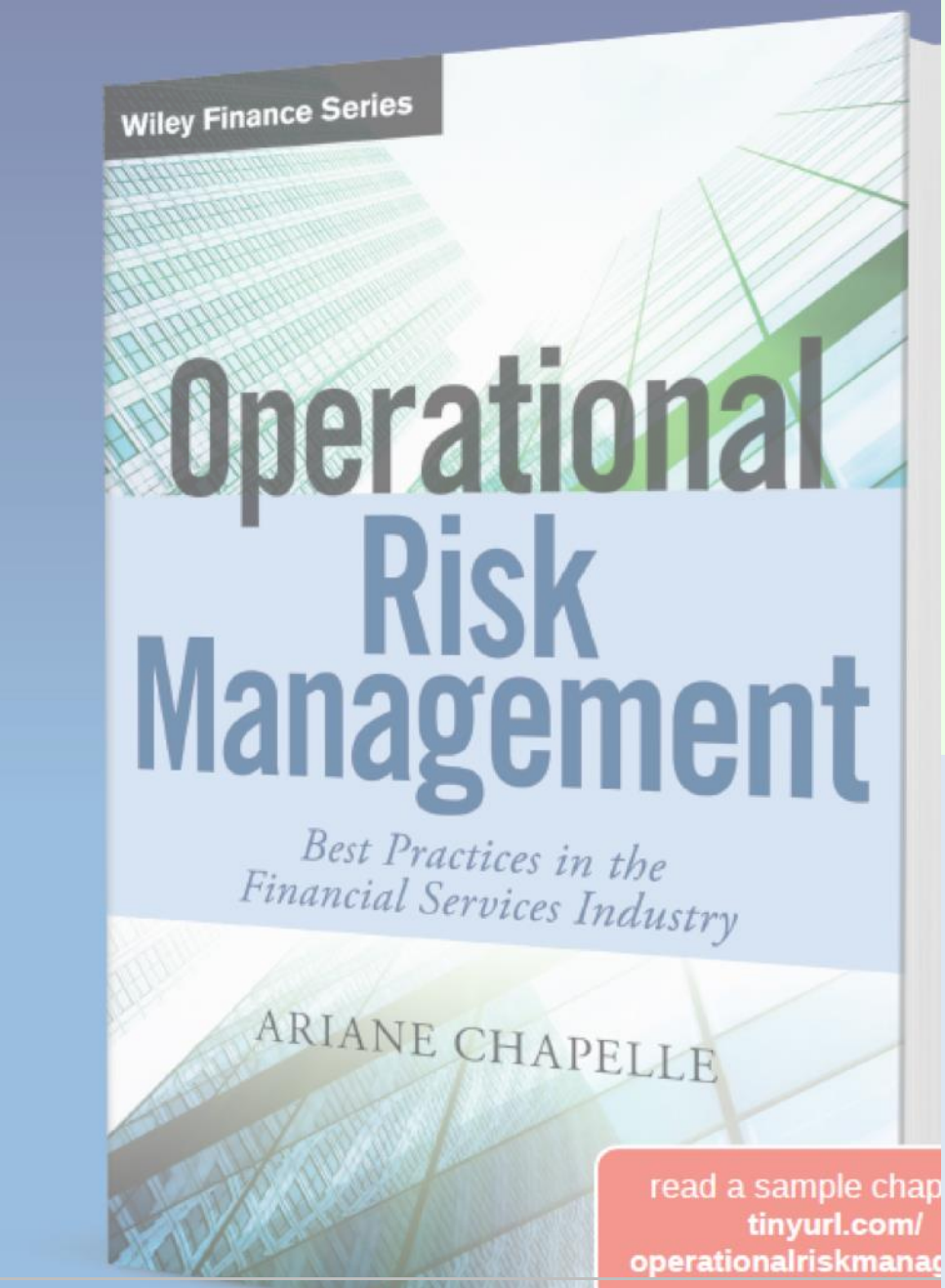


Recent trends and best practices in operational risk management

Cyprus Economic Society

Dr. Ariane Chapelle

November 28, 2018

CHAPELLE CONSULTING

Topics

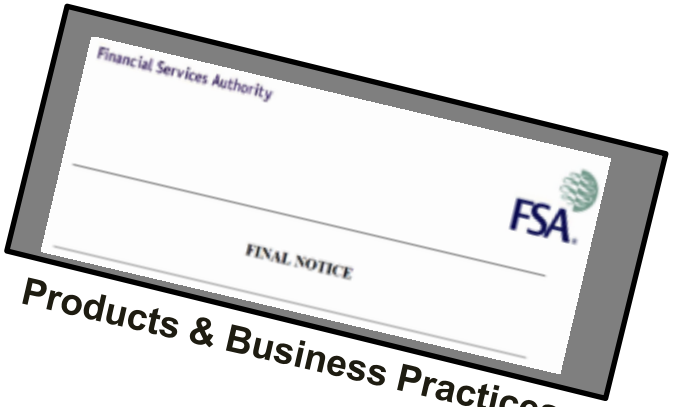
1. Definition and Scope of Operational Risk
2. Frameworks and Tools
3. Partners and Decision-Making
4. Governance and Culture
5. Maturity Criteria and Risk Management Trends

Operational Risk

.. is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. (Basel II, Solvency II)

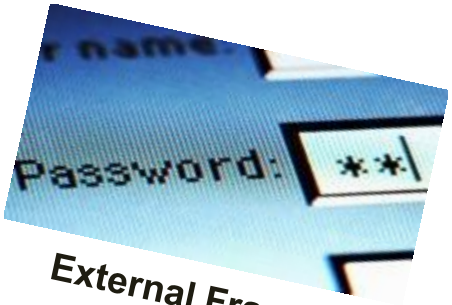
Processing errors

Internal Fraud



Products & Business Practices

Systems failure



External Fraud

Employment practice

Damage to physical assets

Risk Events (in just one day)

OUTSOURCING GIANT CARILLION'S COLLAPSE

TSB ROCKED BY FRAUD ATTACKS

JASPER JOLLY

@jjjolly

UNDER fire high street bank TSB has been hit by more than 10,600 alerts of potential fraud since its computer systems meltdown at the end of April, MPs heard yesterday.

