The traditional risk assessment models, which assess risks based on their individual impact or likelihood have been widely applied by many organizations. The existing models, however, fail to recognize the interconnections among the risks which may reveal enhanced assessment dimensions and more pertinent risk mitigating actions. In response to this, the Dynamic Risk Assessment (DRA) has been developed based on proven scientific modeling, expert elicitation, and advanced data analytics. DRA enables organizations to gain a deeper understanding into how risks impact the different parts of the firm and, subsequently, to design more effective and efficient risk mitigating measures.

Above and Beyond the Hidden Structure of Interconnections between Risks

A. Kristamuljana MSc is a Senior Consultant in Risk & Regulatory at KPMG The Netherlands.

kristamuljana.archimedes@kpmg.nl

Drs. B. van Loon RA is a Partner in Risk & Regulatory at KPMG The Netherlands.

vanloon.bart@kpmg.nl

Drs. J. Bolt RC is a Senior Manager in Risk & Regulatory at KPMG The Netherlands.

bolt.jeroen@kpmg.nl

Prof. Dr. A. Terblanché is a Partner at KPMG in the United Kingdom.

andries.terblanche@kpmg.co.uk

Dynamic Risk Assessment

INTRODUCTION

One of the main things learned in risk management since the new millennium is the previously unobserved levels of correlation. We have since learnt that volatility itself is volatile, an attribute for which most financial mathematical models make insufficient allowance. It re-introduced the question of whether structural breaks in the system exist and how to allow for their presence in modeling, impairment assessments and other financial valuation techniques.

The above developments pose ominous warnings for risk and financial managers alike as they infer that risk assessments and asset valuations can drift to levels that, in certain cases, grossly underestimate risks and can cause valuations to gyrate violently.

Unless business, academic institutions and regulators get better at managing these cycles and corrections, businesses will be subjected to ever increasing public scrutiny, more intrusive regulation and regulators, new-found antagonistic behavior from the public, reduced market capitalization and greater friction costs in doing business.

Whilst this plays to a populist agenda, it does little to improve economic growth, which we have now seen constitutes the tide that most lifts most personal wealth boats. Risk management has a crucial role to fulfill: not only within the business, but also for its immediate and wider stakeholders.

The Dynamic Risk Assessment Approach

In response KPMG has developed an innovative approach referred to as 'Dynamic Risk Assessment' (DRA). DRA is based on the science of expert elicitation, invented by the US military in the 1950s. At the time it faced the challenge of remaining ahead of Soviet military developments that were taking place behind an impenetrable iron curtain. The military, similar to risk managers today, faced a fu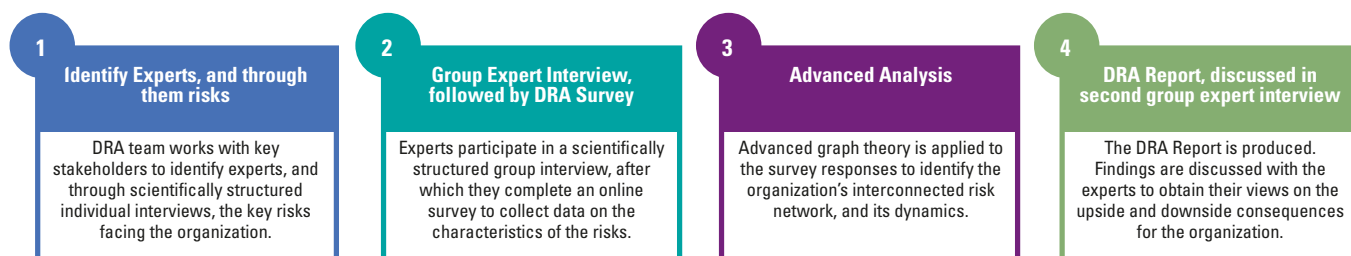ture that could not be credibly modeled by traditional means. They quickly learned that expert elicitation is a helpful alternative, to the point where it aided the US military not only to match covert Soviet developments, but to stay abreast throughout the Cold War and thereafter.

