FINANSINSPEKTIONEN

FI supervision

Governance and Control of ~~Information and Communications~~ Technology Operations in Insurance Undertakings

No. 8

15 November 2018

15 November 2018
Ref. 18-9203

CONTENTS

FI supervision

Finansinspektionen frequently publishes supervision reports in a numbered series. These supervision reports are part of FI's communication. The reports describe the thematic investigations and other supervision carried out by FI. Through these reports, we present the observations that FI has made and its expectations in various matters. This information can support firms in their operations.

Summary

The digitalisation of the financial sector is increasing. This report shows that insurance undertakings in general employ adequate governance and control practices in their ICT operations, but FI also observed that some undertakings have difficulties identifying and managing the consequences of outsourced ICT operations. One important reason for this is that outsourced operations are not as transparent as when operations are conducted in-house.

As the digitalisation of the financial sector increases, creative innovations lead to new insurance products, business models and partnerships, which in turn require a higher level of risk management, governance and control of ICT operations. This is particularly the case in the governance of outsourced ICT operations since outsourced operations are not as transparent as operations conducted in-house.

However, outsourcing can lead to both better service quality and cheaper ICT operations, and new or small actors, with the assistance of professional ICT firms, can thus offer modern and comparatively cheap insurance services in markets where they would otherwise have been uncompetitive.

The scope and extent of ICT outsourcing agreements can have a large impact on an insurance undertaking's ability to overview and manage the consequences of its strategic ICT choices. Given the increased digitalisation of the insurance sector, FI's analysis points to a number of focus areas in need of improvement:

- Updated ICT strategies;
- A complete overview of ICT service providers, including those that do not contribute to the provision of ICT services that are of material importance;[1]
- Description of the impact of outsourcing on the insurance undertaking's business;
- The written outsourcing policy;
- Exit strategies for outsourced critical or important functions or activities;
- Regular control of the outsourced operations to determine if the risk assessment performed at the time of the outsourcing arrangement is still relevant;
- Regular tests of business continuity plans;

1 Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) and EIOPA's guidelines for corporate governance systems, EIOPA-BoS-14/253 (the Guidelines) uses the term "critical or important operational functions or activities". The Insurance Business Act (2010:2043) uses the term "operational activities or functions of material importance".

- Understanding of operational risks in the ICT governance processes;
- Training in and systematic monitoring of cyber risks.

Background, Aim and Implementation

As the digitalisation of the financial sector increases, creative innovations are leading to new insurance products, business models and partnerships that are placing greater demands on insurance undertakings' risk management, governance and control of their ICT operations.

Industry-wide questionnaire 2016

In 2016, FI conducted a questionnaire study[2] that covered all Swedish insurance undertakings. One of the observations from this study was that 60 per cent of all ICT-related incidents were related to internal or external infrastructure. FI also observed that there was extensive outsourcing within ICT operations, that the use of cloud services was growing and that certain service providers could constitute a concentration risk.

Cyber risks in focus 2017

The number of cyber-attacks increased markedly in 2017. In its Christmas letter to insurance undertakings in December 2017, FI underlined the importance of security measures and appropriate contingency plans for enabling these companies to prevent and manage cyber risks. FI also pointed out the need for particularly strong governance and control of outsourcing within ICT operations in light of the risks identified in 2016 and 2017.

In-depth analyses 2018

Between February and May 2018, in-depth analyses were conducted of a selection of insurance undertakings in order to follow up the insights from 2016 and 2017 and improve FI's knowledge of insurance undertakings' governance and control of their ICT operations. The insurance undertakings were selected primarily on the basis of the model they had chosen for provision of their ICT operations with regard to ICT service providers that were both external and within the same group.

FI first audited the companies' ICT strategies, written outsourcing policies and contingency plans. Site visits were conducted in April and May, during which the seven selected insurance undertakings described in detail the governance and control of their ICT operations, focusing specifically on outsourcing.[3]

Insurtech 2019

New innovative insurance products and new technological opportunities are one of the reasons why FI chose in 2018 to analyse the governance and control of ICT operations, focusing specifically on outsourced operations. New technology, new business models and new partnerships are placing greater demands on operational risk management, governance and control. Consequently, FI would like to ensure that the interpretation and application of the Swedish regulations applicable to ICT operations within insurance undertakings are relevant and reasonable in relation to the changes we

2 See https://www.fi.se/sv/publicerat/nyheter/2016/resultat-av-enkat-till-forsakringsforetag/

3 See agenda, Appendix 1.

see in the insurance market. This work will continue in 2019, both in partnership with EIOPA[4] and in the form of a dialogue with Swedish insurtech companies.