The bank's chief executive Paul Pester faced stinging criticism from regulators and politicians during a grilling in front of the influential Treasury Select Committee.

TSB has experienced more than 2,200 confirmed fraud attempts, with more than 1,300 customers having money stolen. TSB has promised to compensate customers who are left out of pocket in any way.

Pester said the bank had been hit by an "unprecedented attack on UK banking from organised crime", with fraud attacks 70 times higher than normal. More than 12,500 TSB customers have switched their current accounts to competitors since

MAYFAIR BLAZE A huge fire broke out yesterday afternoon at the five-star Mandarin Hotel on William Street, Knightsbridge

A GIANT blaze engulfed the top floors of the Mandarin Hotel in Knightsbridge yesterday. Plumes of smoke were seen billowing from the hotel's rooftop. The London Fire Brigade said 15 fire engines and more than 100 firefighters were called to the scene. There were no reports of any injuries. The fire is thought to have spread to multiple floors across a "vertical facade" containing plants.

Credit Suisse agrees to pay US $47m over Asia hiring practices

REBECCA SMITH

@BexKSmith

CREDIT Suisse will pay $47m (£35m) to the US Department of Justice over hiring practices in Asia, the bank confirmed yesterday.

The Swiss bank is paying the penalty to resolve a probe into hiring practices in Asia between 2007 and 2013, after it was announced in February that US authorities were investigating whether Credit Suisse had hired referrals from government agencies in Asia in return for business and regulatory green lights.

Credit Suisse said no criminal charges have been brought and the $47m has been "substantially provided" for in prior periods.

CITYAM.COM

Data firm was victim of media storm, boss says

JOSH MINES

@Josh_Mines

THE BOSS of Cambridge Analytica Alexander Nix has come out all guns blazing as he claimed the company was the victim of a "concerted campaign" by the "global liberal media".

In a heated encounter with the Digital, Culture, Media and Sport Committee yesterday, Nix told MPs: "If you were sitting where I am right now you'd probably feel quite victimised."

The hearing comes weeks after the company filed for bankruptcy in the UK and the US.

The fake news enquiry kicked off in

current state of Cambridge Analytica.

Nix also piled into the broadcast press, as he described Channel 4 News of running "a very deliberate programme of deception" against his company.

The TV station secretly filmed Nix claiming the company used bribes, honey traps and extortion to win elections. Nix claims the news broadcast deliberately edited his words out of context to misrepresent what he said on the film.

In response, Channel 4 News said "absolutely" disagreed with and rejected Nix's claims, adding that all comments used in the program were put in context.

Risk Events – cont'd

Facebook comes under fire over data sharing deals with Chinese tech firms

EMILY NICOLLE

@emilyjnicolle

FACEBOOK confirmed yesterday it holds several data sharing partnerships with Chinese mobile device makers, as its second user privacy scandal worsens under the gaze of US Congress.

The deals include relationships with firms like Huawei, Lenovo, Oppo and TCL, despite longstanding national security concerns from the US government over ties between companies like Huawei and the Chinese state.

It was revealed earlier in the week that Facebook reached at least 60 deals with device makers over the last decade, giving firms access to some users' data for the purpose of building on "the Facebook experience" with features like address books and messaging.

Facebook denied allegations that any of these deals conflicted with its founder Mark Zuckerberg's earlier testimony to US Congress, nor did they represent a new data breach.

A Facebook vice president said that all integrations with Chinese device makers were "controlled from the get go", with all features built being approved by the company itself. He added that at no point was any data stored on company servers.

The US Senate commerce committee has written to Facebook, asking for further clarification.

CYBER WARRIORS

Luke Graham examines the frontline defence business has against digital attacks: the chief information officer

promote a career
to young women
e discouraged due
ypes, in order to
ential candidates.
rm strategies, and
something in the
re against cyber

lertake structured
they would react
ttack, what meas-
ke to get back on
s how they should
nt regulatory issues
the problem to cus-
also gives general
anisations should be
prepared.
acks right still matters.
ving an antivirus, fire-
and password manage-
hose basic things right

will stop a lot of attacks and is well worth doing."

The changing nature of these attacks is also a cause for concern to many CIOs. For most people, when they hear about cyber attacks, they might imagine individual criminals acting alone, or think of hackers who treat it as a "sport" and are only breaking into organisations for bragging rights.

But the amateur hacker is far down the list of fears for CIOs – instead, the survey found that 77 per cent of these IT leaders are most concerned by the threat of organised cyber crime, up from 71 per cent the year before.

Organised cyber crime can take many forms, from ransomware attacks, like last year's WannaCry assault which targeted systems around the world, to phishing scams and fraud, as seen in the aftermath of the recent TSB meltdown.

