Business & Decision

OPERATIONAL RISK

Keeping Up With New Challenges

The world of operational risk is changing quite drastically, whether it relates to the rise of cybercrime, the change of regulatory methods of measurement or other topics like the set-up of an enterprise culture change regarding operational risk. The note summarizes the current discussion points, both on the agenda of operational risk managers and IT risk managers. It suggests some actionable ideas for further improvement on this often overlooked but crucial and impactful risk topic.

1.

CYBER SECURITY

Cyber-attacks are in the news more & more frequently. This is pushing business & regulators alike to work on ways to better control these risks.

Mitigating such threats is becoming especially crucial with the arrival of Cloud systems and the related issue of outsourcing data. To cope with such risk, the following should be considered:

- Use data encryption to ensure confidentiality
- Train employees on cyber security best practices
- Identify, control and monitor the potential threats on IT and Business processes
- Reorganize your operating models by creating a transversal function accountable for the cyber security initiatives
- Be prepared to respond to any new cyber security threats

2.

COPING WITH INCREASING LEGAL REQUIREMENTS AND LIMITED RESOURCES

Legislation is changing and new topics are appearing such as the replacement of the AMA model, the supervision of the risk culture and outsourcing of departments.

In the short term, the big challenge is to avoid resource overload in converting all requirements into practice.

A set-up of properly managed & updated check lists containing all requirements is essential as best practice, in order to answer efficiently to regulatory expectations.

3.

WHAT IF AMA DISAPPEARS?

Financial authorities are looking at replacing the Advance Measurement Approach model (AMA), judging on its inadequacy to fully capture the real need in capital for operational risks.

While this is forcing institutions to reflect on what's next, it is important to note that not all aspects of the methodology is to be thrown away.

We believe that some methodological elements of AMA remain of high value and usable in other modeling efforts such as:

- the construction of scenarios, that could be applied to liquidity risk models to measure operational failures in key payments systems.
- The copula methodology to model dependencies between financial risks.

4.

THIRD PARTY PRIORITIZATION FOR BOTH SECURITY & BUSINESS CONTINUITY PLANS (BCP)

Operational Risk departments are often seen as police departments. However they can play a consultancy and advisory role to solve incidents.

In many institutions, incidents are often solved using the logic of “*the squeaky wheel gets the grease*”, especially when it is related to critical processes such as security and Business Continuity Plans topics.

We strongly suggest that the Operational risk department:

- Plays a central role as third-party prioritization
- Arbitrates what is urgent or not

So both IT and Business departments will receive a clear and transversal roadmap to handle operational issues.

5.

RISK CULTURE AND THE HERO MODE

Risk culture is a topic that both regulators and financial practitioners see as a key element in many operational failures.

The culture of solving operational risks today often relies on particular people, office heroes, that take the problem at heart and attempt to solve issues on their own, despite roadblocks within the organization. These Heroes put extra efforts to solve severe incidents as soon as possible but then, nothing happens structurally…

Therefore we suggest:

- To work on the root cause of the problem behind processes and systems failures instead of applying quick fixes.

In this manner, whenever a problem happens, you will no more rely solely on “extra effort” from your hero, but on an improved process.

6.

