FI Supervision

Continuity management at banks

No. 18

9 June 2020

9 June 2020
Ref. 20-11770

TABLE OF CONTENTS

FI Supervision

Finansinspektionen publishes regular supervision reports in a numbered report series. The supervision reports are part of FI's communication and describe investigations and other supervision carried out by FI. Through these reports, FI presents its observations and assessments as well as its expectations in various matters. This information can support firms in their operations.

Summary

Finansinspektionen's (FI) supervision shows that many banks are working actively with continuity management and have implemented key measures for reducing the risk of severe interruptions to their operations. At the same time, we see a need for the banks to further strengthen their continuity management. FI expects the banks to continue to focus on enhancing the resilience of their critical functions.

This supervision report is being published at the same time as the new coronavirus continues to spread. The impact of the pandemic further emphasises the importance of the banks' continuity management. Some time has passed since the banks activated their crisis management. They are updating relevant scenarios and plans for the current situation on an ongoing basis. This work has largely functioned well, but the banks' ability to sustain this work over time remains to be evaluated. Since this supervision report covers FI's supervision for 2018 and 2019, it does not specifically discuss the banks' continuity management in relation to the impact of the pandemic on the business.

Many of the banks' products and services fulfil critical functions, interruption to these services could have a major impact on consumers. Severe, recurring interruptions to the banks' services could also lead to reduced confidence in the financial system and, in a worst-case scenario, threaten financial stability.

The increasing digitalisation and globalisation combined with a change in consumer behaviour has made the infrastructure for the banks' services more complex. Many banks are making comprehensive changes to adapt their business and their service portfolio as the world around them changes. FI takes the position that this, at least in the short term, could lead to higher operational risks in the banks, with severe disruptions as one potential consequence.

In 2020, the impact of the new coronavirus has further shown the importance of preparedness for scenarios that may seem improbable not only in all sectors but in the financial sector in particular.

The banks therefore need to have robust continuity management in place that is deeply integrated into their operations and resilient to all types of events that could cause severe interruptions. Our supervision shows that the banks are working actively with their continuity management at the same time as there continues to be a need for improvement. In summary, FI would like to see in general that the banks improve their continuity management as follows:

- Strengthen the internal governance and control of continuity management, including the continuity management strategy,

risk appetite for operational risk and independent control functions.

- Further develop the methods of impact analysis to ensure that all critical functions, including those dependent on one another and on support functions, are identified.
- Clarify content and structure of contingency plans, continuity plans and recovery plans.
- Ensure that appropriate continuity tests are conducted for all significant processes and the IT systems that support these processes.
- Improve reporting of results from completed continuity tests to provide management and boards with relevant and meaningful information.

FI's supervision of continuity management

In this report, FI presents a general overview of the conclusions drawn from its supervision of the banks' continuity management during the years 2018 and 2019. This chapter describes why continuity management is prioritised in FI's supervision, FI's current view on the risk profile, and the rules the banks primarily need to follow when it comes to continuity management.

IMPORTANCE OF CONTINUITY MANAGEMENT

Continuity management can be described as processes and procedures that aim to ensure that the most critical activities in a business can be maintained at an acceptable level during a severe operational disruption. A business's continuity management also includes being able to restore operations to normal after such a severe disruption. The activities that can be classified as critical and the determination of an acceptable level are dependent on the potential impact of a disruption.

Many of the banks' products and services fulfil critical functions, and an interruption to these services could have a major impact on consumers. Severe, recurring interruptions to the banks' services could also lead to reduced confidence in the financial system and, in a worst-case scenario, threaten financial stability. The banks therefore need to have functional continuity management that is deeply integrated into their operations and resilient to all types of events that could cause severe interruptions.

In 2020, the impact of the spread of the coronavirus has further shown the importance of preparedness for scenarios that may seem improbable in all sectors and in the financial sector in particular.

