



RISK & MORE

# RISK DIAGNOSIS

A TOOL FOR BANKING ORGANIZATIONS

MAY 2019



## REGULATORY COMPLIANCE IN THE EUROPEAN UNION

# CONTENT



		Page
1.	Possible Challenges for you	4
2.	Possible Visions for you	7
3.	How Risk & More can support	11
4.	Our Tool	13
5.	Benefits for you	20
6.	Why Risk & More	22
7.	Contact Details	26

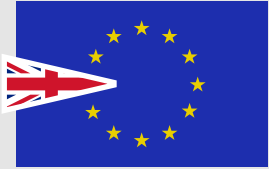


# 1. POSSIBLE CHALLENGES FOR YOU



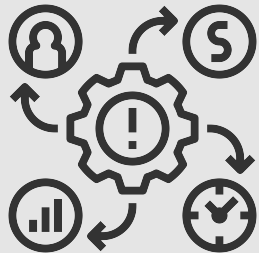


# POSSIBLE CHALLENGES FOR YOU - ESTABLISHING A NEWLY LICENSED ENTITY IN THE EU



## Brexit

As widely known, Brexit is the withdrawal of the United Kingdom (UK) from the European Union (EU), following a referendum in June 2016. There continues to be uncertainty on UK's exit from Europe.



## Brexit: Impact on the Financial Sector

Since the referendum, Brexit has created uncertainty in many industry segments. The financial services industry is facing significant challenges, particularly related to regulatory uncertainty.



## Establishing a licensed entity in the EU

A significant number of banks are in the process of establishing a newly licensed entity in the EU, which means that firms will be able to continue to service its European clients post-Brexit, regardless of the outcome of the EU/UK negotiations.



# ESTABLISHING A NEWLY LICENSED ENTITY IN THE EU

## REGULATORY CHALLENGES

- Institutions may be challenged to set up a new EU subsidiary which optimizes the firm's EU structure to mitigate any potential impact to its clients, its staff and the group as a result of Brexit, including loss of EU passporting rights.
- Set-up activities need to progress well and must eventually obtain the full banking license to commence operations in line with CRR/CRD<sup>1</sup> requirements.

### Key regulatory challenges

- Sound risk management framework
- Risk assessment / measurement
- Capital and liquidity adequacy (statements)
- Capital / liquidity planning (ICAAP / ILAAP)
- Stress testing
- IT requirements
- Internal control system

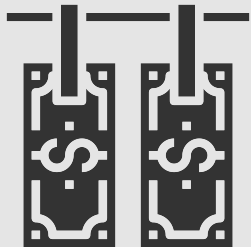
<sup>1</sup> Capital Requirements Regulation / Capital Requirements Directive

# OTHER POSSIBLE CHALLENGES FOR YOU



## **Weaknesses in Risk Management and Controls**

Quantitative and qualitative issues in risk management, inadequate controls. Material risk not adequately covered. Large number of audit findings. High likelihood of high Pillar 2 capital requirement.



## **Weaknesses in other Areas of Compliance**

Violations of anti-money laundering laws/rules, i.e. unsound practices such suspicious funds/ transactions and client base. High likelihood of regulatory enforcement actions.



## **Weaknesses related to Information Technology**

Non-compliance with IT rules and standards, in particular IT strategy, IT governance, IT operations and critical infrastructure, information and security risk management, user access management, IT projects, and outsourcing



## 2. POSSIBLE VISIONS FOR YOU



# POSSIBLE VISION 1 - ESTABLISH NEWLY LICENSED ENTITY IN THE EU<sup>1</sup>



- Comply with CRR/CRD requirements
- Be able to manage operational and regulatory risks that will arise
- Ensure that risk management perfectly supports business needs
- Adapt group culture and risk framework
- Align risk management processes and infrastructure with group developments
- Operate within CIR requirements, keep operating costs to a minimum
- Avoid unnecessary regulatory risk —> keep Pillar 2 capital requirement as low as possible

<sup>1</sup> as a consequence of Brexit, e.g. from current operating entity in the United Kingdom

