EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Stocktake of IT risk supervision practices

IT supervision outside European banking supervision

1 Introduction

Between December 2015 and July 2016 the ECB organised working visits with the prudential banking supervisors in the United States, the United Kingdom, Canada, Singapore and Hong Kong and with the chief information officers (CIOs) of global systemically important banks (G-SIBs) whose parent companies are subject to supervision by the ECB. The purpose of these visits was to identify common views and explore best practices in the area of IT risk supervision.

The visits revealed a fairly consistent picture of the IT risk landscape. The meetings, combined with the work already done by the national competent authorities (NCAs) and the ECB as part of European banking supervision, as well as by the European Banking Authority (EBA), resulted in the identification of the following as the most important IT risk areas:

1. cyber risk and cyber resilience;
2. IT continuity and operational resilience;
3. vendor management and outsourcing risks;
4. identity and access management;
5. patch and vulnerability management;
6. IT complexity;
7. transformation programme risk;
8. data architecture, quality and governance;
9. IT skills.

Market participants do not consider the increased use of clouds and cloud technology as a specific IT risk; in fact, most of the G-SIBs even see this as an opportunity. Supervisors are mostly concerned with the use of external (public) cloud solutions, which in general is considered to be no different from regular IT outsourcing and subject to the same supervisory expectations. Only one supervisor explicitly prohibits the use of public clouds for business critical processing.

Developments in fintech were also discussed with supervisors and G-SIBs. In general, this topic is not primarily seen as a technology-related risk area, but rather as a business model and potential profitability issue for banks (and as such not part of the IT risk landscape).

It is disconcerting that most G-SIBs indicated that they were currently dealing with IT risks that exceeded the level they are comfortable with in terms of risk appetite. Notwithstanding the many risk-reduction programmes in these banks, the risks will remain high for years to come. This is, however, not unique to the euro area; the supervisors in the other jurisdictions expressed the same concerns.

2 Stocktake of most important IT risk areas

2.1 Cyber risk and cyber resilience

Cyber risk[1] was mentioned as an IT risk area by almost all supervisors and G-SIBs. Red-teaming[2] by banks and tests organised by supervisors and/or based upon supervisory instructions show that determined or well-informed adversaries can almost always find a way in. This also increases the importance of cyber resilience, i.e. the ability to anticipate, absorb, adapt to, rapidly respond to and recover from disruption caused by a cyberattack.

2.2 IT continuity and operational resilience

IT continuity and resilience need to be sufficiently robust and tested to ensure timely recovery from operational disruptions. This is predominantly an area of concern for supervisors. None of the G-SIBs interviewed identified IT continuity and operational resilience as a primary area of concern. Achieving operational resilience is complicated by the fact that many banks have a very high degree of IT complexity.

2.3 Vendor management and outsourcing risks

For large institutions, vendor management and outsourcing are seen as significant risk areas, especially given the large amount of suppliers that are active at those banks. Supervisors tend to focus more on the level of control of the outsourced activities, whereas the G-SIBs are more concerned about losing core banking competences and knowledge (especially related to application development).

---

1 Cyber risk refers, in general, to threats related to globally connected networks like the internet.

2 Red-teaming is a process designed to detect network and system vulnerabilities and to test security by taking an attacker-like approach to system/network/data access. This process is also called “ethical hacking” and its ultimate purpose is to enhance security.

2.4 Identity and access management (IAM)

IAM was a recurring theme in conversations with both the G-SIBs and the supervisors, in line with the observations made during on-site inspections conducted by the ECB and NCAs. As banks turn to cloud services and mobile apps to boost productivity and cut costs, managing user identities and access to IT resources has never been more important, yet banks struggle to do so properly. This, in turn, can lead to large fraud events owing to “toxic” combinations of access, and this can also lead to the door being opened to intrusive and potentially very disruptive cyberattacks.

2.5 Patch and vulnerability management

Vulnerability management is the cyclical practice of identifying, classifying, remediating and mitigating vulnerabilities, especially in software and firmware. Vulnerability management is integral to computer as well as network security and is an IT risk area mentioned by both G-SIBs and supervisors. It is closely related to the complexity of banks’ IT environments as this level of complexity, combined with the sheer amount of components, makes keeping up with patches an ever more difficult task.

2.6 IT complexity

Although complexity as such is not a problem, it turns into a risk when the level of complexity is unmanageable or not managed properly. Owing to often fragmented and outdated (legacy) core IT systems, the IT environment of large banks can be complex on multiple levels (infrastructure, applications and processes, etc.). Many banks struggle to manage this IT complexity properly. Only a few banks are ahead in managing the risks associated with this; in particular, banks that have invested in standardisation and consolidation on both the infrastructure and the application level showed far better control of their level of IT complexity.

2.7 Transformation programme risk

Many banks are undergoing large transformation programmes with the aim of simplifying their IT landscape and/or further digitalising the banking business and achieving operational improvements. Most of the expected improvements in risk control will be delivered through these types of programmes. On the other hand, these large change initiatives also introduce new risks that need to be properly mitigated (it is like “trying to rebuild a plane while it is in the air”, as one of the CIOs explained it).