RISKS OF OPERATIONAL INTERRUPTIONS

Given the increasing digitalisation and globalisation combined with a change in consumer behaviour, the infrastructure for the banks' services has become more complex. Many banks are implementing comprehensive changes within their organisations, and in their IT environments in particular, to renew their service portfolio and adapt to new regulations. This means, for example, that the banks are introducing new methods of working and IT systems while at the same time phasing out some older solutions.

This pressure to change can lead to higher operational risks at the banks, one of the effects of which could be operational interruptions. It is also often necessary to have a transition period after a new solution has been introduced until it is possible to completely remove an old solution, if removal is even possible. This means that during this period the operations will become even more complex.

Furthermore, the service portfolio and related processes and IT systems must be updated on a regular basis and adapted in order to quickly reach the market. This means that the strong pressure to change is currently a constant part of the banks' business. In addition, the banks place a large share of their operations with external

suppliers, who many times are international firms with operations in different parts of the world. These firms, in turn, might use subcontractors, which means the banks become dependent on multiple external suppliers.

Overall, it is FI's assessment that the increasing degree of complexity and the pressure to change within the banks' organisations have also resulted in a higher risk of severe interruptions to the banks' services.

RULES AND STANDARDS FOR CONTINUITY MANAGEMENT

The continuity management requirements placed on banks are based on the risk management rules set out in Chapter 6, section 2 of the Banking and Financing Business Act (2004:297). FI has also issued the following regulations and general guidelines to specify the legal requirement:

- Regulations and general guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions.
- Regulations and general guidelines (FFFS 2014:4) regarding the management of operational risks.
- Regulations and general guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems.

The European Banking Authority (EBA) has also issued guidelines[1] on continuity management within the frameworks of, for example

- guidelines for internal governance (EBA-GL-2017-11),
- guidelines on ICT and security risk management (EBA-GL-2019-04), and
- guidelines on outsourcing arrangements (EBA-GL-2019-02).

There are also a number of international standards and accepted practices that in full or in part focus on continuity management:

ISO 22301:2012, Societal security – Business continuity management systems,

Control Objectives for Information & Related Technology (COBIT),

The Business Continuity Institute Good Practice Guidelines (GPG), and

FSPOS Vägledning för Kontinuitetshantering (Guidance on Continuity Management).

In recent years, industry organisations and supervisory authorities within the financial sector have continued to work with the term *operational resilience*, which can be described as a progression of the continuity management concept. However, this supervision report focuses on the supervision FI has conducted of continuity management and will not discuss operational resilience further.

1 Guidelines issued by the EBA are to be viewed as general guidelines.

Observations from FI's supervision

The banks need to take into account their size and their nature, scope and complexity in their work to achieve sufficiently adequate and effective continuity management. They also need to have processes and controls in place based on the rules that apply[2].

GOVERNANCE AND CONTROL

Strategy and risk appetite for continuity management

FI requires the banks to have a documented risk appetite that includes all types of risks, including operational risks[3]. FI also requires the banks to have a risk strategy. The risk strategy can be viewed as a tool for the board of directors and the management teams to reasonably assure that the bank's risk exposure is in line with the established risk appetite.

The risk of severe business interruptions may be viewed as a significant operational risk that the banks' boards of directors and management teams need to actively manage. FI therefore considers it reasonable for this risk to be managed as part of the banks' adopted risk appetites. An example of risk appetite in this context could be which specific scenarios the bank must be able to handle in the event of a severe disruption.

We would like the continuity management to be an integrated part of the bank's risk strategy since it is a crucial part of how robust and resilient the bank's operating activities are in the presence of severe disruptions. Factors such as the number of data centres a bank uses and the availability of alternative worksites and remote work solutions can be key in how well a bank can maintain its most important functions in the presence of a severe disruption. The extent to which the bank has identified and managed its dependence on key staff members can also be crucial.

