

September 2017

The 'Cyber-Aware' ORMF

Our point of view



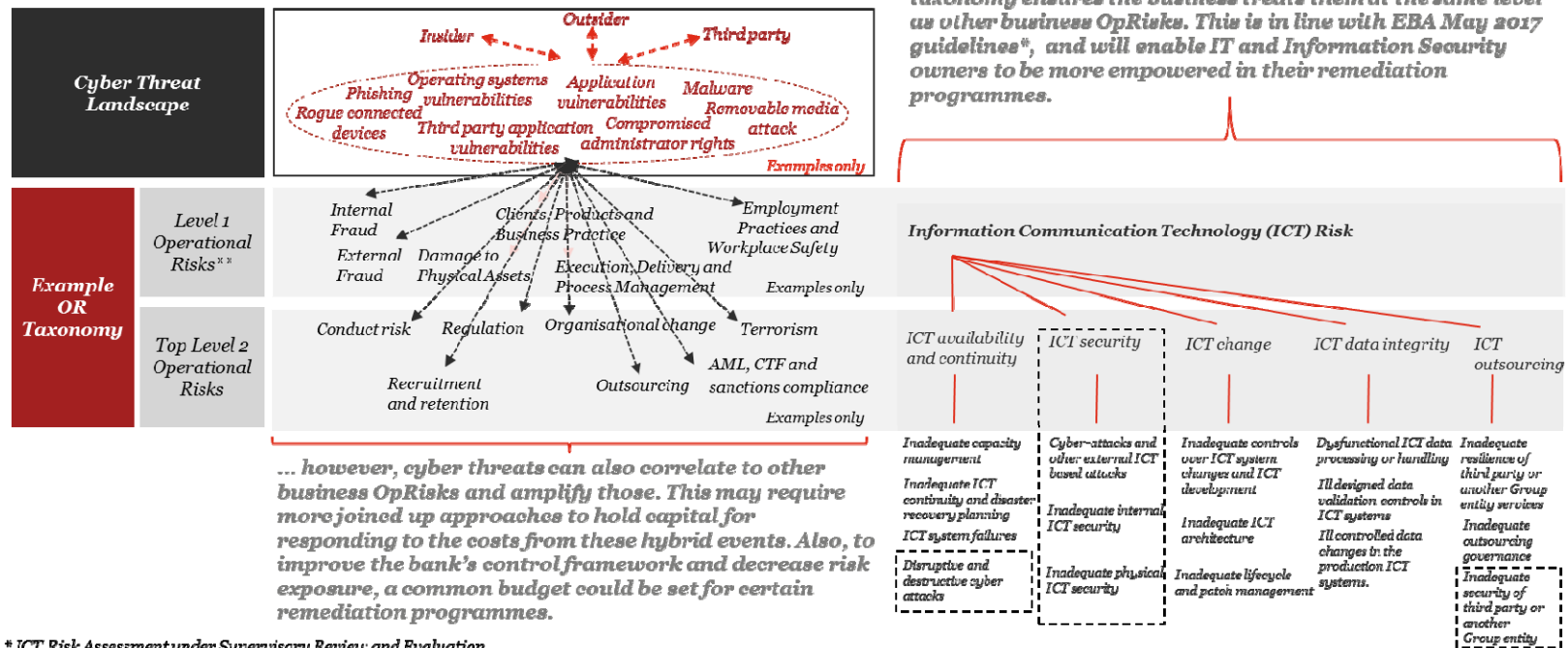
pwc.co.uk/cyber

Confidential information for the sole benefit and use of PwC's client.

Why build a 'Cyber-Aware' ORMF, quantifying cyber risk?

- 1** Ensure that the Operational Risk (OpRisk) appetite is backed by ongoing **quantification** of cyber risk exposure, considering also how they correlate to and **amplify exposure of other OpRisks**
- 2** Use the quantification of cyber risk exposures in your **decision-making to prioritise investments** in mitigation (e.g. cyber resilience programmes, cyber insurance)
- 3** **Communicate to your stakeholders** (internal, 3rd party partners, customers, shareholders and regulators) that you understand and have appropriately assessed your Cyber Risk exposure in line with **changing regulations** and industry good practice

Cyber risk is a stand-alone OpRisk but can also amplify other business OpRisks



Having technology and cyber risks as part of the OpRisk taxonomy ensures the business treats them at the same level as other business OpRisks. This is in line with EBA May 2017 guidelines*, and will enable IT and Information Security owners to be more empowered in their remediation programmes.