More specifically, the US military discovered that, by (1) identifying experts scientifically and (2) conducting scientifically structured individual and group interviews, a credible future threat/risk landscape could be generated. DRA capitalizes on these insights and extends them into a third and fourth dimension: the experts are requested to provide their individual perspectives on how the risks can be expected to trigger or exacerbate each other, and the velocity with which they can affect the organization. With these risk perspectives an organization-specific risk network can be constructed to obtain key insights into the organization's systemic risk landscape.

These insights are presented back to the experts to obtain their views on the consequences and the opportunities available to the organization, whereupon it is circulated to Those Charged With Governance to enrich their risk mitigation decision-making.

> One of the main things learned in risk management since the new millennium is the previously unobserved levels of correlation

Figure 1. The four steps of Dynamic Risk Assessment.

1 Identify Experts, and through them risks
DRA team works with key stakeholders to identify experts, and through scientifically structured individual interviews, the key risks facing the organization.

2 Group Expert Interview, followed by DRA Survey
Experts participate in a scientifically structured group interview, after which they complete an online survey to collect data on the characteristics of the risks.

3 Advanced Analysis
Advanced graph theory is applied to the survey responses to identify the organization's interconnected risk network, and its dynamics.

4 DRA Report, discussed in second group expert interview
The DRA Report is produced. Findings are discussed with the experts to obtain their views on the upside and downside consequences for the organization.

DYNAMIC RISK ASSESSMENT EXPLAINED

Clustering of risks

Traditional risk models assess the prioritization of risks on individual impact or likelihood. Although these assessments are useful, the traditional model (Figure 2) fails to recognize the interconnections between risks (Figure 3) or the effect of clustering risks. As illustrated in Figure 4, a seemingly low 'risk of failure to attract talent' could potentially form part of a high severity risk cluster, that of operational risks.

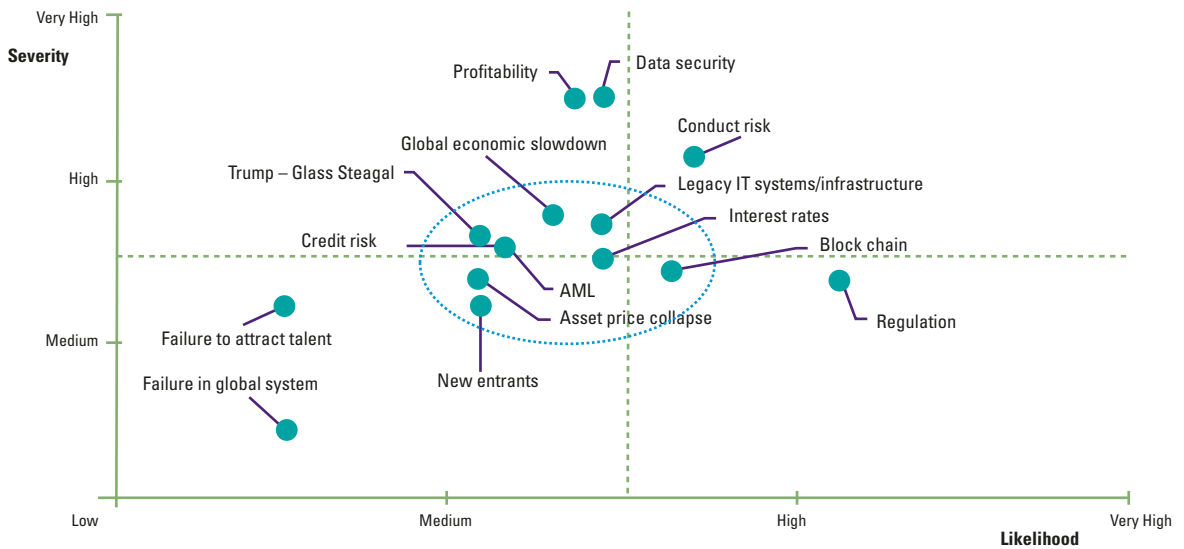**Figure 2.** Traditional depiction of risks (illustrative).