A bank needs in this respect to make a large number of strategic decisions. It is important for these decisions to be well-founded, deliberate and in line with the bank's risk appetite. These strategic decisions can be expressed to the bank's benefit through a strategy for continuity management. A strategy that clearly presents the bank's desired capacity and ability with regard to continuity management and the types of scenarios that the bank intends to manage or accepts that it cannot manage helps facilitate this work. For example, the bank, as part of its strategy, could account for how its most critical functions can be maintained if one data centre fails (on the condition that the bank conducts its business in two separate data centres). However, it

2 For example, the provisions set out in Chapter 6, section 2 of the Banking and Financing Business Act (2004:297), Finansinspektionen's regulations and general guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions, and (FFFS 2014:5) regarding information security, IT operations and deposit systems.

3 FFFS 2014:1

will not be possible to maintain the most critical functions if both data centres fail at the same time, the risk of which the bank must be aware. FI takes the position that this type of documented position is a central and, most importantly, understandable tool for the bank's management team and board of directors to use in their governance of continuity management. We also consider it appropriate for the bank's board of directors, which is ultimately responsible for the bank's operations, to make decisions regarding the continuity management strategy. This ensures the board's awareness of the bank's operational resilience in the event of a severe disruption as well as the board's involvement in how the bank should handle its continuity management.

Observation from the supervision of strategy and risk appetite for continuity management.
FI's observations from its supervision show that the banks can be better at designing and clarifying how the risk of severe interruptions is considered in their risk appetite. We also believe that the banks can clarify their strategies for continuity management. For example, the following can be clarified:

- Which types of events the business should be able to manage and with what means.
- Which parts of the business will be prioritised and to what extent the prioritised parts must be maintained.
- Which types of events the business reasonably cannot manage and which risks the bank thereby accepts.

FI also considers there to be room for improvement in the extent to which the banks' management teams and boards of directors are involved in these matters.

Organisation and division of responsibility
The work with continuity management, just like all other activities within the banks, must be conducted based on the principles of the three lines of defence. This means that the first line of defence, the business units, owns the risks within its area and is ultimately responsible for maintaining continuity to the extent that the bank has decided in the event of a severe disruption.

FI believes that all parts of the operational work with a bank's continuity management should be carried out in the functions of the first line of defence. *Operational work* refers in part to the various processes and procedures that fall within a bank's framework for continuity management, for example conducting impact and risk analyses, preparing continuity plans, and conducting continuity tests. This work also includes leading and coordinating the above-mentioned processes and procedures and making decisions about them. This clarifies the business's ultimate responsibility for its own continuity management.

The second line of defence, which consists of the independent control functions for risk control and compliance, should monitor and control the work that is carried out by the first line of defence. The purpose is to ensure that the business's continuity management is appropriate,

effective and follows internal and external regulations. These control functions can also fulfil an advisory role within the organisation. *Monitor and control* refers to activities such as preparing, monitoring and evaluating metrics and risk indicators that cover the bank's continuity management as well as carrying out independent controls to assess whether the processes and procedures are followed within the business and specific risks related to severe disruptions are managed effectively. Advice from the independent control functions can also be included in these activities and can consist of, for example, recommendations provided by the control functions after completing a control activity.

The third line of defence, the internal audit function, in turn should conduct independent evaluations of the continuity management work of both the first and second lines of defence while applying a risk-based approach to their audits.

Observations from the supervision of the organisation and the division of responsibility

Observations from the supervision show that the banks need to improve their organisation and division of responsibility. There are some areas that FI would like to highlight in particular.

The independent control functions in the second line of defence in some cases have been responsible for parts of the continuity management, which could have a negative impact on their independence. We have found examples where control functions are responsible for the coordination of the bank's continuity management and thus run the operational work related to the bank's continuity management. We have also found examples where an independent control function, instead of the business units, makes decisions about which practical continuity-related solutions the units in question should use.