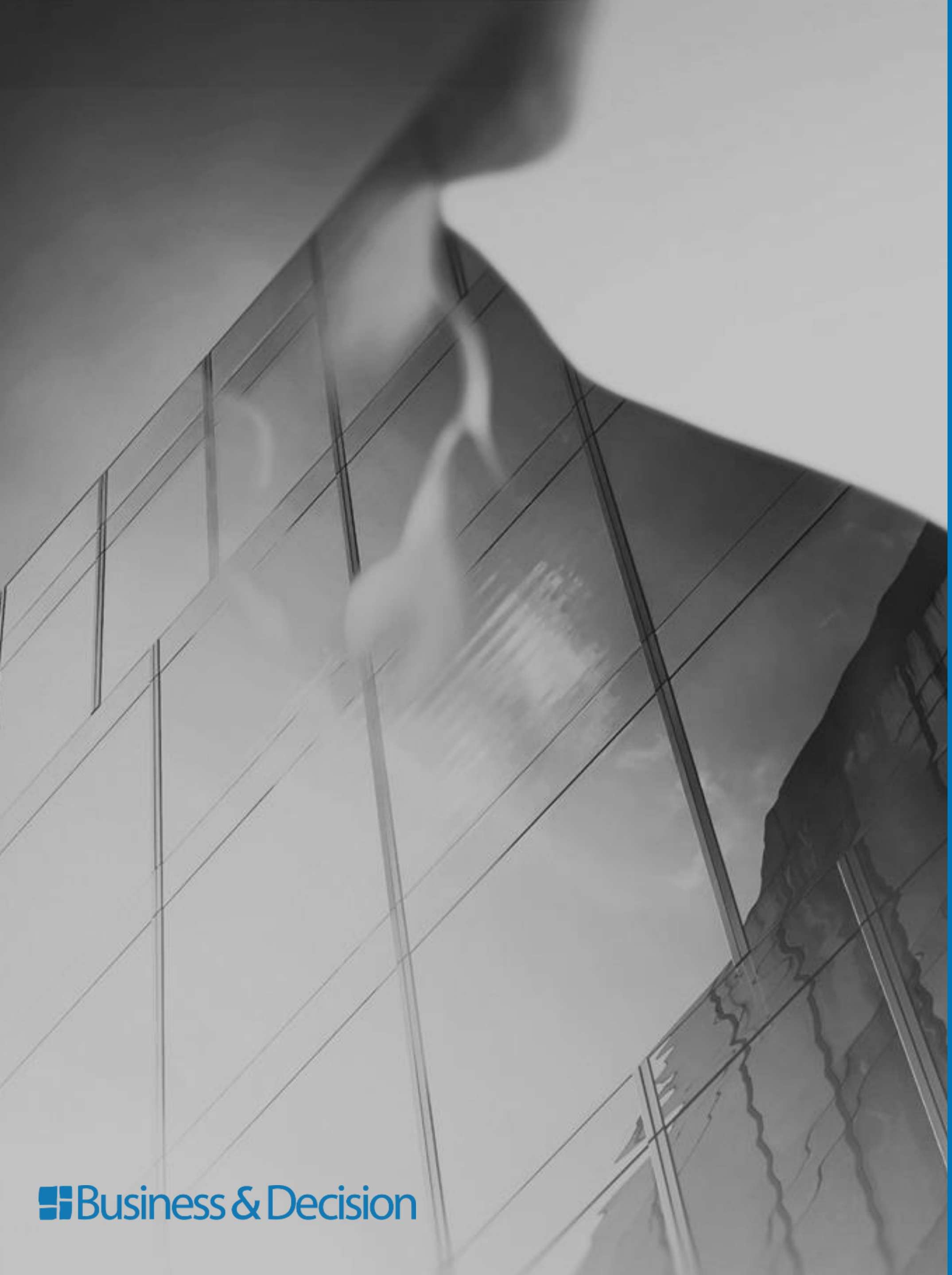
GOVERNANCE OF NEW CHANNELS

Security, governance, Internet of Things (IoT), cybercrime and clouds are currently amongst the biggest sources of operational risk.

As usual the good practices to follow are already developed, like ISO 2700 or PSI DSD 3.0. However the question is how to tackle them and not get drown in a heavy governance?

The answer is simple:

- Acknowledge that these standards cannot be 100% applied in your organization
- Use them as basis to create your own and simplified policies that will be smoothly adopted and used.



ROI^2

return on investment
through
return on information

IF YOU WANT TO KNOW HOW BUSINESS & DECISION CAN HELP YOU FACE THESE CHALLENGES, PLEASE CONTACT:

Frederik Cuppens
Digital Business Solutions
frederik.cuppens@businessdecision.com

Arnaud Piccin
Risk Practice
Arnaud.Piccin@businessdecision.com

Business & Decision