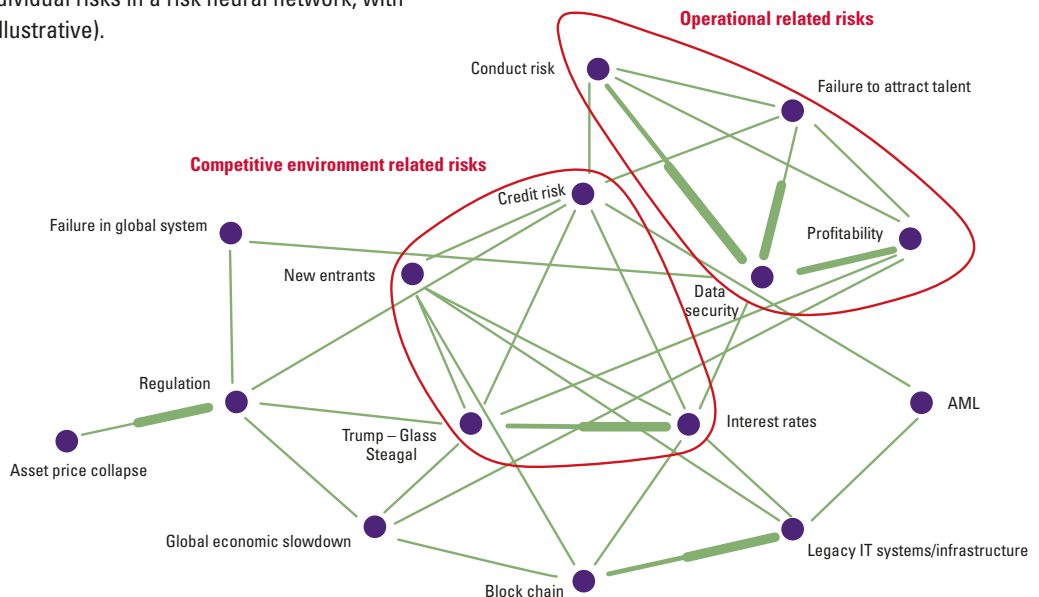**Figure 3.** Individual risks in a risk neural network, with clusters (illustrative).