Ferbrache adds that organisation increasingly have to deal with cry tocurrency malware – hackers infecting computer systems with c that causes a device to begin mining cryptocurrency such as bitcoin that to the hacker, which diverts com

power
"Fro
grou
indu
por
too
wi
c

> Only 22 per cent of those surveyed said that their organisation was well-prepared for a cyber attack

Top 10 risks in 2018

	2018 position	2017 position	Change
IT disruption	1	1*	→
Data compromise	2	1*	→
Regulatory risk	3	2	↓
Theft and fraud	4	9	↑
Outsourcing	5	3	↓
Mis-selling	6	5*	↓
Talent risk	7	new	
Organisational change	8	6	↓
Unauthorised trading	9	5*	↓
Model risk	10	-	↑

Source: Risk.net, Feb 22, 2018

ORM Strengths and Weaknesses: CRO survey 2017

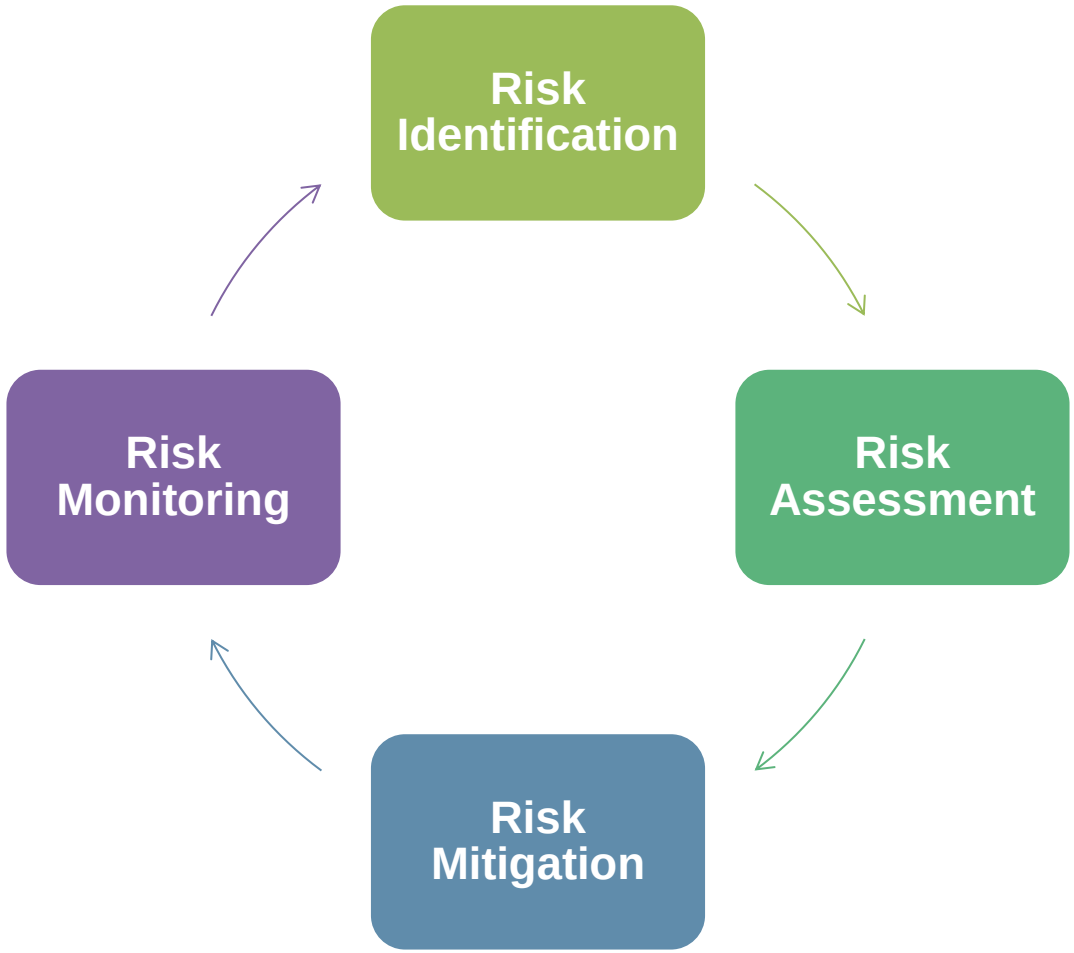
Table 1: Frequently cited strengths and weaknesses in operational risk management

Strengths	Weaknesses
Risk-neutral framework	Sub-optimal management information
Well-developed set of standard and mature tools	Minimal integration of advanced analytics
Good visibility of major risks	Ineffective and inefficient controls
Strong senior management mandate	Risk culture not sufficiently embedded
	Lack of business and specialist skills

Source: *The Future of Operational Risk*, ORX / McKinsey, May 2017

Framework and Tools

Risk is the effect of uncertainty on objectives



Risk Management Process

Risks Identification tool: *Exposures* and *Vulnerabilities*

Exposures

- Key distribution channels
- Main clients
- Main suppliers and third parties
- Critical systems
- Regulatory exposure
- Main drivers of revenues, drivers of value
- Brand value
- ...