FI also believes that the independent control functions in the second line of defence can increase the number of and improve the risk-based controls of the continuity management. We have noted in our supervision that these activities in some cases appear neither to be sufficiently in-depth nor to sufficiently highlight the actual risks. One example of this is that the controls have focused solely on whether the business units properly filled in the check lists instead of reviewing whether the units' continuity management is effective in practice.

Furthermore, FI would like to point out the importance of the internal audit function evaluating in its risk assessments the appropriateness and effectiveness of the bank's continuity management. This also includes evaluating if the risk control function and the compliance function have had sufficient and effective monitoring and control of the area. The internal audit function, based on this assessment, needs to adapt the scope and intensity of its own audits of the bank's continuity management.

FI would also like to highlight that there are several good examples related to the organisation and the division of responsibility. For example, we observed that committees or forums had been established to focus on continuity management and they included decision-makers

from all business areas within the bank[4]. Another good example is the establishment of specific continuity management functions within the business units that have overall responsibility for coordinating the bank's continuity management. FI also observed several good examples of control activities conducted by independent control functions within both the second and third lines of defence, such as in-depth analyses of how a specific business area has conducted its continuity management in practice and review of the continuity management for particularly important IT systems.

IMPACT ANALYSIS

FI prescribes that the banks regularly conduct impact analyses of interruptions or major operational disruptions that could occur within the business[5]. The analysis should include all business units and support functions.

We consider the impact analysis, in simplified terms, to be about putting all the cards on the table. The impact analysis gives the bank the possibility of reviewing its entire organisation and gaining a solid overview of all activities. In this work, the bank must take into consideration the interdependencies of its activities, for example deliveries from other activities, staff and IT systems. The impact analysis must also include outsourced activities. Based on this analysis, the bank can systematically assess how any interruptions to each activity could impact the bank. Using the impact analysis, the bank, in its continuity management, can prioritise the activities that prevent the most severe impact from an interruption.

FI takes the position that it is important for the impact analysis to be well documented and reasoned. The analysis must clearly specify how the bank has reasoned and why some activities are prioritised over others, so it is evident which active and deliberate decisions have been made. It is also important for the analysis to be conducted consistently across the bank's various business areas so the results are comparable.

The impact analyses should be used as a basis for ranking the bank's most-prioritised activities. The analyses must be updated regularly to ensure that they are up to date and adapted to the business. We consider it appropriate for them to be updated at least annually and following each event within the business that materially could impact the assessments made within the impact analysis. Examples of such events could be the implementation of a new IT system or the occurrence of a serious incident.

The close link between the impact analysis and the identification of significant processes is set out in FI's regulations, which state that the bank, as part of its continuity management, must specify the maximum tolerable downtime for each significant process. Therefore, we consider separate, isolated methods for the impact analysis and the identification of significant processes to complicate the link between these two processes.

4 Such a committee has often been created to coordinate the continuity management at the strategic level.

5 FFFS 2014:4.

Observations from the supervision of impact analyses
FI observed in its supervision that the banks need to improve their impact analyses. Several banks have initiated development projects to strengthen their impact analyses, which FI considers positive.

Observations from the supervision have shown, for example, that it is not always clear if the impact analyses has included all affected activities within the business. There appear to be challenges in identifying all important dependencies on critical activities. Another example is cases where the bank has not sufficiently included outsourced activities in its impact analysis. This could result in the bank making less appropriate choices and priorities in its continuity management since there is a risk that the information underlying the priorities is incomplete or inaccurate.

Based on observations from the supervision, we also consider the banks in general to need to improve the documentation of their impact analyses. FI noted that the documentation can be relatively limited and the possibility of tracing the bank's arguments and reasoning is therefore also limited. This could decrease the bank's own understanding of the assessments that have been made. It could also impact the follow-up and control by the second and third lines of defence and the external auditor as well as FI's ability to exercise effective supervision.

CONTINGENCY PLANS, CONTINUITY PLANS, AND RECOVERY PLANS

FI prescribes that banks must establish contingency plans, continuity plans, and recovery plans[6].