2.8 Data architecture, quality and governance

Poor data quality was a recurring IT risk area mentioned by both banks and supervisors; it results in inaccurate and inefficient regulatory reporting and impedes sound business decisions. To address data quality and risk data aggregation issues, all G-SIBs have large programmes underway, driven by BCBS 239 or by the goal of providing “big data” and “data lake” solutions.

2.9 IT skills

It was mainly the G-SIBs that explicitly mentioned the risk of an ageing IT workforce and being unable to attract or retain sufficiently qualified IT personnel. This risk is partly self-inflicted owing to large staff reduction plans and offshoring initiatives at many G-SIBs, but is also caused by high competition in the market from the big technology companies and by the continuing use of legacy systems (e.g. mainframes, COBOL).

3 G-SIBs’ expectations of European banking supervision in the area of IT

In conversations with the CIOs of the G-SIBs, the following expectations where mentioned.

- **Ensure a level playing field.** The CIOs of the largest institutions in particular operate across many different jurisdictions and as a consequence need to comply with many different rules and regulations, which are not necessarily aligned between supervisors and are sometimes even contradictory. Their explicit request is to make sure that, at least within the euro area, there is a common understanding of IT risk and one set of requirements. They would also like the regulations to be aligned with those enforced by other supervisors outside the euro area, where possible.
- Although the CIOs welcomed principle-based supervision, they would favour **more specific supervisory expectations** in certain cases. In the opinion of the CIOs, some of the principles they have to adhere to are too high level, leaving the banks (according to their own interpretation) uncertain as to what is actually allowed and what is not (an example mentioned is cloud computing).

4 Stocktake of leading supervisory practices

Based on recent experience in European banking supervision and discussions with banking supervisors in other jurisdictions on their approach to supervising IT risk, the following leading supervisory practices have been identified.

1. **Central coordination of IT risk supervision.** To make the best possible use of scarce IT supervisory resources, centralising IT expertise in a specialised organisational unit for IT risk supervision is important. Such a unit can focus on developing methodologies, providing guidelines to the market, performing complex and thematic IT risk assessments and supporting the "front-line" supervisors with their IT expertise.

2. **A comprehensive IT risk assessment framework to assess banks and prioritise activities.** This enables supervisors to consistently assess banks' IT risk and prioritise their supervisory activities based on the outcome of these assessments.

3. **Use of self-assessments and questionnaires.** These make it possible to cover more ground than can be achieved with supervisory visits or examinations only. Independent reviews, approval of bank senior management and zero tolerance for intentionally misleading self-assessments were mentioned as key success factors.

4. **Issuing more detailed guidance to the market**, to complement the existing legal framework, is a means to manage expectations and to set out specific minimum requirements that financial institutions must adhere to with respect to IT risk. Although the level of detail may differ, such guidance needs to remain, as a minimum, principle-based and technology agnostic.

5. **Use of red-teaming techniques to assess cyber preparedness.** Red-teaming makes it possible for penetration testers to assess a bank's security, often unbeknown to the bank's staff. This provides a more realistic picture of security readiness than exercises or announced assessments. The red team may trigger active controls and countermeasures within a bank's operational environment. This technique is very effective for obtaining an insight into the bank's protective and responsive measures. It also effectively raises awareness at a bank's board level.

6. **Actively promote information sharing between banks and between banks and regulators.** In order for banks (and supervisors) to be able to quickly respond to new threats and attack patterns, timely sharing of information is essential. Sharing solutions can differ, but active information sharing needs to be promoted. IT incident reporting requirements for banks are important, especially for cyber incidents.

7. **Thematic/horizontal supervisory approach to key risk areas.** This may ease resource constraints and make it possible to focus on recurring issues at banks.

8. **Performing in-depth on-site inspections** is costly from a resource perspective, but achieves a high level of intrusiveness and greater assurance. Such inspections are generally indispensable if the only other instruments used are based on self-assessments.

9. **Provide training activities for non-IT supervisors** to enhance the base level of IT supervision. With scarce IT risk expertise, a good solution is for the "front-

line" supervisor to act as a general practitioner and involve the specialist only when help is needed. For this to be effective, the general practitioners must be provided with training and tools developed by the specialists.

5 Way forward for European banking supervision

Against this background and in order to improve the IT supervisory effectiveness of European banking supervision, the ECB, in close collaboration with the NCAs, will continue to:

- strengthen the **IT risk assessment methodology** as part of the Supervisory Review and Evaluation Process (SREP), drawing on the EBA's work in this area, to make sure it is applied consistently across the euro area, thereby resulting in assessments that can be better compared with each other and can be used to prioritise supervisory activities; and
- **develop more detailed and uniform supervisory expectations for banks under European banking supervision** on topics relating to IT risk by replacing or complementing guidance already in place at the national level (e.g. issuing guidelines after a public consultation). This would level the playing field for banks in the euro area and at the same time make them more resilient to IT risk. This would be done by the ECB and NCAs, in close cooperation, and should cover the most important risks as identified in this stocktake.

These supervisory expectations should **demand a maturity level of IT risk management that is well above what is considered basic.** As much as possible, these more detailed expectations should be aligned with those of non-euro area supervisors.