32] These are further discussed in Section 3 below.

36. To promote the effective practices outlined in the G7FE, in 2017 the G7 published *Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector (*G7FEA*)*.[33] This non-binding guidance is intended to serve as a tool to guide and drive internal and external discussions on risk management decisions critical to cybersecurity, encompassing both "desirable outcomes" and "assessment components."

37. The G7FEA focuses on how well the practices outlined in the G7FE are performed, and how that performance can be assessed. Part A of the G7FEA provides a set of desirable outcomes that a mature entity implementing the G7FE should be expected to achieve, "and that less mature entities can aim for." The Part A elements of the G7FEA are linked to the various elements of the G7FE and are addressed below in Section 3.

38. Part B of the G7FEA presents components of an effective process for assessing the progress of entities in achieving the desired outcomes of a cybersecurity programme. These are discussed below in Section 5.

[32] Relying on then-current literature, the 2016 IAIS Issues Paper identified a similar list of "generally recognized ... best practices for cyber resilience." Issues Paper Paragraph 39

[33] *G7 Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector* (October 2017), available at http://www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf.

3.0 Supervision of Insurer Cybersecurity Practices

39. The Task Force's cybersecurity practices survey confirmed that the maturity of jurisdictional regulatory and supervisory regimes for cybersecurity varies widely among IAIS members. Insurance supervisors may consider the practices described below when developing regulatory and supervisory efforts directed at insurers' cybersecurity. To help identify sectoral and jurisdictional gaps, insurance supervisors should consider the evolving level of cyber maturity of their insurance sector compared with the rest of the financial sector in their jurisdictions, and initiatives related to international cybersecurity standards. The principle of proportionality applies regardless of the level of cyber maturity of the jurisdiction or its insurance sector.

40. By providing the building blocks for an entity to design and implement its cybersecurity strategy and operating framework, the G7FE also provides a useful starting point for insurance supervisors to organise their management and assessment of insurance sector cybersecurity standards. Accordingly, this section uses the eight G7FE to frame a discussion on supervisory approaches to insurer cybersecurity. The discussion also addresses, where applicable, how the G7FE and suggested practices conform to existing ICP standards and guidance.[34]

41. This Application Paper draws primarily upon previous international work regarding financial sector cybersecurity, including the guidance developed by the CPMI-IOSCO WGCR. Although that guidance is specifically directed to financial market infrastructures, much of it is appropriate for consideration to varying degrees for all financial institutions.[35] Providing consistent, cross-sectoral guidance for financial institution cybersecurity, where appropriate, may contribute to harmonization of regulatory approaches.

42. It is notable that in its 2017 stocktake on cybersecurity regulations, guidance, and supervisory practices, the FSB observed that the member jurisdictions all reported "drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies" in developing their regulatory approach to cybersecurity. The FSB concluded from this observation that "jurisdictions have found existing guidance and standards to be useful and that there is some degree of international convergence in cybersecurity regulation and supervision of the financial sector."[36]

[34] Mapping of each G7FE to the ICPs in the following section is based on the ICPs as of November 2017 (with exceptions noted in the case of certain planned changes to ICPs).

[35] "This guidance is first and foremost directed to FMIs as defined in the Principles for Financial Market Infrastructures (PFMI), namely: systemically important payment systems, central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs). Relevant authorities, however, may decide to apply this guidance to types of infrastructure not formally covered by this report." CPMI-IOSCO Guidance at 1.31.

[36] Financial Stability Board, *Summary Report of Financial Sector Cybersecurity Regulations, Guidance, and Supervisory Practices* (October 2017), available at http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/.

43. The discussion in this section is intended to provide insurance supervisors with guidance which may be useful when developing or updating their regulatory regimes and supervisory practices applicable to insurance sector cybersecurity. It does not express a preference for a particular supervisory model, i.e., principles-based, rules-based, direct or indirect.

3.1 G7FE -- Element 1: Cybersecurity Strategy and Framework

44. **The first of the G7FE calls for financial institutions to "[e]stablish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines."**

45. As explained by the G7, the purpose of a firm's cybersecurity strategy and framework is "to specify how to identify, manage, and reduce cyber risks effectively in an integrated and comprehensive manner." As described above in Section 2, a range of international, national, and industry standards and guidelines are now available and should be considered when insurers establish their approach to cybersecurity and when supervisors develop or update their regulatory regimes and practices applicable to insurance sector cybersecurity as well as when they examine the cybersecurity posture of insurers subject to their jurisdiction.

A. Mapping G7FE Element 1 to Insurance Core Principles

46. ICP 8 addresses "risk management and control." Consistent with ICP 8.1 and supporting guidance regarding developing suitable risk management strategies and processes, insurance supervisors should encourage every insurer to develop or adopt a cybersecurity strategy and framework and have such strategy and framework ratified by its Board.

47. The explanation in G7FE 1 that a firm's cybersecurity strategy and framework should be tailored to its nature, size, complexity, risk profile, and culture, is consistent with the principle of proportionality underlying the ICPs.[37]

B. Recommendations for Supervisors Regarding Cybersecurity Strategies and Cybersecurity Frameworks

48. With regard to insurers' cybersecurity strategy and framework, it may be appropriate for supervisory practices to encourage or reflect the following:

a. Cybersecurity strategies should clearly articulate principles regarding how the insurer intends to address cyber risks. A firm's cybersecurity strategy should be closely aligned with, and complementary to, its cybersecurity framework, to ensure that the framework is capable of achieving its objectives.

b. The insurer's cybersecurity framework should support and promote both its operational security and the protection of policyholder data. Therefore, framework objectives should aim to maintain and promote the insurer's ability to anticipate, detect, withstand, contain,

[37] See IAIS Insurance Core Principles (ICPs), Introduction, paragraph 8.

and recover from cybersecurity incidents, so as to limit the likelihood or impact of a cybersecurity incident, which could damage the insurer's operations, its reputation, and the data privacy of its policyholders and third parties.

c. The insurer's framework should clearly define its cybersecurity objectives and horizon as well as the requirements for people, processes, and technology necessary for managing cyber risks and timely communication in order to enable an insurer to collaborate with relevant stakeholders to effectively respond to and recover from cybersecurity incidents.

d. To maximize its effectiveness, the framework must be supported by clearly defined roles and responsibilities of the insurer's Board and its management, and it is incumbent upon the Board and management to create a culture which recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity.

e. The insurer should try to align its cybersecurity framework with its enterprise operational risk management framework. Such consistency is important, and recognizes that an insurer's cybersecurity framework is likely to overlap with the policies, procedures, and controls that it has established to manage other areas of risks. For example, cyber risk should also be a consideration in an insurer's physical security framework (e.g., to limit access to critical ICT infrastructure) and its human resource policies (e.g., to manage "insider" threats).

f. Cybersecurity framework documentation should clearly articulate how the insurer plans to effectively identify the cyber risks that it faces, determine its cybersecurity objectives and risk tolerance, and mitigate and manage its cyber risks.

g. An insurer's cybersecurity framework should consider how the insurer would regularly review and actively mitigate the cyber risks that it bears from and poses to its stakeholders such as policyholders, other insurers, third party service providers (including the services and products provided by those third party service providers), and other third parties (the insurer's cybersecurity ecosystem).

h. Maintaining an effective approach to cyber risk management is particularly challenging. Because cyber risks may rapidly evolve, an insurer's cybersecurity strategy and framework should be reviewed and updated with sufficient frequency to ensure that they remain effective.

C. Examples of Current Practices

49. **France**. In France, the l'Autorité de contrôle prudentiel et de résolution (ACPR) is highly involved in the supervision of cyber resilience. The insurer's cybersecurity framework should include the IT governance goals as well as the risk management framework to be complete. On 30 March 2018, the ACPR published a Discussion paper on IT risk[38] to create a common ground for controlling IT risk management in the banking and insurance sectors. ACPR uses COBIT 5, NIST, and ISO 2700x frameworks. Based on them, ACPR developed its own methodology to perform controls.

50. **Germany**. Pursuant to Section 23 of the German Insurance Supervision Act (Versicherungsaufsichtsgesetz - VAG), insurers and pension funds shall, as a basic

[38] ACPR, *Discussion Paper on IT Risk* (March 2018), available at https://acpr.banque-france.fr/node/61411.

requirement, have in place a proper business organisation, which includes proper management of its IT infrastructure. As per Section 32 VAG, these governance requirements also apply to outsourced functions and activities. According to Article 258 (1) lit. (j) of the Delegated Regulation (EU) 2015/35 (Delegierte Verordnung (EU) 2015/35 - DVO) insurance undertakings shall safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question. In addition, there are further legal requirements for insurance undertakings concerning data quality regarding technical provisions, internal models and undertaking specific parameters which also include requirements regarding data processing (see, e.g., Article 231 of the DVO).

51. Furthermore, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) issued its draft circular on IT requirements in order to elaborate the aforementioned basic requirement set out in Section 23 of the German Insurance Supervision Act by formulating detailed requirements for specific areas of cybersecurity.[39] The circular will obligate insurers to have an IT strategy in place that must contain at least:

- strategic development of the organisational and operational IT structure of the insurer and the outsourcing of IT services;
- allocation of the established standards on which the insurer bases its strategy to the areas of IT;
- responsibilities and the incorporation of information security into the organisation;
- strategic development of IT architecture;
- statements on emergency management taking into account IT matters; and
- statements on the IT systems (hardware and software components) operated and/or developed in the business units.

52. **Netherlands**. De Nederlandsche Bank (DNB) has published an Assessment Framework for Information Security.[40] This framework can be used by insurers to assess the maturity of their information security, including cyber resilience. DNB uses this framework as well to perform yearly assessments of the sector. The framework is linked to the Dutch Financial Supervision Act. More information is provided with the case study in Section 4.

53. **Québec, Canada**. One of the objectives of the Autorité des marchés financiers (AMF) Integrated Risk Management Guideline[41] is the implementation by firms of an adequate management framework, supported by strategies, policies, and procedures to identify, assess, quantify, control, mitigate, and carefully monitor material risks within each insurer. The cyber risk related to a firm's information and communication technologies is one of the many operational risks considered by the AMF within this framework.

[39] Issued on 13 March 2018 for public consultation, available at https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2018/dl_kon_0418_vait_va.html.

[40] DNB, *Assessment Framework for DNB Information Security Examination* 2017 (April 2017), available at http://www.toezicht.dnb.nl/en/3/51-203304.jsp.

[41] AMF, *Integrated Risk Management Guideline* (May 2015), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/

54. Accordingly, as part of its oversight work seeking to promote sound and prudent management practices within insurers, the AMF assesses the degree to which the principles set forth in its guidelines are followed, taking into account the specific characteristics of each institution. The effectiveness and relevance of implemented strategies, policies, and procedures as well as the quality of the supervision and control carried out by the board of directors and senior management are also assessed.

55. The AMF has developed a detailed self-assessment tool based on recognised cyber-related international standards and processes (such as those published by NIST and COBIT). This tool is used by the insurers to assess the cybersecurity posture based on their risk profiles and report it to the AMF. Among the questions of particular relevance (to the first G7FE element), the tool clearly establishes the expectation of AMF that institutions should designate a specific person to be in charge of developing and implementing a cybersecurity framework and related plans and strategies.

56. In all cases, the AMF expects all governance frameworks to be developed and implemented based on the insurer's nature, size, complexity, and risk profile and expects the insurer to ensure the effectiveness of the frameworks.

57. **Switzerland**. The Swiss legislator has enacted a principle based, risk-oriented approach to supervision of insurers.

58. In this regard, Article 22 of the Insurance Supervision Act (ISA)[42] requires insurers to be able to detect, control, and limit all major risks. According to the same article, the Federal Council enacts the relevant regulations, while FINMA regulates the monitoring of the risks by the insurers. Article 96 of the Ordinance on the Supervision of Private Insurance Companies,[43] states requirements for the insurers' risk management.

59. Further, according to the legal provisions and the overarching governance principles for insurers stipulated in FINMA Circular 17/2 "Corporate governance – insurers",[44] FINMA expects the insurers to have in place an effective governance framework as well as an appropriate Risk and Control environment regarding cybersecurity. This broad regulation allows FINMA to implement other components of the G7FE as well. FINMA can therefore urge insurers to maintain an appropriate cybersecurity strategy and framework, which take into account both the leading standards and guidelines as well as the principle of proportionality.

60. To monitor the general degree of its supervisees' maturity in a specific field, FINMA generally uses surveys based on self-assessment. However, especially in case of the presence of evidence of irregularities, in-depth on-site reviews can take place. Depending on the findings during such on-site review, the insurer may be called upon to elaborate an action plan with deadlines for the elimination of the violations of the

[42] *Insurance Supervision Act*, available at https://www.admin.ch/opc/de/classified-compilation/20022427/index.html.

[43] *Ordinance on the Supervision of Private Insurance Companies*, available at https://www.admin.ch/opc/de/classified-compilation/20051132/index.html.