4 FI participates in EIOPA's Insurtech Task Force.

Strategy

The scope and extent of ICT outsourcing can have a major impact on an insurance undertaking's ability to gain an overview of and manage the consequences of its strategic ICT choices. In some cases, the ICT strategies audited were also outdated. Some insurance undertakings do not have an overview of those of their service providers that are not contributing to the provision of material[5] ICT services. In general, the description of the impact of outsourcing is incomplete.

ICT STRATEGY

An insurance undertaking shall have a clearly defined risk management strategy that is consistent with the undertaking's overall business strategy. The objectives and key principles of the strategy, the risk tolerance limits and the assignment of responsibilities across all the activities of the undertaking shall be documented[6]. It is therefore important that the objectives and focus of the undertaking's ICT operations are consistent with the business strategy.

The documentation sent to FI by the insurance undertakings ahead of the site visits mainly contained their strategic choices and considerations for ICT operations in relation to their insurance operations. In some cases, however, the content was outdated.

During the subsequent site visits, the undertakings were able to describe how they worked with strategic ICT issues in practice, especially in relation to their most important service providers. There are some undertakings where FI sees a clear link between written policies, processes and strategies, while at others, it is more difficult to assess how strategic choices are put into practice.

FI observed cases in which certain strategies lead to practical problems with governance and control. The organisational choices that had been made were beneficial from the perspective of costs, but impaired certain important stakeholders' opportunities to influence the priorities of ICT operations. In some boards, decision-making items were, in practice, information points.

When it comes to the strategic choices an insurance undertaking makes for its ICT operations, FI places great importance on the following questions:

- How does the undertaking determine whether its systems, resources and procedures are appropriate in relation to its continuity requirements?[7]

5 In the supervision report, the term "material" is used where "critical or important" is used in the text of some legislation.

6 Article 259(1)(a) of the EU regulation.

7 Chapter 10, Section 3 of the Insurance Business Act.

- How does the undertaking identify and evaluate risks within its ICT operations in relation to other strategic risks that are affected by the ICT risks:[8]
    - in conjunction with changes to the undertaking's business strategy?[9]
    - in major projects and investments?[10]
- How are new ICT requirements identified, assessed and managed in relation to the undertaking's overall business objectives?[11]

FI's assessment is that the insurance undertakings are generally able to describe this, but the extent of outsourcing, both within and outside of the group, may have a major impact on an undertaking's ability to obtain an overview of and manage the consequences of strategic ICT choices. The structure of the ICT organisation and its decision-making processes may also have a major impact on the potential for success. For example, it may be the case that formal processes are ineffective, outdated, benefit special interests or are simply not applied.

STRATEGIC CHOICES FOR ICT PRODUCTION

One important strategic choice for an insurance undertaking is determining how its ICT operations shall be run and by whom. In the in-depth analysis, FI requested that the insurance undertakings describe the structure of service provision for the whole of their ICT operations, i.e. ICT services that

a) are produced within the undertaking;

b) are provided by subsidiaries, sister companies or parent companies;

c) are provided by external parties via subsidiaries, sister companies or parent companies;

d) are provided by external parties directly to the undertaking;

e) are provided by external parties' subcontractors, or where external parties' subcontractors contribute to the provision of a service.

FI detected shortcomings in the description of services in cases where service providers' subcontractors undertake or contribute in some way to the provision of an ICT service. These shortcomings may derive primarily from the fact that the undertaking draws a line for how far back in the supply chain it is reasonable to exercise control. In general, the insurance undertakings draw this line at outsourced operations that are deemed to be of material importance.

Without a complete overview of the architecture of its ICT production, it is difficult for an insurance undertaking and its decision makers to determine how various types of change to its operations affect or are affected by changes to its supply chain and its ICT

8 Chapter 10, Section 6 of the Insurance Business Act.

9 Article 262(1)(a) of the EU regulation.

10 Article 269(1)(d) of the EU regulation.

11 Article 258(6) of the EU regulation.

infrastructure. Without this type of overview, it is also difficult to judge whether a part of the architecture is becoming more or less important or more or less vulnerable as time goes by. Having a complete overview of the supply chain does not mean that an undertaking needs to apply the same principles for risk management, governance and control to all service providers.

Governance and Control

The insurance undertakings generally use proven and adequate models for their governance and control and ICT operations and collaboration with ICT service providers. The scope of the written outsourcing policy differs between the insurance undertakings. The policy documents that FI has audited were of varying quality and were often supplemented by other documents or procedures for compliance with statutory requirements. Some insurance undertakings lack a clear exit strategy for outsourcing agreements.