# POSSIBLE VISION 2 - IMPROVE RISK, COMPLIANCE AND IT INFRASTRUCTURE



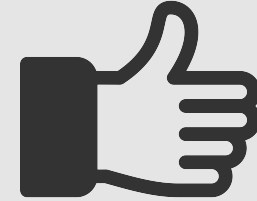
## Risk Management and Controls

Efficient and effective risk management, low Pillar 2 capital requirement



## Anti-money Laundering

Compliance with laws/rules



## Information Technology

High-quality and efficient information technology infrastructure

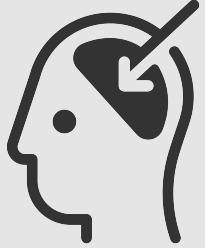
Low operational risk, low compliance risk, no regulatory enforcement action

# 3. HOW RISK & MORE CAN SUPPORT



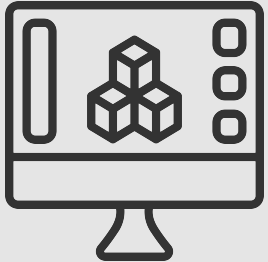


# HOW RISK & MORE CAN SUPPORT



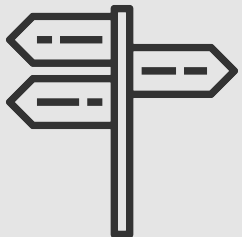
## Experience

Risk & More has **experience** in setting up regulatory compliant financial institutions.



## Tool

Based on our experience **we have developed a comprehensive management tool** based on key EU regulatory requirements that can assist you with your project challenges.



## Guidance

We can assist your project and your targeted integrated risk operating model in terms of **regulatory compliance, efficiency, robustness, completeness and credibility** in order to avoid failure and higher costs in case unforeseen deficiencies may arise.





## 4. OUR TOOL

The Risk Profile Diagnostic is the latest tool from Risk & More to evaluate and help improve your enterprise risk posture



# OUR TOOL



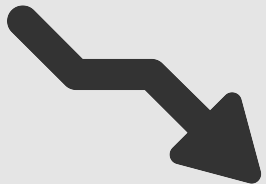
## Risks and Vulnerabilities

Analysis of all key risk and performance indicators, in line with CRR/CRD requirements.



## Coverage

Comprehensive subject coverage, including ICAAP and ILAAP requirements.