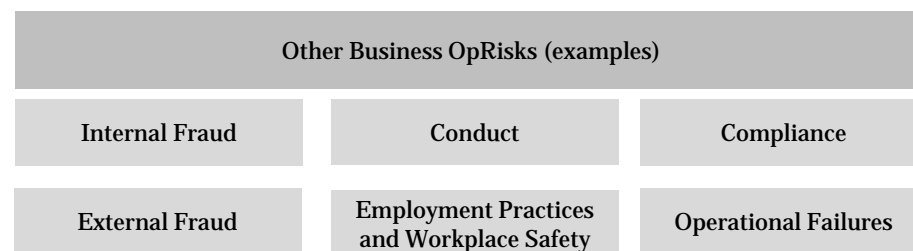
... however, cyber threats can also correlate to other business OpRisks and amplify those. This may require more joined up approaches to hold capital for responding to the costs from these hybrid events. Also, to improve the bank's control framework and decrease risk exposure, a common budget could be set for certain remediation programmes.

* ICT Risk Assessment under Supervisory Review and Evaluation
 ** Basel OR Loss event categories taken as example for Level 1 Operational Risks

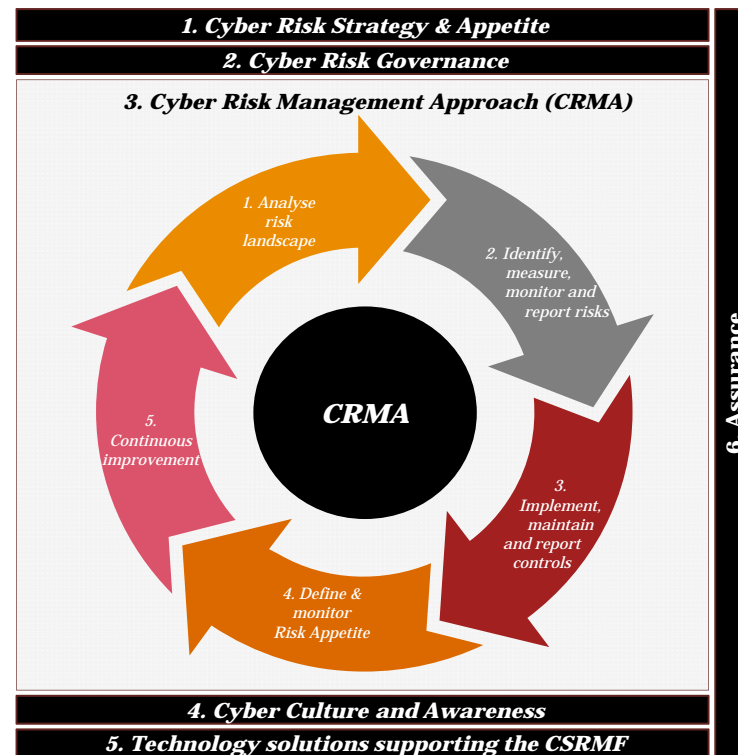
Cyber risk exposure vs risk appetite: stand-alone and correlated

Example Level 1 operational risk types	Risk Appetite			OpRisk Exposure			Cyber-OpRisk Exposure				
	Qualitative	Quantitative		OpRisk Scenarios Exposure	Risk and Control Self-Assessments Exposure	OpRisk Events/Incidence Exposure	Cyber Threat Ref#	Cyber Scenario Ref#	Likelihood	Financial Impact	Exposure
		Cumulative loss Tolerance	Individual material loss threshold								
Internal Fraud	Low	£500k	£100k	£1m	Low	£50k	12,13,16	1,2,3,4	Medium	£1m	High
External Fraud	Low	£500k	£100k	£1m	Low	£20k	12,15,17,20,21,22	5,6,7	High	£1m	High
Clients, Products and Business Practice	Medium	£1m	£200k	£1m	Medium	£150k	12,17,19	8,9	Medium	£1m	Medium
Business Disruption and Systems Failures	Low	£500k	£100k	£5m	Low	£70k	14,1,17,18	10,11,12,13	High	£5m	High
Execution, Delivery and Process Management	Low	£500k	£100k	£5m	Low	£80k	17,18,19	14,15,16	High	£5m	High
Damage to Physical Assets	Medium	£1m	£200k	£1m	Medium	£130k	18,21,35	17,18	Low	£1m	Medium
Employment Practices and Workplace Safety	Low	£500k	£100k	£200k	Low	£60k	25,27,47	19,20	Low	£200k	Low
Cyber	Medium	£1m	£200k	See Cyber-OpRisk Exposure columns	Medium	£140k	All	21,22,23,24	High	£14.2m	High