The plans should be based on the impact analyses the bank has carried out (see the section *Impact Analysis*). They must contain the information and the practical procedures needed to prepare for, maintain and restore the bank's operations in the event of a severe disruption. According to FI, the requirement to establish contingency plans, continuity plans, and recovery plans is a way of saying that the bank must take into consideration all three phases in its continuity management. There is nothing preventing the information and procedures for the phases from being consolidated into a single plan[7]. The term *continuity plan* is used hereafter to refer to all three types of plans and phases.

FI considers it important that the continuity plans are applicable in practice and designed as simply as possible. A continuity plan must clearly state which procedures and priorities apply to the business in the event of a severe interruption. The plan must also specify which roles are responsible for carrying out the procedures and, if appropriate, when the procedures need to be completed. This deadline must be in line, where relevant, with the maximum tolerable downtime as specified in the section *Impact Analysis*.

Well-documented continuity plans can function as verification that the bank has worked actively with the issues and carefully thought through the events that may occur. The continuity plans, just like the

6 FFFS 2014:4.

7 FI has described this in the decision memorandum for FFFS 2014:4.

impact analyses, should be updated regularly and within the same interval as the impact analyses, i.e. at least annually.

Observations from the supervision of contingency plans, continuity plans, and recovery plans

Observations from the supervision show that the banks have basically implemented continuity plans for their most critical functions. In other words, backup resources and procedures are in place for these functions. However, FI also makes the assessment that the quality of the plans can be improved. We believe that the plans can be clearer when it comes to the actual measures that will be prioritised, the order of priority, and any deadlines the business units need to consider. Even if there are experienced staff within the business today who largely have the knowledge required to ensure continuity following severe disruptions, FI takes the position that the bank cannot take its staff or their knowledge for granted over time. For this reason, the continuity plans need to be clear and well documented.

We also noted in the supervision that at times there were a large number of continuity plans due to, for example, several functions preparing plans for the same activities since the functions belong to different parts of the bank's organisation. An unnecessarily high administrative burden in the management of continuity plans could lead to a deterioration in the plans' quality and efficiency, particularly if there is a risk that the structure for the plans could lead to overlaps and double work. FI would like to see the banks focus on creating as few, simple and user-friendly continuity plans as possible by working on the bank's processes across the organisation.

Observations from the supervision also showed that the banks can be better at regularly updating their continuity plans. FI would like to highlight in particular that many banks are carrying out extensive change initiatives. It is therefore important for the impact of any changes on the continuity management to also be reflected in the continuity plans.

CONTINUITY TESTS

FI prescribes that the banks regularly test their continuity plans. Continuity plans for significant processes and IT systems that support these processes should be tested at least annually[8]. The banks need to test their continuity plans to obtain reasonable assurance that the plans are appropriate and effective. The tests can be designed and conducted in different ways. For a given scenario, a test as a rule becomes more resource-intensive the more realistic the conditions for the test are. At the same time, the degree of the assurance of the bank's ability to maintain continuity for a given scenario increases the more realistic the conditions for the test. FI expects the banks to regularly develop their test methodology and use the continuity tests to challenge their business's resilience to severe disruptions. For the banks' most critical functions, the tests should preferably be designed in such a way as to be as close to a real-life scenario as possible. We would also like to highlight the importance of the banks ensuring that the design of the tests, and thus the degree of assurance, is in line with the bank's risk

8 FFFS 2014:4.

appetite. It is also important for the tests not to create unacceptable risks to the operations that would in turn threaten a bank's continuity.

FI would like to emphasise the importance of having well-documented tests, where the documentation clearly states the goals, premises and limitations of the test. Acceptance criteria are important for clarifying each test case. It is also important after completing a test to evaluate whether the acceptance criteria, the goals and the maximum tolerable downtime have been achieved and which deficiencies, if any, need to be addressed. The test results, for example, could show that there is a need to update impact analyses and continuity plans.