Figure 4. Aggregated likelihood and severity of a cluster of risks (illustrative).
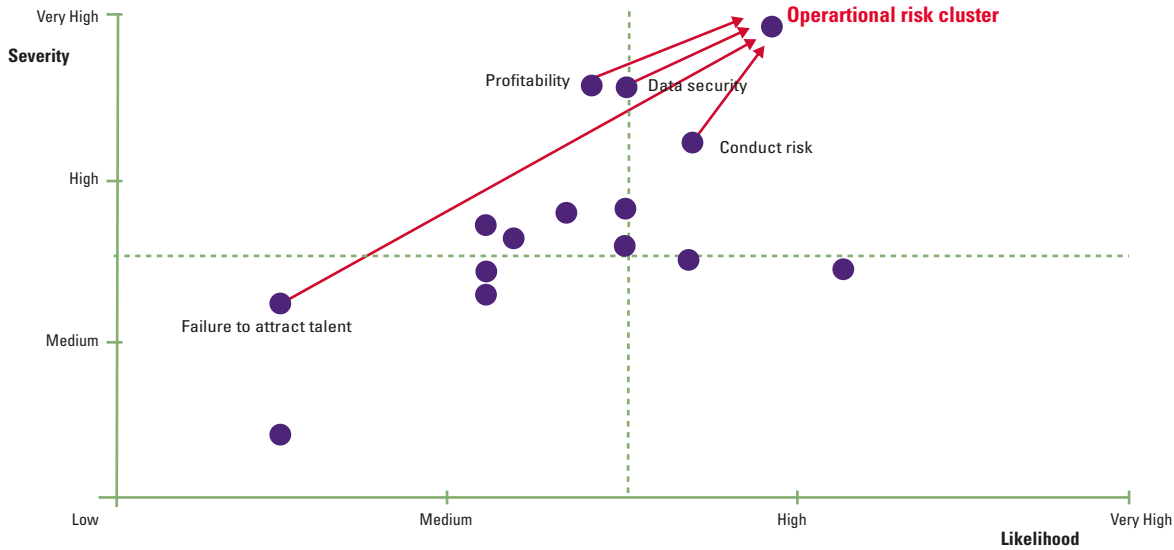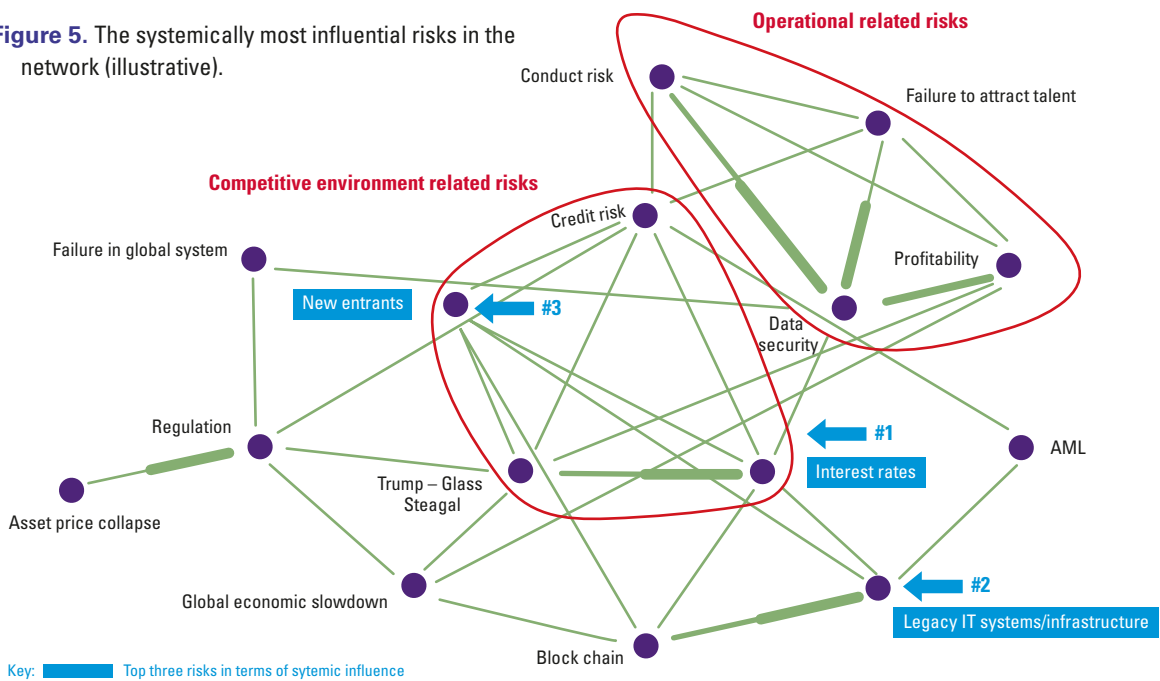

Operartional risk cluster

Severity axis: Very High, High, Medium, Low
Likelihood axis: Low, Medium, High, Very High

Labels: Profitability, Data security, Conduct risk, Failure to attract talent

Figure 5. The systemically most influential risks in the network (illustrative).

Operational related risks
Competitive environment related risks

Labels: Conduct risk, Failure to attract talent, Credit risk, Profitability, Failure in global system, New entrants #3, Data security, Interest rates #1, AML, Regulation, Trump – Glass Steagal, Asset price collapse, Global economic slowdown, Legacy IT systems/infrastructure #2, Block chain

Key: Top three risks in terms of sytemic influence

Risk Influences

DRA also calculates influences between risks, i.e. to what extent will the occurrence of one risk trigger the occurrence of other risks, and vice versa. In this manner the three most influential risks can be identified (Figure 5). These are the risks that, when they occur, will trigger most of the other risks - across the network.