WRITTEN OUTSOURCING POLICY

A written outsourcing policy is required pursuant to Chapter 10, Section 2 of the Insurance Business Act[12]. This policy shall be adopted by the board of directors each year.

The scope of the written outsourcing policy differs between the insurance undertakings that were included in the in-depth analysis. FI was not able to establish from the policies audited whether all the regulatory requirements[13] were fulfilled, in spite of there being references to the requirements in these policies. However, dialogue with the undertakings revealed that what was missing from the written policies was often to be found elsewhere, albeit more or less well documented.

Where the written policy is supplemented by other instructions or procedures, there should be explicit references to these so that it is possible even for inexperienced employees, substitutes or new resources to perform tasks without failings or delays.

There were no persistent weaknesses that were shared by all of the insurance undertakings. The shortcomings observed by FI differed between undertakings and some undertakings had written policies with only isolated shortcomings.

FORMAT OF AGREEMENTS

In the in-depth analysis, FI requested that the insurance undertakings describe the format of their agreements[14] according to a selection of the following statutory requirements:

- The insurance undertaking's and FI's right to information concerning the activities or functions encompassed by the outsourcing agreements.[15]
- The insurance undertaking's and FI's right to conduct on-site inspections in the service provider's premises.[16]

12 Insurance Business Act (2010:2043).

13 Article 274 of the EU regulation and Guideline 63 in the Guidelines.

14 Agreements pertaining to critical or important ICT services.

15 Article 274(4)(h) of the EU regulation.

16 Article 274(4)(h) of the EU regulation.

- FI's right to address questions directly to the service provider.[17]
- That the service provider's duties and responsibilities are not affected by any sub-outsourcing.[18]
- The insurance undertaking's right to terminate the outsourcing agreement without detriment to the continuity or quality of the provision of services to policyholders.[19]

All of the insurance undertakings that were audited were able to demonstrate that the agreements included in the in-depth analysis contained clauses that covered these rights and obligations. The insurance undertakings were also able to provide examples of on-site inspections at service providers that were conducted without restrictions.

As stated in the memorandum that FI has published previously on the matter of audit rights and cloud services[20], the issue of audit rights is by no means straightforward, particularly with regard to small insurance undertakings and their bargaining position in relation to large service providers. FI's view is that audit rights be non-negotiable, but that the application of this must be determined by the insurance undertaking on a case-by-case basis.[21]

The EU regulation's section on outsourcing agreements states that service providers are under obligation to disclose any development which may have a material impact on their ability to carry out the outsourced functions and activities effectively and in compliance with applicable laws and regulatory requirements.[22]

FI's interpretation is that this is applicable not simply to planned events such as upgrades, changes of premises or new owners, but also to operational phenomena, incidents and near misses that by chance did not affect provision of the ICT service. Examples of such events can be high staff turnover, lack of staff in key positions or physical or digital intrusion in the production environment that does not result in production anomalies.

COLLABORATION WITH SERVICE PROVIDERS

An outsourcing agreement does not limit an insurance undertaking's liability[23] and the quality of the insurance undertakings' corporate governance system may not be impaired materially when operations are outsourced.[24] An insurance undertaking must be able to demonstrate that governance and monitoring of its ICT operations are

17 Article 274(4)(i) of the EU regulation.

18 Article 274(4)(k) and (l) of the EU regulation.

19 Article 274(4)(e) of the EU regulation and Guideline 63(d) in the Guidelines.

20 See *Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer* [Finansinspektionen's view on the audit right for operations that are outsourced to providers of cloud services], which is published at fi.se.

21 "Non-negotiable" means that an outsourcing agreement for ICT operations must encompass a minimum of the audit right stipulated under the applicable statutory requirements.

22 Article 274(1)(c) of the EU regulation.

23 Chapter 10, Section 19 of the Insurance Business Act.

24 Chapter 10, Section 20, point 1 of the Insurance Business Act.

fit for purpose[25] and that these operations are compliant with the requirements concerning risk management[26].