Observations from the supervision of continuity tests
FI noted in its supervision that the banks are conducting continuity tests of their most critical functions. In some cases the tests are extensive and complex. One example of this could be to test the failover procedures, transferring large parts of the operations to a single data centre. The banks also supplement in some cases real-life exercises with desktop tests, in part to also be able to prepare for scenarios that are not possible to simulate without exposing the business to unacceptable risks. We view these tests positively but would also like to highlight the importance of the banks continuing to focus on further development of their test methodology. This is important in order to be able to conduct realistic tests over time of all material scenarios to which the banks could be exposed. FI would like to emphasise the importance of the tests being conducted on all processes of significant importance and the IT systems that support these processes.

We also consider there to be room for improvement in the test documentation, such as more clearly describing test cases, acceptance criteria and the results of completed tests.

REPORTING

FI prescribes that the banks inform the board of directors at least annually about the results of the continuity plan testing.

Since the continuity plan testing that is mentioned above is an important tool for reasonably assuring the effectiveness of the plans, the reporting of the test results becomes an important step in the management team's and the board of directors' assessment of the bank's continuity management[9]. This reporting needs to be well formulated and contain meaningful information about the tests so the management team and the board of directors can obtain a good overview of the bank's overall ability in terms of continuity management. FI believes that this reporting as a minimum should contain clear descriptions of the completed tests' goals and scope as well as the scenarios that were used. We would also like to see a description of the extent to which the test result was in line with any maximum tolerable downtime and any significant deviations that arose during the tests. It is also preferable for a comment to be included on whether the completed tests as a whole indicate that the

9 More information about FI's view on reporting can be found in the decision memorandum for FFFS 2014:4.

risks associated with severe disruptions are not considered to be within the bank's risk appetite.

Observations from the supervision of reporting
Observations from the supervision show that there is room for the banks to improve in their reporting of the results from the continuity tests to the management team and the board of directors. FI noted that the reporting in some cases consists of limited information from which the recipients of the information, in FI's opinion, cannot draw any meaningful conclusions about what the test results mean. One example of this is when a bank only announces that the tests have been conducted, and how many, without any additional information about the implementation and the test results.

FI would like to mention that several good examples were observed in the supervision. For example, there were detailed annual reports on continuity management for management teams and boards of directors that pedagogically summarised the entire bank's work in the area over the past year.

Conclusions

FI can see that the banks are working actively with continuity management. Many banks have structures and processes in place that enable them to systematically carry out their continuity management. The banks have also taken measures to reduce the risk of severe interruptions. However, FI asserts that the banks need to continue to develop and improve their continuity management in order to further strengthen their resilience to severe disruptions.