[44] FINMA, Circular 17/2 *Corporate Governance – Insurers*, available at https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-02.pdf?la=en.

regulations and submit it to FINMA for approval. FINMA generally closely monitors the implementation of such action plans. In addition, FINMA can appoint third parties, known as mandataries, to assist it in performing its duties, thereby making targeted use of this efficient, resource-saving tool in both supervision and enforcement proceedings.

61. **United Kingdom**, The UK Financial Conduct Authority (FCA) has set cyber resilience as a key supervisory priority for the past 3 years, and continues to do so. The FCA Handbook details a number of principles for business which are relevant to cyber risk supervision. The Principles are a general statement of the fundamental obligations of firms under the UK financial regulatory system. Breaching a Principle makes a firm liable to disciplinary sanctions. Principles specifically relevant to cyber risk supervision are:

- PRINCIPLE 2- Skill, care and diligence; A firm must conduct its business with due skill, care and diligence.
- PRINCIPLE 3 - Management and control; A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
- PRINCIPLE 11 – Relations with Regulators; A firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice.

62. Underneath these principles, the FCA considers that firms should employ suitably skilled senior staff capable of managing cyber risk with due skill, care and diligence (PRINCIPLE 2), firms should employ risk management systems capable of assessing cyber risk in an appropriate manner, recognising the fluidity and complexity of the risk (PRINCIPLE 3), and that the FCA is informed of any material deficiencies in cyber risk management arrangements, or any other material cyber events (PRINCIPLE 11).

63. **United States**. In the United States, cybersecurity and data security are national policy issues, requiring coordination among federal and state public sector entities and partnership between the public and private sectors. Accordingly, federal officials are working with state regulators and insurers to improve industry cybersecurity, while promoting harmonization of data security and data breach notification laws and regulation.

64. The National Association of Insurance Commissioners (NAIC) adopted the *Insurance Data Security Model Law*[45] in 2017, creating rules for insurers, agents, and other licensed entities covering data security, investigation, and notification of breach. This includes maintaining an information security program based on ongoing risk assessment, overseeing third party service providers, investigating data breaches and notifying regulators of a "cybersecurity event."

65. NAIC members, the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories, are the primary regulators of insurance in the United States. As with all NAIC model laws, the *Insurance Data Security Model Law* needs to be enacted into law at the state level in order to come into force. In October 2017 the

[45] NAIC, *Insurance Data Security Model Law*, available at http://www.naic.org/store/free/MDL-668.pdf.

U.S. Department of the Treasury noted that "data security, data breach notifications, and more broadly, cybersecurity are … issues of national concern," and recommended prompt adoption of the *Insurance Data Security Model Law* by the states and also that the states "work to expeditiously pass uniform legislation regarding data breach notification for insurers."[46]

66. Section 4A of the NAIC *Insurance Data Security Model Law* requires insurers[47] to implement an "Information Security Program" that is "commensurate with the size and complexity of the insurer, the nature and scope of the insurer's activities, including its use of third-party service providers, and the sensitivity of the non-public information used by the insurer or in the insurer's possession, custody, or control."

67. In addition, the NAIC *Financial Condition Examiners Handbook* (Examiners Handbook) provides guidance that regulators use as part of the financial examination process, and includes a review of whether and how the insurer is addressing its cyber risk. The *Examiners Handbook* was recently updated to incorporate the NIST Functions of Identify, Protect, Detect, Respond, and Recover.[48] As part of the scoping process, examiners obtain documentation on each insurer's set of policies, which typically includes the insurer' cybersecurity strategy and framework, to give regulators an opportunity to identify strategy and framework gaps or issues at the beginning of the examination.

68. Effective March 1, 2017 the New York State Department of Financial Services (NYDFS) promulgated 23 NYCRR Part 500, [49] a regulation establishing cybersecurity requirements for financial services companies.

69. Under Section 500.02 of the NYDFS *Cybersecurity Requirements for Financial Services Companies*, insurers[50] are required to "maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems."

D. Assessing Outcomes of G7FE Element One

70. There are five "Outcomes Associated with Effective Cybersecurity" under the G7FEA. Not every one of the G7FEA Outcomes are applicable to every G7FE Element. But, taken together, "the five desirable outcomes ... set out broad characteristics that a financial sector entity with a mature understanding, delivery, and oversight of

[46] United States Treasury, *A Financial System that Creates Economic Opportunity: Asset Management and Insurance* (October 2017), available at https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf.

[47] The *Insurance Data Security Model Law* uses the term "Licensee," which includes insurers. For readability, in this Paper the term "insurer" is substituted for "Licensee."

[48] NIST Cybersecurity Framework, discussed above.

[49] NYDFS, *Cybersecurity Requirements for Financial Services Companies*, available at https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[50] The NYDFS *Cybersecurity Requirements for Financial Services Companies* uses the term, "Covered Entity," which includes insurers meeting the definition of a Covered Entity and which are not exempt under the provisions of Part 500.19. For readability, in this Paper the term "insurer" is substituted for "Covered Entity" (except in the case of quotations).

cybersecurity can demonstrate to an assessor." Both insurers and supervisors should make use of this assessment guidance, as appropriate, "in regulatory examinations, self-assessments, and independent review by third parties."[51]

71. For G7FE number One, the desirable outcomes proposed by the G7 are:

72. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. The G7FE provide the foundational elements for cybersecurity, both for entities who are in the early stages of building cyber resilience and for those who are more mature.

73. The G7FE are wide ranging, reflecting the nature of the challenge. Effective cybersecurity requires entities to maintain a cybersecurity strategy and framework (Element 1) and adapt or reinforce their governance processes (Element 2). It requires risk and control frameworks, including the relevant set of mitigation controls and protection mechanisms (Element 3) and effective monitoring (Element 4). Clearly defined and regularly exercised response (Element 5) and recovery (Element 6) procedures are in place in case of disruptive cyber events. Finally, information sharing (Element 7) and continuous learning (Element 8) reinforce each G7FE and contribute towards strengthening overall cybersecurity.

74. **G7FEA Outcome 2 – Cybersecurity Influences Organization Decision-Making**. Building on Element 1 (Cybersecurity Strategy and Framework) and 2 (Governance), incorporating cybersecurity into entities' normal decision-making processes, specifically by including cyber risk management into these processes early, informs and facilitates strategic outcomes across the organization. Cybersecurity should not be viewed as separate from the concept, design, and operation of entities' core business processes but as a key strategic consideration, both when developing new products and services, and when assessing the effectiveness of business operations that utilize existing technology or infrastructures.

75. Active senior management or board-level engagement implies oversight of the design, implementation and effectiveness of cybersecurity programmes. Informed by information on threats and vulnerabilities and their entity's risk appetite, boards and senior management can drive risk-management decisions, oversight, and accountability in both the short and long term. As such, boards and senior management can use decision making to drive cybersecurity programmes beyond the traditional views of compliance.

3.2 G7FE -- Element 2: Governance

76. **The second of the G7FE calls for financial institutions to "[d]efine and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability; and [to] provide adequate resources, appropriate authority, and access to the governing authority (e.g., board of directors or senior officials at public authorities)."**

[51] G7FEA page 2.

77. Generally, "cyber governance" refers to the arrangements an institution has put in place to establish, implement, and review its approach to managing cyber risks. Strong cyber governance helps an insurer maintain a systematic and proactive approach to managing the prevailing and emerging cyber risks that it faces. It also helps an insurer appropriately consider and manage cyber risks at all levels within the organization, as well as consistently bring to bear appropriate resources and expertise to deal with these risks.

A. Mapping G7FE Element 2 to Insurance Core Principles

78. The emphasis of G7FE 2 on "effective governance structures," "accountability," and clear articulation of "responsibilities and lines of reporting and escalation," as well as addressing priorities and communication among "operating units, information technology, risk, and control-related activities" is consistent with ICP 7 (Corporate Governance).

79. ICP 7 calls for "a corporate governance framework which provides for sound and prudent management and oversight of the insurer's business and adequately recognises and protects the interests of policyholders."

80. Further, ICP 8 (Risk Management) requires that "as part of its overall corporate governance framework," insurers have in place "effective systems of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters and internal audit." ICP 8 materials note that a typical governance approach incorporates the "three lines of defense" model.[52]

B. Recommendations for Supervisors Regarding Governance

81. With regard to cybersecurity governance, it may be appropriate for supervisory practices to encourage or reflect the following:

a. The insurer's Board should be ultimately responsible for setting strategy and ensuring that cyber risk is effectively managed. The Board should endorse the insurer's cybersecurity framework and set the insurer's tolerance for cyber risk.

b. Further, the Board should be regularly apprised of the insurer's cyber risk profile to ensure that it remains consistent with the insurer's risk tolerance as well as the insurer's overall business objectives. As part of this responsibility, the Board should consider whether changes to the insurer's products, services, policies or practices, and the threat landscape materially affect its cyber risk profile.

c. Senior management should closely oversee the insurer's implementation of its cybersecurity framework, and the policies procedures, and controls that support the framework.

d. An insurer's Board and senior management should cultivate awareness of and commitment to cybersecurity. The Board and senior management should include members with skills appropriate to their oversight and management roles with respect to the risks posed by cyber threats. In addition, the Board and senior management should

[52] ICP 8.2.3 and footnote 11.

promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity and lead by example.

e. Insurers should have in place information security policies, procedures and processes including definitions of roles and responsibilities across the organization. These policies, procedures and processes should include oversight of third party service providers, as well as cyber risk management processes and determination of priorities, constraints, assumptions, and risk tolerance level.

f. In particular, each insurer should designate a senior executive, such as a Chief Information Security Officer (CISO), to be responsible and accountable overall for the cybersecurity framework within the organization. This role should have sufficient authority, independence, resources, and access to the Board. The senior executive performing this role should possess the requisite expertise and knowledge to competently plan and execute the cybersecurity initiatives at a management level.

g. Insurers should implement assessment programmes to help the Board and senior management evaluate and measure the adequacy and effectiveness of the insurer's cybersecurity framework including, where appropriate and in line with the proportionality principle, through independent compliance programme and audit carried out by qualified individuals to assess the cybersecurity framework and measure implementation.

C. Examples of Current Practices

82. **France**. ACPR performs IT controls to assess the level of maturity of cyber security systems (organisation and governance) and to verify that the insurer comply with the paragraph 1, article 258 of Solvency II Delegated Acts. These controls aims at verifying that a governance system has been deployed to cover the cyber risks and that information concerning that risk is shared at all the essential management levels.

83. **Germany**. According to BaFin's draft circular on IT requirements the management board is responsible for ensuring that the regulations for the organisational and operational IT structure are determined on the basis of the IT strategy and that they are amended to reflect any changes in the insurers' activities and processes as soon as possible.

84. In particular, the insurer has to staff the information risk management, information security management, IT operations and application development appropriately, in terms of both quantity and quality.

85. **Québec, Canada**. The AMF establishes guidelines setting out its expectations with respect to a financial institution's legal requirement to follow sound and prudent management practices. The AMF considers governance, integrated risk management and compliance (GRC) as the foundation stones for sound and prudent management of insurers and, consequently, as the basis for the prudential framework provided by the AMF.

86. As part of its Governance Guideline, the AMF expects financial institutions to have effective and efficient governance by implementing a formal operating framework, monitoring and accountability through policies, procedures and information systems that help organize and oversee the management of the financial institution. The AMF expects also the roles and responsibilities of the board of directors and senior management to be

clearly defined and separate to ensure that their members act competently and independently. In this regard, the AMF encourages financial institutions to adopt the three lines of defense model which provides a reliable structure for delineating roles and responsibilities and because it is suitable for all types of institutions and can be adapted according to their nature, size, complexity and risk profile.

87. With regards to cybersecurity, as part of its supervision activities the AMF recommends the implementation of a sound governance of IT for the organization to ensure that the use of IT contributes positively its performance. This is done using ISO and COBIT recognised frameworks, principles and processes (e.g., ISO 38500, EDM01 Ensure Governance Framework Setting and Maintenance, EDM03 Ensure Risk Optimisation, EDM05 Ensure Stakeholder Transparency processes). Among its activities, the AMF also reviews the on-going development of strategies and frameworks to manage information and communication technology-related risks (including cyber risks) and focuses on the sets of roles and responsibilities (Responsible-Accountable-Consulted-Informed charts) to reinforce accountability.[53]

88. **United Kingdom.** The FCA aligns its supervisory strategy with the UK National Cyber Security Centre (NCSC) strategy, the "National Cyber Security Strategy 2016 to 2021"[54] and associated guidance publications. Specifically, the FCA considers cyber a board level responsibility and considers that the boards of financial institutions should have access to independent expertise allowing them to discharge their responsibilities effectively. The FCA refers to the NCSC's publication "10 Steps: A Board Level Responsibility"[55], when supervising firms, as well as existing international frameworks including those referenced in this document.