What this means in practice is that collaboration with service providers within ICT operations shall encompass the following:

- There shall be effective cooperation, internal reporting and communication of information at all relevant levels in the collaborative model.[27]
- The collaborative model shall clearly specify reporting lines and allocate functions and responsibilities.[28]
- The collaborative model shall take into account the nature, scale and complexity of the risks inherent in the undertaking's business.[29]
- There shall be information systems which produce complete, reliable, clear, consistent, timely and relevant information concerning the business activities, the commitments made and the risks to which the undertaking is exposed.[30]
- The operational risk management policy shall identify which risks there are and how these can be mitigated, define activities and processes for managing the operational risks, including the ICT systems that support them, and shall specify the risk tolerance limits for the most important operational risks the undertaking might be exposed to.[31]
- The monitoring and reporting mechanisms within the internal control system should provide the undertaking's administrative, management or supervisory body with relevant information for decision-making processes.[32]
- Emerging risks at the operational, tactical and strategic levels shall be identified, assessed, compiled and escalated, including the ICT systems affected.[33]
- It shall be possible to establish risk tolerance limits for the areas that are most important with respect to the undertaking's exposure to operational risk.[34]

All insurance undertakings that were included in the analysis have collaborative models that encompassed operational, tactical and strategic meetings and information sharing. The insurance undertakings' representation in the various forums were very similar,

25 See in particular Article 258(1)(b) and (j) of the EU regulation.

26 Articles 259(1)-(3) and 260(1)(f) of the EU regulation.

27 Article 258(1)(a) of the EU regulation.

28 Article 258(1)(b) of the EU regulation.

29 Article 258(1)(b) of the EU regulation.

30 Article 258(1)(h) of the EU regulation. This requirement applies regardless of whether a function or activity is performed within the insurance undertaking or by a service provider. ref. Chapter 10, Section 19 of the Insurance Business Act.

31 Guideline 21 in the Guidelines.

32 Guideline 39 in the Guidelines.

33 Article 260(1)(f) and 269(1)(e) of the EU regulation and Guideline 21 in the Guidelines.

34 Guideline 21(c) in the Guidelines.

aside from at the strategic level, where some insurance undertakings had chosen not to involve their managing director, while others did so as a matter of course.

FI also observed that the format of the collaborative model was dependent to some extent on the insurance undertaking's bargaining position. Some large ICT service providers tailor their collaborative models to suit the insurance undertaking's requirements, while others are less flexible. Some service providers accept the insurance undertaking's standardised agreement as a basis for the provision of services, while others provide services on the basis of their own standard agreements.

FI would like to underline the fact that an insurance undertaking's need to comply with the regulatory requirements places stringent demands on the transparency of service providers, regardless of which templates are used as the basis of the outsourcing agreements.[35]

FI is able to conclude that the insurance undertakings generally have a good overview of their ICT service providers, but that comparable insurance undertakings that purchase the same ICT services from the same service provider made different assessments of the ICT service providers' and their subcontractors' relevance with respect to governance and control.

The differences in the assessments are primarily due to different opinions on how reasonable it is to monitor peripheral subcontractors and difficulties in drawing clear boundaries for how different types of services are to be categorised[36]. However, the differences are also the result of experience gained by the insurance undertakings when testing contingency plans. Accordingly, this demonstrates the importance of regularly testing contingency plans in order to make collaboration, governance and control within ICT outsourcing fit for purpose.

SPECIFIC OBSERVATIONS CONCERNING CLOUD SERVICES

Outsourcing agreements may not pertain to operational activities or functions that are of material importance if this may lead to a substantial increase in the undertaking's operational risk. Consequently, insurance undertakings must be able to describe, among other things, the information security and physical security procedures applied in its infrastructure, regardless of where the information is stored or processed.

Insurance undertakings must also decide themselves whether risk management, governance and control of each part of their ICT operations are adequate given the various services' importance to insurance operations and in light of the requirements concerning risk management, consumer protection, privacy and continuity.[37]

35 See also the section on cloud services.

36 For example, "what is a cloud service", "what is a system", "what is a function".

37 See also *Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer*, which is published on FI's website.

In those case where FI discussed cloud services with the insurance undertakings in the in-depth analysis, a great deal of emphasis was placed on understanding the undertakings' geopolitical intelligence-gathering and how this influences the insurance undertakings' decisions and monitoring of cloud services.

FI's assessment is that the insurance undertakings' governance and control are generally adequate in relation to the structure of cloud services, but that the insurance undertakings should have a clear understanding of the political systems and practices in the countries where their data is stored or processed.

TERMINATION OF OUTSOURCING AGREEMENTS

The insurance undertakings in the analysis were able to demonstrate that they secured the right to terminate an agreement without detriment to the continuity or quality of the provision of services to policyholders. However, on the matter of documentation of the undertaking's exit strategy for outsourcing agreements that cover critical or important functions[38], it appeared that some of the strategies consisted simply of rudimentary plans at the level of a project template. Accordingly, the approach in practice was to draw up a plan as and when this was required.

The explanation given for this was that the outside world and circumstances change so rapidly that the exit strategies would need to be constantly updated. In order to avoid the risk of having an outdated plan when it is actually needed, a decision was made to instead simply have a template.