Vulnerabilities

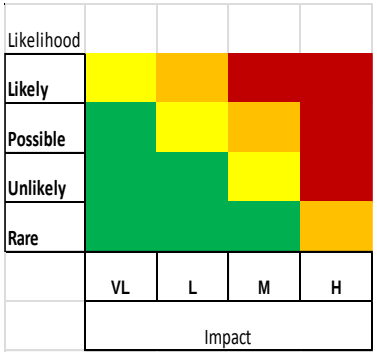
- Weakest links
- Fragile systems
- Revenue channels at risk
- Systems or processes not integrated
- Parts of the business resistant to risk management
- Small, unmonitored operations or people
- Unmaintained systems
- BCP due for testing or updates
- ...

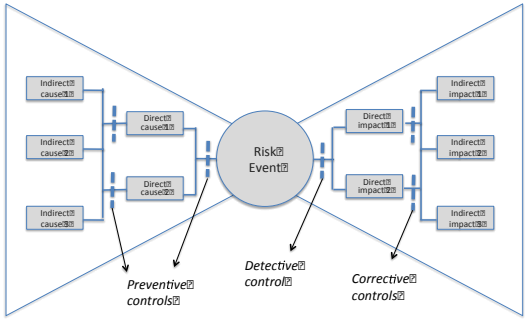
Some key messages

1. Make your own personal list of key risks
2. An institution's risk profile is personal, related to its exposures and vulnerabilities
3. Don't neglect risks that haven't materialised yet
4. Focus and prepare for large events… just in case
5. Watch the trends, but don't forget blind spots

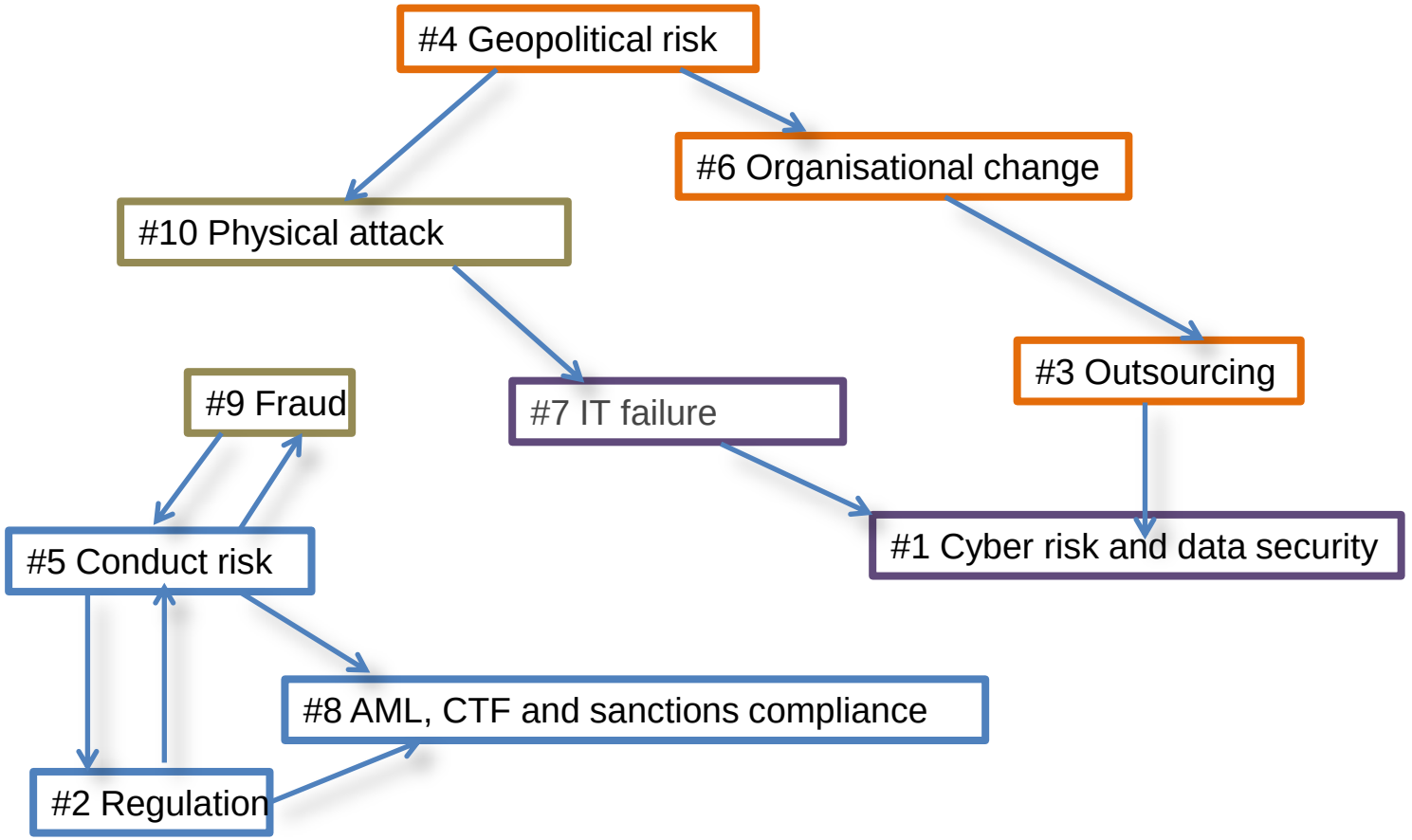
ORM tools and best practices in a nutshell

- **RCSA**: updated when needed (yearly or trigger event) and back-tested with loss experience and in line with risk appetite
- **KRIs – Key Risks Indicators**: leading, preventative
- **Scenario analysis**: to guide risk management actions and priorities
- **Risk reporting and root cause analysis:** effective, helping decision-making