89. **United States**. Section 4E of the NAIC *Insurance Data Security Model Law* requires that, if the insurer has a Board of directors, the Board will provide oversight of the Information Security Program. The Board must require executive management to implement and maintain the Information Security Program. The Board also must require executive management to report to the Board, in writing, the status of the Information Security Program, the insurer's compliance with the Act, and any material matters related to the Information Security Program, including "issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program."

90. Under the NAIC *Examiners Handbook*, a company's governance structure is typically most stringently assessed during the general part of the examination (i.e., as part of a holistic view of the company's operations). However, the *Examiner's Handbook* includes

[53] AMF, *Governance Guideline* (September 2016) available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

[54] FCA, *National Cyber Security Strategy 2016 to 2021* (Updated September 2017), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[55] NCSC, *10 Steps: A Board Level Responsibility* (Updated August 2016), available at https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility.

specific testing procedures for review and assessment of the adequacy of the IT governance model. Testing may include review of organization charts, reporting lines, biographical information for key IT executives, and a review of board committee activity. The *Examiner's Handbook's* guidance emphasizes the importance of the review of Board / Senior management oversight of the company's cybersecurity program.

91. Section 500.03 of the NYDFS *Cybersecurity Requirements for Financial Services Companies* requires that a written cybersecurity policy be approved by a Senior Officer or the Board of Directors of the insurer. The policy must set forth the insurers "policies and procedures for the protection of its Information Systems and Non-public Information stored on those Information Systems." Section 500.04 requires the insurer to designate a Chief Information Security Officer (CISO). The CISO shall report at least annually to the Board of Directors. Section 500.17 requires the insurer's Board of Directors or a Senior Officer to certify compliance with the regulations.

D. Assessing Outcomes of G7FE Element Two

92. For G7FE number Two, the desirable outcomes proposed by the G7 are:

93. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. Discussed above at Paragraph 72-73.

94. **G7FEA Outcome 2** – Cybersecurity Influences Organization Decision-Making. Discussed above at Paragraph 74-75.

3.3 G7FE -- Element 3: Risk and Control Assessment

95. **The third Fundamental Element calls on financial institutions to "[I]dentify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritize their relative importance, and assess their respective cyber risks," and to "[i]dentify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within the tolerance set by the governing authority."**

96. Thus, "[i]deally as part of an enterprise risk management program," entities should evaluate the inherent cyber risk (or the risk absent any compensating controls) presented by the people, processes, technology, and underlying data that support each identified function, activity, product, and service" and then "identify and assess the existence and effectiveness of controls to protect against the identified risk to arrive at the residual cyber risk."

A. Mapping G7FE Element 3 to Insurance Core Principles

97. G7FE Element 3 is consistent with ICP 8 (Risk Management). As stated in ICP 8.1, under this standard: "the supervisor requires the insurer to establish, and operate within, an effective risk management system." Further, this risk management system should "allow for the identification, assessment, monitoring, mitigation and reporting of all risks of the insurer in a timely manner. It takes into account the probability, potential impact and time horizon of risks."

98. As summarised in the Issues Paper, ICP 8 Guidance lists a minimum set of categories that the risk management system should cover. These include "operational risk

management," "conduct of business," and "other risk-mitigation techniques." In addition, ICP 8 Guidance states that the risk management system should take into account all reasonably foreseeable and relevant material risks, including current and emerging risks.

99. ICP 8 Guidance also describes typical components of an effective internal control system. The description of the "policies and processes" component explains that effective internal control system should include "appropriate controls for all business processes and policies," including "critical IT functionalities," and "access to databases" and to "IT systems by employees."

100. In addition, ICP 8 Guidance addresses the need for insurers to devote sufficient resources to the control functions, including appropriate IT/management information processes. It also states that the internal audit function should provide independent assurance to the Board and Senior Management in respect of the continued ability of the insurer's IT architecture to support the firm's operations.

101. Outsourcing arrangements are also addressed in ICP 8 Guidance, which notes that when entering into or revising an outsourcing arrangement, the Board and Senior Management should consider how the insurer's risk profile and business continuity will be affected by the contemplated arrangements. Specifically, ICP 8.8. states: "The supervisor requires the insurer to retain at least the same degree of oversight of, and accountability for, any outsourced material activity or function (such as a control function) as applies to non-outsourced activities or functions." This can apply to the service provider's governance, risk management, and internal controls with respect to cybersecurity.

102. Finally, ICP 19 (Conduct of Business) is also relevant to G7FE 3. Under this standard, ICP 19.12 calls on the supervisor to "require[s] insurers and intermediaries to have policies and procedures for the protection and use of information on customers." As an example of such policies and procedures, ICP 19.12 mentions "assessing the potential impact of new and emerging risks that could threaten the privacy of personal information, such as the risk of cyber attacks, and taking appropriate steps to mitigate these through measures such as internal controls, technology and training."[56]

B. Recommendations for Supervisors Regarding Risk and Control Assessment

103. With regard to insurers' cybersecurity risk and control assessment, it may be appropriate for supervisory practices to encourage or reflect the following:

Identification and classification of functions including information assets and interconnectedness

a. Insurers should identify and classify functions including information assets and data sensitivity, as well as their interconnectedness; proactive technology and processes; external dependency management; and situational awareness.

[56] ICP 19.12.5.

b. The insurer should adequately account for cyber risks in its overall risk management system, identifying its business functions and supporting processes and conducting a risk assessment to ensure that it thoroughly understands the importance of each function and supporting processes, and their interdependencies, in performing its functions. Identified business functions and processes should then be classified by insurers in terms of criticality, which in turn should guide the insurer's prioritization of its protection, detection, response, and recovery efforts.

c. To the extent practicable, the insurer should identify and maintain a current inventory or mapping of its information assets and system configurations, including interconnections with other internal and external systems, in order to know at all times the assets that support its business functions and processes. The insurer should carry out a risk assessment of those assets and classified them in terms of criticality.

d. As part of this mapping process, the insurer also should identify dependencies in its information assets and system configurations, for example, from third party service providers.

e. The inventory should encompass hardware, software platforms and applications, devices, systems, data, personnel, external information systems, critical processes, and documentation on expected data flows.

f. Insurers should identify and maintain a current record of both individual and system access rights to know who has access to information assets and their supporting systems, and to use this information both to ensure that access rights are no broader than necessary, and to facilitate identification and investigation of anomalous activities.

g. Insurers should integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials, as well as its inventory of information assets to ensure that they remain current, accurate and complete.

h. Similarly, insurers should conduct business impact analysis for cyber risks (i.e., a determination of risks and prioritization of risk responses through identification of threats, vulnerabilities, likelihoods, and impacts).

Inclusion of Cyber Risk in Risk Profile

i. Insurers' risk profiles should identify key operational areas exposed to cyber risk, arising from both internal and external sources.

j. Using the same precepts as in the development of an enterprise-wide risk profile, the insurer would aim to describe the overall cyber risk to which the enterprise is exposed. The risk profile may benefit from inclusion of assessment processes that encompass assessments of likelihood and impact of harm. At a more detailed level, the risk profile may also include and be informed by the result of insurers' vulnerability scanning and management process. A typical vulnerability management system includes enumeration

of platforms, software flaws, and improper configurations as well as an assessment of the vulnerability impact.[57]

k. Insights from both processes may be organised, for example, within the following categories: (1) technologies and connection types; (2) delivery channels; (3) organizational characteristics; and (4) external threats. [58]

- *Technologies and Connection Types*. Certain technologies and connection types may pose a higher cyber risk depending on the complexity and maturity, connections, and nature of the specific technology products or services of the insurer. For example, it may be appropriate for an insurer to assess the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the presence and number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices by insurer personnel.
- *Delivery Channels*. Insurers should be aware that some delivery channels for products and services may pose a heightened cyber risk depending on the nature of the specific product or service offered. Cyber risk increases as the variety and number of delivery channels increases. For example, online and mobile delivery channels may present increased levels of risk to an insurer.
- *Organizational Characteristics.* Those Characteristics to consider include past and planned mergers, demergers, acquisitions, and sales, the number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in information technology (IT) environment, locations of business presence, locations of operations and data centres (including legacy systems), and reliance on third party service providers, including cloud service providers.
- *External Threats.* External threats, particularly the volume and type of attacks (attempted or successful) reflect and affect an insurer's cyber risk exposure. An insurer should consider the volume and sophistication of the attacks targeting it and other similarly situated organizations.

Implementation of Proactive Technology and Processes

l. Insurers should protect data both when at-rest, in-transit and in-storage commensurate with the criticality of the information held and associated classification, extending to backup systems and offline data stores as well.

Management of External Dependencies

m. Insurers should actively manage cyber risks presented by third parties. For example, many insurers' systems and processes are directly or indirectly interconnected with

[57] "NIST PR.IP-12: A vulnerability management plan is developed and implemented". (informative references include NIST SP 800-53 Rev.4 RA-3, 5, & SI-2) in "Table 2: Framework Core" of *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1 released on 16 April 2018), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[58] Federal Financial Institutions Examination Council (FFIEC), *Cybersecurity Assessment Tool* (Update May 2017) available at https://www.ffiec.gov/cyberassessmenttool.htm.

numerous third parties, including cloud service providers and providers of outsourced functions. The cybersecurity of those entities may significantly affect the cyber risk that an insurer faces.[59]

n. Insurers should verify that third-party service providers have implemented appropriate administrative, technical, and physical measures to protect and secure the data of an insurer and its customers to the same degree expected of the insurer.

o. Insurers should be aware that the significance of the risks the third parties may pose to the insurer is not necessarily proportionate to the criticality of their business relationship with the insurer. Therefore, an insurer should identify the cyber risks that it bears from and poses to third parties and, to the extent practicable, coordinate with its relevant stakeholders, as these third parties design and implement their own resilience efforts with the objective of improving the overall resilience of the insurer and its stakeholders.

Enhancing Situational Awareness

p. An insurer should have appropriate situational awareness of the cyber risks that it faces. An insurer should seek to proactively identify cyber threats that could materially affect its ability to perform or to provide services as expected, or that could have a significant impact on its ability to meet its own obligations, including protection of confidential data. The insurer should regularly review and update this analysis.

q. Cyber threats to be considered should include those which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. Insurers should consider threats to the confidentiality, integrity, and availability of the insurer's business processes, policyholder data, and to its reputation. Threats arising from both internal and external sources, such as employees or third-party service providers, respectively, should be considered.

C. Examples of Current Practices

104. **European Union**. In the European Union, under Solvency II, an ERM Framework[60] should include operational and more precisely IT risk. This supervision targets external and internal networks notably via penetration test and interview with different teams. Mobile deported applications are also tested in some cases to control the level of data protection. Cyber risk should be addressed in the written policy on risk management. The first main goal is to ensure a sufficient level of understanding of this risk, a correct identification and assessment in the frame of Solvency II operational risk.[61]

105. **France**. Taking into account the development of cyber risk and its impact on the security, the ACPR has multiplied surveys and analysis to improve its knowledge of the market practices and to develop appropriate risk management in the undertakings. In this view, the ACPR recently has developed specific visits and interview with the insurance sector to understand exactly the level of development of the insurer's

[59] See, e.g., Dave Shackleford, Combatting Cyber Risks in the Supply Chain (SANS Institute Sept. 2015), available at https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252.

[60] Article 44 of Solvency II Directive.

[61] Article 13 (33) of Solvency II Directive.

cybersecurity maturity. The ACPR also met innovative firms offering risk management solutions to the market. ACPR performs penetration tests from front office to back office systems of the insurer to evaluate the global sensitivity and resilience of the systems to cyber threats (black box and white box tests). The ACPR ensures also that the cyber risk is correctly apprehended in the IT operational risk management.

106. **Germany**. BaFin's draft circular on IT requirements obligates insurers to have a current overview of the components of the specified information network, its interdependencies and interfaces. The insurer should focus here in particular on internal requirements, business activities and the risk situation.

107. Regular reviews and adjustments to changed conditions are required using a risk-based approach. Changes to the organisational and operational structure and the IT systems of an insurer (business processes, specialist duties, organisational structure) must be taken into account in this process, as must changes to external framework conditions (e.g., statutory provisions, regulatory requirements), threat scenarios and security technology.

108. **Québec, Canada**. One of the objectives of the AMF's Integrated Risk Management Guideline is the implementation of an adequate management framework to identify, assess, quantify, control, mitigate and carefully monitor material risks within each insurer. The AMF believes that financial institutions should gravitate toward integrated risk management rather than take an approach where risks are considered separately. Furthermore, the AMF promotes a holistic approach, which takes into consideration the interrelationship and interdependence between risks, to the management of all information and communication technology-related risks within financial institutions. As a result, financial institutions will need standardized processes and reliable information systems that allow them to identify connections between risks.