Although there is some reason to this argument, FI is of the opinion that a rudimentary project template for terminating an outsourcing agreement is not sufficient. Exit and withdrawal strategies should contain concrete activities that the insurance undertaking intends to implement, and these activities should be described in such detail that it is possible to decide if and how and under what conditions their implementation will be possible. The majority of the insurance undertakings succeeded in explaining this to FI.

Please note that when procuring important ICT services, the process normally includes the purchaser deciding which exit strategy is to be applied if and when the agreement is terminated. The scope of the exit strategy is therefore included in the documentation on which the undertaking bases its decisions when choosing service providers for the purpose of creating awareness of and preventing lock-in effects.

38 Guideline 63(d) on written outsourcing policies in the Guidelines.

Risk Management

In some of the insurance undertakings, no regular controls of the outsourced operations are conducted for the purpose of determining whether the risk assessment made at the time they were outsourced is still relevant. Regular testing of contingency plans is just as important as having them. Some of the insurance undertakings also underestimate the operational risks associated with the overall governance processes. However, all of the insurance undertakings in the analysis are working systematically to monitor cyber risks. They are also using training and the information to employees as an important part of their security measures.

ICT OPERATIONS OF MATERIAL IMPORTANCE

It shall be possible for an insurance undertaking to describe how it identifies, assesses, compiles and escalates emerging risks at the operational, tactical and strategic level in its business, including the ICT systems affected.[39] It shall also be possible for the insurance undertaking to describe what impact outsourcing has on the undertaking's business.[40]

Insurance undertakings that have entered into or are considering entering into an outsourcing agreement should specify in the written outsourcing policy which process they shall adhere to, how selection shall be carried out and how the agreement shall be followed up.[41] This specifically includes a description of the process for determining whether a function or activity is critical or important, i.e. of material importance.

FI determined that the process for establishing whether an outsourced function is of material importance was typically tied to the purchasing process and each individual procurement. The majority of the insurance undertakings analysed have processes for monitoring by some means whether the assessment has to be altered. However, FI also observed cases in which there was no such follow-up, or the processes were inadequate.

FI is of the opinion that an insurance undertaking should regularly evaluate whether the nature of outsourced services has changed, i.e. whether, over time, the services have become more or less critical to operations, or more or less vulnerable than at the time they were outsourced.[42] Emerging risks at the operational, tactical and strategic level should also be taken into account in other regular assessments of processes and procedures.

39 Article 269(1)(e) of the EU regulation and Guideline 21 in the Guidelines.

40 Chapter 10, Section 19 of the Insurance Business Act and Articles 260(1)(f) and 274 of the EU regulation.

41 Guideline 63 in the Guidelines.

42 Article 274.5 of the EU regulation and Guideline 63 in the Guidelines.

OPERATIONAL CONTINUITY

An insurance undertaking shall have contingency plans[43] and its risk management system shall include strategies for identifying, evaluating, monitoring, managing and reporting risks that it is or may become exposed to, as well as their interdependencies[44]. Accordingly, an insurance undertaking is required to supervise not just its own risk profile, contingency plans and security measures and those of its service providers, but also those of its service providers' subcontractors.

The insurance undertakings in the in-depth analysis had chosen various formats for their contingency plans. Some kept their contingency plans at an overarching level and supplemented these with check-lists and procedures contained in other documents and tools. For others, the documented contingency plans were the tool that they intended to use in an emergency situation.

As part of the in-depth analysis, FI wanted to ensure that the contingency plans fulfilled four important criteria[45]:

- A description of operations and which scenarios the plan intends to prevent and manage.
- Management options for the different scenarios.
- Introduction into operations, i.e. what to do in practice when different events occur.
- Continual improvement, i.e. regularly testing and updating the plan so that it is always up to date and relevant.

What all the audited contingency plans shared was that further explanation was required during the site visits in order for FI to gain an understanding of whether the plans had an appropriate format and are fit for purpose.

The audit also showed that realistic tests of the contingency plans did not normally lead to the conclusion that everything is proceeding as planned, rather there were always surprises, weaknesses and important new insights to be gained.

All of the insurance undertakings in the in-depth analysis were able to describe their service providers' contingency plans and the status of these.[46] FI's assessment is that the undertakings by and large have adequate contingency plans, but that there is in all of them room for improvement in some aspect of their life cycle. The fact that the undertakings regularly test the plans is critical to their ability to identify where improvement is needed.