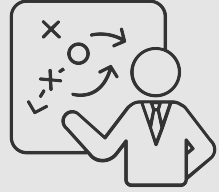


## Reduction of Project Risk

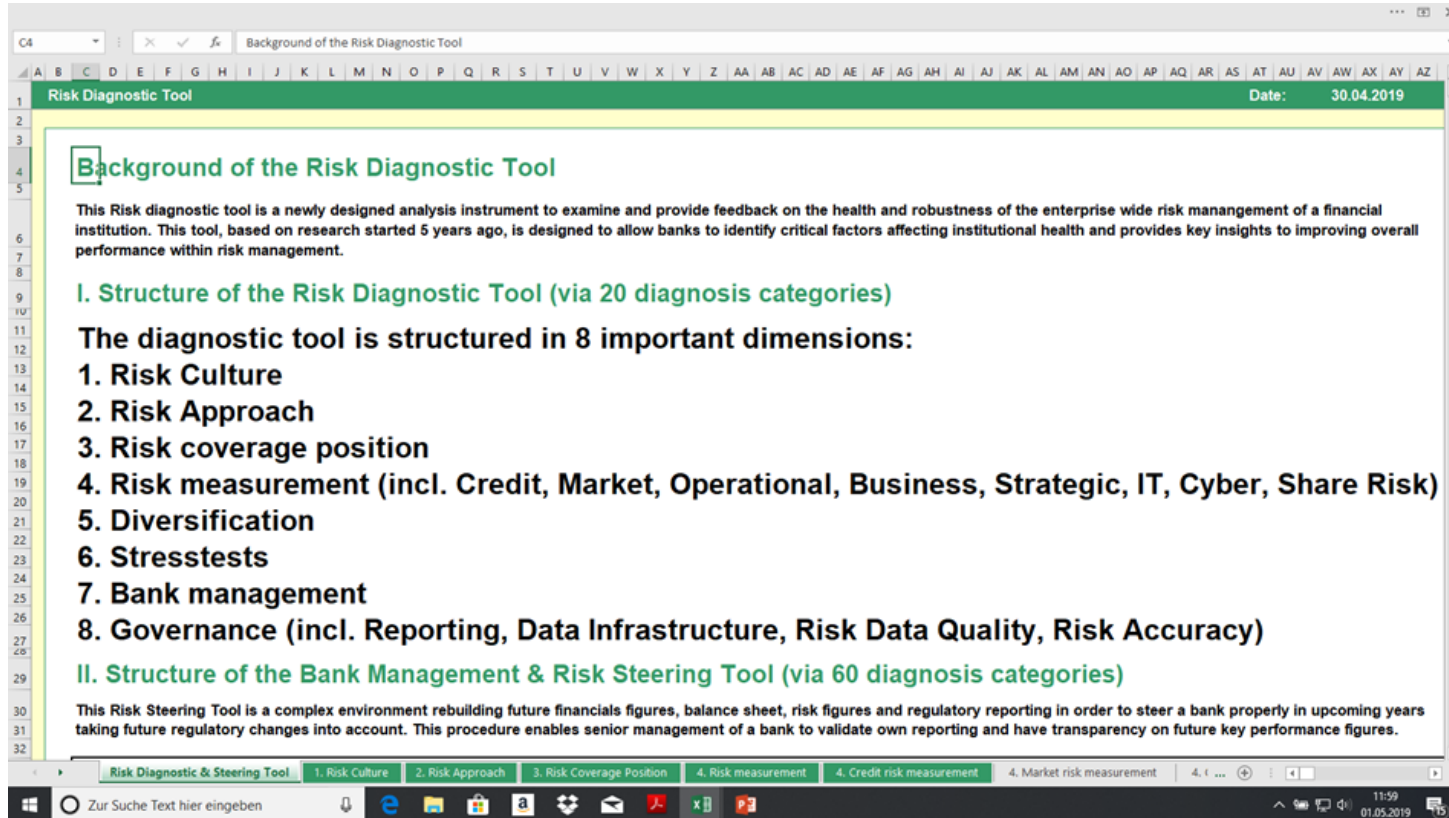
Significantly decreases your project challenges / risks.



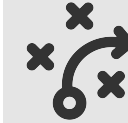
# OUR TOOL - FUNCTIONAL FOCUS

				
<b>Balance Sheet</b>	<b>Credit Risk</b>	<b>Market Risk</b>	<b>Operational Risk</b>	<b>Business and Strategic Risks</b>
Capital adequacy	Retail lending	Interest rate risk	People, processes, events	Macro-economic risks
Liquidity & funding	Corporation and institutions	FX	IT and data	Strategic risks
ICAAP and ILAAP	Counterparty credit risk	Other market risks	Conduct and compliance	Reputation

# OUR TOOL - MAIN STRUCTURE



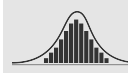
Risk culture



Risk approach



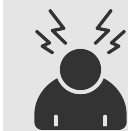
Risk coverage



Risk measurement



Diversification



Stresstests



Bank management



Governance

4. IT Risk Measurement							
1. Risk Culture	2. Risk Approach	3. Risk Coverage Position	4. Risk Measurement	5. Diversification	6. Stresstests	7. Bank management	8. Governance
4. IT Risk Measurement							
Overall Process		Key Topics and Questions to be addressed					Comments
<b>Risk assessment framework</b>  <u>Structured brainstorming activities are performed for identifying IT shortcomings, BAIT and other regulatory requirements, threat scenarios, bottlenecks associated with organisational assets, risks, estimated impact of risk and suitable treatments for identified risks.</u>	1. Does your institute have an IT strategy?		...			obligation	
	2. In the design of the IT systems and the ...		to comply with common standards (e.g. ISO 27001)?				
	3. Does your IT strategy include statements ...		strategic development of IT?				
	...		information security organization?				
	...		emergency management?				
	...		individual data processing in specialist areas?				
	4. Does your management assume the responsibility that, based on the IT strategy, regulations for the IT setup and organization...		...				
	...		be determined?				
	...		be adapted promptly in case of changes?				
	...		be implemented effectively?				
	5. Is your management responsible for ensuring that staffing levels are adequate in terms of quantity and quality for ...		...				
	...		information risk management?				
	...		information security management?				
	...		IT operation?				
	...		Application development?				
	6. Are conflicts of interest and incompatible activities within the IT build-up and roll-out organization avoided (for example, by defined role definitions and authorizations)?						
	7. Does your management use appropriate qualitative and quantitative control criteria...		...				
	...		of IT operations?				
	...		of IT developments?				
	8. Are you operating an user authorization management...						
	...		by which incompatible activities and conflicts of interest of the staff are avoided?				