Similarly, the three most vulnerable risks can be identified (Figure 6). These risks are the risks most likely to occur *following* the occurrence of any other risks in the network.

Knowing the contagion forces between risks is important in a) selecting the key risks to focus on, and b) selecting the appropriate controls (in type and strength) to mitigate them. For example, since the most influential risks can trigger other risks, mitigation of the organization's systemic risks should commence with these risks. For the most vulnerable risks, preventive controls should be preferred over detective controls.

Figure 7 depicts a consolidated view of individual risks, risk clusters, most influential and most vulnerable risks.

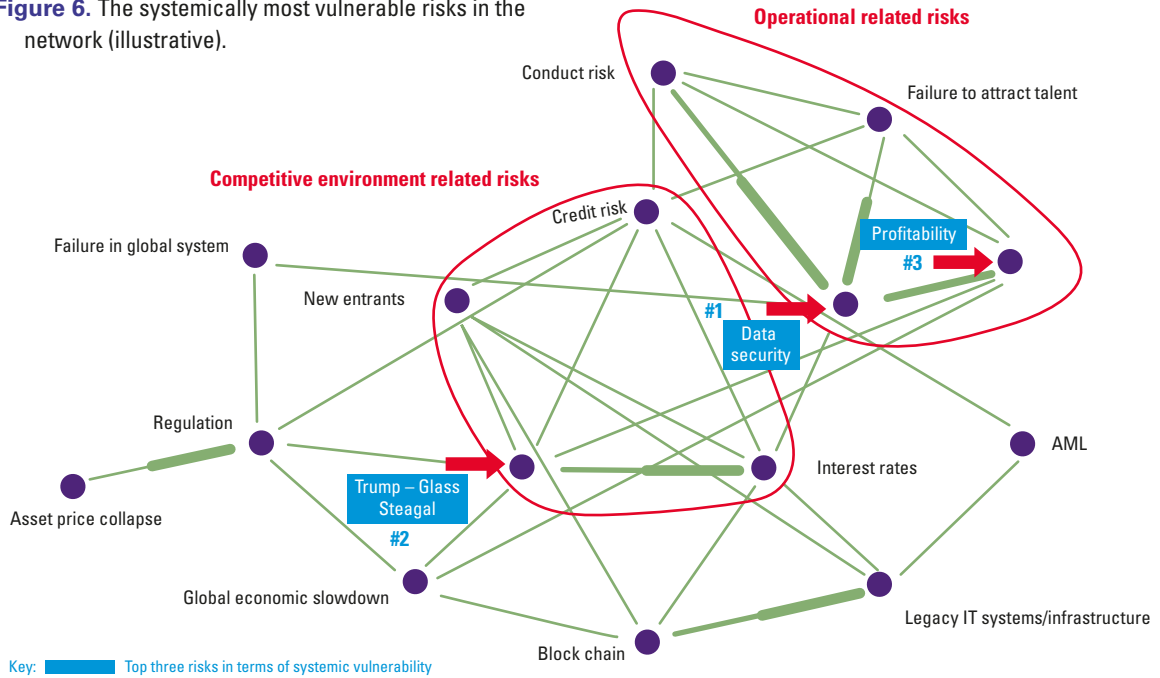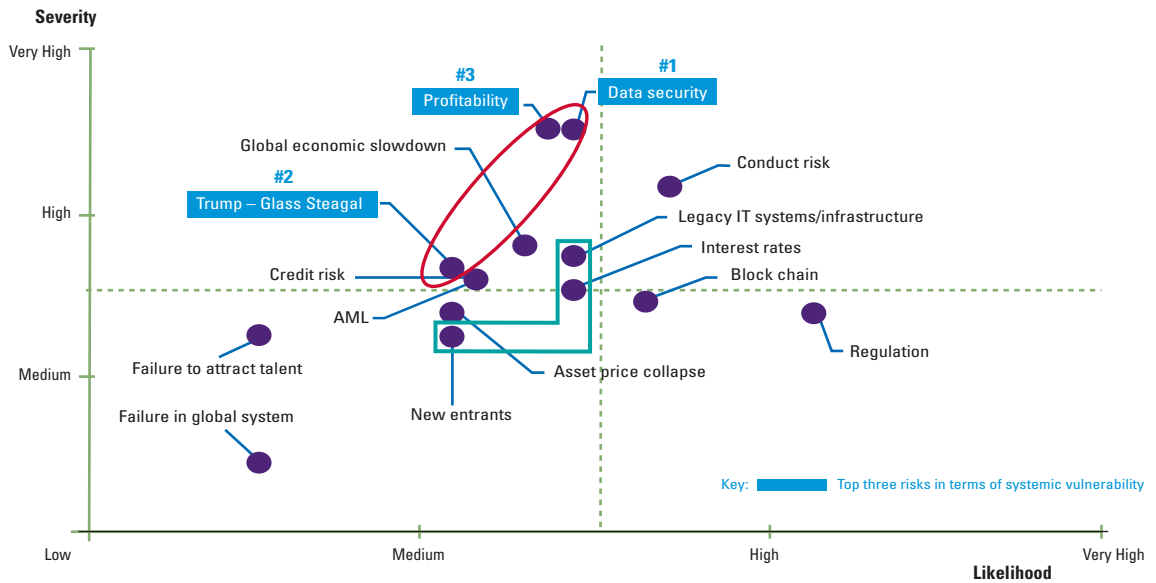**Figure 6.** The systemically most vulnerable risks in the network (illustrative).

