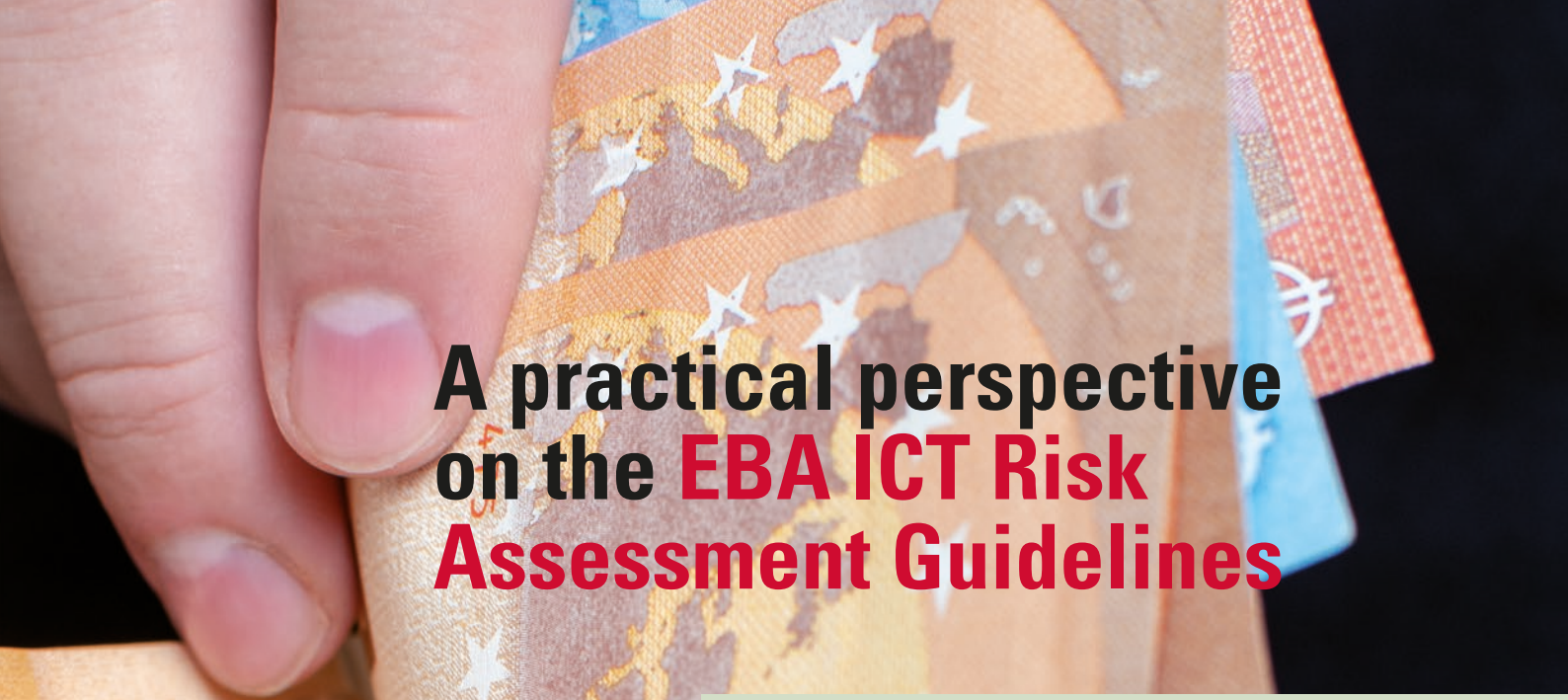


A practical perspective on the EBA ICT Risk Assessment Guidelines

Developments in regulatory oversight of ICT risk

The European Banking Authority (EBA) has issued guidelines for the assessment of the ICT risk at large banks which became effective as of January 1st, 2018. In this article we elaborate on the background and content of these guidelines, the impact for banks, the comparison of these guidelines in relation to other regulatory requirements on ICT and how banks can provide an answer to the EBA guidelines based on IT tooling. The EBA asked the large banks to fill out an ICT questionnaire at the beginning of 2018. The expectation is that on a yearly basis this request will be made towards the banks and the scope will be expanded to other banks in the future. KPMG developed a tool that facilitates this yearly process of submission of the assessment to the EBA.