109. In its Operational Risk Management Guideline, the AMF does not promote particular tools for identifying or assessing operational risk. However, the chosen tool or set of tools should be used consistently throughout all business sectors in order to achieve a comprehensive assessment of operational risk exposure. In the same guideline, the AMF expects internal control mechanisms - which should be adaptable to changes in the financial institution's business and in technology - to efficiently mitigate the financial institution's operational risk exposure inherent to people, processes, systems or external events, according to their importance. In addition, the AMF states that financial institutions using insurance to transfer operational risk should ensure that it always complements their own control mechanisms for this type of risk.

110. Also, in its Business Continuity Management Guideline, the AMF expects a financial institution to identify its critical business continuity functions, their concentration at a single site, their interdependencies as well as their dependence on a single system, staff or service providers. The AMF also expects financial institutions to assess the impact of major incidents on its resources, operations and environment and determine the measures to be taken in light of this assessment.

111. Cyber risk is considered one of the many operational risks involving technology that are examined by the AMF. In its supervisory efforts, the AMF recommends insurers to conduct self-assessments of their risks and controls to evaluate their cybersecurity posture, determine if their residual risk-level is within the enterprise risk-appetite

predefined levels and plan specific actions to minimize their risks. In this context, the AMF makes available a self-assessment tool to insurers. It covers among other things a number of cyber incident prevention and detection processes to ensure that all IT assets used by an institution (including those used externally) are inventoried. It also ensures that the institution maps all of its communications networks and identifies critical functions, data, interdependencies and needs required to maintain essential services. The self-assessment tool also recommends the prioritization of all resources based on their criticality and business value for the institution and the implementation of effective security measures based on the established classification of information and sensitivity levels.

112. **Canada**. Office of the Superintendent of Financial Institutions (OSFI) recognizes that many institutions assess their current level of cyber security preparedness. OSFI believes that Federally Regulated Financial Institutions (FRFIs) can benefit from guidance related to such self-assessment activities, thus has provided this template to assist in their self-assessment activities.[62]

113. FRFIs are encouraged to use this template or similar assessment tools to assess their current level of preparedness, and to develop and maintain effective cyber security practices.

114. OSFI may request institutions to complete the template or otherwise emphasize cyber security practices in connection with supervisory assessments.

115. Further, FRFIs are encouraged to reflect the current state of cyber security practices in their assessments rather than their target state, consider cyber security practices on an enterprise-wide basis, and provide sufficient justification for their ratings.

116. In addition, the self-assessment tool recommends that cyber risks be considered an integral part of the institution's integrated risk management process.[63]

117. **United Kingdom**. The FCA includes guidance for insurers on how to meet the requirements in the Handbook to take reasonable care to establish and maintain such systems and controls as are appropriate to its business. This guidance, contained within Systems and Controls 13.7.7 (SYSC 13.7.7), informs firms that they should have regard to:

- confidentiality: information should be accessible only to persons or systems with appropriate authority, which may require firewalls within a system, as well as entry restrictions;
- integrity: safeguarding the accuracy and completeness of information and its processing;

[62] OSFI Cyber Security Self-Assessment Guidance (October 28, 2013), available at. http://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/cbrsk.aspx.

[63] AMF, *Integrated Risk Management Guideline* (May 2015), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/; AMF, *Business Continuity Management Guideline* (April 2010), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/; AMF, *Operational Risk Management Guideline* (December 2016), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

- availability and authentication: ensuring that appropriately authorised persons or systems have access to the information when required and that their identity is verified;
- non-repudiation and accountability: ensuring that the person or system that processed the information cannot deny their actions.

118. Reviews against these rules and associated guidance is performed on a risk based approach, which considers the profile and scale of the firm and the associated potential harms that may occur on UK consumers and markets in the event of a material cyber attack.

119. **United States**. Section 4C of the NAIC *Insurance Data Security Model Law* requires the insurer to perform an ongoing risk assessment and Section 4D lists requirements for managing the risk, based on the insurer's ongoing risk assessment. Examples of security measures an insurer should consider are listed in Section 4D(2) and include: the use of controls to authenticate and permit access only to authorized individuals to limit access to non-public information; use of encryption or other appropriate means to protect the transmission of information over external networks; and the storage of information on portable storage devices.

120. Additionally, Section 4F requires the insurer to exercise due diligence in selecting its Third-Party Service Providers and to require its Third-Party Service Providers to implement appropriate administrative, technical, and physical cybersecurity measures.

121. The *Examiners Handbook* includes specific procedures to consider how the company integrates cybersecurity related enterprise risks into the overall enterprise risk management (ERM) program. Moreover, as the examiner identifies specific risk exposures (for instance third party access to the network), the *Examiner's Handbook* includes various risk statements to facilitate the examiner's performance of testing as appropriate. As part of the broader financial examination, examiners also consider a company's integration of cybersecurity risk management into the overall ERM program. The Handbook also includes language to highlight the need for examiners to closely scrutinize the insurer's assessment of cybersecurity exposures.

122. Section 500.02 of the NYDFS *Cybersecurity Requirements for Financial Services Companies* requires the insurer's Cybersecurity Program be based on its Risk Assessment. Likewise, Section 500.03 requires the insurer's Cybersecurity Policy to be based on its Risk Assessment. The regulations require the insurer to adopt a number of security measures including: restricting access privileges (Section 500.07); use of multi-factor authentication (Section 500.12); and encryption of Non-public Information (Section 500.15). Additionally, Section 500.11 requires the insurer to implement written policies and procedures "to ensure the security of Information Systems and Non-public Information that are accessible to, or held by, Third Party Service Providers."

D. Assessing Outcomes of G7FE Element Three

123. For G7FE number Three, the desirable outcomes proposed by the G7 are:

124. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. Discussed above at Paragraph 72-73.

125. **G7FEA Outcome 3 – There is an Understanding that Disruptions Will Occur.** Building on *Element 3* (risk and control assessment), the layering of detective and protective controls is critical, and reduces the likelihood of loss of availability, integrity or confidentiality. However, mature entities recognize that it is impossible to guarantee a zero-failure environment. By adopting a mind-set that operational disruptions will occur, key decision makers understand that strategy-aligned investment choices seek a balance across all aspects of the G7FE.

126. Entities that fail to recognize this concept may exhibit an imbalance by having an over reliance on perimeter controls, at the detriment of clearly defined and regularly exercised responses (*Element 5*) and a viable, tested contingency plan for the resumption of operations (*Element 6*).

3.4 G7FE -- Element 4: Monitoring

127. **The fourth of the G-7 Fundamental Elements calls for financial institutions to "[e]stablish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises."**

128. As explained in G7FE 4, "[e]ffective monitoring helps entities adhere to established risk tolerances and timely enhance or remediate weaknesses in existing controls," and "[t]esting and auditing protocols provide essential assurance mechanisms for entities and public authorities alike."

129. The explanation also proposes that "the testing and auditing functions should be appropriately independent from the personnel responsible for implementing and managing the cybersecurity program."

130. Authorities' understanding of sector-wide cyber threats as well as how well individual firms are prepared to counter such threats can be enhanced through "examinations, on-site and other supervisory mechanisms, comparative analysis of entities' testing results, and joining public-private exercises."

A. Mapping G7FE Element 4 to Insurance Core Principles

131. Cyber-related monitoring addressed in G7FE 4 is consistent with the risk management system discussed in ICP 8.1, which "should include early warnings or triggers that allow timely consideration of, and adequate response to, material risks."[64]

132. It is also consistent with ICP 8.2, under which "the supervisor requires the insurer to establish, and operate within, an effective system of internal controls." Such a monitoring system includes "periodic testing and assessments (carried out by objective parties such as an internal or external auditor) to determine the adequacy, completeness and effectiveness of the internal controls system and its utility to the Board and Senior Management for controlling the operations of the insurer."[65]

[64] ICP 8.1.8.

[65] ICP 8.2.4.

B. Recommendations for Supervisors Regarding Monitoring

133. With regard to insurers' cybersecurity monitoring, it may be appropriate for supervisory practices to encourage or reflect the following:

Continuous Monitoring

a. Insurers should protect network (hardware, firmware and software components) integrity including control of information flow, boundary protection, and network segregation if needed.

b. For example, An insurer should establish real-time, or near real-time continuous monitoring capabilities to detect anomalous activities and events. One practice currently in use to accomplish this is commonly referred to as a Security Operations Centre (SOC). Insurers should consider establishing a SOC or developing similar capability to provide round the clock monitoring and such capabilities should be adaptively maintained and tested.

c. The insurers should be able to recognize signs of a potential cyber incident, or detect that an actual breach has taken place, which is essential to strong cybersecurity. Early detection provides an insurer with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches. In the latter case, early containment could effectively mitigate the impact of the attack – for example, by preventing an intruder from gaining access to confidential data or exfiltration of such data.

d. In view of the stealthy and sophisticated nature of cybersecurity incidents and the multiple entry points through which a compromise could take place, an insurer should maintain effective capabilities to extensively monitor for anomalous activities.

e. The insurers should monitor relevant internal and external activities and events, seeking to detect vulnerabilities through a combination of signature monitoring for known vulnerabilities and behaviourally-based detection mechanisms.

f. Insurers' detection capabilities should also address misuse of access by third party service providers, policyholders, potential insider threats, and other advanced threat activity. These processes should be informed by and integrated with a strong cyber threat intelligence programme.

g. As part of the monitoring process, insurers should manage the identities and credentials for physical, logical, and remote access to information assets, based on principles of least privilege and separation of duties.

h. An insurer should implement, within relevant legal boundaries, measures to capture and analyse anomalous behavior by persons with access to the corporate network.

i. The insurers should have the ability to detect an intrusion early, as this capability is critical for swift containment and recovery. Insurers should take a defence-in-depth approach by instituting multi-layered detection controls covering people, processes, and technology, with each layer serving as a safety net for preceding layers.

j. In addition, an effective intrusion detection capability could assist insurers in identifying deficiencies in their protective measures for early remediation. These capabilities would include data loss/leaks prevention and detection, the recording and documentation of

audit logs, event data aggregation, correlation, analysis and communication, as well as network, personnel and external dependency activity monitoring.

k. The insurer should employ monitoring and detection capabilities to facilitate its incident response process and support information collection for the forensic investigation process.

Testing

l. Testing is an integral component of any effective cybersecurity framework. Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the insurer's cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cybersecurity posture and reduce or eliminate identified gaps. Such testing could include vulnerability assessments, scenario-based testing, penetration tests, and tests using red teams.

m. Insurers should rigorously tests all elements of their cybersecurity framework to determine their overall effectiveness before being employed within an insurer, and regularly thereafter. Such testing should encompass the extent to which the framework is implemented correctly, operating as intended, and producing desired outcomes.

n. Insurers should tests their cybersecurity framework and communicate the results within their organisation. For example, insurers should establish an appropriately comprehensive testing programme to validate the effectiveness of all elements of their cybersecurity framework, employing appropriate available cyber threat intelligence to inform its testing methods – such as by designing tests to simulate advanced threat agent capabilities and extreme but plausible scenarios.

o. The results of the testing programme should be used by the insurer to support the ongoing improvement of its cybersecurity (see discussion of G7FE Element 8). Where applicable and practicable, these tests should include other stakeholders and functions within the organization, such as business line management including business continuity, incident and crisis response teams, and relevant external stakeholders. An insurer should have proper procedures in place to ensure that its Board and Senior Management are appropriately involved (e.g., as part of crisis management teams) and informed of test results.

p. The insurers should consider using a combination of the available state-of-the-art testing methodologies and practices. Currently, such state-of-the-art testing methodologies and practices, include the following elements (which partly overlap and can be combined):

q. *Vulnerability Assessment (VA).* Insurers should regularly perform vulnerability assessments to identify and assess security vulnerabilities in their systems and processes. Insurers should establish a process to prioritize and remedy issues identified in VAs and perform subsequent validation to assess whether gaps have been fully addressed in a timely manner.

r. *Scenario-Based Testing.* An insurer's response, resumption, and recovery plans should be subject to periodic review and testing. Tests should address an appropriately broad scope of scenarios, including simulation of extreme but plausible cybersecurity incidents, and should be designed to challenge the assumptions of response, resumption, and

recovery practices, including governance arrangements and communication plans. Insurers should use cyber threat intelligence and cyber threat modelling to the extent possible to imitate the unique characteristics of cyber threats. They should also conduct exercises to test the ability of their staff and processes to respond to unfamiliar scenarios, with a view to achieving stronger operational resilience.

s. *Penetration Tests.* Insurers should carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. To provide an in-depth evaluation of the security of insurers' systems, those tests should simulate actual attacks on the systems. Penetration tests on internet-facing systems should be conducted regularly and before updated systems are deployed. Where applicable and practicable, the tests could include wider business stakeholders, such as those involved in business continuity, incident and crisis response teams, as well as third parties, such as service providers.

t. *Red Team Tests.* Insurers should consider challenging their own organizations and external dependencies through the use of so-called red teams to introduce an adversary perspective in a controlled setting. Red teams serve to test for possible vulnerabilities and the effectiveness of an insurer's mitigating controls. A red team may consist of insurer's own employees and/or outside experts, who are in either case independent of the function being tested.

u. An insurer should, to the extent practicable/possible, promote, design, organize, and manage exercises designed to test its response, resumption, and recovery plans and processes. Such exercises should include the insurer as well as critical service providers, and linked insurers (such as affiliates within an insurance group). Where appropriate, insurers should participate in exercises organized by relevant authorities and in industry-wide tests.

v. Insurers and supervisors should take note that traditional isolated testing implicitly assumes that all other players operate as usual, which may be an unrealistic limitation. Removing that hypothesis helps an insurer to identify plausible complexities, dependencies and weaknesses that may have been overlooked in its recovery plans. Accordingly, testing should include scenarios that cover breaches affecting external dependencies.