MONITORING OF OPERATIONAL RISKS

An outsourcing agreement does not limit an insurance undertaking's responsibilities[47] and an insurance undertaking must be able to

43 Chapter 10, Section 3 of the Insurance Business Act.

44 Chapter 10, Section 6 of the Insurance Business Act.

45 This is often called the business continuity planning life cycle.

46 Article 274(5)(d) of the EU regulation.

47 Chapter 10, Section 19 of the Insurance Business Act.

demonstrate how the risk management requirements are fulfilled in its operations[48].

The operational risk management system shall include the identification, evaluation, monitoring, management and reporting of risks and their interdependencies, and the system shall be integrated into the undertaking's organisational and decision-making structure.[49]

Operational risks cover all types of ICT-related risks and the requirement to maintain adequate and orderly records of the undertaking's business and internal organisation also encompasses the undertaking's ICT operations and their organisation.[50] In the event of outsourcing, the insurance undertaking is fully liable for ensuring that the outsourced operations are run in accordance with applicable laws and other regulations. The undertaking must therefore be able to describe all parts of its ICT operations, regardless of where and by whom these are run.[51]

With regard to the reporting and monitoring arrangements[52], all the insurance undertakings in the in-depth analysis undertake some form of regular status reporting in relation to the agreed service provision. Some undertakings use scorecards with key performance indicators that are reused in tactical and strategic forums.

Written outsourcing policies or handbooks generally contain descriptions of how the undertakings are to design the control environment and apply the different types of control over their service providers. However, written outsourcing policies often do not contain references to supporting documents or to the location of a description of the impact of the outsourcing agreement on the insurance undertaking's business.[53]

In insurance undertakings that are part of an insurance group (or equivalent), there are substantial differences in terms of how much influence some of these undertakings have when sister or parent companies are providing an ICT service that is either produced centrally or provided to the entire group by an external service provider.[54] In insurance groups where the individual insurance undertaking has a strong influence, the undertaking takes part in group-wide decision-making forums where responsibilities, mandates and freedom of action are clearly defined and firmly rooted.

In insurance groups where the individual insurance undertaking has a weak influence, decisions are made centrally without the undertaking being involved to any appreciable extent. Written outsourcing policies (and even decision-making documents) may specify that the process is supposed to be different, but in practice, the insurance undertaking that has the service provided by another company in the group cannot

48 Articles 259 and 260(1)(f) of the EU regulation.

49 Chapter 10, Section 6 of the Insurance Business Act.

50 Article 258(1)(i) of the EU regulation.

51 Article 258(1)(b) of the EU regulation.

52 Article 274(1) of the EU regulation.

53 Article 274(1) of the EU regulation.

54 Article 274(2) of the EU regulation.

influence the service or decision. The decision-making point on the board's agenda is, in reality, an information item.

In summary, the monitoring of operational risks in insurance undertakings largely focuses on metrics and processes that pertain to the ICT production itself. FI is able to conclude that some insurance undertakings underestimate the monitoring and management of weaknesses that may arise in key processes that are supposed to lead to the ICT operations producing adequate services.

CYBERSECURITY AND INFORMATION SECURITY

With regard to the insurance undertakings' descriptions of cyber risks, FI's main interest was in understanding how the undertakings work with the monitoring of cyber risks generally and how they identify cyber risks that are particularly relevant to their business.[55]

None of the undertakings addressed of their own accord the issue of the degree to which risks associated with political systems and practices in third countries constitute a threat to their ICT operations. FI is of the opinion that it is important to evaluate and monitor the geopolitical situation when outsourcing ICT operations to countries outside of the EU, and also to audit the ICT service providers' ownership and group structure.

In addition to information security and physical security measures[56], the insurance undertakings' in the analysis work with training and information distribution in order to increase the risk awareness of their staff. Senior managers from the insurance business are often included in working groups that focus on cyber risks.

FI is able to conclude that all of the insurance undertakings included in the in-depth analysis work systematically with cyber risks and are able to describe what threat is constituted by different types of risk and what the impact will be on them if these occur. Many of the undertakings stress the importance of local knowledge in addition to the risks that are known globally.

However, it is apparent from the descriptions that both risks and their impact are often difficult to assess and that the knowledge of these matters that is required is becoming increasingly specialised.