Brigitte Beugelaar RE RA
is a partner at KPMG.
beugelaar.brigitte@kpmg.nl

Ali Alam MSc RE CISA
is a manager at KPMG.
alam.ali@kpmg.nl

INTRODUCTION

If we take a look at banks in the current environment, we cannot deny the fact that banks turned more and more into IT-driven companies with banking licenses. In the operation of its business for customers, IT plays a pivotal role. This results in the fact that banks are highly dependable on their IT, and increasingly place their trust in their IT systems to carry out daily operations. As a consequence, it is not surprising that regulators, and in this case, the European Banking Authority (EBA), are also interested in how banks address the dependency on IT in its operations and addresses related information and communication technology (ICT) risks. With this in mind we do see that regulators have a high interest in how the ICT risks are managed and how trust in IT is achieved and maintained. A diversity of guidelines and regulations has been issued over time on the topic of ICT. The EBA guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) is one of many, and will certainly not be the last one. However, one can argue how all of these guidelines and requirements relate to each other, and whether there is an overlap between them. This article provides insight into the EBA ICT risk assessment guidelines and gives an impact analysis in terms of how to comply, where will it go to, how to address overlap, and how to efficiently address the requirements e.g. by means of tooling.

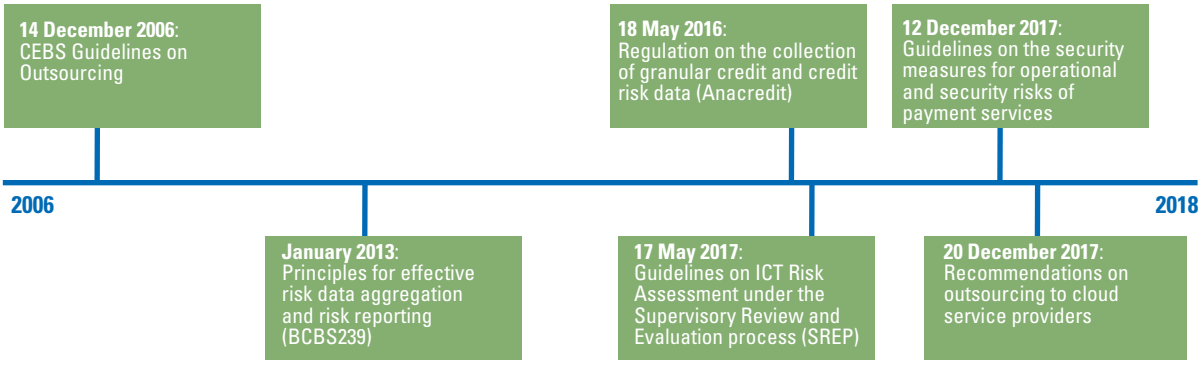
BACKGROUND OF THE EBA ICT RISK ASSESSMENT GUIDELINES

Technological innovation plays a crucial role in the banking sector from a strategic standpoint, as a source of competitive advantage, as it is a fundamental tool to compete in the financial market with new products, as well as through facilitating the restructuring and optimization of the value chain. Due to this, banks are forced to depend on their IT systems and consequently place their trust into it. A number of trends are a result of the increasing importance of ICT in the banking industry, two of these trends include:

1. the emergence of (new) cyber risks, together with the increased potential for cybercrime and the appearance of cyber terrorism ([AD17], [WSJ17]);
2. the increasing reliance on outsourced ICT services and third-party products, often in the form of diverse packaged solutions, resulting in manifold dependencies and potential constraints and new concentration risks ([CIO15], [CoWe14]).

Acknowledging the growing importance of ICT systems, and therefore the increasing potential adverse prudential impact of failures on an institution and on the sector as a whole (due to the cross-border nature of this risk), the EBA launched the *Guidelines on Information and Communication Technology (ICT) Risk Assessment* under the SREP to enhance the existing SREP Guidelines, establishing common practice and application by National Competent Authorities in ICT risk assessment and strengthening prudential supervision ([EBA17-1]).

Figure 1. Timeline release of ICT related regulation by European Banking Authority (EBA).



The guidelines aim to ensure the convergence of supervisory practices and achieve uniformity in the assessment of the ICT risk under the SREP, and are further specified in the EBA Guidelines on common procedures and methodologies for the SREP. The topics that are being covered in the guidelines address the mentioned trends and include the background and scope addressed in Table 1.

When considering the topics in Table 1, an overlap with other (existing) regulations appears at first glance. Concerning ICT security risks, the Dutch Central Bank issued the Self-Assessment for Information Security based on the Cobit 4.1 framework [(DNB17]) and PSD2 Guidelines on the security measures for operational and security risks of payment services ([EBA17-2]).