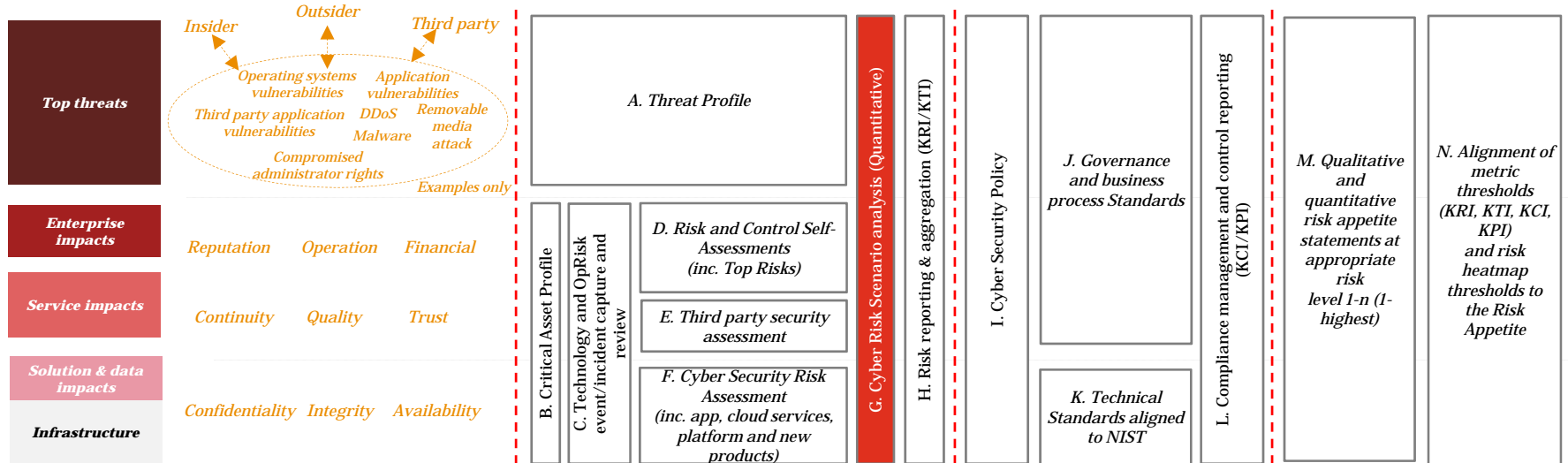
Cyber risk is an operational risk and managed as part of ORMF