55 Article 260(1)(f) of the EU regulation.

56 See separate section.

Appendix 1

INFORMATION FI REQUESTED IN ADVANCE OF THE SITE VISITS

- The written policy for operations that are covered by outsourcing agreements;[57]
- Contingency plans, including the outcome of the latest test of these plans;[58]
- A list of ICT service providers and of which services they provide;[59]
- ICT strategy or equivalent that shows how ICT operations are organised and how ICT operations aim to promote the undertaking's strategic goals;[60]
- The internal audit function's assessment of the undertaking's corporate governance system with respect to ICT operations and outsourcing agreements in the last two years, provided that the function has audited these parts during the period specified.[61]

AGENDA[62]

1. Describe the structure of service provision for ICT operations[63], i.e. which services
    a. are produced within the undertaking;
    b. are provided by subsidiaries, sister companies or parent companies;
    c. are provided by external parties via subsidiaries, sister companies or parent companies;
    d. are provided by external parties directly to the undertaking;
    e. are provided by external parties' subcontractors (or where external parties' subcontractors contribute to the provision of a service).
2. Describe the undertaking's process for determining and documenting whether a function or activity covered by an

57 Chapter 10, Section 2, first paragraph, point 4 of the Insurance Business Act.

58 Chapter 10, Section 3 of the Insurance Business Act.

59 Chapter 17, Section 5 of the Insurance Business Act.

60 Article 258(1)(b) of the EU regulation.

61 Chapter 10, Section 17 of the Insurance Business Act.

62 The agenda differed slightly between insurance undertakings, depending on their group structure.

63 Article 258(1)(b) of the EU regulation.

outsourcing agreement is a critical or important function or activity.[64]

3. Describe
    a. which of the services in points 1(a)–(e), above, are deemed to be critical or important;[65]
    b. what the format is for collaboration with the providers of these services, (e.g. follow-up and forward planning).

In points 4–7 of the agenda, below, FI would like the undertaking's descriptions to focus on a selection of services. FI will inform the undertaking of the services and service providers this concerns about a week before the meeting.

4. Describe how the undertaking monitors the operational risks associated with points 1(a)–(e), above.[66] Under this point, FI would also like the undertaking to describe
    a. the reporting and monitoring procedures that apply to *each service provider*[67];
    b. the status and scope of the service provider's contingency plans,[68] ("status" denotes when the plan was last updated and tested);
    c. what control and influence the undertaking has with respect to services provided by subsidiaries, sister companies or parent companies;[69]
    d. what control and influence the undertaking has with respect to services provided by external service providers via subsidiaries, sister companies or parent companies.[70]
5. Describe the physical and digital security in place where information is processed and stored
    a. by the undertaking;[70]
    b. by subsidiaries, sister companies or parent companies;[71]
    c. by external parties;[71]
    d. by external parties' subcontractors.[71 and 72]

64 Guideline 63(a) in the Guidelines.

65 Guideline 60 in the Guidelines.

66 Article 260(1)(f) of the EU regulation.

67 Article 274(1) of the EU regulation.

68 Article 274(5)(d) of the EU regulation.

69 Article 274(2) of the EU regulation.

70 Article 258(1)(j) of the EU regulation.

71 Chapter 10, Section 20 of the Insurance Business Act and Article 274(3)(a), (e) and (f) of the EU regulation.

72 Chapter 10, Section 20, point 3 of the Insurance Business Act.

6. Describe *the format of each agreement* with respect to
    a. the undertaking's and FI's right to information concerning the activities or functions encompassed by the outsourcing agreements;[73]
    b. the undertaking's and FI's right to conduct on-site inspections in the service provider's premises;[74]
    c. FI's right to address questions directly to the service provider that shall answer these questions;[75]
    d. the fact that the service provider's duties and responsibilities are not affected by any sub-outsourcing;[76]
    e. the right to terminate the agreement without detriment to the continuity or quality of the provision of services to policyholders.[77]
7. Describe each of the planned exit strategies for the outsourcing agreements in point 6, above.[78]
8. Describe the cyber risks the undertaking has identified that are relevant to the business and the security measures put in place by the undertaking.[79]

    What Finansinspektionen means with the term "cyber risks" is risks that arise when using electronic data and its transfer over, for example, the internet and telecommunications networks.

73 Chapter 10, Section 22, point 2 of the Insurance Business Act and Article 274(4)(h) of the EU regulation.

74 Chapter 10, Section 22, point 3 of the Insurance Business Act and Article 274(4)(h) of the EU regulation.

75 Article 274(4)(i) of the EU regulation.

76 Article 274(4)(k) and (l) of the EU regulation.

77 Article 274(4)(e) of the EU regulation.

78 Article 274(4)(e) of the EU regulation and Guideline 63(d) in EIOPA's guidelines.

79 Article 260(1)(f) of the EU regulation.

Appendix 2

TERMS AND DEFINITIONS

Cyber risks: Risks that arise when using electronic data and its transfer over, for example, the internet and telecommunications networks.

Information security: Safeguarding the confidentiality, accuracy and accessibility of information.

Insurtech: New technology and innovative solutions that make it possible to create new, better or cheaper insurance products.