On the topic of ICT outsourcing risks, requirements were issued in the past by both the Dutch Central Bank as well as the European Central Bank (ECB). In 2006 the ECB published their guidelines on outsourcing ([CEBS06]), explaining that in context of outsourcing, ultimate responsibility for daily management and management of risk lies with the financial institution and cannot be delegated to the outsourced party. Recently, as of December 2017, the ECB expanded these guidelines by also including recommendations on the use of cloud service providers by financial institutions ([EBA17-3]). The Dutch Central Bank followed a similar approach in the past: the requirements for outsourcing in general and cloud computing in specific were launched simultaneously ([DNB14a], [DNB14b]).

ICT data integrity risk requirements have an overlap with the BCBS239 principles for effective risk data aggregation and risk reporting ([BCBS13]), Anacredit ([ECB16]) and General Data Protection Regulation ([EUPA16]). For a full overview, please see the comparative analysis further on.

Table 1. Topics addressed in the EBA ICT Risk Assessment Guidelines.

ICT Topic	Background and scope
ICT Governance and Strategy	Assessment whether the institution's general governance and internal control framework duly cover the ICT systems and related risks and if the management body adequately addresses and manages these aspects
ICT Risk Exposures and Controls	Assessment whether the institution has properly identified, assessed and mitigated its ICT risks
a. ICT availability and continuity risks	Review the ability to timely recovery of the services, due to a failure of ICT hardware of software components
b. ICT security risks	Review the measures against unauthorized access to ICT systems
c. ICT change risks	Review the ability to manage ICT system changes in a timely and controlled manner
d. ICT data integrity risks	Review the completeness, accuracy and consistency of the different ICT systems
e. ICT outsourcing risks	Review the measures against potential adverse impacts from engagements with third party ICT systems and related services providers

IMPACT ANALYSIS: WHAT IS THE PRACTICAL IMPACT ON BANKS?

As for the practical impact on banks, these guidelines require banks to make an inventory on how they address the topics in the ICT risk guidelines (i.e. by formulating internal controls), to be able to demonstrate compliance if the ECB asks for further elaboration and substantiation. Overlap with other IT regulations increase the importance of having insight into what is already addressed via other regulations. Having this overview helps banks in efficiently and effectively addressing new requirements on ICT risk, and prevent any duplication in answering to requests of regulators. The use of for instance GRC systems will help gain the total overview. In the next paragraph we elaborate on how to determine potential gaps in compliance with guidelines.

The overlap between the EBA ICT risk guidelines and previous regulations creates a need for banks to clearly identify the sources of ICT risks in the EBA guidelines, that are not (fully) addressed by prior regulations. For these "potential gaps", banks will need to take measures (varying from preventative to detective in nature) in order to mitigate these unaddressed sources of ICT risk.

Table 2 provides a comparative analysis between the guidelines and other IT regulations, through a high-level mapping of the different ICT risk topics of the EBA guidelines to existing regulations. This is needed to identify the extent of overlap and gaps, so that banks can take action and fulfill their compliance with the EBA ICT risk guidelines.

Based on Table 2, we see that the EBA ICT risk Guidelines overlap with the DNB Information Security Framework and Payment Service Directive 2 (PSD2) guidelines for the specific ICT risk topics. For DNB

ICT outsourcing risk is a topic that is addressed by multiple regulations on Dutch Central Bank level, as well as EBA level

Information Security Framework, the main gaps lie in the ICT data integrity risk, whereas in PSD2 ICT Change, risks are not discussed at all. Furthermore, the DNB Information Security Framework does not address the exception of the handling process of ICT data integrity, and the risk reporting and data aggregation capabilities in the context of the BCBS239 regulation.

There are also gaps in the domains of ICT security risks and ICT change risks, as the DNB Information Security Framework does not sufficiently cover aspects of regular and proactive threat assessments for ICT security, security and vulnerability screening of changes and source code control. A possible explanation for the mentioned gaps is that DNB based its Information Security Framework on the COBIT4.1 framework, which dates back to 2007 ([ITGI07]). It is – to some extent – plausible to say that eleven years ago, ICT security, ICT change and ICT data integrity risks were not as prevalent in the banking sector and pervasive in nature as they are today. PSD2 does address security in the Guidelines, but focuses more on security in the context of payment processing.

ICT outsourcing risk is a topic that is addressed by multiple regulations on Dutch Central Bank level, as well as EBA level.

Table 2. Comparison of EBA ICT Risk Guidelines vs. existing regulations.