C. Examples of Current Practices

134. **European Union**. Under Solvency II, the supervisory authority can audit directly a third party or provider[66].

135. **France**. The ACPR encourages insurance companies to deploy organisations dedicated to security monitoring such as SOC (security operations center) to supervise the information system security network, if it is judged relevant and commensurate with the size of the company.

136. **Germany**. BaFin's draft circular on IT requirements demands that reports of unplanned deviations from standard operation (faults) and their causes must be suitably collected,

[66] Considerant (37) of Solvency II Directive.

assessed, prioritised – in particular with regard to the possible resulting risks – and escalated in accordance with set criteria. Processing, causal analysis and solution finding, including follow-up, must be documented. There must be an orderly process for the analysis of possible correlations between faults and their causes. The state of processing of open reports on faults, including the appropriateness of the assessment and prioritisation, must be monitored and managed. The insurer must set suitable criteria for informing the management board about faults.

137. **Netherlands**. In collaboration with institutions comprising the Dutch financial core payment infrastructure, including insurers, DNB has developed a program for further improvement of the sector's protection against advanced cyber attacks by means of an overarching framework including red team testing.

138. The framework is known as Threat Intelligence- Based Ethical Red teaming (TIBER).[67] TIBER learned from the CBEST framework launched by the Bank of England in 2014,[68] and further developed it to adapt to the changing nature of advanced cyber threats. Its purpose is to enhance the country's financial core institutions' cyber resilience by learning from each other's best practices.

139. TIBER tests mimic potential cyber attacks from real threat actors. The test mimics high level threat groups only (organised crime groups / state proxy/ nation state attackers) and thereby tests whether defensive measures taken are effective (capability assessment), supplementing the present periodic information security audits (process assessments) by e.g., supervisors and overseers. The tests also supplement current penetration tests and vulnerability scans executed by the financial institutions.

140. Insurers in the Netherlands are encouraged to use this framework.

141. **Québec, Canada**. In its Business Continuity Management Guideline, the AMF expects financial institutions to identify the major operational incidents likely to disrupt, slow down or interrupt their critical functions.

142. Also, in its Operational Risk Management Guideline, the AMF expects operational risk reports to reflect a financial institution's risk tolerance levels. These reports should also enable the institution to track changes in risk exposure and the effectiveness and efficiency of the measures put in place to manage such risks.

143. More precisely, the analysis of the most significant incidents reported should allow the board of directors and senior management to identify the main sources of unmitigated operational risk. Such reports should incorporate the recommendations made by both the AMF and the audit functions.

144. As part of its supervision activities, the AMF has developed a detailed self-assessment tool based on recognised cyber-related international standards and processes (such as those published by the NIST and COBIT organizations). This tool is used to assess the cybersecurity posture of many financial institutions based on their risk profiles. Where

[67] See also DNB, *TIBER-NL GUIDE - How to Conduct the TIBER-NL Test*, (November 2017), available at https://www.dnb.nl/en/news/news-and-archive/nieuws-2017/dnb365801.jsp.

[68] Bank of England, *Financial Sector Continuity*, available at https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity.

needed, the tool is also made available to financial institutions the AMF oversights. Among other things, it recommends the monitoring of network infrastructure and personnel and external service provider activity to detect potential cybersecurity events. It recommends the monitoring of all remote accesses, the use of technological tools to monitor outgoing traffic and the aggregation, correlation and analysis of anomalous activities and events from various sources to understand attack targets and methods.[69]

145. **United Kingdom**. The FCA operates a multi-layered approach to reviewing and approving the sectors approach to cyber resilience. This includes the issuance of self-assessment cyber questionnaires seeking to evaluate firms' capabilities against foundational cyber resilience capabilities, and the implementation of Risk Mitigation plans where severe deficiencies are found.

146. The FCA was also a key member of the CBEST design group and co-implements the framework with the Bank of England. CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests. The tests replicate behaviours of threat actors, assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions. The FCA has broadened the scope of CBEST such that the tests can be deployed on a wider range of firms than those considered systemically important, in order that broader consumer harm becomes a key consideration for the scope of these tests.

147. The FCA also operates a third party risk evaluation tool to passively and silently scan the publically visible interfaces of its regulated firms to detect vulnerabilities and weaknesses that may also be visible to criminals. The discovery of these vulnerabilities informs discussion with regulated entities to evaluate the severity of such issues and informs risk remediation plans.

148. **United States**. Section 4D of the NAIC *Insurance Data Security Model Law* directs the insurer to include network monitoring among its potential security measures "to detect actual and attempted attacks on, or intrusions into, Information Systems or other system failures."

149. Additionally, Section 4I requires the insurer to submit an annual written statement certifying to the Commissioner, that the insurer is in compliance with the Information Security Program requirements of the Act.

150. Furthermore, Section 7 provides the Commissioner with the power to examine and investigate the insurer to ensure compliance with the Act, pursuant to such powers that already exist under state law.

151. The *Examiner's Handbook* includes specific procedures to review and consider network monitoring in terms of controls that may be present and testing that should be performed. The *Handbook*'s guidance also provides insight on the review of third-party audits to facilitate the integration of the insights generated therein into the exam procedures and any follow up performed.

[69] AMF, *Operational Risk Management Guideline* (December 2016), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

152. Section 500.05 of NYDFS *Cybersecurity Requirements for Financial Services Companies* requires that the insurer perform monitoring and testing developed in accordance with its Risk Assessment to assess the effectiveness of its cybersecurity program, including annual penetration testing and bi-annual vulnerability assessments (annual penetration testing and bi-annual vulnerability assessment requirements do not apply if there is continuous monitoring). Section 500.17 requires the insurer, through its Board of Directors or a Senior Officer, to certify compliance with the regulations to the Superintendent.

D. Assessing Outcomes of G7FE Element Four

153. For G7FE number Four, the desirable outcomes proposed by the G7 are:

154. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. Discussed above at Paragraph 72-73.

155. **G7FEA Outcome 4 – An Adaptive Cybersecurity Approach is Adopted**. Both cyber threats and the vulnerabilities which they exploit continue to emerge and evolve. Correspondingly, entities need to be adaptive and avoid a static fortress mentality to ensure their cybersecurity procedures reflect the ever changing landscape within which they operate.

156. Building on Element 5 (response) and Element 6 (recovery), incident response mechanisms need to be well-rehearsed such that economic functions can continue to operate through disruption or stress, whether at the entity, sector, cross-sector or international levels. As disruptions may impact the financial sector in unexpected ways, flexibility is key in reactive functions. Coupled with Element 4 (monitoring), it is the agility and experience to rapidly identify and contain disruptions that largely influence the resulting impacts. Related, the overall focus should be on fostering an environment of continuous improvement and learning as part of the cybersecurity programme.

3.5 G7FE -- Element 5: Response

157. **The fifth of the G7FE calls for financial institutions to "[t]imely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and customers as appropriate); and (d) coordinate joint response activities as needed."**

158. The fifth G7FE calls on entities to implement incident response policies and other controls to facilitate effective incident response," and notes "[a]mong other things, these controls should clearly address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders."

A. Mapping G7FE Element 5 to Insurance Core Principles

159. G7FE 5 is consistent with ICP 8.1.2, which suggests contingency planning as a part of suitable processes and tools for effective risk management system. Such contingency planning can include response and recovery process after a cyber incident.

B. Recommendations for Supervisors Regarding Response

160. With regard to insurers' cybersecurity response, it may be appropriate for supervisory practices to encourage or reflect the following:

a. In advance of a cybersecurity incident, insurers should raise awareness among all its stakeholders by providing training for employees and others with access to its systems. Insurers should also develop response plans (Incident Response and Business Continuity) and communication plans regarding cyber incidents. These plans should be subject to review and improvement as appropriate.

b. Upon detection of a cybersecurity incident (or an attempt), it is good practice for an insurer to perform a thorough investigation to determine its nature and extent as well as the damage inflicted. While the investigation is ongoing, the insurer should also take immediate actions to contain the situation to prevent further damage, and commence recovery efforts to restore operations based on its response planning.

c. Insurers should also be cognizant not to bring systems back up too quickly and risk another attack or expansion of the cybersecurity incident.

d. While an insurer should plan to resume critical operations as soon as is safely possible after a cybersecurity incident, it should analyse critical functions, transactions, and interdependencies to prioritize resumption and recovery actions while remediation efforts continue. Insurers should also plan for situations where critical people, processes, or systems may be unavailable for significant periods – for example, by potentially reverting, where feasible and practicable, to manual processing if automated systems are unavailable.

e. Insurers should plan to have access to external experts, recognizing that a large-scale or industry wide event may reduce the availability of such key resources on short notice.

f. Insurers should develop and test response, resumption, and recovery plans. These plans should support objectives to protect the confidentiality, integrity, and availability of its assets, including policyholder data. Plans should be actively updated based on current cyber threat intelligence, information-sharing, and lessons learned from previous events, as well as analysis of operationally and technically plausible scenarios that have not yet occurred. An insurer should consult and coordinate with relevant internal and external stakeholders during the establishment of its response, resumption, and recovery plans, including supervisors and other relevant authorities.

g. System and process design and controls for critical functions and operations should support incident response activities to the extent possible. Insurers should design systems and processes to limit the impact of any cyber incident and protect the privacy of policyholder data. An insurer's incident response, resumption, and recovery processes should be closely integrated with crisis management, business continuity, and disaster recovery planning and recovery operations, and coordinated with relevant internal and external stakeholders.

h. Insurers should have a specific team in place for all stakeholder communications – inclusive of policyholders, business partners, and appropriate authorities, to ensure adequate preparation and consistency of message.

i. As part of its overall governance framework and in compliance with relevant laws, insurers should have a policy and procedure to enable the responsible disclosure of potential vulnerabilities following a risk-based approach. In particular, insurers should prioritize disclosures that could facilitate early response and risk mitigation by stakeholders for the benefit of the cyber ecosystem and broader financial stability.

j. In the event of an exposure of policyholder data, an insurer should have a policy and procedure to meet the disclosure obligations set forth in the laws and regulations of all relevant jurisdictions.

k. Insurers should have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process. In this regard, insurers should establish relevant system logging policies that include the types of logs to be maintained and their retention periods. While forensic analysis may need to be postponed and ICT resources may be focused on recovering critical systems, insurers should ensure that investigations can still be performed post-event to the extent possible, e.g., through preservation of necessary system logs and evidence.

C. Examples of Current Practices

161. **France**. To perform its supervision, the ACPR leverages different tools notably records of the incidents, business continuity plan and IT management.[70] Solvency II framework[71] obliges the insurer to have a BCP (business continuity plan). Even if it is not clearly specified, ACPR will verify that scenarios used to build those plans include cyber threat and other information security scenarios.

162. **Germany**. German legislation empowers BaFin to require insurers to provide, among other things, information on their contingency planning. As part of its supervisory practice, BaFin assesses insurers´ contingency plans and may require necessary amendments. As far as emergency tests are performed by insurers BaFin may as their supervisor attend the execution of the test on the premises of the insurer.

163. **Québec, Canada**. In April 2018, the Government of Canada published an Order in Council that will bring into force, as of November 1, 2018, the mandatory breach notification and record-keeping requirements under the Personal Information Protection and Electronic Documents Act (PIPEDA). Once implemented, these changes will more closely align the Canadian breach reporting regime with those in the United State and European Union.

164. Under the new provisions of PIPEDA, a data breach, or “breach of security safeguards,” is defined as a loss or unauthorized access or disclosure of personal information resulting from a breach of the organization’s security safeguards. Organizations that experience a data breach must report the incident to the Office of the Privacy Commissioner of Canada (OPC) and notify affected individuals where it is reasonable to believe that the breach creates a “real risk of significant harm to the individual.” The term

[70] Article 228(1) of the delegated act and Article 40 and followings of the SII Directive represent the main robust legal basis.

[71] Article 258 para 3.

"significant harm" includes, among other things, bodily harm, humiliation, damage to reputation or relationships, financial loss, identity theft, negative effects on the credit record and damage to, or loss of, property.