Connectivity for management priorities: a network view of the top risks - 2017



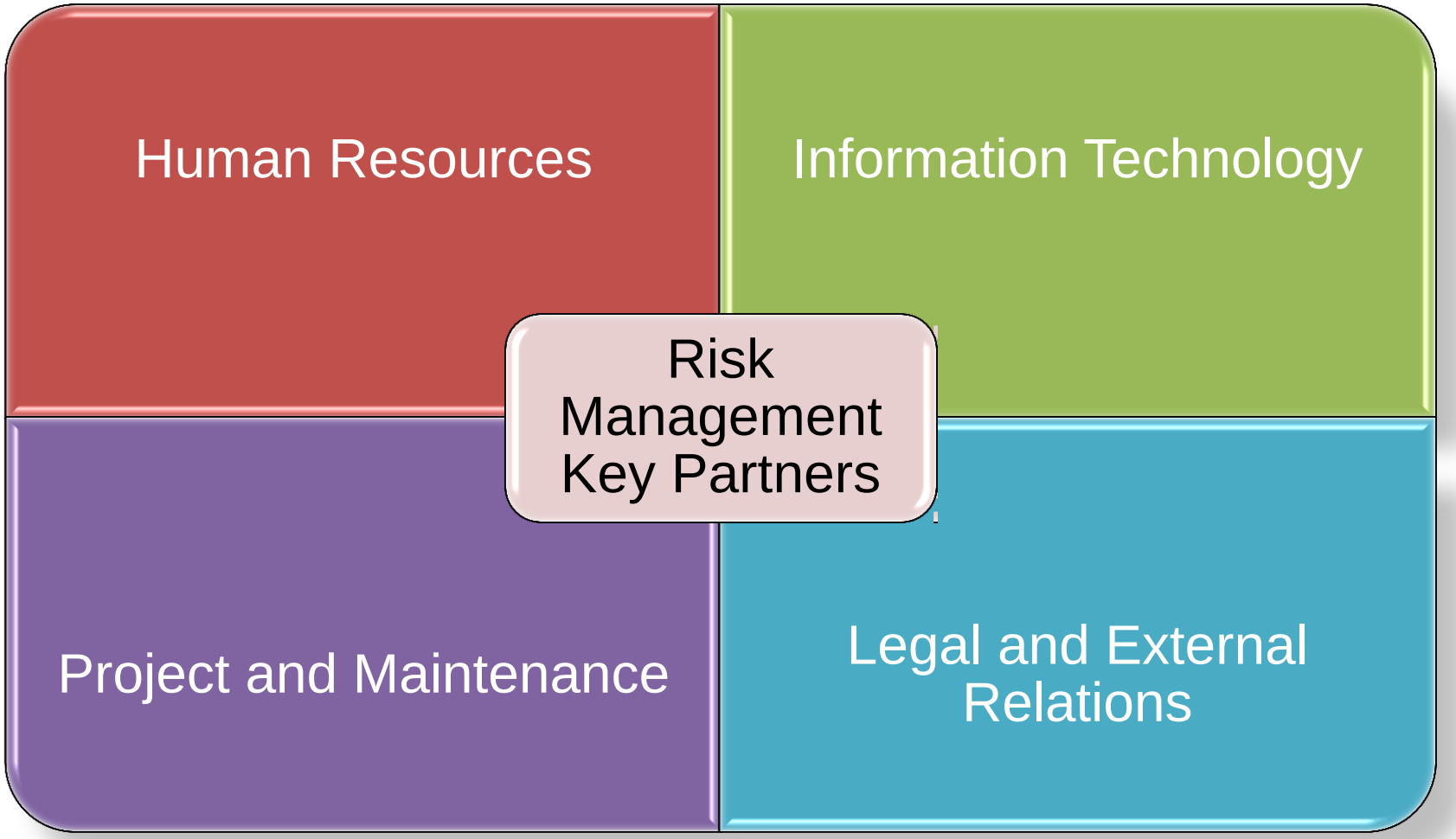
Source: A. Chapelle "Reflections on Operational Risk Management", 2017, Risk books.