EBA ICT Risk Guidelines	DNB Information Security Framework	DNB Cloud Computing Risk Assessment	BCBS239	EBA Cloud Outsourcing	GDPR	ECB Guidelines on Outsourcing	Payment Service Directive 2 (PSD2) Guidelines on Security and Operational risk
ICT Governance and Strategy							
ICT Risk Exposures and Controls	X	X	X	X	X	X	X
a. ICT availability and continuity risks	X	X	X	X	X	X	X
b. ICT security risks	X[1]	X	X	X	X	X	X
c. ICT change risks	X[2]	X	X	X	X	X	X
d. ICT data integrity risks							
e. ICT outsourcing risks	X	X	X	X	X	X	X

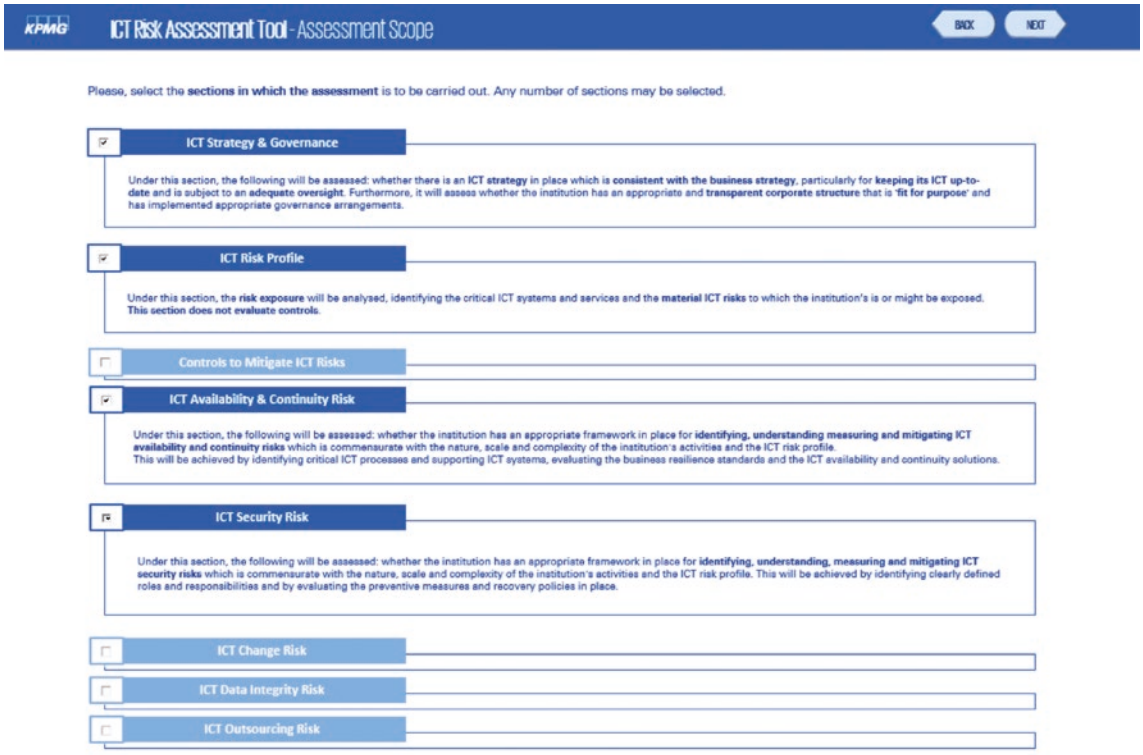
1. Regular and proactive threat assessments not sufficiently covered.

2. Security and vulnerability screening of changes and source code control not sufficiently covered.

Apart from the smaller gaps mentioned above, the main point of attention for banks is the ICT Governance and Strategy domain of the EBA Guidelines, as it represents the largest gap in terms of coverage with the existing regulations. The guidelines in this domain are – among others – directed towards alignment between the ICT and business strategy, involvement of senior management bodies, assignment of roles and responsibilities for the implementation of ICT programs. These topics are not incorporated into any ICT related regulation. They are, however, discussed in the COBIT4.1 control framework ([ITGI07]), which can form a starting point for potential implementation. Only the aspect of positioning the ICT risk in the risk management framework of the banks is addressed in the DNB Information Security Framework and PSD2 Guidelines. Furthermore, the impact on banks of not being able to comply with the guidelines ICT Governance and Strategy is high, as the ICT Governance and Strategy is at the basis of a secure and in-control IT organization.

Figure 2. Main screen assessment tool.

Figure 3. Scoping of Assessment.