8 Main Areas

4. IT Risk Measurement							
1. Risk Culture	2. Risk Approach	3. Risk Coverage Position	4. Risk Measurement	5. Diversification	6. Stresstests	7. Bank management	8. Governance
4. IT Risk Measurement							
Overall Process	Key Topics and Questions to be addressed						Comments
<u>Risk assessment framework</u>  <u>Structured brainstorming activities are performed for identifying IT shortcomings, BAIT and other regulatory requirements, threat scenarios, bottlenecks associated with organisational assets, risks, estimated impact of risk and suitable treatments for identified risks.</u>	1. Does your institute have an IT strategy tailored to the business and risk strategy?						
	2. In the design of the IT systems and the associated IT processes, have you ensured the fundamental obligation to comply with common standards (e.g. ISO 2700X)?						
	3. Does your IT strategy include statements about ...						
	... strategic development of IT?						
	... information security organization?						
	... emergency management?						
	... individual data processing in specialist a						
	4. Does your management assume the re						
	... be determined?						
	... be adapted promptly in case of changes						
	... be implemented effectively?						
	5. Is your management responsible for e						
	... information risk management?						
	... information security management?						
	... IT operation?						
	... Application development?						
	6. Are conflicts of interest and incompatible activities within the IT b						
	avoided (for example, by defined role definitions and authorizations)						
	7. Does your management use appropriate qualitative and quantitative						
	... of IT operations?						
	... of IT developments?						
	8. Are you operating an user authorization management...						

Main subjects  
break down in  
sub-elements

80 sheets  
in total



Compliance checks															
1. Risk Culture		2. Risk Approach		3. Risk Coverage Position		4. Risk Measurement		5. Diversification		6. Stresstests		7. Bank management		8. Governance	
4. Cyber Risk Measurement															
Overall Process		Assessed Items		Key Topics and Questions to be addressed				Compliance checks				Comments			
<p><u>Structured brainstorming activities are performed for identifying threats, threat scenarios, vulnerabilities associated with organisational assets, risks, estimated impact of risk and suitable treatments for identified risks.</u></p> <p>cyber thief. Remember that customer data is often the most important thing to protect, because although the direct cost of losing it may be small compared with research data or intellectual property, you're likely to lose more through fines and lawsuits. Furthermore, the cost to your public image and the loss of customer trust can take years to recover.</p>		<p>1. Understand the Value of Your Data</p>		What data is mission-critical to your business, and what are the systems that handle it?											
				What data might be of value to someone else?											
				And what must be protected by law?											
				Consider all your company's data, as well as where it comes from, where it's stored, who has access to it and what security procedures they must go through to reach it? Network administrators have the challenging responsibility of assessing risk to the networks at any time and then to plan the remedies accordingly.											
				Are these measures secure enough?											
				Do you use two-factor authentication (additional security beyond basic password protection)?											
				Are your people trustworthy?											
				Who might want your data or wish to disrupt your operations?											
		<p>4. Quantify Potential Threats.</p>		What are their capabilities and typical attack methods?											
				Is it worse if they steal data, render it inaccessible, or alter it? Think of recent ransomware attacks in hospitals,											
				Look at your data from an attacker's perspective-to what extent will they go to achieve their goal? Consult your IT team about appropriate hardening, scanning, and monitoring of critical systems to protect your business against the most likely and harmful attack opportunities.											
				Do you have strict protocols, policies or automated restrictions in place to protect your networks, email and other systems?											
				Do you encrypt data on your network, and do you dispose of old computers safely?											
				How do you deal with the danger of "undercover hackers," who join companies to gain easy access to their security systems and to steal data?											
				Do you have a business-continuity plan in place to prepare for and deal with any issues that may arise?											
				Many cyber-specific methodologies are based on identifying assets, threats and vulnerabilities. You prepare lists of each and then identify how a vulnerability in one of your systems presents an opportunity for an attacker to threaten one or more of your assets. Whenever all three occur, there is a risk. If there is a vulnerability but no threat, or a vulnerability and a threat but no asset that can be attacked, there is no risk.											
		<p>5. Identify where your systems are vulnerable.</p>		What level of risk are you willing to accept? Addressing all the risks and fixing all vulnerabilities in every system is beyond most technical or financial resources											
				Do you have an advanced cybersecurity incident-response plan in place?											
		<p>6. Determine the impact of threats and how likely they are to occur.</p>		Create a cyber risk framework including strategy and risk appetite as well as internal control environment.											
		<p>7. Define Your Risk Threshold.</p>													
		<p>8. Prioritize risks and start resolving them.</p>													