Partners and Decision-Making

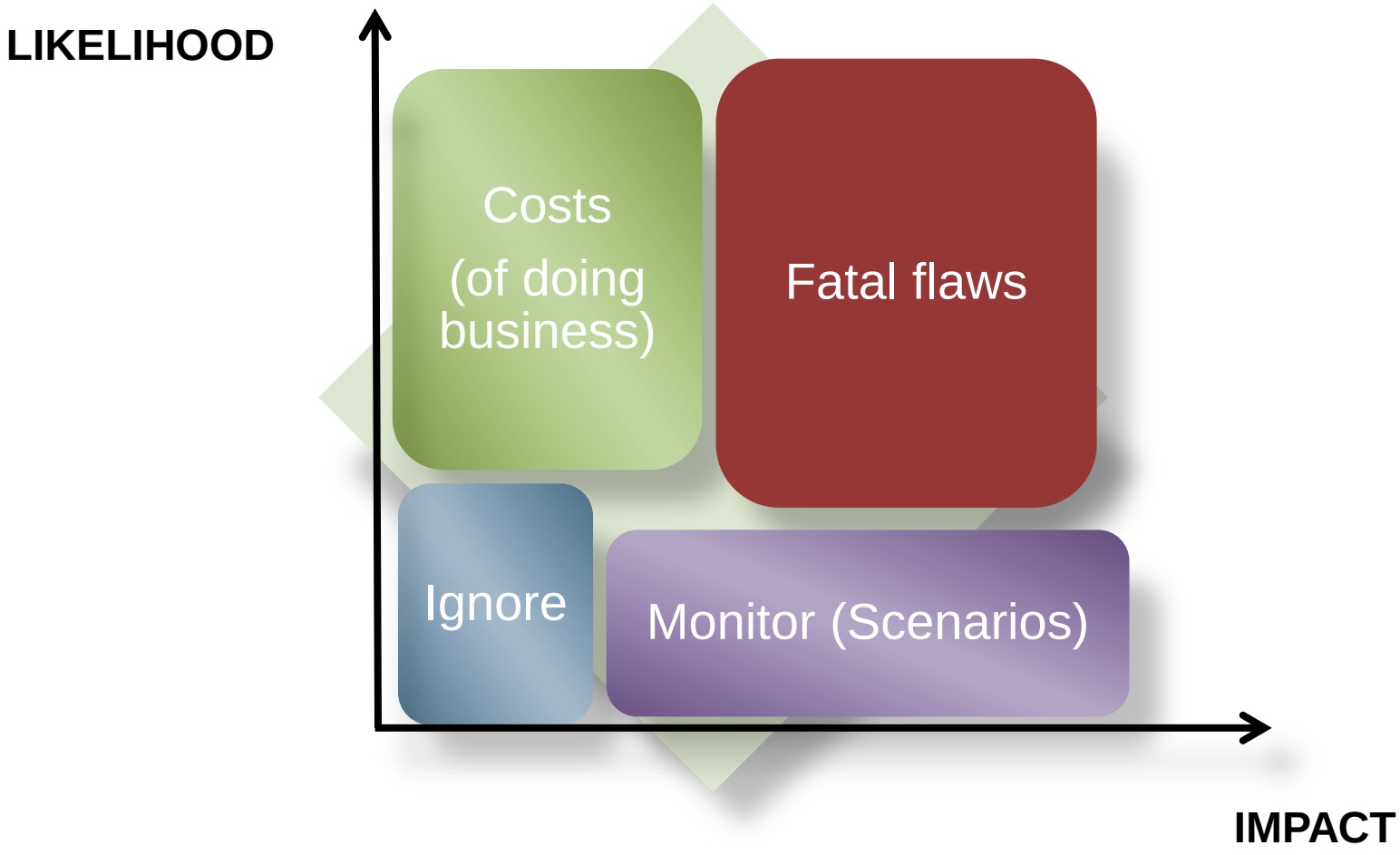
Drivers of Operational Excellence: PPSE

People	Process	Systems	External Events
Resourcing	Automated	Integration	External fraud and threats monitoring
Ability	Integrated	Capacity	Cyber crime protection
Engagement	Standardised	Performance	Legal & Regulatory monitoring
Retention	Documented	Maintenance	Technological veil
Related literature: Human Reliability Analysis (HRA)	Related literature: Business Process Reengineering (BPR)	Related literature: IT performance management	Related literature: business intelligence and strategy

Source: A. Chapelle “Reflections on Operational Risk Management”, 2017, Risk books.


Human Resources
Information Technology
Risk Management Key Partners
Project and Maintenance
Legal and External Relations

Prioritising risk management for better decision-making



Risk and Opportunity – Typology of decisions

Type	Characteristics	Examples
Silly risky decisions	Large downside, no upside, small cost of control	Not buckling a car seat belt, not locking a work station
Violating decisions	Attractiveness of large personal upside (profit) or fear of a large personal downside (sanction, lay-off) conducing to break a rule	Rogue trading, compliance breaches, conduct violations, misstatements of accounts
Chilly decisions	Fear-driven, excessive protection destroying the likelihood and value of the initial upside	Redundant controls on non critical processes, more financial, human and technical resources dedicated to the controls than to the operations, more controls layers than execution layers, "quality assurance of quality assurance" (sic)
Balanced decisions	Striking an accepted trade-off between risks and expected rewards, balancing the prospects of upside with the eventuality of downside.	All thought-trough investments decisions, commercial initiatives, entrepreneurial projects, where risk is accepted if fairly compensated by expected returns.

Source: A. Chapelle "Reflections on Operational Risk Management", 2017, Risk books.

Governance and Culture

Three lines of defense model

First line: business operations / risks owners

- Front line of risk management
- Real line of risk management
- Risk is managed where it is generated