IT TOOLING FOR EBA ICT RISK ASSESSMENT

In order to address the gaps as discussed previously and measure the level of compliance with the EBA ICT Risk Guidelines, KPMG has developed an IT tool (the KPMG EBA ICT Risk Assessment Tool). This tool incorporates the EBA ICT risk assessment guidelines by formulating a set of questions for each of the ICT topics and ranks the answers on a scale of 1 to 4, 1 being no discernible risk and 4 representing a high level of risk.

The tool is designed to allow maximum adaptation to the banks in scope. First of all, it allows the banks to assess the compliance bank-wide or on a subsection of the bank (international subsidiaries to business lines within one country branch). This places the correct focus and enables comparison and benchmarking between locations and/or business lines. Secondly, it gives the choice between a quick scan and detailed assessment depending on the level of exposure of the bank to ICT risks. Whereas the former option only allows evaluation of the most significant points in the EBA ICT Risk Guidelines, the latter covers all aspects of the guidelines.

Thirdly, the user is able to scope the applicable ICT risks and exclude irrelevant ICT risks. For instance, in the case that the bank executes and manages all their ICT in-house, ICT outsourcing risk becomes obsolete.

Figure 4. Entity Identification.

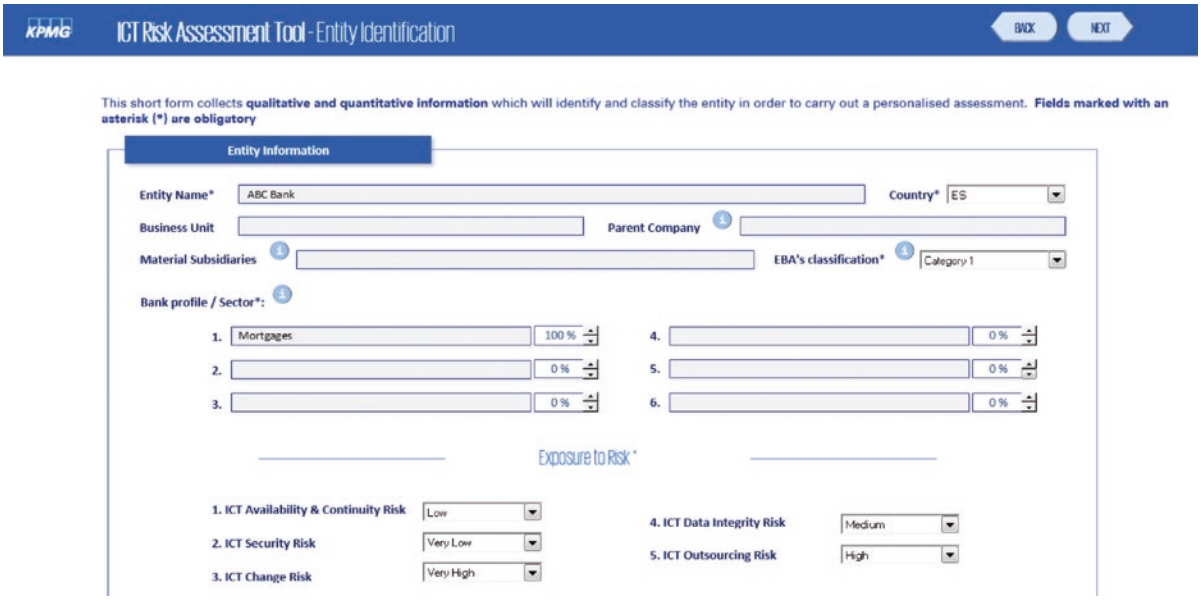
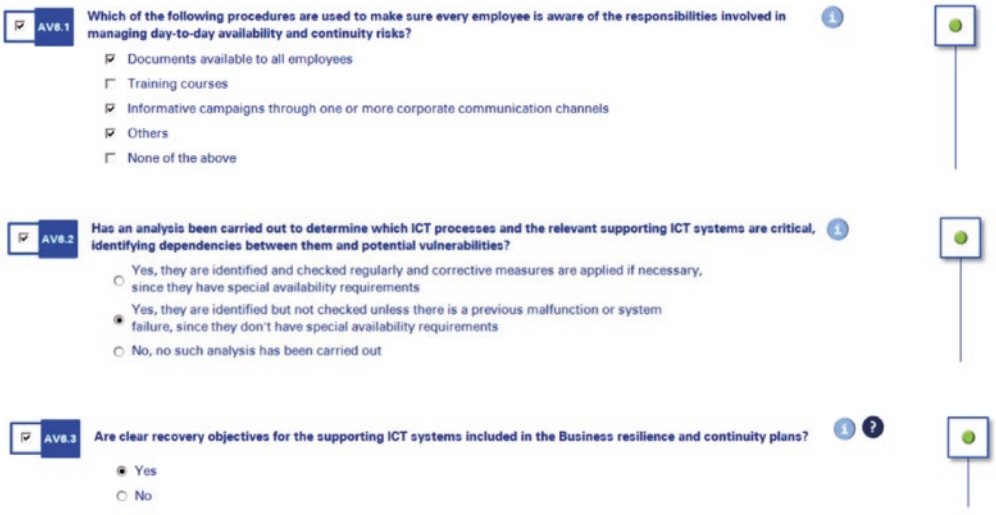


Figure 5. Example questions on ICT Availability and Continuity Risk.