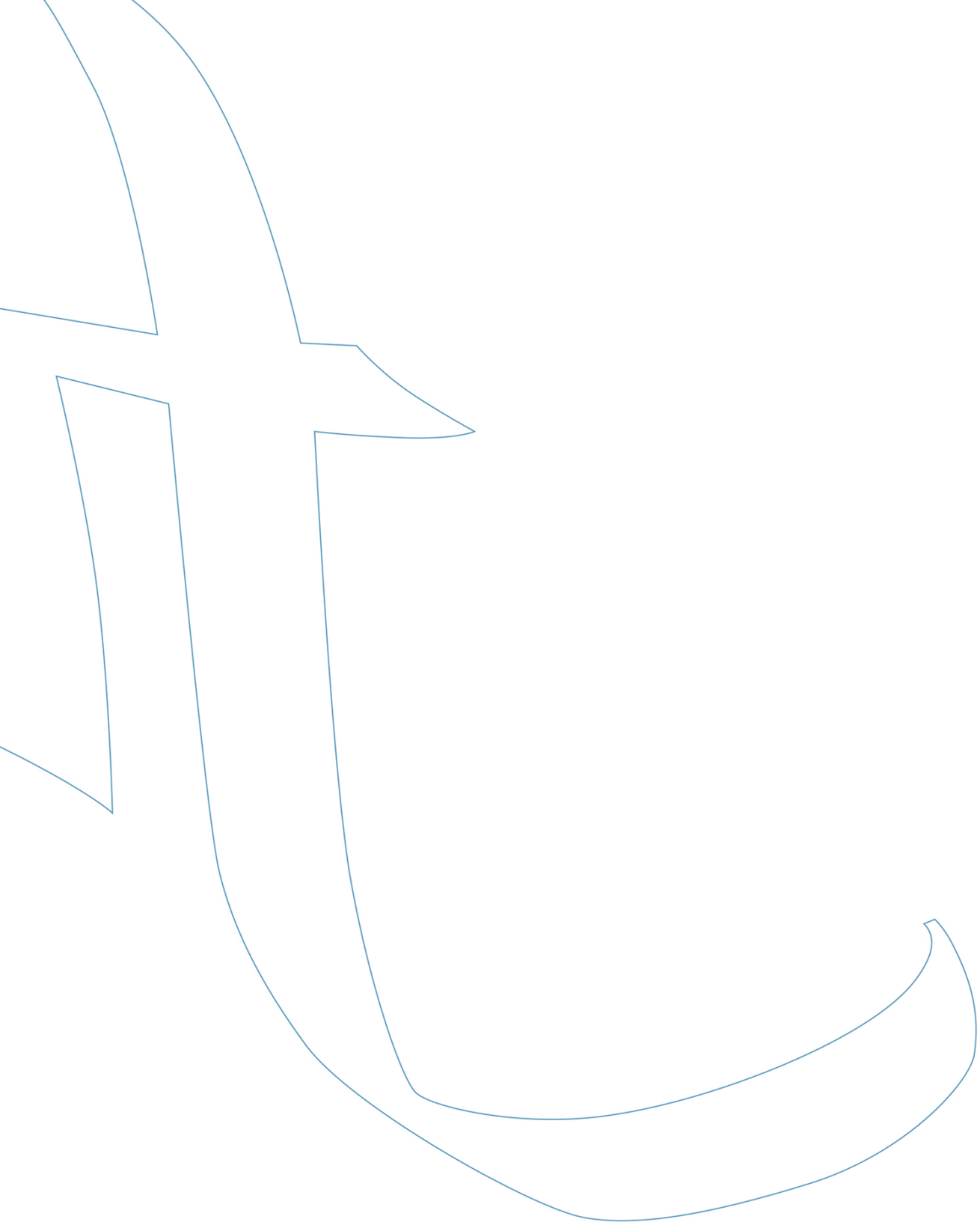
ICT risks: Risks associated with staff, processes, systems and external factors that affect ICT operations.

ICT strategy: Fundamental choices for ICT operations in order to support the critical success factors of the [insurance] business.

ICT operations: The organisation, processes and staff used by an undertaking to manage ICT systems.

Cloud services: ICT services that are provided with the help of *cloud computing*, i.e. technology infrastructure and architecture that allows simple and flexible access to computing resources by sharing capacity between a large number of users. Cloud services can be based on different types of infrastructure:

- Public cloud: accessible to the general public.
- Private cloud: only accessible within an institution.
- Community cloud: accessible to members/participants.
- Hybrid cloud: a combination of the above.



Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
Fax +48 8 24 13 35
finansinspektionen@fi.se

www.fi.se