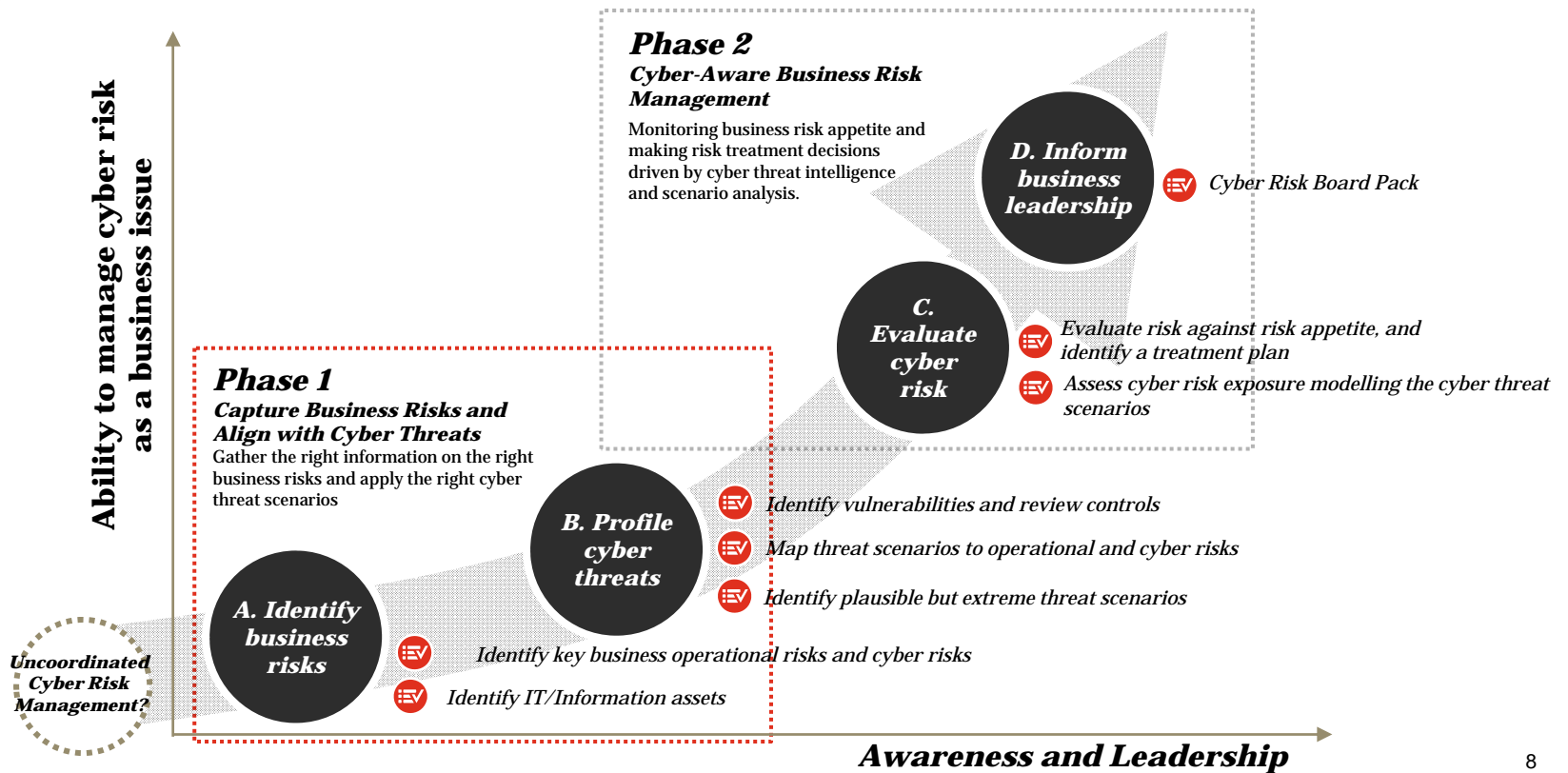
Example Cyber Risk Management Framework (CRMF)



Example Cyber Risk Management Approach (CRMA)



Approach to establish the Cyber-OpRisk exposure to the business



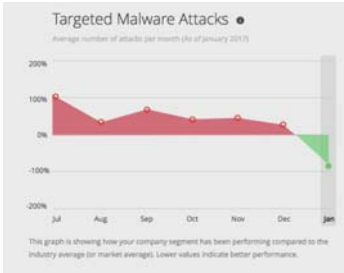
Cyber Risk Quantification Tool powered by Symantec™

- Company Analytics**
- Company Specific Business Information
- Specific External Cyber Security Metrics
- Aggregated Internal Security Metrics
- Company Specific Cyber Security Scenarios
- Deep Dive Questions to increase precision

1. Company Specific Assessment



2. Historic Cyber Security Metrics



3. List of Cyber Risk Scenarios

Severity	Threat Scenario	Frequency
4	Financial Pretexting	1/3
3	C&C Takeover	1/4
3	Hacktivist Attack	1/3
2	DDoS Attack	1/2
2	Website Defacement	1/2
1	Crypto Malware	1/1

Extensive company coverage	Readily available quantitative data on companies	Insight to drive qualitative assessments and drive more business
200,000+ Companies with enhanced underwriting data	200+ External Cyber Security Metrics	430+ Deep Dive Questions available in dynamic questionnaire
7 Million Companies with standard underwriting data	200+ Internal Cyber Security Metrics	23 Cost Center Specific Sections
130 Million Domains with basic IT and security data	100 Cyber security scenarios with sized financial impacts for your clients	90% Faster Decision making, in some cases



This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2017 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.