To tailor the results of the tool the user is requested to provide qualitative and quantitative information. This information forms input for qualitative rating of the risk exposure for each ICT risk type defined by the EBA and for benchmarking purposes.

Each assessment of the risks consists of questions on sub-topics ranging from "Policies and Procedures" to "Preventive measures". The questions are either multiple choice (as many answers as necessary may be selected), single choice (only one can be selected) and dichotomous being yes or no.

When the assessment is completed, three reports are generated being: 1) ICT Score Heat Map, 2) Operational Risk Homologation, and 3) Urgency Reports.

ICT Score Heat Map

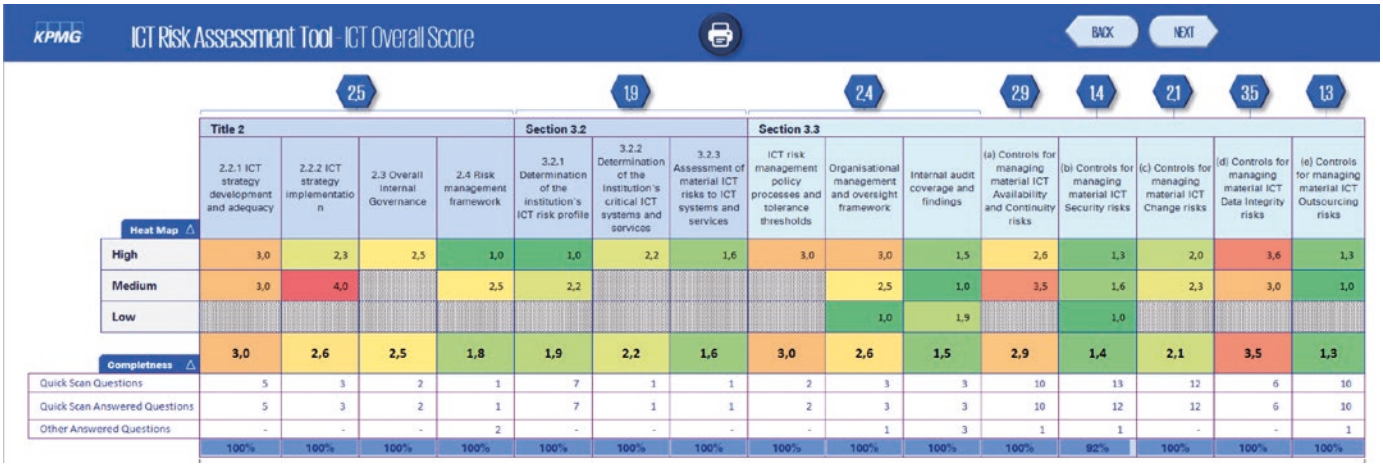
The ICT Score Heat Map provides the average score of the questions per section combined with the criticality level of the ICT risks. Based on Figure 6, "Controls for managing material ICT Data Integrity risks" has an average score of 3,5, and ICT Data Integrity risk is highly critical.

In this way, a high score in the "Low" row has less impact in the general ICT Risk of the institution than a high score in the "High" row due to its low criticality.

The last row displays the average of all of the questions of each section, giving the user the ability to see a general score for every section defined in the EBA ICT Risk Guidelines, along with the weighted average of the scores and arithmetic average score obtained in each section of the questionnaire. See Figure 6.

> The Urgency Report displays only those questions in which the user has obtained a "bad score"

Figure 6. ICT Score Heat Map.



