CORE®

KEY POINTS FOR THE SUPERVISION AND MONITORING OF IT IN BANKS

A BaFin information event regarding IT supervision

Christian Everts
Dr. Waldemar Grudzien

30 March 2017
COREtechmonitor | Blogpost

Key Facts

- Key points of bank IT monitoring by BaFin and the Bundesbank announced
- Sourcing in the Cloud outside the EU, including the US, permitted – stricter requirements
- Mandatory Information Security Officer – overlap with Data Security Officer still to be clarified
- IT Security Act – special regulations governing the financial sector
- Increasing degree of regulatory assurance and supervisory maturity

On 16 March 2017, BaFin – Germany's financial regulator – held its fourth information meeting on the supervision of IT for banks with roughly 500 attendees. The press and media coverage (FAZ, Handelsblatt, Börsenzeitung) placed emphasis on the vulnerability of bank IT systems to attacks and the need for them to improve their IT security, whereas BaFin and the Bundesbank announced important details regarding future supervision and monitoring of bank IT, with keynote presentations on BAIT (supervisory requirements for bank IT), monitoring of IT matters in practice by banking regulators, and the implementation of the IT Security Act by means of the Federal Office for Information Security Act (BSI) and the Payment Service Directive (PSD) II.

Outsourcing in the US Cloud is permitted – but with stricter requirements

The supervisory bodies are paying ever more attention to monitoring IT outsourcing. How thorough the checks need to be depends on the risk, which is assessed based on location, access rights and processes, in addition to ongoing compliance with statutory, regulatory and data protection requirements. Banks, in particular, were given useful information in answers to questions about the transparency of the Cloud service provider (see figure).

It is worth pointing out that the location and legal jurisdiction of the Cloud provider chosen by a bank has an impact on the stringency of checks, and thus, in turn, on the number and level of requirements. In other words, outsourcing to a US Cloud or one with a US parent company leads to disadvantages in terms of monitoring.

Information Security Officer is mandatory – overlap with Data Security Officer role needs to be clarified

There was a lengthy discussion about whether the new role of Information Security Officer could be combined with that of the Data Security Officer. BaFin reported on its consultation with the German Federal Data Protection Officer – the outcome was that the two roles cannot be fulfilled by a single individual. This view was contradicted by a representative of the Bavarian Data Protection Officer. BaFin undertook to raise the matter once more with the Federal Data Protection Officer. For smaller institutions in particular, this would be a challenge if both functions had to be manned by two separate individuals.