Operational related risks

Competitive environment related risks

Conduct risk
Failure to attract talent
Credit risk
Profitability #3
Failure in global system
New entrants
Data security #1
Regulation
AML
Asset price collapse
Trump – Glass Steagal #2
Interest rates
Global economic slowdown
Legacy IT systems/infrastructure
Block chain

Key: ▬▬ Top three risks in terms of systemic vulnerability

Figure 7. Putting it together (illustrative).

Severity

Very High

#3 Profitability | #1 Data security

Global economic slowdown
#2 Trump – Glass Steagal

High

Conduct risk
Legacy IT systems/infrastructure
Interest rates
Block chain
Credit risk
AML
Regulation

Medium

Failure to attract talent
Asset price collapse
New entrants
Failure in global system

Low   Medium   High   Very High

Likelihood

Key: ▬▬ Top three risks in terms of systemic vulnerability

Based on this view, we can design risk mitigating activities and assign related governance responsibilities.

Risk mitigation

Risk mitigation is aimed at addressing how a particular risk should be optimally responded to. Within DRA, mitigation is accomplished through the application of bow ties. The first step for risk mitigation therefore begins with determining the clusters and calculating their aggregate severities (Figure 4). This process is followed by the identification of the most influential and most vulnerable risks,

and thereafter the black swans – risks that display weak links to other risks yet, in aggregate, have catastrophic outcomes. DRA's mitigation phase identifies the most vulnerable risks as well as risks that could form part of a black swan chain, and assigns these to the CRO as these risks have the gravest systemic consequences.

In identifying the most influential risks, responsibility for monitoring is allocated to the CEO since these risks have the widest systemic reach. The CEO can then be challenged to invert them into competitive advantages.