	2.5				1.9				2.4		2.9	1.4	2.1	3.5	1.3
	Title 2				Section 3.2			Section 3.3							
Heat Map	2.2.1 ICT strategy development and adequacy	2.2.2 ICT strategy implementation	2.3 Overall Internal Governance	2.4 Risk management framework	3.2.1 Determination of the institution's ICT risk profile	3.2.2 Determination of the institution's critical ICT systems and services	3.2.3 Assessment of material ICT risks to ICT systems and services	ICT risk management policy processes and tolerance thresholds	Organisational management and oversight framework	Internal audit coverage and findings	(a) Controls for managing material ICT Availability and Continuity risks	(b) Controls for managing material ICT Security risks	(c) Controls for managing material ICT Change risks	(d) Controls for managing material ICT Data Integrity risks	(e) Controls for managing material ICT Outsourcing risks
High	3,0	2,3	2,5	1,0	1,0	2,2	1,6	3,0	3,0	1,5	2,6	1,3	2,0	3,6	1,3
Medium	3,0	4,0		2,5	2,2				2,5	1,0	3,5	1,6	2,3	3,0	1,0
Low									1,0	1,9		1,0			
Completness	3,0	2,6	2,5	1,8	1,9	2,2	1,6	3,0	2,6	1,5	2,9	1,4	2,1	3,5	1,3
Quick Scan Questions	5	3	2	1	7	1	1	2	3	3	10	13	12	6	10
Quick Scan Answered Questions	5	3	2	1	7	1	1	2	3	3	10	12	12	6	10
Other Answered Questions	-	-	-	2	-	-	-	-	1	3	1	1	-	-	1
	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	92%	100%	100%	100%

Operational Risk Homologation

This report displays every question and allows the user to link each question and score to the relevant operational risk loss event or strategy area, enabling the user to view the vulnerability of each area of operational risk and possible impact in the context of ICT Risk in a potential cause and effect structure. Furthermore, it increases the link between the assessment with the SREP and the configuration set up in the guidelines by the EBA (see Figures 7 and 8).

The Operational Risk Homologation is divided in two parts:

1. **Business Model & Governance**. This pertains to the assessment sections regarding the ICT Strategy and Governance, ICT Risk profile and Controls to Mitigate ICT risks. Results in these sections may impact the Business Model and Internal Governance and Control and require follow-up.
2. **Operational Risk Loss Events**. This links the different types of ICT risks to a number of operational risk loss events. The tool has the following operational risk loss events in scope: Internal Fraud, External Fraud, Workplace Safety, Clients, Products & Business Practices, Damage to Physical Assets, Business Disruption and System Failures and Execution, Delivery & Process Management.

Figure 7. Operational Risk Homologation Report Business Model & Governance.

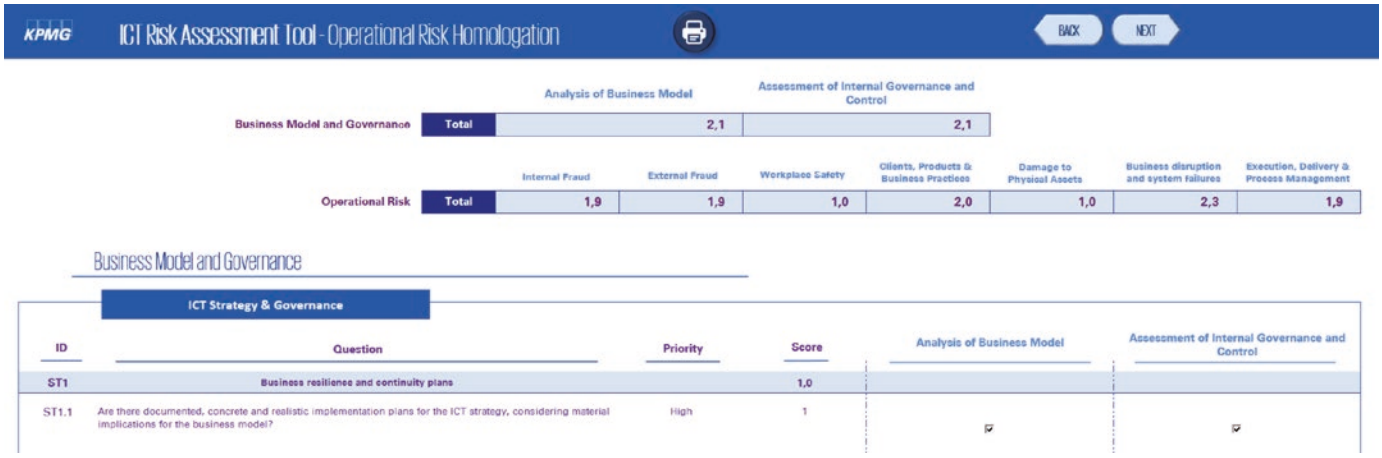


Figure 8. Operational Risk Homologation Report Operational Risk Loss Events.