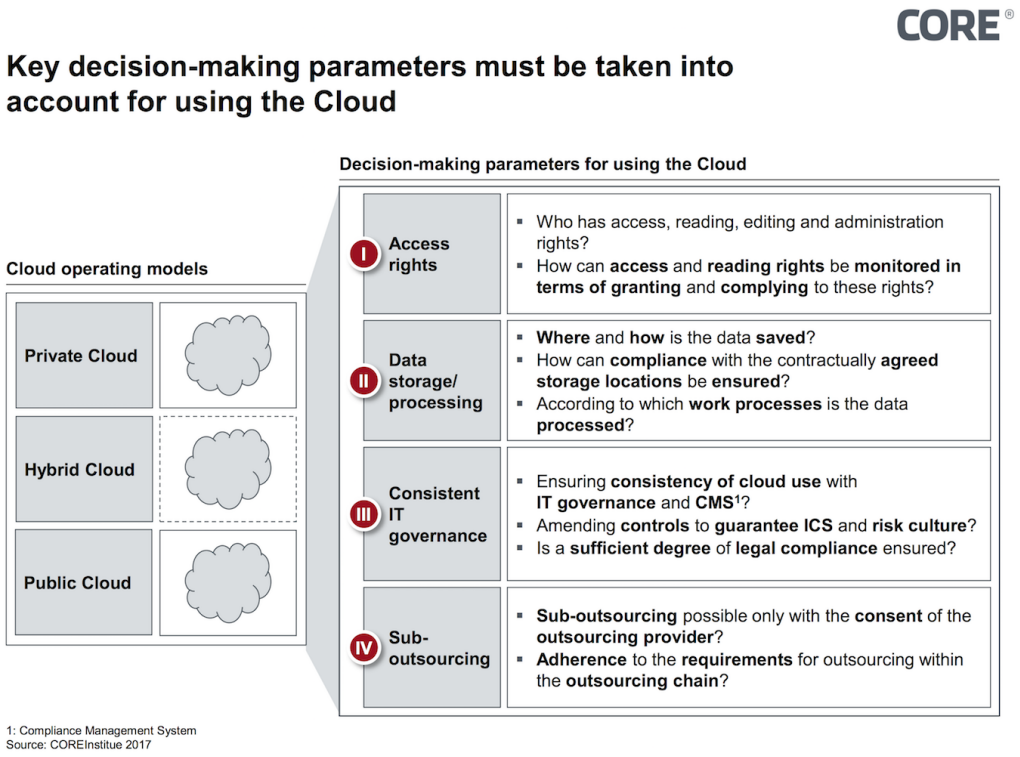

Figure 1: Relevant monitoring criteria for the use of Cloud services

IT Security Act – special regulations for the finance sector

The German IT Security Act (IT-SiG) requires those who operate critical infrastructure in energy, information and telecommunications technology, transport and movement of goods, health, water, food, and the finance and insurance sectors to adhere to minimum IT security standards, as well as to report serious IT security incidents to the Federal Office for Information Security (BSI). The Act will be implemented by the BSI Act and through the concrete measures contained in the KRITIS regulations (on critical infrastructure), which are due to come into force during the second quarter of 2017. For the first time, BaFin and the BSI will be overseeing compliance with the requirements of IT-SiG jointly, with BaFin supervising banking matters and practice, and the BSI taking responsibility for technical expertise.

A significant change brought about by the new regulations of February 23, 2017 was the change in the way that the term “operator” is defined in the three sectors of traffic and transport, health, and finance and insurance, compared to the definition used in the KRITIS Regulation covering the four sectors of energy, information and telecommunications technology, water and food that came into force in May 2016. The operator previously referred to whoever had a prevailing influence on the structure and operation of an installation, or parts of it, taking into consideration the legal, commercial and actual circumstances. This has been altered by the new regulations, but only concerning the financial and insurance sector. An “operator” simply has to have a significant influence on critical infrastructure, i.e. the legal and commercial circumstances are no longer taken into account. According to IT-SiG, the bank itself will no longer automatically be deemed to

be a “critical” operator because of the legal responsibility it bears. Instead, the service provider actually carrying out the service classed as “critical” will be considered to be the operator. Consequently, both the banks and their service providers will have more checking to do regarding how they are affected by IT-SiG.

Summary

BaFin made use of its fourth meeting on the supervision of bank IT to give more detailed information on various existing or pending regulations, as well as to announce further plans on the part of both BaFin and the European Banking Authority. Besides BAIT, the supervisory requirements for bank IT which have already been published for consultation, these include MaRisk (minimum requirements for risk management, expected in the first quarter of 2017) and the EBA’s “Recommendations on Outsourcing to Cloud Service Providers” (in the third quarter of 2017).

One surprise was the clear statements made on Cloud providers based outside the EU, or acting within the EU, but provided by a subsidiary of a foreign Cloud service, especially in the case of a US company.

Overall, the meeting was a sign of greater regulatory assurance and supervisory maturity. Those are both positive indications on the long road to the professionalization of IT within banking.

Sources

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Pressemitteilung/2017/pm_170316_it-aufsicht_banken_html

http://www.faz.net/aktuell/finanzen/bafin-bemaengelt-it-sicherheit-der-banken-14928430.html

https://www.boersen-zeitung.de/index.php?li=1&artid=2017054026&artsubm=ueberblick&r=Banken%20&%20Finanzen

http://www.handelsblatt.com/my/finanzen/banken-versicherungen/it-auslagerung-bei-banken-finanzaufseher-fuerchten-kontrollverlust/19532670.html

Christian Everts is a Transformation Manager at CORE and is particularly experienced in the field of regulation. Prior to joining CORE, Christian worked for several banks as a compliance manager, where he primarily implemented regulatory requirements in German and international investment and universal banks.

Mail: christian.everts@coretransform.com

Dr. Waldemar Grudzien is a Transformation Engineer at CORE and focused on the security regulations of the financial industry and their technological effects on IT infrastructures. During his work at a national federation of the financial industries he was a specialist for retail banking and banking technologies. He graduated in electrical engineering at the TU Berlin.

Mail: waldemar.grudzien@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
office@coretransform.ae