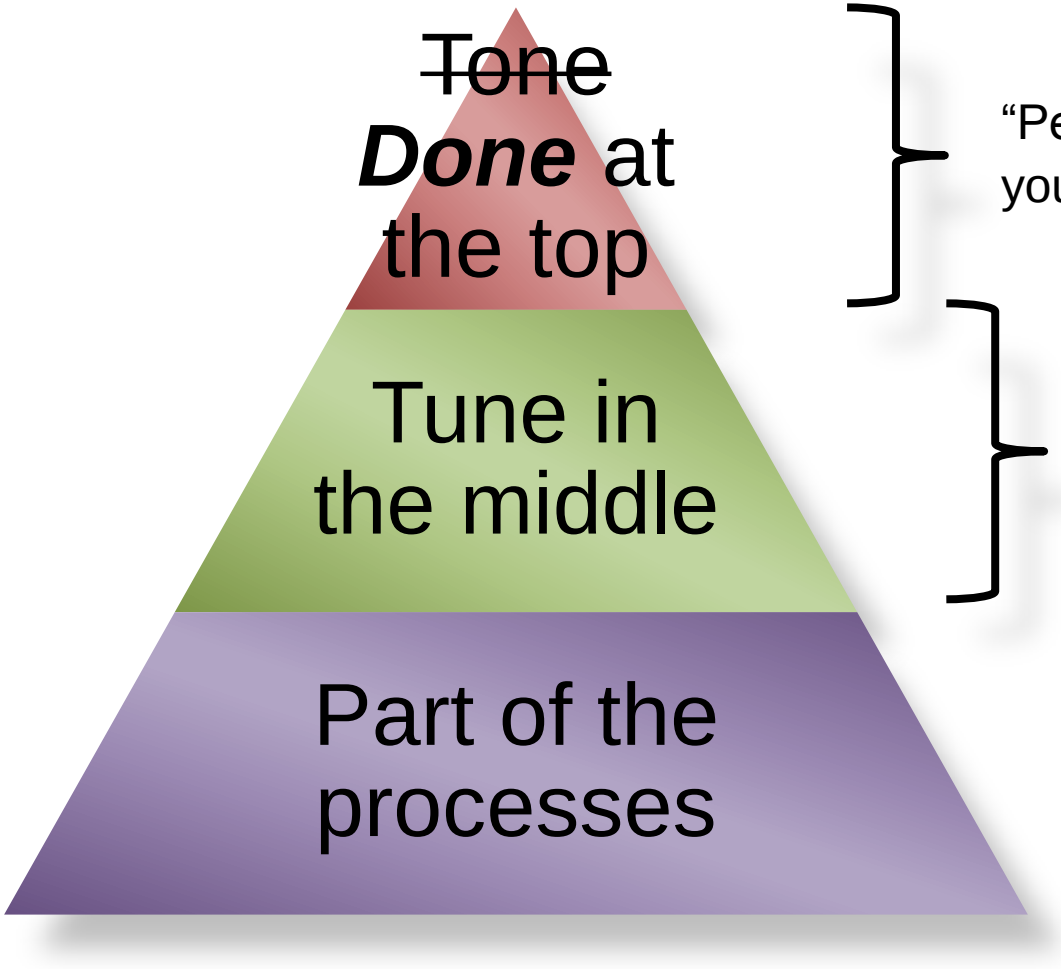
Second line: risk management

- Methodology unit and coordination
- Oversight and harmonisation of practice
- Advice and support
- Challenge if need be

Third line: internal audit

- Independent review and assurance

How to embed a risk culture?



"People do what you ***do***, not what you ***say***" -> lead by example

"Tell people what to ***do***, not only what the objectives are
-> focus on **key behaviours**

OpRisk is about PPSE
People – Process - Systems
External Events
-> focus on fundamentals

Risk Buy in - The role of the Risk Function

Building an ***Invisible Framework*** **, for risk management it is:**

- Adjusting to the business
- Accounting for existing practices and leverage them
- Avoiding jargon outside of the risk management specialists
- Solving problems
- Enabling business to grow safely
- Providing technical support
- *Making friends*

Source: A. Chapelle “Reflections on Operational Risk Management”, 2017, Risk books.

Maturity Criteria & Risk Management Trends

Framework Maturity Criteria

1. Incident Data Base is comprehensive.
2. Risk reporting is fed from and back to business lines with benchmarks and comparisons across similar entities.
3. Risk assessments are consistent and comparable across business lines
4. Action plans and mitigating actions are based on risk assessment, not just in response to incidents. They are linked to risk appetite.
5. Results of scenarios identification and assessments are used to improve management decisions.
6. KRIs are preventative, relevant and actively used
7. Executive directors understand the concept of risk appetite to agree on limits of exposure and necessary controls.
8. Risk management culture is valued throughout the organisation

Source: Chapelle, Operational Risk Management: Wiley, 2019.