165. As recommended by its Governance and Operational Risk Management Guidelines, the AMF trust insurers to meet the disclosure and transparency expectations by implementing the necessary mechanisms for promptly advising internal and external stakeholders likely to sustain serious harm due to a major operational incident (cyber incident, system failure, etc.). Such an approach will enable the AMF, as a stakeholder, to be proactive in identifying practices that can undermine operational risk management. Also, the AMF expects internal control mechanisms to efficiently mitigate the financial institution's operational risk exposure inherent to people, processes, systems or external events, according to their importance.

166. Furthermore, the AMF is currently developing a formal communication channel and processes to standardize the treatment of the notifications received from the insurers it supervises.[72]

167. **United Kingdom**. The FCA supports a number of initiatives to enable effective response to cyber events. The UK Financial Services Incident Response Guide is co-authored with the UK financial authorities and a group of regulated firms and shared on the UK Cyber Information Sharing Partnership (CiSP) and details how impacted firms should meet mandatory reporting requirements and where response assistance can be obtained.

168. The FCA is also a part of the Authorities Response Framework (ARF) with the Bank of England, HM Treasury, National Cyber Security Centre and National Crime Agency. The ARF provides a coordination and response mechanism to allow the collective authorities to react to major incidents in a cohesive and collaborative manner, ensuring that all parties are aware of the response actions underway by all participants.

169. The FCA regularly reviews the response arrangements of regulated firms, performing these reviews using a risk based approach to focus on those firms posing the greatest risk of harm.

170. **United States**. Section 4H of the NAIC *Insurance Data Security Model Law* requires the insurer to establish a written incident response plan that indicates how the insurer will respond to and recover from any identified incidents. The plan must include information on communications that need to take place in the event of an incident, how weaknesses in information systems and associated controls will be remediated, the definition of clear roles, responsibilities, and levels of decision-making authority. Under Section 6, the insurer is required to notify the Commissioner (i.e., the State insurance supervisor), the affected consumers, and certain other stakeholders.

171. The *Examiner's Handbook* generally addresses these elements through a number of procedures that include a review of how the company responds to incidents that could result in interruption of services (e.g., review of incident response plan) and a review of

[72] AMF, *Governance Guideline* (September 2016) available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/; AMF, *Operational Risk Management Guideline* (December 2016), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

how the company assures the continuity of critical business functions (e.g., review of system recovery functionality).

172. Section 500.16 of the NYDFS *Cybersecurity Requirements for Financial Services Companies* requires the insurer to establish an incident response plan designed to promptly respond to, and recover from, a Cybersecurity Event. The plan must include information on communications that need to take place in the event of an incident, how weaknesses will be remediated, definition of clear roles, responsibilities, and levels of decision-making authority. Section 500.17 requires that the insurer report Cybersecurity Events to the Superintendent (i.e., the New York insurance supervisor).

D. Assessing Outcomes of G7FE Element Five

173. For G7FE number Five, the desirable outcomes proposed by the G7 are:

174. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. Discussed above at Paragraph 72-73.

175. **G7FEA Outcome 3 –There is an Understanding that Disruptions will Occur**. Discussed above at Paragraph 125-126.

176. **G7FEA Outcome 4 –An Adaptive Cybersecurity Approach is Adopted**. Discussed above at Paragraph 155-156.

3.6 G7FE -- Element 6: Recovery

177. **The sixth G7FE calls for financial institutions to "[r]esume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally."**

178. Recovery of operations that are interrupted by a cyber incident should occur "[o]nce operational stability and integrity are assured." G7FE 6 notes that where "critical functions, processes, and activities" have been affected, restoration should be undertaken "in accordance with objectives set by the relevant public authorities," and that "trust and confidence in the financial sector significantly improves when entities and public authorities have the ability to mutually assist each other in resumption and recovery."

A. Mapping G7FE Element 6 to Insurance Core Principles

179. As described in the previous section, this is consistent with ICP 8.1.2, which suggests contingency planning as a part of suitable processes and tools for effective risk management system. Such contingency planning can include response and recovery process after a cyber incident.

B. Recommendations for Supervisors regarding recovery

180. With regard to cybersecurity recovery, it may be appropriate for supervisory practices to encourage or reflect the following:

a. Insurers should have in place validated plans and procedures to recover from a cybersecurity incident.

b. Cyber incident recovery arrangements should be designed to enable insurers to resume operations safely with a minimum of disruptions to policyholders and business operations.

c. Insurers should design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, insurers' systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including, to the extent possible, application source code), to be used in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls. In addition, the insurer's cybersecurity framework should include data recovery measures, such as keeping a backup copy of all policyholder data in the event such data is corrupted.

d. Insurers' recovery plans (Incident Recovery and Disaster Recovery) should be subject to review and improvement as appropriate.

e. Because an insurer's systems and processes are often interconnected with the systems and processes of third parties, in the event of a large-scale cyber incident it is possible for an insurer to pose contagion risk (i.e., propagation of malware or corrupted data) to, or be exposed to contagion risk from, its third party service providers or other interconnected systems. An insurer should work with these third parties to resume operations in a safe manner.

f. Insurers should have formal plans for communicating with policyholders, internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders and third-party service providers as appropriate) likely to sustain harm due to a major cybersecurity incident. Communication plans in accordance with governing law should be developed through an adaptive process informed by scenario-based planning and analysis as well as prior experience. Because rapid escalation of cybersecurity incidents may be necessary, insurers should determine decision-making responsibilities for incident response and recovery in advance, and implement clearly defined escalation and decision-making procedures.

C. Examples of Current Practices

181. **France**. Recovery from cyber-attacks or catastrophe is often covered by the business continuity planning or the Own Risk and Solvency Assessment (ORSA) of the company.

182. **Germany**. BaFin's draft circular on IT requirements demands that, after an information security incident, the effects on information security must be analysed and appropriate follow-up measures arranged.

183. **Québec, Canada**. The AMF Business Continuity Management Guideline propose a set of core principles based on those published by the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors and the Joint Forum with respect to sound operational risk management practices and sound business continuity management practices. With this in mind, each insurer is expected to adopt a carefully developed business continuity plan to ensure it is optimally prepared to handle major operational incidents.

184. Furthermore, the AMF self-assessment tool made available to the insurers recommends that response and continuity plans for all critical services specifically considers cyber incidents. The tool further specifies that strategies and processes be put in place to rapidly isolate cyber incidents and compromised locations so as to mitigate the institution's exposure to the new vulnerabilities detected. Also, the insurers should validate, according to a pre-established frequency, the effectiveness of its response and recovery plans using cyber attack simulation exercises.[73]

185. **United Kingdom**. The FCA expects firms to plan for recovery and resumption of services following a cyber incident. This includes communications that need to take place and stakeholder maps detailing the timeliness and criticality of such communications. The FCA may request and review public communications. The UK Listing Authority may also require listed firms to make public disclosure following a major cyber attack.

186. **United States**. As described above under the "response" element, Section 4H of the NAIC *Insurance Data Security Model Law* requires the insurer to establish a written incident response plan that indicates how the insurer will respond to and recover from any identified incidents. The plan must include information on communications that need to take place in the event of an incident, how weaknesses will be remediated, the definition of clear roles, responsibilities, and levels of decision-making authority. Under Section 6, the insurer is required to notify the Commissioner (i.e., the State insurance supervisor), the affected consumers, and certain other stakeholders.

187. Similarly, Section 500.16 of the NYDFS *Cybersecurity Requirements for Financial Services Companies* requires the insurer to establish an incident response plan designed to promptly respond to, and recover from, a Cybersecurity Event. The plan must include information on communications that need to take place in the event of an incident, how weaknesses will be remediated, definition of clear roles, responsibilities, and levels of decision-making authority. Section 500.17 requires that the insurer report Cybersecurity Events to the Superintendent (i.e., the New York insurance supervisor).

D. Assessing Outcomes of G7FE Element Six

188. For G7FE number Six, the desirable outcomes proposed by the G7 are:

189. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. Discussed above at Paragraph 72-73.

190. **G7FEA Outcome 3 –There is an Understanding that Disruptions will Occur**. Discussed above at Paragraph 125-126.

191. **G7FEA Outcome 4 –An Adaptive Cybersecurity Approach is Adopted**. Discussed above at Paragraph 155-156.

[73] AMF, *Business Continuity Management Guideline* (April 2010), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

3.7 G7FE -- Element 7: Information Sharing

192. **The seventh G7FE calls for entities to "[e]ngage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning."**

193. The seventh G7FE notes that "[s]haring technical information, such as threat indicators or details on how vulnerabilities were exploited, allows entities to remain up-to-date in their defences and learn about emerging methods used by attackers."

194. Further, "[s]haring broader insights among entities, between entities and public authorities, and among public authorities deepens collective understanding of how attackers may exploit sector-wide vulnerabilities that could potentially disrupt critical economic functions and endanger financial stability."

A. Mapping G7FE Element 7 to Insurance Core Principles

195. For insurers, the recommendations of G7FE 7 can be mapped to the contingency planning requirements addressed in ICP 8.1.2.

196. ICP 16 (Enterprise Risk Management for Solvency Purposes) speaks to sharing technical information and broader insights can be practiced as a part of risk responsiveness and feedback loops, addressed under ICP 16.10.[74]

197. Information sharing among supervisors is generally covered under ICPs 3, 25, and 26,[75] among others[76]. These ICPs provide frameworks and guidance for information exchange and supervisory cooperation, including cross-border crisis situation.

B. Recommendations for Supervisors Regarding Information Sharing

198. With regard to cybersecurity information sharing, it may be appropriate for supervisory practices to encourage or reflect the following:

a. Insurers should establish a process to gather and analyse relevant cyber threat information. Insurers should consider participating actively in information-sharing groups and collectives, including cross-industry, cross-government, and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats, and early warning indicators relating to cyber threats. Insurers may participate in system-wide initiatives such as Incident Response Teams (IRT), if established in relevant jurisdictions.

b. It may be appropriate for insurers to engage with the Financial Services Information Sharing and Analysis Center (FS-ISAC), an acknowledged global resource to the

[74] ICP 16.10 will be moved and integrated into ICP 8.10.

[75] ICP 3 (Information Exchange and Confidentiality Requirements), ICP 25 (Supervisory Cooperation and Coordination) and ICP 26 (Cross-border Cooperation and Coordination on Crisis Management). ICP 26 will be removed and integrated into ICPs 12 and 25.

[76] ICP 21 (Countering Fraud in Insurance) and ICP 22 (Anti-Money Laundering and Combating the Financing of Terrorism) also mention information sharing among supervisors in terms of its respective topic.

financial sector for cyber and physical threat intelligence analysis and sharing.[77] In 2012, the FS-ISAC established an Insurance Risk Council that allows members to share information, best practices, and threat information with peer institutions.

c. An insurer's analysis of cyber threat information should be in conjunction with other sources of internal and external business and system information so as to provide business-specific context, turning the information into usable cyber threat intelligence that provides timely insights and informs enhanced decision-making by enabling the insurer to anticipate a cyber attacker's capabilities, intentions, and modus operandi.

d. If practicable, an insurer's cyber threat intelligence operations should include the capability to gather and interpret information about relevant cyber threats posed by the insurer's third-party service providers, as well as utility providers and other critical infrastructure resources. Additionally, cyber threat intelligence operations should interpret this information in ways that allow the insurer to identify, assess, and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems. In this context, relevant cyber threat intelligence could include information on geopolitical developments that may trigger cyber attacks on the insurer or any of its external dependencies.

e. When properly contextualized, cyber threat information enables an insurer to validate and inform the prioritization of resources, risk mitigation strategies, and training programmes. Therefore, an insurer should make cyber threat intelligence available to appropriate staff within the insurer with the responsibility for the mitigation of cyber risks at the strategic, tactical, and operational levels. Cyber threat intelligence should be used to ensure that the implementation of any cybersecurity measures is threat-informed.

f. To facilitate sector-wide response to large-scale cybersecurity incidents, insurers should plan for information-sharing through trusted channels, collecting and exchanging timely information that could facilitate the detection, response, resumption, and recovery of its own systems and those of other sector participants during and following a cybersecurity incident. Insurers should, as part of their response programmes, determine beforehand which types of information will be shared with whom and how information provided to the insurer will be acted upon. Reporting requirements and capabilities should be aligned with relevant laws and regulations as well as information-sharing arrangements within insurer communities and the financial sector.

g. An insurer should consider exchanging information on its cybersecurity framework bilaterally with its third-party service providers to promote mutual understanding of each other's approach to securing systems that are linked or interfaced. Such information exchange would facilitate an insurer's and its stakeholders' efforts at dovetailing their respective security measures to achieve greater cybersecurity.