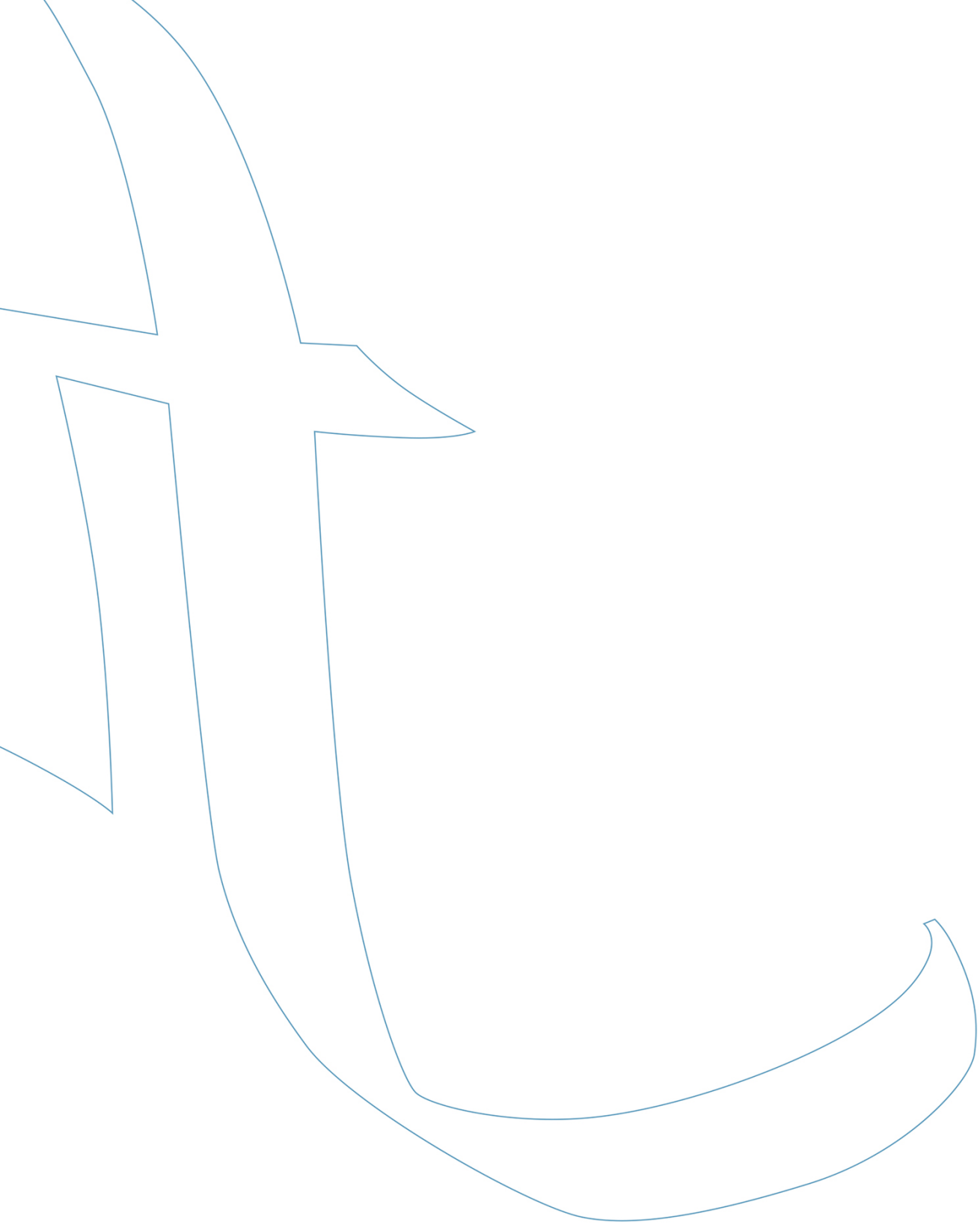
FI's supervision shows that the banks in general have established structures and processes for their continuity management. Frameworks and internal rules are in place, as are appointed functions with specific responsibility for continuity management. The banks conduct regular impact analyses of their operations. We view positively that many banks carry out their continuity management systematically.

FI's supervision also shows that the banks, as part of their continuity management, have taken measures to reduce the risk of severe interruptions to their critical functions. Continuity plans that describe backup resources and procedures are in place and these plans are tested regularly. The banks' management teams and boards of directors are also informed to some extent about the results of the tests.

FI, however, does still consider there to be room in general for the banks to further improve their continuity management. We have described the areas for improvement in this supervision report, and in summary the main improvements are to

- Strengthen the internal governance and control of continuity management, including the continuity management strategy, risk appetite for operational risk and independent control functions.
- Further develop the methods of impact analysis to ensure that all critical functions, including those dependent on one another and on support functions, are identified.
- Clarify content and structure of contingency plans, continuity plans and recovery plans.
- Ensure that appropriate continuity tests are conducted for all significant processes and the IT systems that support these processes.
- Improve reporting of results from completed continuity tests to provide the board of directors with relevant and meaningful information.

FI will continue to review the banks' continuity management in its supervision and follow up on the improvement areas that we identified.



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