Figure 8. Data security bow tie (illustrative).
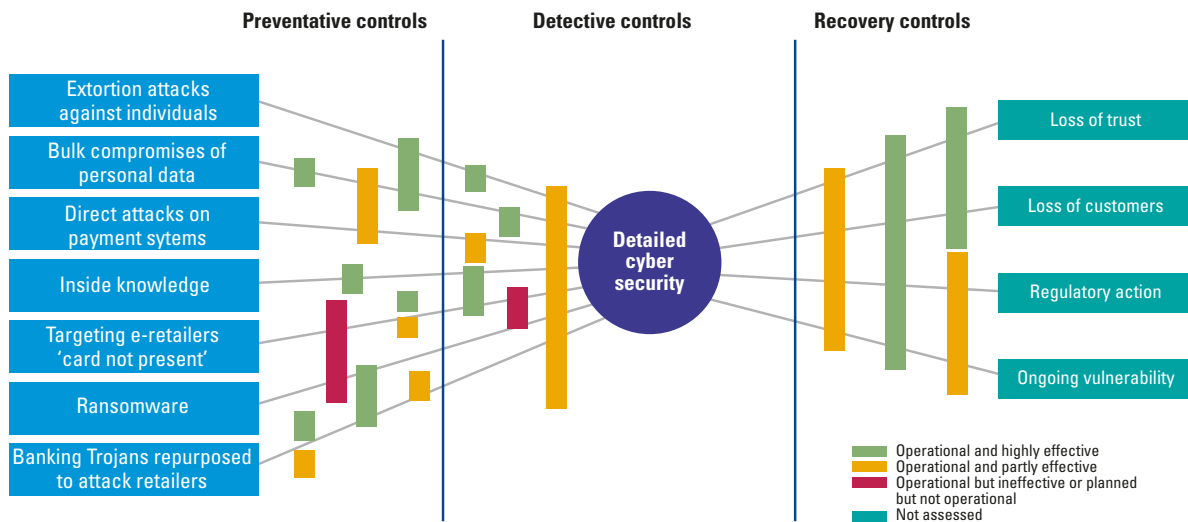
Risks that are individually insignificant and not connected to any significant outcomes are delegated to subordinates.

Data security, for instance, is classified in Figure 7 as a risk that carries a high severity individually, and forms an Operational Risk Cluster with significant aggregate outcomes together with *profitability*, *conduct risk*, and *failure to attract talent*. The risk mitigating measures for data security can subsequently be designed as shown in Figure 8. The diagram shows various related (external and internal) threats, key controls (preventive, detective, and recovery, with their current status of effectiveness) and the risk consequences. For each key control responsibilities can be allocated across the three lines of defense – ownership lies with the first line, supervisory roles with the second line, and evaluations on the third line. The frequency of reporting back to Those Charged With Governance is determined based on the criticality of control and significance of risk.

CONCLUSION

Traditional models assess risks based on their individual impact or likelihood, but fail to recognize the interconnections among the risks. In response to this, KPMG designed the Dynamic Risk Assessment based on proven scientific modeling, expert elicitation and advanced data analytics. The Dynamic Risk Assessment enables users to gain a deeper understanding into how risks impact the different parts of the organization and, subsequently, to the design of more effective and efficient risk mitigating measures.

About the authors

Archimedes Kristamuljana MSc is a Senior Consultant at the Risk and Regulatory practice of KPMG The Netherlands. His experience includes identification and analysis of Corporate Governance, Internal Control, and Risk Management issues at Fortune Global 500 and Dutch listed companies.

Drs. Jeroen Bolt RC is a Senior Manager at the Risk and Regulatory practice of KPMG The Netherlands. He is responsible for the advisory service in the area of Risk Management and Internal Control. He has extensive experience in the field of Governance Risk and Compliance (GRC), as well as the design, implementation, and optimization of risk and control frameworks.

Drs. Bart van Loon RA leads the Internal Audit, Risk, and Compliance (IARCS) practice of KPMG The Netherlands. He has more than 20 years of experience in the field of Enterprise Risk Management, Internal Control, and Internal Audit. Bart also leads the Governance, Risk & Compliance (GRC) service at KPMG in the Europe, Middle East, and Africa (EMA) region.

Prof. Dr. Andries Terblanché is the Global Lead of Dynamic Risk Assessment, which he conceived, spent ten years developing and is now scaling for use across KPMG's network of member firms. He advises on systemic risk to clients across industries such as banking and finance, insurance, aviation, energy, retail, motor vehicle and natural resources. An Adjunct Professor of Risk and Actuarial Studies at the University of New South Wales in Australia, he is also a guest lecturer at the University of Technology in Sydney.