C. Examples of Current Practices

199. **European Union**. The General Data Protection Regulation (GDPR)[78] introduces a specific treatment of personal data depending on its confidentiality level in the

[77] Information about the FS-ISAC is available at https://www.fsisac.com/about.

undertaking. Between supervisors, a wide range of coordination is foreseen via Solvency II Equivalence and Memorandum of Understanding (MoU). As a further framework, the NIS Directive[79] may be of relevance as far as insurance companies are identified as providers of essential services.

200. **France**. ACPR collaborates with experts: the ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), which is the French National cybersecurity agency; and the CERT (computer emergency team) of the Banque de France. The ACPR also carries out cyber watches and exchanges with the banking sector in order to ensure consistencies of approaches and practices on cyber security matters for financial sectors companies. . As supervisor, ACPR is fully involved in cyber risk supervision in this new ecosystem. The ACPR adopts a prudential and sectorial-specific approach on cyber security and data protection.

201. To achieve this goal, the ACPR develops multiple interactions with :

- CNIL (National Commission of IT and freedom);
- ANSSI;
- ENISA;
- Ministry of Defence;
- Undertakings and their federations, i.e., Insurance Europe; Fédération Française de l'Assurance (FFA); L'Association des professionnels de la réassurance en France (APREF); and
- Institute of Actuaries.

202. The ACPR acknowledges the necessary smooth articulation between the military programming Law, the GDPR, and Solvency II and supports the exchange of information among supervisors to refine its analysis of cyber security.

203. In France, a specific law already covers some of the GDPR requirements[80]. Considering this framework, the ACPR acknowledges the new strengthened rights for individuals including right to access and right to rectification and deletion of data, portability of information to a third party, product governance and anonymity. These new harmonized principles may be relevant for insurer cybersecurity supervision.

204. A transposition of Network and Information Security Directive is also taking place in France through a national strategy on digital security and a Military Law Programs. ACPR collaborates with CNIL, ANSSI and FR-CERT to develop a consistent and appropriate approach for insurers on Information security and data protection of insured persons.

[78] General Data Protection Regulation Portal, available at: https://www.eugdpr.org/. GDPR is a new regulation, adopted on 24 May 2016 and enforced on 25 May 2018.

[79] The Directive on security of network and information systems (NIS Directive), 2016/1148, was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States were to transpose this Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018.

[80] Loi pour une République numérique, 7 October 2016.

205. **Germany**. In Germany there is a public-private cybersecurity coordination forum that is called "UP KRITIS", which stands for "Implementation Plan Critical Infrastructure Protection". UP KRITIS is the initiative for cooperation between critical infrastructure operators, associations, and the state in order to protect critical infrastructure in Germany with a focus on IT security.

206. Additionally there are sector-specific working groups established for, among others, the insurance sector. In these working groups all members of the corresponding sector, the BSI (Federal Office for Information Security) and the BaFin participate and share information about cybersecurity issues.

207. **Québec, Canada**. The AMF self-assessment tool made available to the insurers recommends that institutions develop internal and external communication plans for managing material cyber incidents that considers, in particular, officers, senior management, board of directors, clients, media, suppliers and regulators.

208. The tool also recommends that insurers participate in specialized information exchange forums and that an oversight process which mainly draws on interest groups, specialized forums and professional associations active in the area of security, be put in place to detect cybersecurity issues and trends.

209. **Singapore**. In Singapore, Monetary Authority of Singapore (MAS) continuously monitors for new and evolving cyber threats through information gathered from IT security vendors, law enforcement agencies and international financial regulators. MAS also monitors the Singapore financial sector's cyber threat landscape through collecting monthly IT security threat indicators from key financial institutions (FIs). This has allowed MAS to pick up broad shifts in cyber-attack volumes and vectors facing key FIs, even if attacks were unsuccessful. Where relevant, the surveillance findings are shared with the FIs.

210. To strengthen partnership with the industry and other stakeholders, MAS has established a secure platform (FINTEL) to facilitate sharing of cyber intelligence among major FIs in Singapore. Major FIs in Singapore have also signed up as members of the US Financial Services Information Sharing and Analysis Center (FS-ISAC) to tap on its information sharing network.

211. With support from MAS, FS-ISAC has set up in Singapore, the industry body's only cyber intelligence centre in the Asia-Pacific region. This centre will help the Singapore financial industry better monitor cyber threats and provide improved intelligence support to FIs. It will also help deepen the capabilities of the cyber security community in Singapore and the broader APAC region.

212. **United Kingdom**. The FCA implemented and co-chairs the Cyber Coordination Group initiative, bringing together circa. 175 firms on a quarterly basis, aligned to specific sectors. This includes the Insurance Sector Cyber Coordination Group (ISCCG). These groups consist of around 25 firms each and also include the FCA, Bank of England, HM Treasury, National Cyber Security Centre and National Crime Agency. They provide a safe and trusted group within which information can be shared about cyber risk, remediation activity, new and evolving threats and cyber incidents. The groups have also convened after major cyber events (i.e., WannaCry) to review collective industry response.

213. The FCA also collaborates bilaterally with a range of key partners, sharing information about the cyber risk , supervisory practices and examination approaches. These include all relevant domestic agencies as well as international regulatory peers.

214. More broadly in the UK, the NCSC hosts the Cyber Security Information Sharing Partnership (CiSP), funded by the national cyber security budget and free of charge for member firms. CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

215. Firms in the UK are obliged to report material cyber events to the FCA, the PRA and, where personal data is involved, the Information Commissioners Office (ICO) under GDPR.

216. **United States**. Section 4D of the NAIC *Insurance Data Security Model Law* requires the insurer to stay informed regarding emerging threats or vulnerabilities with discretion left to the insurer to determine the execution of that practice. Section 6 requires the insurer to notify the Commissioner (i.e., the state insurance supervisor), the affected consumers, and certain other stakeholders of a cyber security event. Section 8 governs sharing of documents among certain governmental entities and the National Association of Insurance Commissioners.

217. The *Examiner's Handbook* focuses on evaluating how an insurer integrates insights learned from other parties to strengthen their control response. A risk profile is developed using threat and vulnerability information received from information-sharing forums and sources (e.g., Financial Services Information Sharing and Analysis Center, FS-ISAAC).

218. State insurance regulators coordinate regularly with federal and state financial regulators. As part of these collaborative efforts, state insurance regulators and the NAIC engage with financial regulators through the Financial and Banking Information Infrastructure Committee (FBIIC), chaired by the U.S. Treasury Secretary, to facilitate communication and consider ways to effectively coordinate regulatory approaches to managing and evaluating cybersecurity risk. FBIIC member organizations have established a MoU to facilitate the sharing of timely, actionable information regarding cybersecurity events across the financial sector.

219. The FBIIC regularly collaborates with the Financial Sector Coordination Council (FSSCC), a private sector body that works with the U.S. Treasury toward the shared goal of maintaining a robust and resilient financial services sector. In addition, state insurance regulators participate in the Executive Branch and Independent Agency Regulatory Cybersecurity Forum to discuss best practices and common regulatory approaches to cybersecurity challenges across different sectors of the U.S. economy.

220. State insurance regulators recognize the value of information sharing and underscored its importance in the NAIC's *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, [81] which encourages insurers to utilize information sharing and analysis

[81] NAIC, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), available at http://naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

organizations such as FS-ISAC to help identify, assess, and monitor emerging cyber threats.

221. Section 500.17 of the NYDFS *Cybersecurity Requirements for Financial Services Companies* requires that the insurer report Cybersecurity Events to the Superintendent (i.e., the New York insurance supervisor) within 72 hours.

D. Assessing Outcomes of G7FE Element Seven

222. For G7FE number Seven, the desirable outcomes proposed by the G7 are:

223. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. Discussed above at Paragraph 72-73.

224. **G7FEA Outcome 5 – There is a Culture that Drives Behavior**. Building on Element 7 (information sharing) and Element 8 (continuous learning), a continuous focus on skills and behaviors is essential for embedding effective cybersecurity into the fabric of an organization.

225. In many cybersecurity incidents, flawed procedures or human factors play a key role (e.g., leveraging weak passwords, social engineering, poor security awareness, etc.). Effective cybersecurity strategies consider aspects of people and processes on an equal footing with technical solutions, and reflect this in investment decisions taken. Training and awareness are equally important, targeted at the end user, employee, and senior management.

226. In a world where individuals often trade security for convenience, the manipulation of human psychology is as relevant as an adversary's technological sophistication. Each individual understands that they have a role to play. Effective cybersecurity relies on engaging and educating people, and enabling them to handle information safely. Cybersecurity training and awareness can enhance technical knowledge as well as offer opportunities to change behaviors. Effective training aims for genuine and measurable change, shaping culture in a meaningful way, rather than seeking compliance with a set of policies. The adage that people are considered as the weakest link is reversed, instead promoted as the most valuable asset.

3.8 G7FE -- Element 8: Continuous Learning

227. **The eighth G7FE calls for financial institutions to "[r]eview the cybersecurity strategy and framework regularly and when events warrant—including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned."**

228. G7FE number 8 explains, "[c]yber threats and vulnerabilities evolve rapidly, as do best practices and technical standards to address them." Therefore, "entity-specific, as well as sector-wide, cybersecurity strategies and frameworks need regular review and update to adapt to changes in the threat and control environment, enhance user awareness, and to effectively deploy resources."

A. Mapping G7FE Element 8 to Insurance Core Principles

229. G7FE number 8 may be captured by the feedback loop in enterprise risk management framework under ICP 16.10, which requires the risk management system of insurers to incorporate a feedback loop based on appropriate information, management processes and objective assessment.

B. Recommendations for Supervisors Regarding Continuous Learning

230. With regard to cybersecurity continuous learning, it may be appropriate for supervisory practices to encourage or reflect the following:

a. Insurers should adopt a cybersecurity framework premised on ensuring continuous cybersecurity amid a changing threat environment.

b. Insurers should implement cyber risk management practices that go beyond reactive controls and include proactive protection against future cyber events.

c. Predictive capabilities and anticipation of future cyber events are based on analysing activity that deviates from the baseline. Insurers should work towards achieving or acquiring predictive capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity, including through outsourcing such expertise.

d. To be effective in keeping pace with the rapid evolution of cyber threats, an insurer should implement an adaptive cybersecurity framework that evolves with the dynamic nature of cyber risks and allows the insurer to identify, assess, and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. An insurer should aim to instill a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

e. An insurer should systematically identify and distil key lessons from cyber events that have occurred within and outside the organization in order to advance its resilience capabilities. Useful learning points can often be gleaned from successful cyber intrusions and near misses in terms of the methods used and vulnerabilities exploited by cyber attackers.

f. An insurer should actively monitor technological developments and keep abreast of new cyber risk management processes that can more effectively counter existing and newly developed forms of cyber attack. An insurer should consider acquiring such technology and know-how to maintain its cybersecurity, including through outsourcing such expertise.

g. As methods for cyber risk quantification continue to develop, insurers may consider using metrics to assess cybersecurity maturity against a set of predefined criteria, such as operational reliability objectives. Benchmarking enables an insurer to analyse and correlate findings from audits, management reviews, incidents, near misses, tests and exercises, as well as external and internal intelligence.

C. Examples of Current Practices

231. **Germany**. According to BaFin's draft circular on IT requirements the management board is responsible for ensuring that the regulations for the organisational and operational IT structure are determined on the basis of the IT strategy and that they are

amended to reflect any changes in the institutions' activities and processes as soon as possible.

232. **Québec, Canada**. The AMF Business Continuity Management Guideline recommends that insurers periodically verify the reliability of their business continuity plans. Technological and procedural changes as well as changes in the roles and responsibilities of employees may affect the plans' reliability. It is therefore important that its reliability be verified on a regular basis. The AMF expects the business continuity management process to be a dynamic one that takes into account any changes affecting the insurer, outside parties and its environment.

233. Furthermore, the AMF self-assessment tool made available to the insurers recommends that institutions designate a specific person to be in charge of developing and implementing a cybersecurity framework and its plans. It recommends that insurers validate, according to a pre-established frequency, the effectiveness of its response and recovery plans using cyber attack simulation exercises. And finally, following material cyber incident, an ex post examination should be performed to document the chronology of events, identify deficiencies in controls and management processes and establish a recovery plan.[82]

234. **United Kingdom**. The FCA routinely requests lessons learned reports and root cause analysis from regulated firms who are the subject of technology outages or cyber attacks, to ensure that incidents allow for the opportunity for continuous learning. Business Continuity plans are expected to be reviewed at least annually, and the CCG initiative allows for the lessons learned by one firm subject to cyber-attack to be shared with others.

235. **United States**. Section 4G of the NAIC *Insurance Data Security Model Law* requires the insurer to monitor, evaluate, and adjust the Information Security Program based on changes in technology, changes in the sensitivity of the information stored on the network, internal or external threats to information, and the insurer's own changing business arrangements.