Including current focus areas, e.g. cyber risk



## 5. BENEFITS FOR YOU



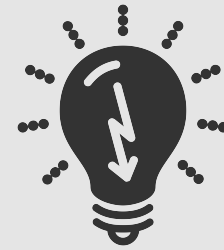
# BENEFITS



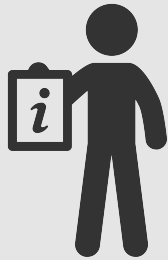
Resource Optimization



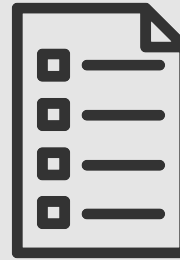
Transparency



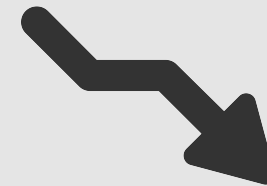
Impact analysis



Tailored recommendations



To do list



Reduced project risk

## 6. WHY RISK & MORE

# WHY RISK & MORE



## Our Team

Significant experience with regulatory audits

KISS —> keep it simple

Do the right thing!

Passion and fun



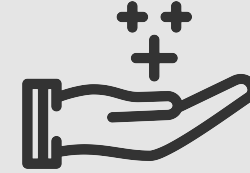
## Competencies

Functional competency and experience

Solutions rather than problems

Communication

Entrepreneurial spirit



## Our Values

Commitment and integrity

Transparency —> turn on the lights

Solve a problem —> add value  
—> fair price

Flexibility —> tailored recommendations

# MEET THE CONSULTANTS



**PETER BUERGER**



- Experience in risk management since 1990
- Managing Director *Risk & More* since 2010
- Former Head of Risk Control & Deputy Chief Risk Officer of a Systemically Important European Bank
- Former Regional Chief Credit Officer, \$50 billion portfolio
- Strong expertise in all key banking divisions: corporate banking including commercial real estate, consumer lending, capital markets, asset management
- Internal committee experience, e.g. Risk Committee, Credit Committee, ALCO
- Significant project experience in projects of all sizes
- Honorary Senior Visiting Fellow in the Faculty of Finance, Cass Business School / City University of London, UK
- Married with 3 children, passionate about Football

# MEET THE CONSULTANTS



MARKUS LINSS



- Experience in risk management since 1996
- Managing Director Risk & More since 2018
- Former General Manager Financial Institution
- Former Head of Risk Management & Control of a Systemically Important European Bank for Real Estate & Infrastructure Finance with strong expertise in bank risk & capital management
- Strong expertise in all key banking divisions: corporate banking including commercial real estate, consumer lending, capital markets, asset management
- Internal committee experience, e.g. Risk Committee, HR & Finance Committee
- Significant project experience in projects of all sizes
- Expert in restructuring & turnaround programs as well as company management & performance concepts
- Married with 2 children, passionate about Motorcycling and Football



## 7. CONTACT DETAILS





## GET IN TOUCH

CHECK OUR LOCATION IN **FRANKFURT AM MAIN**



**RISK & MORE**

### **RISK & MORE CONSULTING**

GIMBACHER TANN 28  
65779 KELKHEIM  
GERMANY

[PB@RISK-AND-MORE.COM](mailto:PB@RISK-AND-MORE.COM)

+49-151-25678555

[WWW.RISK-AND-MORE.COM](http://WWW.RISK-AND-MORE.COM)