Evolutions of Risk Management

Resilience focus

- Better incident management
- Crisis management pre-planning

Control assessment and testing

- Observability of controls
- Optimisation of processes

Behavioural economics

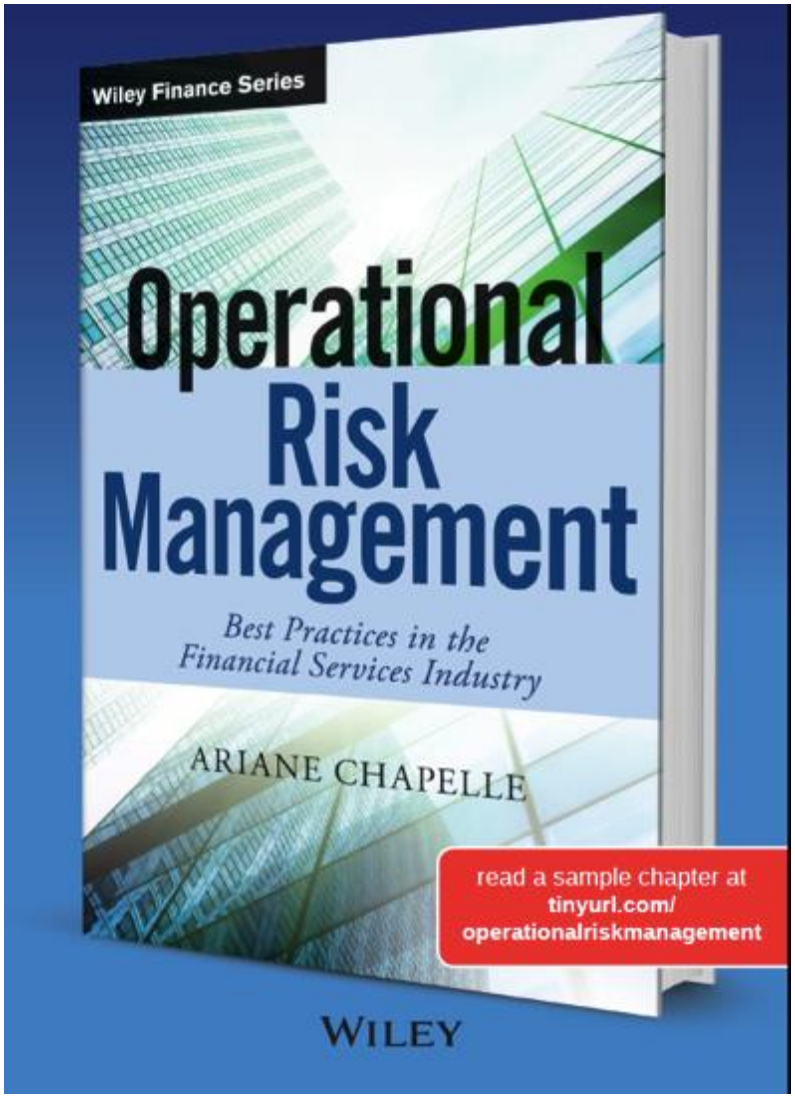
- Culture and Conduct through behaviour drivers
- Desirable versus unacceptable behaviours

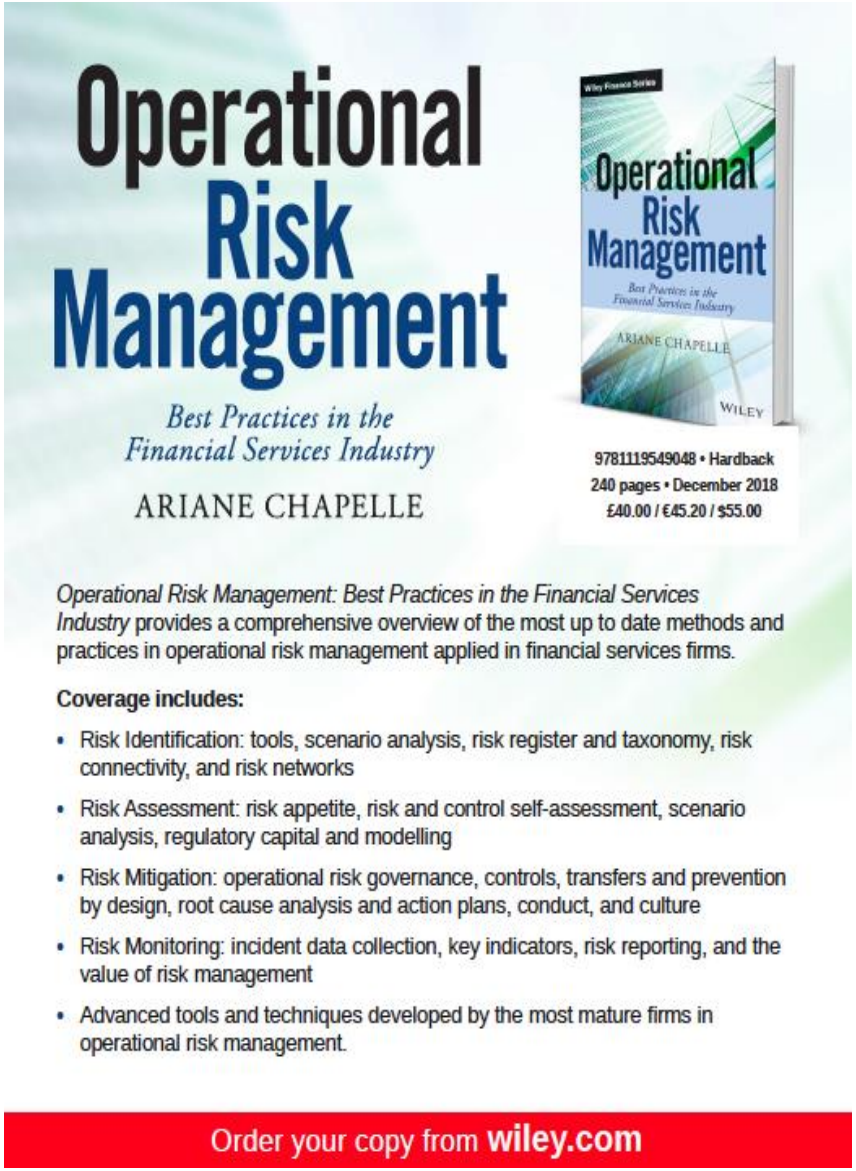
Positive risk management

- Recognise the rewards when taking risk
- Recognise the value of risk management
- Positioning risk management as an enabler of performance

To know more

From December 2018





Since 2017

Reflections on Operational Risk Management

28 articles around 6 themes

1. Essentials of Operational Risk and Risk Management Framework
2. Risk appetite and Risk decisions
3. Key Risk Indicators and reporting
4. Culture and Conduct
5. Scenario Analysis and tail risks
6. Operational risk capital & measurement

Thank you for your attention

Any question or comments:

ariane@chapelleconsulting.com

Need for more resources:

www.chapelleconsulting.com