236. The *Examiner's Handbook* includes testing provisions both for how an insurer updates its security program for information gained from information sharing groups and collectives, and from past incidents and breaches. Handbook guidance also highlights the importance of insurers' continually updating their cybersecurity programs. The guidance specifically highlights that while unsuccessful cybersecurity events may not have significant regulatory implications (fines, reporting, etc.), they represent important occurrences that should be studied by company officials and leveraged as an opportunity to identify how the security program can be enhanced.

237. Section 500.05 of the NYDFS *Cybersecurity Requirements for Financial Services Companies* requires that the insurer perform monitoring and testing developed in accordance with its Risk Assessment to assess the effectiveness of its cybersecurity program. Section 500.14 requires that the insurer provide for regular cybersecurity awareness training for all personnel.

[82] AMF, *Business Continuity Management Guideline* (April 2010), available at https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

238. Section 500.17 of the NYDFS *Cybersecurity Requirements for Financial Services Companies* requires the insurer, through its Board of Directors or a Senior Officer, to certify compliance with the regulations. When an insurer "has identified areas, systems or processes that require material improvement, updating or redesign," the insurer is required to "document the identification and the remedial efforts planned and underway to address such areas, systems or processes."

D. Assessing Outcomes of G7FE Element Eight

239. For G7FE number Eight, the desirable outcomes proposed by the G7 are:

240. **G7FEA Outcome 1 – The Fundamental Elements (G7FE) are in Place**. Discussed above at Paragraph 72-73.

241. **G7FEA Outcome 5 –There is a Culture that Drives Behaviour**. Discussed above at Paragraph 224-226.

4.0 Case study – De Nederlandsche Bank

242. For several years, De Nederlandsche Bank (DNB) has used a framework to assess the level of information security maturity within the Insurance Sector. Cybersecurity is reviewed as part of information security. The framework is based on COBIT and a selection of 54 included control objectives was made in close consultation with the Industry, which led to an accepted model for information security supervision ("DNB's assessment framework").

243. Each year DNB conducts information security reviews at a selection of insurers to determine the extent to which information security at these institutions meets the required level. Insurers are subject to a principle-based assessment, whereby the nature of the sector and the operational management of the specific institution are taken into account. The annual selection of institutions for review comprises follow-up assessments and assessments at institutions not previously selected for an information security review. The latter are called baseline measurements. The intention is to cover every insurer once every three years, until the minimal acceptable level of maturity is reached. It is expected that insurers themselves will frequently assess the quality of their information security and, if necessary, take steps to improve it. Insurers can make use of DNB's assessment framework to do so.

244. In order to determine the level of information security, DNB's assessment framework uses a COBIT based maturity model, which provides an outline of the required level. In general, an insurer's controls should have a minimum maturity level of "3"—meaning that the control is designed and operating effectively throughout the entire period. This applies to 51 of the 54 controls. For the three controls related to Risk Management, a maturity level of '4' is required.

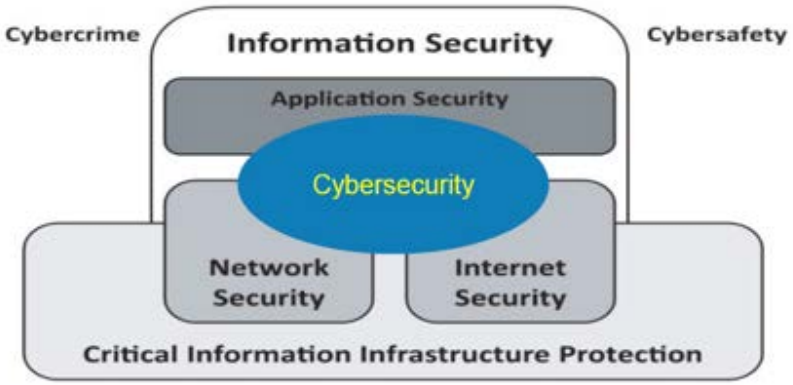
245. The table below sets out the definition of maturity levels considered in DNB's assessment framework.

Level:	Definition of control:
0	**Non-existent** - No documentation. There is no awareness or attention for certain control.
1	**Initial/ad hoc** - Control is (partly) defined, but performed in an inconsistent way. The way of execution is depending on individuals.
2	**Repeatable but intuitive** - Control is in place and executed in a structured and consistent, but informal way.
3	**Defined -** Control is documented, executed in a structured and formalized way. Execution of control can be proved.
4	**Managed and measurable -** The effectiveness of the control is periodically assessed and improved when necessary. This assessment is documented.

Level:	Definition of control:
5	**Optimised** - An enterprise wide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.

246. Supervision on information security is supported through a self-assessment completed by the annually selected insurers and, thereafter, challenged by a team of supervisory IT experts on-site at the insurer.

247. Within the framework of the information security reviews, DNB requests the selected insurers to complete DNB's assessment framework, which is a self-assessment. These insurers are requested to self-assign a maturity level to the 54 controls that DNB considers essential for ensuring adequate information security. Further, DNB requests institutions to substantiate the levels they assign with documentary evidence, and to ensure an independent party or department (preferably an internal or independent external auditor) validates the self-assessment.



Relationship between Cybersecurity and other security domains

248. The on-site challenge by the supervisory IT experts is performed on a selection of controls that could differ on a yearly basis. Every year the selection is applied for all insurers subject to inspection in that year. The inspection team ensures that at a minimum a number of “cyber-related” controls are selected. The assessment covers information security policy (including cybersecurity), governance of cybersecurity, risk assessment, physical security, systems security, personnel training and awareness, monitoring and testing, incident assessment, communications, business continuity, and third parties. DNB analyses the plausibility of the assigned maturity levels on the basis of

spot checks, makes adjustments to these levels where necessary, and then processes the established maturity levels.

249. In those cases where maturity levels are ultimately determined by DNB to be below the standard, DNB requests the institution to submit an improvement plan. DNB monitors the realisation of these improvement plans in its ongoing supervision or through specific risk mitigation programmes.

250. After the challenge sessions, the outcome of the self-assessment is benchmarked with other similar financial institutions for feedback to the insurer and to determine additional supervisory measures. In addition, the results of the self-assessments are published in generic (anonymized) form on DNB's website. The main results of 2017 are:

- The maturity level of information security in the sector is increasing;
- Information security is not yet at the required maturity level;
- Information security throughout the entire chain (including all service providers) is still inadequate;
- The quality of IT risk management must be improved;
- There is strong variation in institutions' explicit attention to cyber controls;
- The cyber threat level is changing; greater cooperation within the sector is required.

5.0 An Approach to Assessing Insurers' Cybersecurity Practices

251. Section 3 above offers guidance on potential components of an effective approach to insurer cybersecurity, keyed to the eight G7FE elements.

252. Jurisdictions may develop supervisory requirements or expectations based on the practices, controls, and desirable outcomes addressed in Section 3 (including, if appropriate, considerations of jurisdictional and entity cyber maturity, as well as the principle of proportionality).

253. This section of the Application Paper addresses considerations for establishing an effective approach to assessing the degree to which insurers are progressing toward or exhibiting compliance with cybersecurity expectations.

254. As used here, assessment means "the systematic collection, review, and use of information on the cybersecurity practices and controls" of individual insurers or the sector collectively "for the purpose of: (i) judging performance, measured against intended outcomes; and (ii) providing feedback and setting out areas for improvement, including remedial actions."[83]

255. Having in place a means of assessing insurers' progress and compliance with expected cybersecurity outcomes should be viewed as an important supervisory role. In developing such an assessment programme, supervisors should consider the "assessment components" proposed in Part B of the G7FEA, summarized below.

256. Depending upon available expertise and other resources, outsourcing of some components of an assessment programme may be appropriate.

257. Embedding the following attributes may be considered when planning and designing effective programmes for conducting cybersecurity assessments:

A. Supervisors / Assessors Establish Clear Assessment Objectives and Communicate Those Objectives to Insurers.

258. As described in the G7FEA, it is important that assessors "establish explicit goals for assessment activities to provide clarity of motivation to both assessor and assessed entity and to facilitate accountability."[84]

259. Both the assessor and the insurer should understand the scope of the assessment – particularly "the aspects of cybersecurity under review."[85] For example, if the supervisor has established expectations for insurance sector cybersecurity as described in this Application Paper, the assessment objective may be to evaluate an insurer's performance against some or all of the expected practices and outcomes.

[83] G7FEA page 3.

[84] G7FEA page 4.

[85] G7FEA page 4.

B. Supervisors / Assessors Set and Communicate Methodology and Expectations.

260. As described in the G7FEA, assessors should "establish clear and measurable expectations against which cybersecurity assessments are to be conducted," and the expectations should be "communicated to, and understood by" the insurer before the assessment begins.[86]

261. "The methodology selected by assessors is aligned to the stated objectives and the complexity of the entity under assessment. Proportionality of assessment can be achieved by following a risk-based approach, taking into account the complex and dynamic nature of the cyber risk."[87]

C. Supervisors / Assessors Maintain a Diverse Toolkit and Process for Tool Selection.

262. As described in the G7FEA, assessors should have a range of assessment techniques and methods available "to reflect the specific breadth, depth of coverage, or maturity sought in a given assessment."[88]

263. Not every assessment will necessarily be on-site, or cover the same breadth of issues. The G7FEA, for example, notes that a "toolkit" for cybersecurity assessment might include, among other techniques and methods: desktop reviews; self-assessments; on-site inspections; threat-based penetration testing; technical reviews; thematic reviews; and exercises – and that such tools can be used singly or in combination.

264. Assessors should determine, ideally through a defined process, which tools are appropriate for the objectives of a particular assessment. The G7FEA suggests that the selection process should "use factors such as the importance and inherent risk of entities to the wider sector; the specific nature and scope of the assessment; the resource and time to be expended on the assessment; and the level of assurance being sought."[89]

D. Supervisors / Assessors Report Clear Findings and Concrete Remedial Expectations.

265. As described in the G7FEA: "Effective security assessments deliver meaningful output to drive decisions and actions. This means developing clear conclusions and identifying concrete remedial measures and/or thematic findings that can lead to future action."[90]

266. "When drawing a key conclusion, assessors summarize observed practices and achievements, and identify gaps or shortcomings against expectations as they emerge from the facts gathered. Assessors describe any associated risks or other issues and the implications therein. Overall, the output of assessments provides value, supports

[86] G7FEA page 4.

[87] G7FEA page 4.

[88] G7FEA page 4.

[89] G7FEA page 4.

[90] G7FEA page 5.

decision making, and generates feedback that leads to significant and sustained improvement."[91]

267. Consider auditing the assessment results and sharing knowledge. Technical competence and assessment quality can be "maintained by independent reviews (i.e., assessing the assessor) of assessments performed and methodologies adopted" as well as through "knowledge sharing between assessors; and individual assessor evaluations."[92]

E. Supervisors / Assessors Ensure that Assessments are Both Reliable and Fair.

268. As described in the G7FEA, to be credible, cybersecurity assessments should be both reliable and fair. Among other factors, assessors must have and maintain both the technical background, industry knowledge, and experience sufficient to conduct the assessment. The process should be transparent to the insurer under assessment, and the findings (shared with the insurer under assessment, per above) should be in confidence to the degree appropriate. The principle of proportionality is also relevant to fairness.[93]

[91] G7FEA page 5.

[92] G7FEA page 5.

[93] G7FEA page 5.

6.0 Conclusion

269. Building on the related 2016 Issues Paper, this Application Paper is intended as a resource to assist supervisors in developing programmes to ensure that insurers under their jurisdiction are appropriately cognizant of the necessity to develop and maintain cyber resilient organizations.

270. Based on the proportionality principle, the regulation and supervision of jurisdictions should be tailored to the specific conditions and characteristics of the jurisdiction, allowing solutions that are adequate to achieve outcomes consistent with the ICPs without becoming excessive. Notwithstanding the proportionality principle, and as originally described in the Issues Paper, "cyber resilience must be achieved by all insurers, regardless of size, speciality, domicile, or geographic reach."

271. Doing so will likely remain a substantially challenging and ongoing endeavour. Recognizing that achieving perfect cybersecurity is at most an aspirational goal, supervisors have an important role in leveraging the work of experts (both public and private sector), such as those referenced in this Application Paper, to develop applicable expectations for the cyber resilience of insurers under their jurisdiction, and holding insurers accountable to those expectations.

272. For insurers to maintain the confidence of policyholders and policy makers in each jurisdiction and for the insurance sector to continue operating as a responsible component of the national and global financial systems, supervisors may consider steps such as those described in this Application Paper to develop and implement standards, tools, and metrics for protecting the confidentiality, integrity, and accessibility of systems and customer data of insurers under their jurisdiction.

273. The interests of supervisors and responsible insurers in protecting the financial system, individual institutions, and policyholders from cybersecurity risks, while avoiding regulatory fragmentation and overlap, are aligned. Accordingly, consultation and coordination among regulators and insurance industry stakeholders should be encouraged as jurisdictions develop and improve supervision of insurer cybersecurity.