For instance, the tool links the lack of business continuity plans and continuity planning to operational risk loss events related to "Business Disruption and System Failures".

Urgency Reports

The Urgency Report displays only those questions in which the user has obtained a "bad score", which by default is 3. This report enables the user to highlight the most critical issues. The "bad score" can be changed per the user's wishes and risk appetite.

This screen displays every question that exceeds the set threshold and provides the extract of the regulation on which the question is based. This way the user can identify the exact guidance and improve current issues in order to reduce the exposure or improve internal controls.

CONCLUSION

The EBA ICT Risk Assessment Guidelines form a new set of guidelines that banks are required to comply with as of this year. These guidelines require banks to think about how they will approach these and make the implementation tangible and demonstrable to the ECB. However, the content of these guidelines is not very new or unknown to the banks. Due to the nature of these guidelines, previous regulations to some extent cover or touch upon the content of the EBA ICT Risk Guidelines, enabling banks to focus on the areas that require major efforts for compliance and achieve quick compliance on recurring topics. Advanced IT tooling developed by KPMG can assist banks by creating insight into their level of compliance with the EBA ICT Risk Guidelines. This is done by filling in a questionnaire for each ICT risk area in scope. This exercise results in a risk heat map and homologation report, pointing out the ICT risk areas of attention and linking these to possible operational risk loss event categories that could be impacted in case of a negative score.

References

[AD17] AD, *Financiële instellingen steeds vaker gehackt*, Algemeen Dagblad, https://www.ad.nl/economie/financieneuml-le-instellingen-steeds-vaker-gehackt~a180d6a7, November 23, 2017.

[BCBS13] Basel Committee of Banking Supervision, *Principles for effective risk data aggegration and risk reporting*, Basel Committee of Banking Supervision, 2013.

[CEBS06] Committee of European Banking Supervisors, *Guidelines on Outsourcing*, Committee of European Banking Supervisors, 2006.

[CIO15] CIO, *Big banks, big applications, big outsourcing*, CIO from IDG, https://www.cio.com/article/3096125/outsourcing/big-banks-big-applications-big-outsourcing.html, July 1, 2015.

[CoWe14] ComputerWeekly, *Why IT outsourcing is increasingly blamed for IT failures at banks*, ComputerWeekly.com, https://www.computerweekly.com/news/2240214081/Why-IT-outsourcing-is-increasingly-fingered-for-IT-failures-at-banks, February 11, 2014.

[DNB14a] DNB, *Cloud computing*, De Nederlandsche Bank, http://www.toezicht.dnb.nl/2/5/50-230433.jsp, May 15, 2014.

[DNB14b] DNB, *Governance: Uitbesteding*, De Nederlandsche Bank, http://www.toezicht.dnb.nl/2/5/50-230431.jsp, May 15, 2014.

[DNB17] DNB, *Assessment Framework for DNB Information Security Examination 2017*, De Nederlandsche Bank, http://www.toezicht.dnb.nl/en/3/51-203304.jsp, April 21, 2017.

[EBA17-1] European Banking Authority, *Guidelines on ICT Risk Assessment under the Supervisory Review*, European Banking Authority, 2017.

[EBA17-2] European Banking Authority, *Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*, European Banking Authority, 2017.

[EBA17-3] European Banking Authority, *Recommendations on outsourcing to cloud service providers*, European Banking Authority, 2017.

[ECB16] European Central Bank, *Regulation (EU) 2016/867 of the European Central Bank of 18 May 2016 on the collection of granular credit and credit risk data (ECB/2016/13)*, Official Journal of the European Union, 2016.

[EUPA16] European Parliament, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)*, Official Journal of the European Union, 2016.

[ITGI07] The IT Governance Institute, *Cobit 4.1 Framework, Control Objectives, Management Guidelines and Maturity Models*. Rolling Meadows, 2007.

[WSJ17] WSJ, *Regulators See Cybersecurity as Top Financial Industry Risk*, The Wall Street Journal, https://www.wsj.com/articles/regulators-see-cybersecurity-as-top-financial-industry-risk-1513288542, December 14, 2017.

About the authors

B. Beugelaar RE RA is a partner at KPMG and is responsible for the Assurance services within KPMG Netherlands. She has been working in the financial sector in the field of ICT risk and IT audit for more than twenty years.

A.N. Alam MSc RE RA is a manager at KPMG working in the Assurance branch of KPMG Netherlands. He has been working in the financial sector forsix years in the field of ICT risk and IT audit and has extens ive experience in carrying out IT Maturity and IT Risk Assessments.